Quantum Series

ENGINEERING

QUANTUM Series

Semester - 7 Information Technology

Cryptography & Network Security

Session 2021-22 Odd Semester

- Topic-wise coverage of entire syllabus in Question-Answer form.
- Short Questions (2 Marks)

Includes solution of following AKTU Question Papers

2014-15 • 2015-16 • 2016-17 • 2017-18 • 2018-19 • 2019-20 • 2020-21

QUANTUM SERIES

For

B.Tech Students of Fourth Year
of All Engineering Colleges Affiliated to
Dr. A.P.J. Abdul Kalam Technical University,
Uttar Pradesh, Lucknow
(Formerly Uttar Pradesh Technical University)

Cryptography & Network Security

By

Kanika Dhama

Quantum
— Page —

QUANTUM PAGE PVT. LTD.
Ghaziabad ■ New Delhi

PUBLISHED BY :

Apram Singh
Quantum Publications®
(A Unit of Quantum Page Pvt. Ltd.)
Plot No. 59/2/7, Site - 4, Industrial Area,
Sahibabad, Ghaziabad-201 010

Phone : 0120 - 4160479

Email : pagequantum@gmail.com **Website: www.quantumpage.co.in**

Delhi Office : 1/6590, East Rohtas Nagar, Shahdara, Delhi-110032

Information contained in this work is derived from sources believed to be reliable. Every effort has been made to ensure accuracy, however neither the publisher nor the authors guarantee the accuracy or completeness of any information published herein, and neither the publisher nor the authors shall be responsible for any errors, omissions, or damages arising out of use of this information.

Cryptography & Network Security (IT : Sem-7)

1st Edition : *2011-12*
2nd Edition : *2012-13*
3rd Edition : *2013-14*
4th Edition : *2014-15*
5th Edition : *2015-16*
6th Edition : *2016-17*
7th Edition : *2017-18*
8th Edition : *2018-19*
9th Edition : *2019-20 (Thoroughly Revised Edition)*
10th Edition : *2020-21*
11th Edition : *2021-22*

Price: Rs. 110/- only

Printed at : Parashar Printers, Delhi.

CONTENTS

KCS 074 : Cryptography & Network Security

1 UNIT

Introduction

CONTENTS

PART-1

Introduction to Security Attacks, Services and Mechanism.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 1.1. **Explain network security attacks on the basis of security goals.**

Answer

Security attacks : Security attack is defined as an attempt to gain unauthorized access to information system.

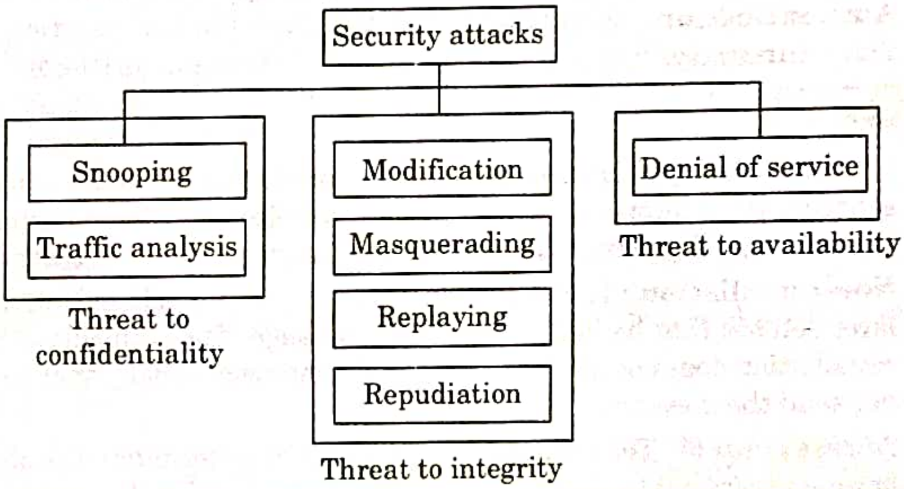


Fig. 1.1.1. Classification of attacks with relation to security goals.

Security attacks on the basis of security goals are of three types :

1. **Attacks threatening confidentiality :** Attacks threatening the confidentiality of information are :
   a. **Snooping :** Snooping refers to unauthorized access of data. To prevent snooping, data is made unreadable to the unauthorized entities by using encryption techniques.
   b. **Traffic analysis :** Traffic analysis is an attempt of analyzing (encoded) messages to come up with likely patterns.
2. **Attacks threatening integrity :** Attacks threatening integrity of information are :
   a. **Modification :** After accessing information, the attacker modifies the information to make it beneficial to himself.

b. **Masquerading :** Masquerading or spoofing happens when one entity pretends to be a different entity.

c. **Replaying :** In replaying, attacker obtains a copy of the message sent by a user and later retransmits it to produce an unauthorized effect.

d. **Repudiation :** This attack is performed by one of the two parties in the communication. The sender of the message may deny that he has sent the message or the receiver of the message might later deny that he has received the message.

3. **Attacks threatening availability :** Attacks threatening availability of information is :

   a. **Denial of Service (DoS) :** This attack may slow down or totally interrupt the service of a system.

Que 1.2. Describe in brief the following security services :

1. Confidentiality
2. Non-repudiation
3. Access control
4. Authentication
5. Data integrity

Answer

1. **Confidentiality :** The principle of confidentiality specifies that only the sender and the intended recipient should be able to access the content of the message. It protects the transmitted data from passive attack.
2. **Non-repudiation :** It is a condition when a user sends message and later refuses that he had not sent the message. The principle of non-repudiation does not allow the sender of a message to deny that he had not send the message.
3. **Access control :** The principle of access control determines who should be able to access data or system via communication link. It provides the prevention of unauthorized use of a resource.
4. **Authentication :** Authentication is concerned with assuring that a communication is authentic. In authentication, there is an assurance that the communicating entity is the one that it claims to be.
5. **Data integrity :** Data integrity is designed to protect data from modification, insertion, deletion and replaying by any entity. Data integrity can be applied to a stream of message, a single message or a selected portion within a message.

Que 1.3. Discuss security mechanisms.

Answer

Security mechanisms : It is mechanism that is designed to detect, prevent, or recover from a security attack.

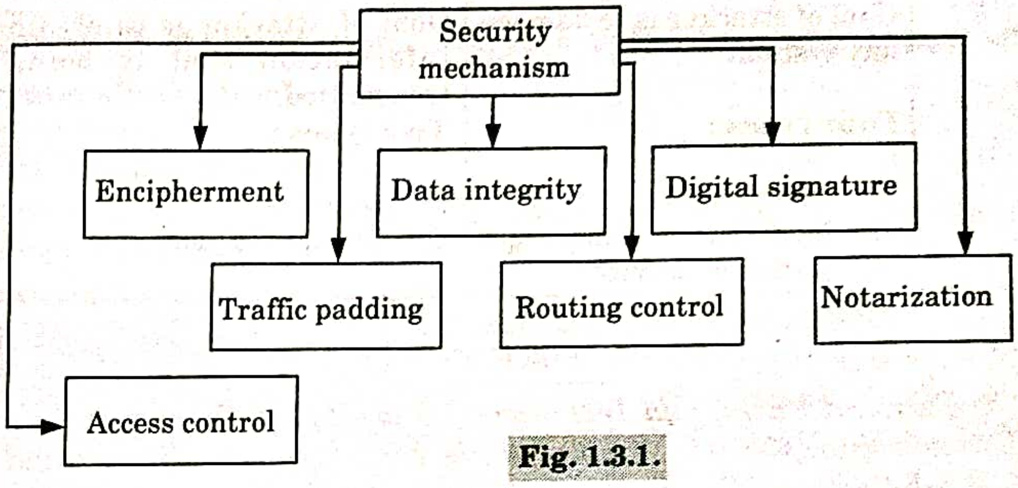


Fig. 1.3.1.

1. **Encipherment :** Hiding or covering data can provide confidentiality.
2. **Data integrity :** Refer Q. 1.2, Page 1–3D, Unit-1.
3. **Digital signature :** It is a way by which the sender can electronically sign the data and the receiver can electronically verify the signature.
4. **Traffic padding :** It is the way of inserting of bits into gaps in a data stream to confuse traffic analysis attempts.
5. **Routing control :** It enables selection of particular physically secure routes for certain data and allows routing changes, especially when a branch of security is suspected.
6. **Notarization :** It means selecting a third trusted party to control the communication between two entities.
7. **Access control :** Refer Q. 1.2, Page 1–3D, Unit-1.

Que 1.4. **Differentiate between active attack and passive attack.**

Answer

S. No.	Active attack	Passive attack
1.	Access and modify information.	Access information.
2.	System is harmed.	No harm to system.
3.	Easy to detect than prevent.	Difficult to detect than prevent.
4.	Threat to integrity, availability.	Threat to confidentiality.
5.	Affect system resources.	Does not affect system resources.
6.	Involve some modification of the data stream or the creation of a false stream.	Involve Eavesdropping and monitoring of data.

7.	Goal of attacker is to damage any system. **Four types :** i. Replay ii. Masquerade iii. Modification of messages iv. Denial of service	Goal of attacker is to obtain information that is being transmitted. **Two types :** i. Release of message contents ii. Traffic analysis.

PART-2

Classical Encryption Techniques : Substitution Ciphers and Transposition Ciphers, Cryptanalysis, Steganography, Stream and Block Ciphers, Modern Block Ciphers : Block Cipher Principles.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 1.5. **Compare and contrast substitution techniques with transposition techniques under classical encryption.**

AKTU 2014-15, Marks 05

Answer

S. No.	Basis for comparison	Substitution techniques	Transposition techniques
1.	Basic	Replaces the plaintext characters with other characters, numbers and symbols.	Rearranges the position of the characters of the plaintext.
2.	Forms	Monoalphabetic and polyalphabetic substitution cipher.	Keyless and keyed transpositional cipher.
3.	Iterations	The identity of the character is changed while its position remains unchanged.	The position of the character is changed instead of its identity.
4.	Demerit	The letter with the low frequency can detect the plaintext.	Keys near to the correct key can disclose the plaintext.
5.	Example	Caesar Cipher.	Rail Fence Cipher.

Que 1.6. **What is cryptanalysis ? Explain the types of cryptanalysis attack.**

Answer

Cryptanalysis : Cryptanalysis is the decryption and analysis of codes, ciphers or encrypted text.

Types of cryptanalysis attack :

1. **Ciphertext only attack :**
   a. A Ciphertext Only Attack (COA) is an attack in which only the encrypted message is available for attack, but because the language is known a frequency analysis could be attempted.
   b. In this situation, the attacker does not know anything about the contents of the message, and must work from cipher text only.
2. **Known plaintext attack :**
   a. In a Known Plaintext Attack (KPA) both the plaintext and matching cipher text are available for use in discovering the key.
   b. The attacker knows or can guess the plaintext for some parts of the cipher text.
3. **Chosen plaintext attack :**
   a. A Chosen Plaintext Attack (CPA) occurs when the attacker gains access to the target encryption.
   b. In an Adaptive Chosen Plaintext Attack (ACPA), the attacker not only has access to the plaintext and its encryption, but can adapt or modify the chosen plaintext as needed based on results of the previous encryptions.
4. **Chosen ciphertext attack :**
   a. In a Chosen Cipher text Attack (CCA), the cryptanalyst can choose different cipher texts to be decrypted and has access to the decrypted plaintext.
   b. This type of attack is generally applicable to attacks against public key cryptosystems.

Que 1.7. **Explain the term steganography in brief.**

Answer

1. Steganography is a technique to implement security mechanisms.
2. It is the technique of writing a message in such a way that apart from the sender and the receiver, no one will suspect the existence of the message. It enables the sender to hide a message inside another message.

3. Cryptography conceals the contents of a message by enciphering, and steganography conceals the message itself by covering it with something.

4. Traditional techniques of steganography include :

   a. Marking selected letters of a printed document with a pencil such that the marks are visible only when the document is exposed at a specific angle to bright light.

   b. Use of some invisible ink to write a secret message such that the contents of a message are not visible until heated or some other chemical is applied.

   c. Use of interodots or pin punchers on selected letters such that these dots are not visible until the paper is exposed in front of a light.

   d. Some modern techniques of steganography include hiding of a secret message within an image, audio or video file by inserting secret binary message information during the digitization process.

Que 1.8. **The hill cipher uses the following key for enciphering the message.**

$$K = \begin{pmatrix} 3 & 2 \\ 5 & 7 \end{pmatrix}$$

Obtain the decryption key to be used for deciphering the cipher text.

AKTU 2014-15, Marks 05

Answer

$$K = \begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix}$$

If
$$K = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

$$K^{-1} = \frac{1}{|D|} \times \begin{bmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{bmatrix}$$

$$D = a_{11} a_{22} - a_{12} a_{21}$$

Therefore,
$$K^{-1} = \frac{1}{11} \begin{bmatrix} 7 & -2 \\ -5 & 3 \end{bmatrix}$$

$$K^{-1} = \begin{bmatrix} 7/11 & -2/11 \\ -5/11 & 3/11 \end{bmatrix}$$

Que 1.9. **Encrypt the message "THIS IS AN EXERCISE" using Playfair Cipher with key = DOLLARS.** **AKTU 2015-16, Marks 10**

OR

Explain Playfair Cipher with example.

Answer

Playfair cipher :

1. The playfair cipher is used for creating a key table.
2. The key table is a 5 × 5 grid of letters that will act as the key for encrypting our plaintext. Each of the 25 letters must be unique and one letter of the alphabet (any) is omitted from the table.
3. In a playfair cipher, the message is split into digraphs, pairs of two letters.
4. If there is an odd number of letters, Z is added to the last letter.
5. The playfair cipher uses following rules for encrypting process :
   a. If both letters are in the same column, take the letter below each one (going back to the top if at the bottom).
   b. If both letters are in the same row, take the letter to the right of each one (going back to the left if at the farthest right).
   c. If neither of the preceding two rules are true, form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle.

Key = DOLLARS and Message = THIS IS AN EXERCISE

D	O	L	A	R
S	B	C	E	F
G	H	I/J	K	M
N	P	Q	T	U
V	W	X	Y	Z

First we break the original text (message) into pairs of two alphabets each as : TH IS IS AN EX ER CI SE

Now, replacing the text with the text diagonally opposite to it :

TH → PK
IS → GC
IS → GC
AN → DT
EX → CY

ER → FA
CI → IQ
SE → BF

Thus, plaintext becomes PK GC GC DT CY FA IQ BF

Que 1.10. **Write as short note on block cipher and stream cipher.**

Answer

Block cipher :

1. A block cipher is defined as a symmetric key cipher where a group of plaintext symbols are encrypted together to create a group of ciphertext of same size.
2. A single key is used to encrypt the whole block even if the key is made of multiple values.
3. During decryption, each ciphertext block is converted to plaintext block, one block at a time.

Stream cipher :

1. A stream cipher is defined as a symmetric key cipher where encryption and decryption are done on one symbol at a time.
2. A plaintext symbol is given as a input to the encryption algorithm one at a time and on the basis of key applied ciphertext characters are also created one at a time.
3. The values depend on the plaintext, ciphertext characters and previous key values.
4. Stream ciphers are designed to approximate an idealized cipher, known as the One-Time Pad.

Que 1.11. **Differentiate between block cipher and stream cipher.**

Answer

S. No.	Block cipher	Stream cipher
1.	In block cipher, keys and algorithm are applied to block of data.	In stream cipher, keys and algorithms are applied to each binary digit one bit at a time.
2.	Block cipher is more time consuming.	Stream cipher is less time consuming.
3.	Block cipher is slower than stream cipher.	Stream cipher is faster than block cipher.
4.	Block cipher is used in chaining modes of operation.	Stream cipher is not used in chaining modes of operation.
5.	Software implementation is easy using block cipher.	Hardware implementation is easy using stream cipher.

Que 1.12. **What is ideal block cipher ?** **AKTU 2016-17, Marks 10**

Answer

1. Ideal block cipher is a block cipher in which the relationship between the input blocks and the output block is completely random but it must be invertible for decryption to work.
2. In ideal block cipher, each input block is mapped to a unique output block.

Problems with ideal block cipher :

1. If a small block size, such as $n = 4$, is used, then the system is equivalent to a classical substitution cipher. Such systems are vulnerable to a statistical analysis of the plaintext.
2. This weakness is not inherent in the use of a substitution cipher but rather results from the use of a small block size.
3. If n is sufficiently large and an arbitrary reversible substitution between plaintext and ciphertext is allowed, then the statistical characteristics of the source plaintext are masked to such an extent that this type of cryptanalysis is infeasible.
4. However, an arbitrary reversible substitution cipher for a large block size is not practical from an implementation and performance point of view.

Que 1.13. **Explain modern block cipher with its components.**

Answer

1. A symmetric-key modern block cipher encrypts an n-bit block of plaintext or decrypts an n-bit block of ciphertext.
2. The encryption or decryption algorithm uses a k-bit key.

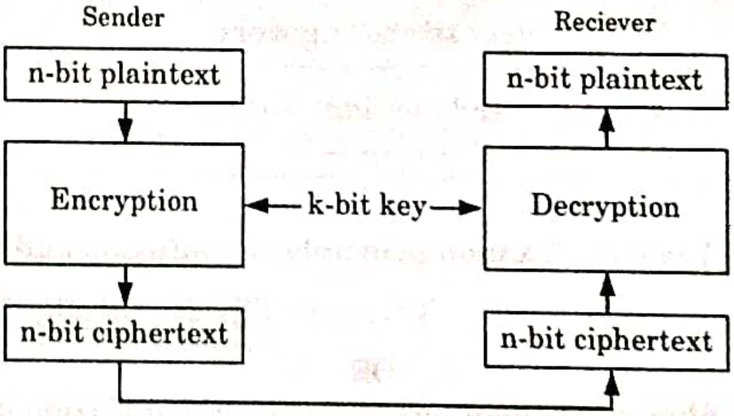


Fig. 1.13.1.

3. Following are the components of modern block cipher :

i. **S-boxes :**

a. This is a substitution box where substitution of several bits is performed in parallel.

b. It takes n bits of plaintext at a time as input and produces m bits of ciphertext as output, where the value of n and m may be the same or different.

ii. **P-boxes :**

a. This is a permutation box that performs transposition at the bit-level, and transposition of several bits is performed at the same time.

b. The input bits are permuted to produce the output bits :

1. **Straight *P*-box :** This *P*-box takes n bits as input, permutes them and produces n bits as output. As the number of inputs and outputs is the same, there are a total of $n!$ ways to map n inputs to n outputs.
2. **Compression *P*-box :** This *P*-box takes n bits as input and permutes them to produce an output of m bits where $m < n$.
3. **Expansion *P*-box :** This *P*-box takes n bits as input and permutes them to produce an output of m bits where $m > n$.

iii. **Circular shift :** In circular shift operation, bits can be shifted either in the left or in the right direction.

PART-3

Shannon's Theory of Confusion and Diffusion, Feistel Structure.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 1.14. **Explain Shannon principle of confusion and diffusion.**

AKTU 2016-17, Marks 10

OR

What is the Shannon's theory of confusion and diffusion in terms of information security ? **AKTU 2018-19, Marks 10**

Answer

Shannon's theory uses diffusion and confusion for transposition and substitution operation as :

Confusion :

1. The property of confusion hides the relationship between the ciphertext and the key.
2. This property makes it difficult to find the key from the ciphertext.
3. If a single bit in a key is changed, most or all the bits in the ciphertext will be changed.
4. Confusion increases ambiguity of ciphertext.
5. It is achieved through substitution algorithm.
6. It is used by stream cipher and block cipher.

Diffusion :

1. The idea of diffusion is to hide the relationship between the ciphertext and the plaintext.
2. This will frustrate the attacker who tries to find out the plaintext from the statistical analysis of ciphertext.
3. Diffusion is implemented such as if a single symbol in the plaintext is changed, several or all symbols in the ciphertext will also be changed.
4. Diffusion increases the redundancy of the plaintext by spreading it across rows and columns.
5. It is achieved through transposition algorithm.
6. It is used by block cipher only.

Que 1.15. **Explain Feistel encryption and decryption algorithms. What is the difference between diffusion and confusion ?**

AKTU 2014-15, Marks 05

Answer

Feistel encryption algorithm : Feistel encryption algorithm takes a block of plaintext as input. The plaintext block is divided into two halves *i.e.*, left (LE_0) and right (RE_0)

a. **Input :** The plaintext (LE_0, RE_0)

b. **Round i** (1 to 16) perform on input (LE_{i-1}, RE_{i-1}) the operations :

   $LE_i = RE_{i-1}$, $RE_i = LE_{i-1} \oplus f(RE_{i-1}, K_i)$

c. This is the input to next round.

d. The key of round i is K_i.

e. **Output :** The ciphertext (RE_{16}, LE_{16})

Feistel decryption algorithm : In Feistel decryption algorithm, we take the output of encryption algorithm as input *i.e.*, $(LD_0, RD_0) = (RE_{16}, LE_{16})$ and perform the operations in reverse order.

a. **Input :** The ciphertext $(LD_0, RD_0) = (RE_{16}, LE_{16})$

b. **Round i** (1, to 16) perform on input (LD_{i-1}, RE_{i-1}) the operations :

$LD_i = RD_{i-1}$, $RD_i = LD_{i-1} \oplus f(RD_{i-1}, K_{16-i})$

c. This is the input to next round.

d. The key of round i is K_{16-i}.

e. This algorithm is CORRECT - after round i we have $LD_i = RE_{16-i}$,

$RD_i = LE_{16-i}$.

Difference :

S. No.	Diffusion	Confusion
1.	Diffusion hides the relation between the ciphertext and the plaintext.	Confusion hides the relation between the ciphertext and key.
2.	If a single symbol in the plaintext is changed, several or all symbols in the ciphertext will also be changed.	If a single bit in the key is changed, most or all bits in the ciphertext will also be changed.
3.	Diffusion is used to create cryptic plain texts.	Confusion is used to create faint cipher texts.
4.	It is possible through transposition algorithm.	It is possible through substitution algorithm.

Que 1.16. **What do you understand by Feistel cipher structure ? Explain with suitable block diagram.** **AKTU 2017-18, Marks 05**

Answer

1. Feistel cipher is a symmetric structure used in the construction of block ciphers.
2. It is commonly known as a Feistel network.
3. The Feistel structure has the advantage that encryption and decryption operations are very similar, even identical in some cases, requiring only a reversal of the key schedule.
4. Therefore, the size of the code or circuitry required to implement such a cipher is nearly halved.
5. A Feistel network is an iterated cipher with an internal function called a round function.

6. Let F be the round function and let $K_0, K_1, ..., K_n$ be the sub-keys for the rounds 0, 1, ..., n respectively. Then, the basic operation is as follows :

   a. Split the plaintext block into two equal pieces (L_0, R_0)

   b. For each round $i = 0, 1, ..., n$ compute

   $$L_{i+1} = R_i$$
   $$R_{i+1} = L_i \oplus F(R_i, K_i).$$

   Then the ciphertext is (R_{n+1}, L_{n+1}).

   c. Decryption of a ciphertext (R_{n+1}, L_{n+1}) is accomplished by computing for $i = n, n-1, ..., 0$

   $$R_i = L_{i+1}$$
   $$L_i = R_{i+1} \oplus F(L_{i+1}, K_i).$$

   d. Then (L_0, R_0) is the plaintext again.

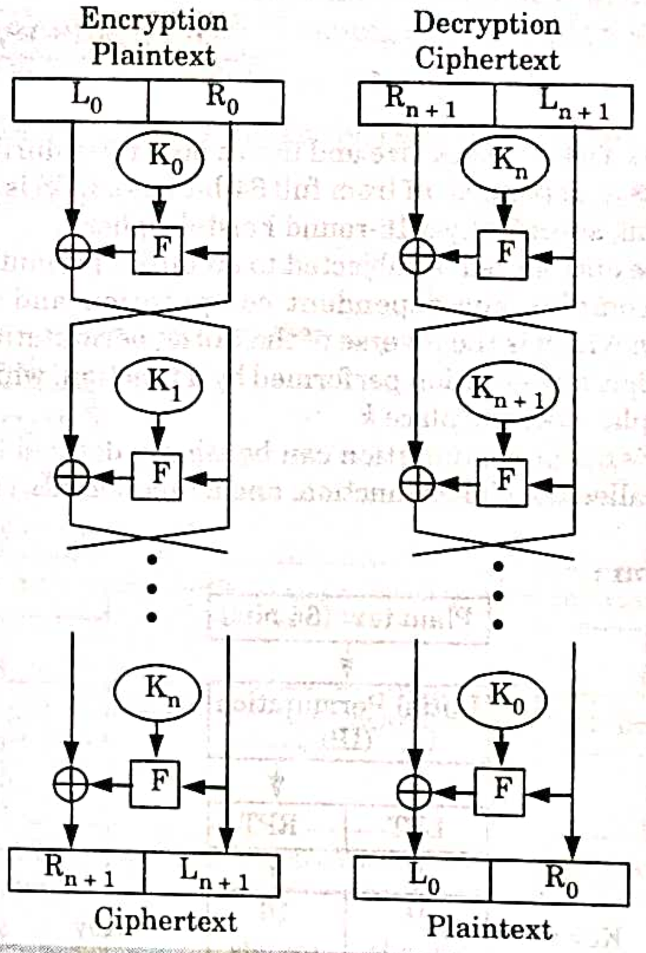


Fig. 1.16.1. Encryption and decryption in Feistel cipher.

PART-4

Data Encryption Standard (DES), Strength of DES, Idea of Differential Cryptanalysis, Block Cipher Modes of Operations Triple DES.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 1.17. Explain DES with diagram. **AKTU 2016-17, Marks 10**

OR

Discuss DES in detail with suitable block diagram.

AKTU 2017-18, Marks 10

OR

Draw the block diagram of DES algorithm. Also explain its functionality. **AKTU 2018-19, Marks 10**

Answer

1. The DES has a 64-bit block size and uses a 56-bit key during execution (8 parity bits are stripped off from full 64-bit key). DES is a symmetric cryptosystem, specifically a 16-round Feistel cipher.
2. A block to be enciphered is subjected to an initial permutation IP and then to a complex key-dependent computation and finally to a permutation which is the inverse of the initial permutation IP^{-1}.
3. Permutation is an operation performed by a function, which moves an element at place *j* to the place *k*.
4. The key-dependent computation can be simply defined in terms of a function *f*, called the cipher function, and a function KS, called the key schedule.

Explanation :

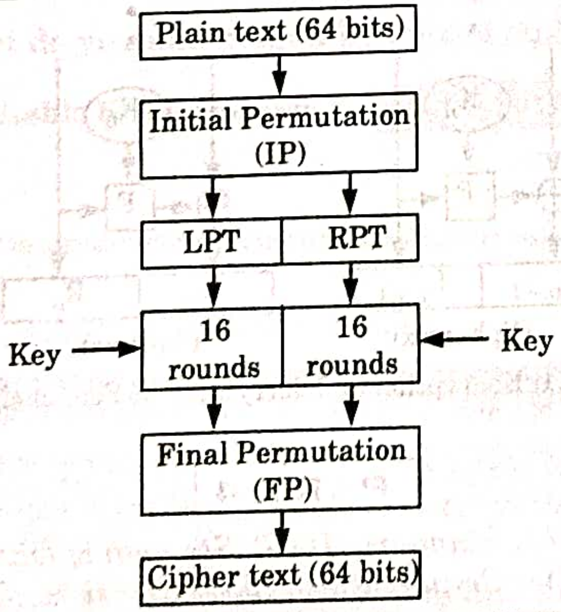


Fig. 1.17.1 Block diagram of DES algorithm.

Step 1 : The 64-bit plain text block is passed to an Initial Permutation (IP) function.

Step 2 : The initial permutation is performed on plain text.

Step 3 : The initial permutation (IP) produces two halves of the permitted block; Left Plain Text (LPT) and Right Plain Text (RPT).

Step 4 : Each of LPT and RPT go through 16 rounds of encryption process.

Step 5 : In the end, LPT and RPT are rejoined and a Final Permutation (FP) is performed on the combined block.

Step 6 : The result of this process produces 64-bit cipher text.

Functionality of DES : DES is generally used for encrypting plain text messages in various algorithm modes such as Electronic Code Book (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB) and Output Feedback (OFB).

Que 1.18. Draw block diagram of DES encryption. Also, discuss the strengths of DES.

AKTU 2015-16, Marks 15

Answer

Block diagram of DES encryption :

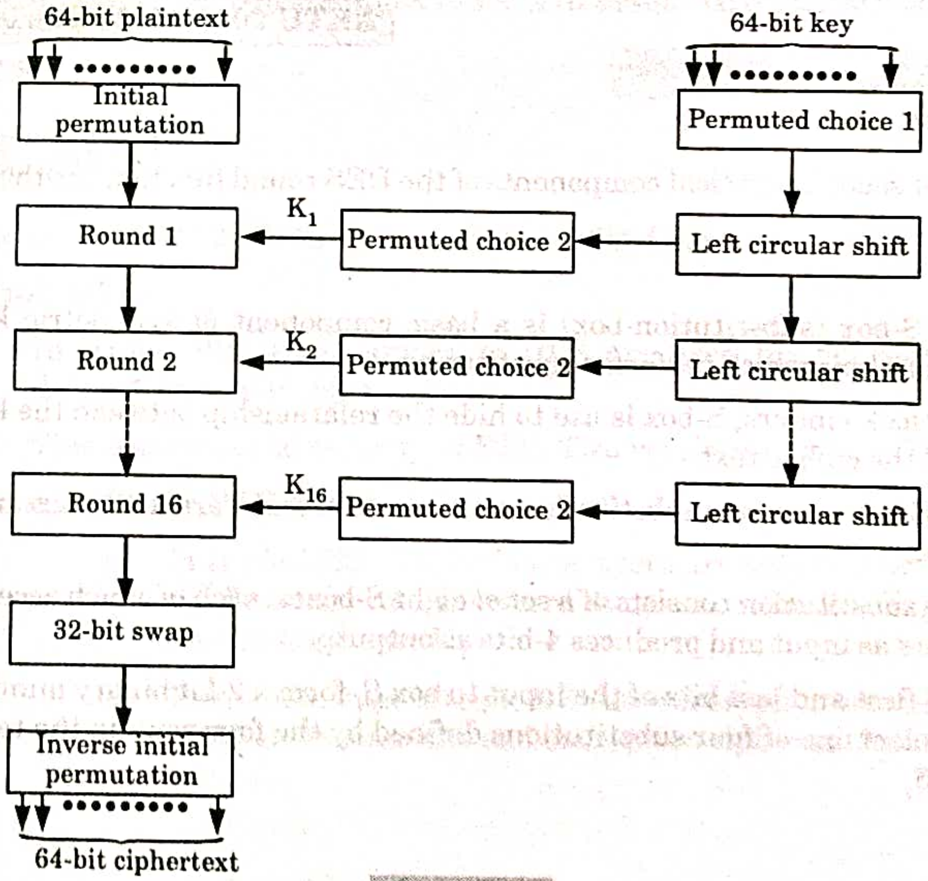


Fig. 1.18.1.

1. In DES encryption, there are two inputs to the encryption function : the plaintext to be encrypted and the key.
2. The plaintext must be 64 bits in length and the key is 56 bits in length.
3. The 64-bit plaintext passes through an initial permutation (IP) that rearranges the bits to produce the permuted input.
4. The output of the last (sixteenth) round consists of 64 bits that are a function of the input plaintext and the key.
5. The left and right halves of the output are swapped to produce the preoutput.
6. The preoutput is passed through a permutation (IP^{-1}) that is the inverse of the initial permutation function, to produce the 64-bit ciphertext.

Strength of DES :

1. The inner workings of the DES algorithm are completely known. The strength of DES lies only in key, which must be secret.
2. It uses 56 bit key in encryption and there are 2^{56} possible keys. A brute force attack on such number of keys is impractical.

Que 1.19. **What is the most security-critical component of DES round function ? Give a brief description of this function.**

AKTU 2014-15, Marks 05

Answer

The most security-critical components of the DES round function are the S-boxes.

S-box :

1. An S-box (substitution-box) is a basic component of symmetric key algorithms which performs substitution.
2. In block ciphers, S-box is use to hide the relationship between the key and the cipher text.
3. An S-box is an $m*n$ substitution unit, where m and n are not necessarily same.
4. The substitution consists of a set of eight S-boxes, each of which accepts 6-bits as input and produces 4-bits as output.
5. The first and last bits of the input to box S_i form a 2-bit binary number to select one of four substitutions defined by the four rows in the table for S_i.

6. The middle four bits select one of the sixteen columns.

7. The decimal value in the cell selected by the row and column is then converted to its 4-bit representation to produce the output.

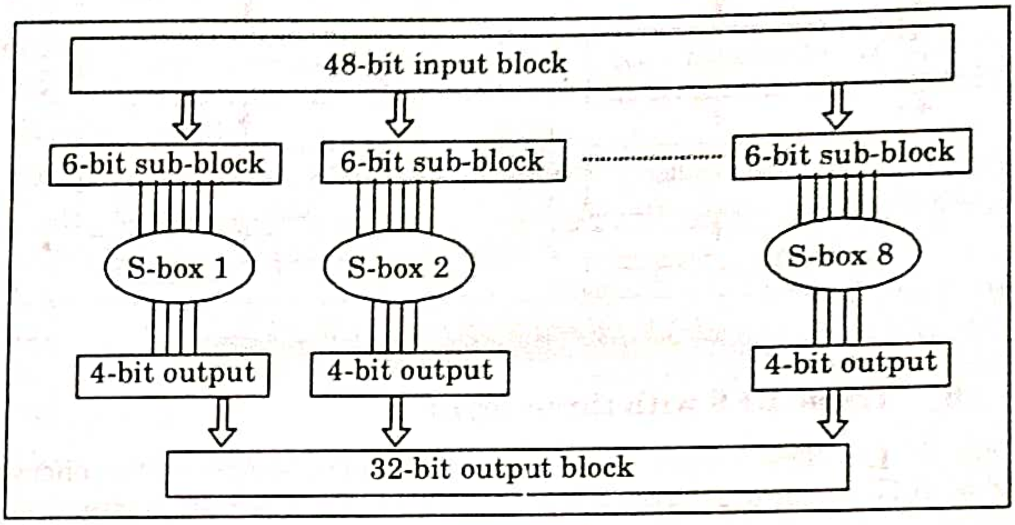


Fig. 1.19.1.

Que 1.20. **List the strength of DES in brief. Also explain the triple DES.**

AKTU 2018-19, Marks 10

Answer

Strength of DES : Refer Q. 1.18, Page 1–16D, Unit-1.

Triple DES :

1. In triple DES, three stages of DES are used for encryption and decryption of messages.
2. This increases the security of DES. Two versions of triple DES are :

   a. **Triple DES with two keys :**

      1. In triple DES with two keys, there are only two keys K_1 and K_2. The first and the third stages use the key K_1 and the second stage uses K_2.
      2. The middle stage of triple DES uses decryption (reverse cipher) in the encryption site and encryption cipher in the decryption site.

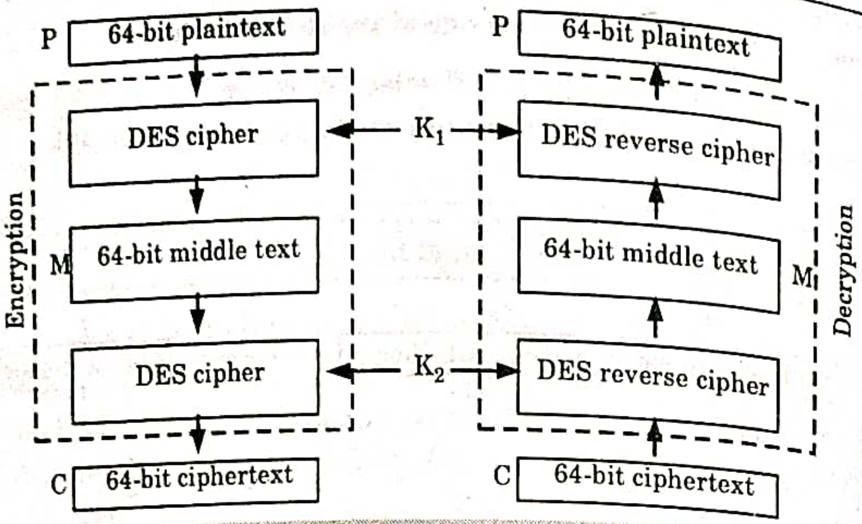


Fig. 1.20.1. Triple DES with two keys.

b. **Triple DES with three keys :**

1. This cipher uses three DES cipher stages at the encryption site and three reverse cipher at the decryption site.

2. The plaintext is first encrypted with a key K_1, then encrypted with a second key K_2 and finally with a third key K_3, where K_1, K_2 and K_3 are all different.

3. Triple DES with three keys is used in PGP and S/MIME. Plaintext can be obtained by first decrypting the ciphertext with the key K_1, then with K_2 and finally with K_3.

$$P = D_{K_3}(D_{K_2}(D_{K_1}(C))).$$

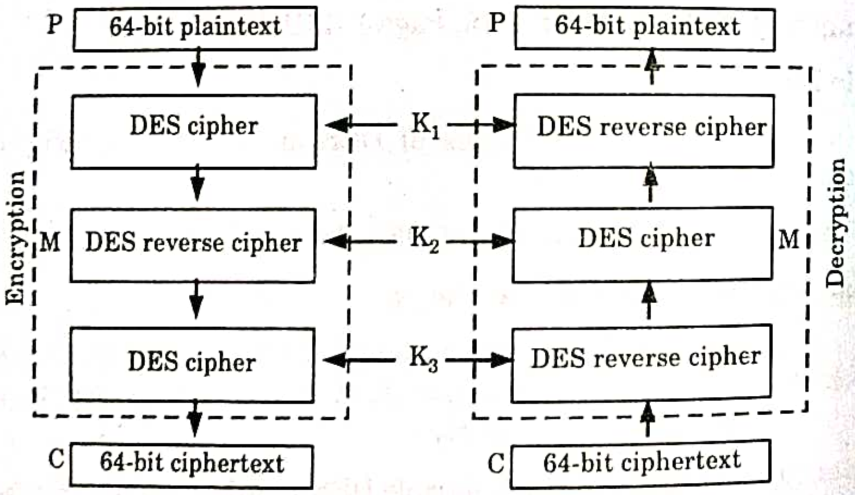


Fig. 1.20.2. Triple DES with three keys.

Que 1.21. **What is the idea behind meet-in-middle attack ? How it can be avoided in 3 DES ?**

AKTU 2014-15, Marks 05

Answer

The main idea behind the algorithm is to dissect the 4-encryption into two 2-encryption schemes, and to apply the meet-in-middle attack to each of them separately.

Meet-in-middle attack can be avoided as :

1. Triple DES can use three key scenarios : two keys are identical and one is independent.
2. While no encryption method is totally uncrackable, the encryption method used (including the number of keys) increases the time and effort needed to break the encryption.
3. Now each encryption level in triple DES is only 56-bits, using three identical keys means once the key is uncovered, a meet-in-middle attack is possible because one key allows across to all the envelopes and the data payload.
4. Using two keys provided 112-bits encryption (56-bits × 2) and s considered a safe way to prevent meet-in-middle attacks. This is how meet-in-middle attack is avoided in triple DES.

Que 1.22. Write a short note on IDEA.

Answer

1. The International Data Encryption Algorithm (IDEA) is a block cipher and cryptographic algorithm that uses a 128-bit long key and both diffusion and confusion for encryption.
2. This makes it more secure than the widely known DES, which is based on the use of a 56-bit key.
3. IDEA also operates on 64-bit plaintext blocks, and uses the same algorithm for encryption and decryption.
4. E-mail privacy technique called Pretty Good Privacy (PGP) is based on IDEA.
5. Following are the strength of IDEA :
   a. The IDEA algorithm is resistant to all known cryptanalysis attack.
   b. It uses a 128-bit long key.
   c. To attempt a cryptanalysis attack on IDEA, the attacker needs to perform 2^{128} encryption operations, which is practically infeasible.

Que 1.23. Describe IDEA encryption and decryption in brief. Also explain, how can we generate cryptographically secure pseudo-random numbers ?

AKTU 2017-18, Marks 10

Answer

IDEA encryption :

1. IDEA (International Data Encryption Algorithm) is a block cipher that works on 64-bit plaintext and 128-bit key.
2. The 64-bit plaintext block is divided into four portion of 16-bit plaintext (P_1 to P_4). These are input to the first round.
3. There are eight such rounds. The key consists of 128-bits.
4. In each round, six sub-keys are generated from the original key; each of these sub-key consists of 16-bits.
5. For the first round we have key K_1 to K_6, for second round we have keys K_7 to K_{12} and finally the last round. The final step consists of an output transformation, which uses four sub-keys (K_{49} to K_{52}).
6. The final output is produced by the output transformation step. The blocks C_1 to C_4 are combined to form the final output.

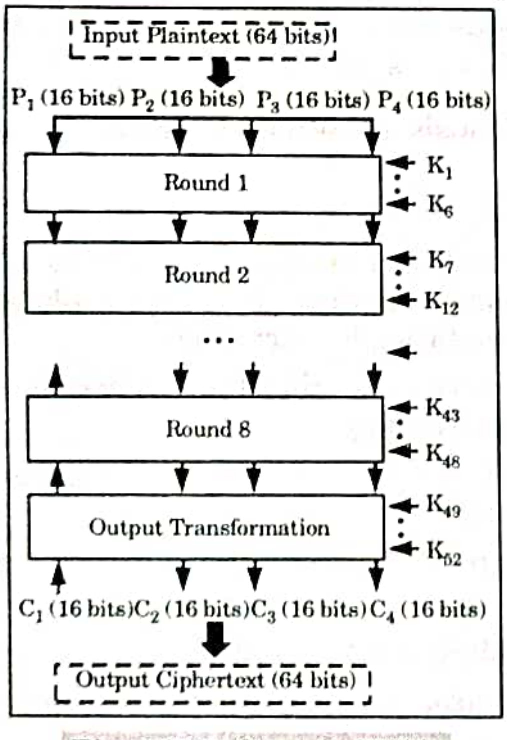

Input Plaintext (64 bits)
P1 (16 bits) P2 (16 bits) P3 (16 bits) P4 (16 bits)
Round 1
K1
K6
Round 2
K7
K12
...
Round 8
K43
K48
Output Transformation
K49
K52
C1 (16 bits) C2 (16 bits) C3 (16 bits) C4 (16 bits)
Output Ciphertext (64 bits)

Fig. 1.23.1. Steps in IDEA.

IDEA decryption : The decryption process is exactly the same as the encryption process with some alterations in the generation and pattern of sub-keys. The decryption sub-keys are actually inverses of the encryption sub-keys.

Cryptographically Secure Pseudo-Random Numbers Generator (CSPRNG) : A Cryptographically Secure Pseudo-Random Number Generator (CSPRNG) is a Pseudo-Random Number Generator (PRNG) with properties that make it suitable for use in cryptography.

Generating pseudo-random numbers cryptographically :

1. The generation of random number in CSPRNGs uses entropy obtained from a high-quality.
2. We can generate pseudo-random number using counter mode.
3. A secure block cipher can be converted into a CSPRNG by running it in counter mode.
4. In counter mode, secure block cipher is converted in cryptographically secure pseudo-random number generator.

Que 1.24. **Explain the sub-key generation in the IDEA algorithm.**

Answer

A sub-key generation process is used to generates the sub-keys as follows :

1. In the first round, six sub-keys of 16 bits each, that is, 96 bits are required. Therefore, the first 96 bits at 128-bit key (say, K) are used for the first round. The rest of the key bits (97-128) remain unused and, thus, are kept for the second round.
2. The second round also requires six sub-keys of 16 bits each; that is, a total of 96 bits. However, we have only 32 unused bits of the key K and, therefore, we need 64 bits more. To generate the rest of the bits, the IDEA algorithm uses the key shifting technique.
3. In the third round, we have 64 unused bits of key K′ generated in the second round, and 32 bits are still required. Thus, the key shifting technique is again applied, and the key K′ is left shifted by 25 bits. This process continues to obtain 96 bits in each round.
4. The output transformation stage also needs four sub-keys of 16 bits each.

Que 1.25. **What is the difference between block cipher and stream cipher ? What are the different modes of block cipher operation ? Explain any one of them.**

AKTU 2014-15, Marks 05

OR

Explain different block cipher mode of operation.

AKTU 2016-17, Marks 10

OR

What is block cipher ? Discuss block cipher mode of operations.

AKTU 2017-18, Marks 05

Answer

Block cipher : Refer Q. 1.10, Page 1–9D, Unit-1.

Modes of operation of block cipher :

1. **Cipher Feedback Mode (CFB) :** CFB mode is used where block size are smaller in size.

2. **Electronic Codebook Mode (ECB) :**
   a. This is the simplest mode. The plaintext is divided into N blocks. The block size is n-bits. If plaintext size is less than multiple of n then extra padding is used in last block.
   b. The same key is used to encrypt and decrypt each block. For lengthy messages, the ECB mode may not be secure.
   c. The relationship between plaintext and ciphertext block is shown below :

   Encryption : $C_i = E_k(P_i)$

   Decryption : $P_i = D_k(C_i)$

   where E : Encryption

   D : Decryption

   P_i : Plaintext block i

   C_i : Ciphertext block i

3. **Ciphertext Block Chaining (CBC) mode :**
   a. In CBC mode, each plaintext block is Exclusive-ORed with the previous ciphertext block before being encrypted.
   b. For the first block a Initialization Vector (IV) is used for EX-ORing the sender, and the receiver agrees upon the predefined initialization vector.
   c. The relationship between plaintext and ciphertext block is shown below :

   Encryption : $C_o = IV$

   $C_i = E_k(P_i \oplus C_{i-1})$

   Decryption : $C_o = IV$

   $P_i = D_k(C_i \oplus C_{i-1})$

4. **Output Feedback (OFB) mode :**
   a. It is very similar to CFB mode, with one difference. Each bit of the ciphertext is independent of the previous bit. This avoids flow of error from one block to another.
   b. One advantage of this method is that bit errors in transmission do not propagate. One disadvantage of this method is that it is more vulnerable to a message stream modification attack than is CFB.

5. **Counter mode :**
   a. In counter mode, a counter equal to the plaintext block size is used. For encryption, the counter is encrypted and then XORed with the plaintext block to produce the ciphertext block.
   b. For decryption, same sequence of counter values is used, with each encrypted counter XORed with ciphertext block.
   c. Counter mode is used in hardware and software efficiency, preprocessing, security and simplicity.

Difference : Refer Q. 1.11, Page 1–10D, Unit-1.

VERY IMPORTANT QUESTIONS

Following questions are very important. These questions may be asked in your SE0SSIONALS as well as UNIVERSITY EXAMINATION.

Q. 1. Compare and contrast substitution techniques with transposition techniques under classical encryption.

Ans. Refer Q. 1.5.

Q. 2. What is the difference between block cipher and stream cipher ? What are the different modes of block cipher operation ? Explain any one of them.

Ans. Refer Q. 1.25.

Q. 3. What is the Shannon's theory of confusion and diffusion in terms of information security ?

Ans. Refer Q. 1.14.

Q. 4. Explain Feistel encryption and decryption algorithms. What is the difference between diffusion and confusion ?

Ans. Refer Q. 1.15.

Q. 5. Discuss DES in detail with suitable block diagram.

Ans. Refer Q. 1.17.

Q. 6. List the strength of DES in brief. Also explain the triple DES.

Ans. Refer Q. 1.20.

Q. 7. Describe IDEA encryption and decryption in brief. Also explain, how can we generate cryptographically secure pseudo-random numbers ?

Ans. Refer Q. 1.23.

☺☺☺

2 UNIT

Advanced Encryption Standard

CONTENTS

PART- 1

Introduction to Group,Field, Finite Field of the form GF(p), Modular Arithmetic, Prime and Relative Prime Numbers, Extended Euclidean Algorithm.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 2.1. **Define group field and finite field of the form $GF(p)$.**

AKTU 2015-16, Marks 10

Answer

Group : A group G, denoted by {G, •}, is a set of elements with a binary operation '•' that satisfies following four properties :

1. **Closure :** $c = a \bullet b$
2. **Associativity :** $(a \bullet b) \bullet c = a \bullet (b \bullet c)$
3. **Identity :** $e \bullet a = a \bullet e = a$.
4. **Inverse :** $a \bullet a' = a' \bullet a = e$.

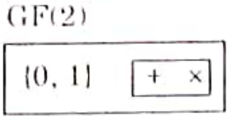
Fields : A field F, denoted by {F, +, ×}, is a set of elements with two binary operations, called addition and multiplication, such that for all a, b, c in F the following axioms are obeyed :

1. F is an integral domain.
2. **Multiplicative inverse :** For each a in F, except 0, there is an element a^{-1} in F such that $aa^{-1} = (a^{-1})a = 1$.

GF(p) fields :

1. When $n = 1$, we have GF(p) field. This field can be the set Z_p, {0, 1, ..., $p - 1$}, with two arithmetic operations (addition and multiplication).
2. In this set each element has an additive inverse and that nonzero elements have a multiplicative inverse (no multiplicative inverse for 0).

For example : A field GF(2) with the set (0, 1) and two operations, addition and multiplication, is shown as :



+	0	1
0	0	1
1	1	0

Addition

×	0	1
0	0	0
1	0	1

Multiplication

Fig. 2.1.1. GF(2) field.

Que 2.2. **Explain finite field of the form GF(p) & GF(2^n) with suitable example.**

AKTU 2017-18, Marks 05

Answer

GF(p) fields : Refer Q. 2.1, Page 2–2D, Unit-2.

GF(p^n) fields :

1. The order of a finite field must be of the form p^n, where p is a prime and n is a positive integer.
2. Using modular arithmetic in Z_p, all of the axioms for a field are satisfied. For polynomials over p^n, with $n > 1$, operations modulo p^n do not produce a field.

For example : Consider the two polynomials in GF(2^8) :

$$f(x) = x^6 + x^4 + x^2 + x + 1 \text{ and } g(x) = x^7 + x + 1.$$

$$(x^6 + x^4 + x^2 + x + 1) + (x^7 + x + 1) = x^7 + x^6 + x^4 + x^2$$

(polynomial notation)

$(01010111 \oplus (10000011) = (11010100)$ (binary notation)

$\{57\} \oplus \{83\} = \{D4\}$ (hexadecimal notation)

Que 2.3. **Define ring and field. Give an example of ring which is not a field.**

AKTU 2014-15, Marks 05

Answer

Ring : A ring R, denoted by $\{R, +, \times\}$, is a set of elements with two binary operations, called addition and multiplication, such that for all a, b, c in R the following axioms are obeyed :

1. **Closure under multiplication :** If a and b belong to R, then ab is also in R.
2. **Associativity of multiplication :** $a(bc) = (ab)c$ for all a, b, c in R.
3. **Distributive laws :**

$$a(b + c) = ab + ac \text{ for all } a, b, c \text{ in } R$$

$$(a + b)\, c = ac + bc \text{ for all } a, b, c \text{ in } R$$

4. **Commutative of multiplication :** $ab = ba$ for all a, b in R.
5. **Multiplicative identity :** There is an element 1 in R such that

$$a1 = 1a \text{ for all } a \text{ in } R.$$

6. **No zero divisors :** If a, b belong to R and $ab = 0$, then either $a = 0$ or $b = 0$.

Fields : Refer Q. 2.1, Page 2–2DA, Unit-2.

Example : $(Z, +, \bullet)$ is an example of a ring which is not a field because not every element of the set Z *i.e.*, integer has a multiplicative inverse.

Que 2.4. **Explain the term modular arithmetic.**

OR

What are the properties of modular arithmetic operation ?

AKTU 2015-16, Marks 10

Answer

1. Modular arithmetic is a system of arithmetic for integers, where numbers reduces to a certain value *i.e.*, the modulus.
2. Modular arithmetic is used in number theory to calculate checksums and identifiers to spot error.
3. Modular arithmetic is used to limit the size of integer coefficients in intermediate calculation and data.

S. No.	Property	Expression
1.	Commutative laws	$(w + x) \bmod n = (x + w) \bmod n$ $(w \times x) \bmod n = (x \times w) \bmod n$
2.	Associative laws	$[(w + x) + y] \bmod n = [w + (x + y)] \bmod n$ $[(w \times x) \times y] \bmod n = [w \times (x \times y)] \bmod n$
3.	Distributive law	$[w \times (x + y)] \bmod n = [(w \times x) + (w \times y)] \bmod n$
4.	Identities	$(0 + w) \bmod n = w \bmod n$ $(1 \times w) \bmod n = w \bmod n$
5.	Additive inverse $(-w)$	For each $w \in Z_n$, there exists z such that $w + z \equiv 0 \bmod n$

Que 2.5. **What is prime and relative prime numbers in cryptography and network security ?**

AKTU 2018-19, Marks 10

Answer

Prime numbers :

1. A prime number is an integer that can only be divided without remainder by positive and negative values of itself and 1.
2. Any integer a > 1 can be factored in a unique way as :

$$a = p_1^{a_1}\, p_2^{a_2}\, p_3^{a_3} \ldots\ldots p_t^{a_t}$$

where $p_1 < p_2 < \ldots . < p_t$ are prime numbers and each a_i is a positive integer. This is known as the fundamental theorem of arithmetic.

3. If p is the set of all prime numbers then any positive integer a can be written uniquely in the form :

$$a = \prod_{p \in P} p^{a_p} \text{ where each } a_p \geq 0$$

Relatively prime numbers :

1. Two integers a and b are relatively prime if gcd $(a, b) = 1$.
2. The integers a_1, a_2, ..., a_n are pair-wise relatively prime if gcd $(a_i, a_j) = 1$ whenever $1 \leq i < j \leq n$.
3. Number that is relatively prime to another number means that the gcd of the two numbers is 1. Therefore, it does not mean that either of the numbers has to be prime.

   For example : Are 15, 17 and 28 pair-wise relatively prime ? Yes, because gcd (15, 17) = 1, gcd (15, 28) = 1 and gcd (17, 28) = 1.
4. The method for calculating the number of relatively prime numbers less than a given number involves prime factorization, which is given as follows :

   Step 1 : Find the exponential prime factorization of the number.

   Step 2 : Taking each term separately, change the term to 2 numbers :

   i. Subtract 1 from the base for the first number.

   ii. Subtract 1 from the exponent and evaluate the expression for the second number.

   Step 3 : Multiply all the numbers together found in step 2.

Que 2.6. **Describe the extended Euclidean algorithm to find the multiplicative inverse.**

Answer

1. The extended Euclidean algorithm is an extension to the Euclidean algorithm.
2. Besides finding the gcd of two positive integers x and y, it simultaneously find the multiplicative inverses a and b such that :

$$m^*x + n^*y = \text{gcd}\ (x, y)$$

where m is the multiplicative inverse of x mod y and n is the multiplicative inverse of y mod x.

Algorithm : To find the gcd of two positive integers along with the multiplicative inverses following steps are involved :

```
1.  a : = x
2.  b : = y
3.  c : = 1
4.  d : = 0
5.  e : = 0
6.  f : = 1
7.  while (b > 0)
    {
        q : = a/b
        r : = a – q*b
        a : = b
        b : = r
        m : = c – q*d
        c : = d
        d : = m
        n : = e – q*f
        e : = f
        f : = n
    }
8.  gcd (x, y) : = a
9.  m : = c
10. n : = e
```

PART-2

Advanced Encryption Standard (AES) Encryption and Decryption, Fermat's and Euler's Theorem, Primality Testing.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 2.7. **State the Advanced Encryption Standard (AES). Also provide the functioning of AES.** **AKTU 2018-19, Marks 10**

OR

Write a short note on AES. **AKTU 2017-18, Marks 05**

Answer

1. AES is a block cipher intended to replace DES for commercial applications. It uses a 128-bit block size and a key size of 128, 192, or 256 bits.
2. AES does not use a Feistel structure. Instead, each full round consists of four separate functions : byte substitution, permutation, arithmetic operations over a finite field, and XOR with a key.
3. AES is a non-Feistel cipher that encrypts and decrypts a data block of 128 bits. AES uses a symmetric key algorithm.

Functioning of AES :

1. **Encryption process :** In encryption process, each round comprise of four sub-processes. The first round process is shown as :

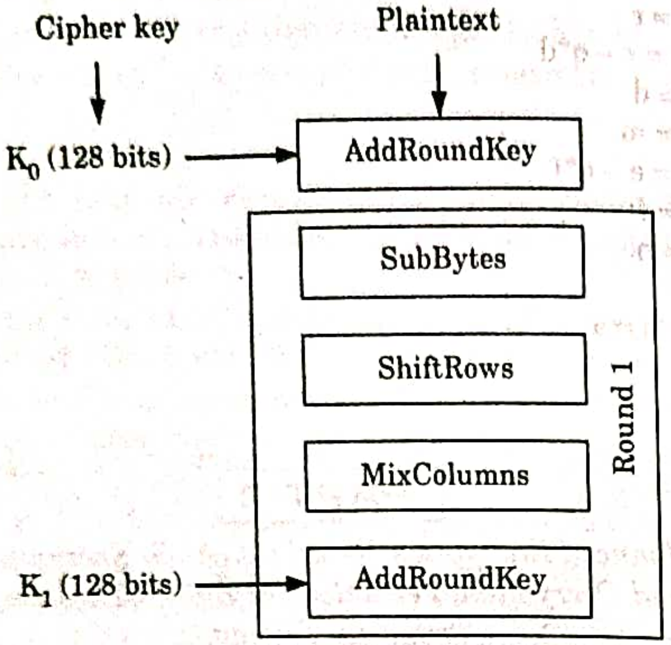


Fig. 2.7.1.

a. **Byte substitution (SubBytes) :** It uses an S-box to perform a byte-by-byte substitution of the block. The result is stored in a matrix of four rows and four columns.

b. **ShiftRows :** Each of the four rows of the matrix is shifted in the left. Any entries that 'fall off' are re-inserted on the right side of row.

c. **MixColumns :** Each column of four bytes is transformed using a special mathematical function. This function takes four bytes of one column as input and generates outputs of four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. This step is not performed in the last round.

d. **AddRoundKey :** The 16 bytes (128 bits) of the matrix are XORed to the 128 bits of the round key. If this is the last round then the output is the ciphertext. Otherwise, the resulting 128 bits are interpreted as 16 bytes and other similar round starts again.

2. **Decryption process :** The process of decryption of an AES ciphertext is similar to the encryption process in the reverse order. Each round consists of the four processes conducted in the given order :

   i. AddRoundKey
   ii. MixColumns
   iii. ShiftRows
   iv. Byte substitution

   Since sub-processes in each round are in reverse manner the encryption and decryption algorithms needs to be separately implemented.

Que 2.8. **What are the advantages and disadvantages of AES ?**

Answer

Advantages :

1. It is most robust security protocol as it is implemented in both hardware and software.
2. It uses higher length key sizes such as 128, 192 and 256 bits for encryption. Hence it makes AES algorithm more robust against hacking.
3. It is most common security protocol used for various applications such as wireless communication, financial transactions, e-business, encrypted data storage, etc.
4. For 128 bit, about 2128 attempts are needed to break. This makes it very difficult to hack it as a result it is very safe protocol.

Disadvantages :

1. It uses simple algebraic structure.
2. Every block is always encrypted in the same way.
3. Hard to implement with software.
4. AES in counter mode is complex to implement in software taking both performance and security into considerations.

Que 2.9. **Describe the Fermat's little theorem. Using Fermat's theorem, find the value of 3^{201} mod 11.** **AKTU 2014-15, Marks 05**

Answer

Fermat's little theorem :

1. Fermat's theorem also known as Fermat's little theorem states that if P is prime and 'a' is a positive integer not divisible by P then :
$$a^{P-1} \equiv 1 \bmod P$$
2. Second condition says that if, P is a prime and a is an integer, then $a^P \equiv a \bmod P$.

Proof : Z_p is the set of integer {0, 1 ... P – 1} when multiplied by a modulo P, the result consists of all the element of Z_p in some sequence, furthermore, $a \times 0 \equiv 0 \bmod P$.

Therefore, the $(P-1)$ numbers $\{a \bmod P, 2a \bmod P, ..., ((P-1)\,a \bmod P)\}$ are just the number $\{1, 2 ... (P-1)\}$ in some order.

Multiplying the numbers in both sets and taking the result mod P gives

$$a \times 2a \times \ldots \times ((P-1)\,a) = [(a \bmod P) \times (2a \bmod P) \times \ldots \times ((P-1)\,a \bmod P)] \bmod P$$
$$= [1 \times 2 \times \ldots \times (P-1)] \bmod P$$
$$= (P-1)! \bmod P$$

But,

$$a \times 2a \times \ldots \times ((P-1)a) = (P-1)!\,a^{P-1}$$
$$(P-1)!\,a^{P-1} \equiv (P-1)! \bmod P$$

$$a^{P-1} \equiv 1 \bmod P$$

Numerical :

$$3^{10} \equiv 1 \pmod{11}$$

Therefore, $3^{201} = (3^{10})^{20} \times 3 \equiv 3 \pmod{11}$

Que 2.10. **State and prove Euler theorem.**

AKTU 2016-17, Marks 10

Answer

Euler's theorem : This theorem states that for every a and n that are relatively prime :

$$a^{\phi(n)} \equiv 1 \pmod n \quad ...(2.10.1)$$

Proof :

a. Equation (2.10.1) is true if n is prime, because in that case $\phi(n) = (n-1)$ and Fermat's theorem holds.

b. We know that $\phi(n)$ is the number of positive integers less than n that are relatively prime to n.

c. Consider the set of such integers :
$R = \{x_1, x_2, ..., x_{\phi(n)}\}$, *i.e.*, each element x_i of R is a unique positive integer less than n with $gcd\ (x_i, n) = 1$.

d. Now multiply each element by a and modulo n :

$$S = \{(ax_1 \bmod n), (ax_2 \bmod n), \ldots, (ax_{\phi(n)} \bmod n)\}$$

e. Because a is relatively prime to n and x_i is relatively prime to n, ax_i must also be relatively prime to n. Thus, all the members of S are integers that are less than n and that are relatively prime to n.
There are no duplicates in S.

f. If $ax_i \bmod n = ax_j \bmod n$ then $x_i = x_j$

Therefore, $\prod_{i=1}^{\phi(n)} (ax_i \bmod n) = \prod_{i=1}^{\phi(n)} x_i$

$$\prod_{i=1}^{\phi(n)} ax_i \equiv \prod_{i=1}^{\phi(n)} x_i \pmod n$$

$$a^{\phi(n)} \times \left[\prod_{i=1}^{\phi(n)}\right] x_i \equiv \prod_{i=1}^{\phi(n)} x_i \pmod n$$

$$a^{\phi(n)} \equiv 1 \pmod n$$

Que 2.11. **Explain Euler's totient function.**

Answer

1. Euler's totient function, (Euler's phi function) denoted as $\phi(n)$, is the function contains number of positive integers that are smaller than n and relatively prime to n. The set of these numbers is represented by Z_n.

2. A set of rules used for calculating the value of $\phi(n)$:

   Rule 1 : $\phi(1) = 1$

   Rule 2 : $\phi(p) = p - 1$, if p is a prime number

   Rule 3 : $\phi(m * n) = \phi(m) * \phi(n)$, if m and n are relatively prime

   Rule 4 : $\phi(p^e) = p^e - p^{e-1}$, if p is prime

3. To compute $\phi(n)$, suppose that we have two prime numbers p and q, such that $p \neq q$ and $n = pq$. Then :

$$\begin{aligned} \phi(n) &= \phi(pq) \\ &\Rightarrow \phi(p) * \phi(q) \\ &\Rightarrow (p-1) * (q-1) \end{aligned}$$

Que 2.12. **What is primality testing ? What are its categories ?**

Answer

1. Primality testing is used to check whether a given large number is prime or composite.
2. The algorithms for checking the primality are divided into two categories :
   a. **Deterministic algorithm :** This algorithm accepts a number (say, p) as input and output the result, either that p is prime or that p is composite. There are two types of deterministic algorithms :
      i. **Basic algorithm :** This algorithm check whether a number p is prime or not is to divide p by all values m (from 2 to $p - 1$) and check whether p is fully divisible by any value of m.
      ii. **Divisibility algorithm :** In this algorithm, instead of testing upto $p - 1$, testing upto only $\sqrt{p}$ is sufficient. The reason behind this is that if p is composite, then it can be factored into two values, and atleast one of the values must be less than or equal to $\sqrt{p}$.
   b. **Probabilistic algorithm :** This algorithm is use to check the probability of a number being prime. These algorithms accept an integer p and output the probability of p being prime. There are two types of probabilistic algorithm tests :
      i. **Fermat's primality test :** This is a probabilistic test that checks whether a number is prime or not.
      ii. **Miller-Rabin test :** It is also a probabilistic test to check whether a number taken at random is prime or not. This test returns the result as composite if p is not prime, or as inconclusive if p may or may not be a prime number.

Que 2.13. **Give the Miller-Rabin algorithm for testing primality.**

Answer

1. The Miller-Rabin algorithm (Rabin-Miller test) is used to test a large number for primality.
2. It is a polynomial-time algorithm with a run-time complexity of $O((\log n)^3)$.
3. In Miller-Rabin algorithm, we take into account two basic properties of prime numbers :
   a. If p is a prime number and x is a positive integer $(1 < x < p)$, then $x^2 \bmod p = 1$ if and only if $x \bmod p = 1$ or $x \bmod p = -1$.
   b. If p is a prime number greater than 2, we can say that $p - 1 = 2^k q$ where $k > 0$ and q is odd, then $x^q \bmod p = 1$ or $x^q \equiv 1 \pmod p$.

Que 2.14. **Write the pseudocode for Miller-Rabin primality testing. Test whether 61 is prime or not using the same Miller-Rabin test.**

AKTU 2014-15, Marks 05

Answer

Pseudocode for Miller-Rabin primality testing :

```
Miller–Rabin(BigInteger n, int s) {// return "true" or "false"
    // test whether n is prime ;
    // if it returns "false", then n is not prime ;
    // if it returns "true", then n is prime ;
    // with probability atleast 1 – 2 ** (–s).
    // s is number of tests we want to perform on n.
    BigInteger a ;
    for (int i = 1; i <= s; ++i) {
    a = Random (2, n – 1);
    if Witness (a, n) return false ;
    }
    return true :
    }
```

Numerical : We know that if n is a prime,

$$a^n - 1 \equiv 1 \bmod n$$

We use base (b) 2,

$$61 - 1 = 15 \times 2^2 \rightarrow n = 15, s = 2, a = 2$$

Initialization : $b = 2^{15} \bmod 61 = 11 \bmod 61$

$s = 1,$ $b = 11^2 \bmod 61 = -1 \bmod 61$ (prime)

Hence, 61 is a prime number.

PART-3

Chinese Remainder Theorem.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 2.15. **Illustrate the concept of Chinese Remainder Theorem. By using Chinese Remainder Theorem solve the simultaneous congruence $X = 2 \bmod P$ for all $P \in (3, 5, 7)$.** **AKTU 2014-15, Marks 05**

Answer

Chinese remainder theorem :

1. The Chinese Remainder Theorem (CRT) is used to solve a set of congruent equations with one variable but different moduli, which are relatively prime.
2. $$x \equiv a_1 \pmod{m_1}$$ $$x \equiv a_2 \pmod{m_2}$$ $$\vdots$$ $$x \equiv a_k \pmod{m_k}$$

   The Chinese Remainder Theorem states that the above equations have a unique solution if the moduli are relatively prime.
3. The solution to the set of equations follow these steps :
   a. Find $M = m_1 \times m_2 \times ..... \times m_k$. This is the common modulus.
   b. Find $M_1 = M/m_1, M_2 = M/m_2, ..., M_k = M/m_k$.
   c. Find the multiplicative inverse of $M_1, M_2 \; . \; . \; . \; M_k$. Using the corresponding moduli $(m_1, m_2, ..., m_k)$. Call these inverses as M_1^{-1}, $M_2^{-1} .... M_k^{-1}$.
   d. The solution to the simultaneous equations is :

   $x = (a_1 \times M_1 \times M_1^{-1} + a_2 \times M_2 \times M_2^{-1} + . . . + a_k \times M_k \times M_k^{-1}) \bmod M$

   Numerical : Solving simultaneous congruence for $X = 2 \bmod P$ for all $P \in \{3, 5, 7\}$

$$X \equiv 2 \bmod P \text{ for all } P \in \{3, 5, 7\}$$
$$X \equiv 2 \bmod 3$$
$$X \equiv 2 \bmod 5$$
$$X \equiv 2 \bmod 7$$

Step 1 : $M = 3 \times 5 \times 7 = 105$

Step 2 : $M_1 = 105/3 = 35$

$M_2 = 105/5 = 21$

$M_3 = 105/7 = 15$

Step 3 : $M_1^{-1} = (35 \times x) \bmod 2 = 1$

$$M_2^{-1} = (21 \times x) \bmod 2 = 1$$

$$M_3^{-1} = (15 \times x) \bmod 2 = 1$$

Step 4 :

$$X = (2 \times 35 \times 1 + 2 \times 21 \times 1 + 2 \times 15 \times 1) \bmod 105$$

$$= (70 + 42 + 30) \bmod 105 = (142) \bmod 105 = 37$$

Que 2.16. **Define the Chinese remainder theorem. Find the values of *x* for the following sets of Congruence using the Chinese remainder theorem.**

$X = 2 \bmod 7$ and $X = 3 \bmod 9$.

AKTU 2015-16, Marks 10

Answer

Chinese remainder theorem : Refer Q. 2.15, Page 2–12D, Unit-2.

Numerical :

$$X = 2 \bmod 7$$

$$X = 3 \bmod 9$$

$$M = m_1 \times m_2$$

$$= 7 \times 9 = 63$$

$$M_1 = 63/7 = 9$$

$$M_2 = 63/9 = 7$$

$$M_1^{-1} = 9^{-1} \bmod 7$$

$$= 9^{\phi(7)-1} \bmod 7$$

$$= 9^{2-1} \bmod 7 = 9 \bmod 7 = 2$$

$$M_2^{-1} = 7^{-1} \bmod 9$$

$$= 7^{\phi(9)-1} \bmod 9$$

$$= 7^{3-1} \bmod 9$$

$$= 7^2 \bmod 9$$

$$= 49 \bmod 9$$

$$= 4$$

$$X = (a_1 \times M_1 \times M_1^{-1} + a_2 \times M_2 \times M_2^{-1}) \bmod 63$$

$$X = (2 \times 9 \times 2 + 3 \times 7 \times 4) \bmod 63$$

$$X = 120 \bmod 63$$

$$X = 57$$

Que 2.17. **What do you understand by Chinese Remainder Theorem ? Solve the following congruent equations by Chinese Remainder Theorem :**

i. X ≅ 2 mod 3

ii. X ≅ 3 mod 5

AKTU 2017-18, Marks 10

Answer

Chinese remainder theorem : Refer Q. 2.15, Page 2–12D, Unit-2.

Numerical :

Step 1 : Given $X \cong 2 \bmod 3$

$a_1 = 2 \quad m_1 = 3$

$X \cong 3 \bmod 5$

$a_2 = 3 \quad m_2 = 5$

Thus, common modulus $M = m_1 \times m_2 = 3 \times 5 = 15$

Step 2 : Compute M_1, M_2

$$M_1 = \frac{15}{3} = 5$$

$$M_2 = \frac{15}{5} = 3$$

Step 3 : Compute the multiplicative inverse of M_1 and M_2 in modulo m_1 nd m_2 respectively

$$M_1^{-1} = (5 \times x) \bmod 2 = 1$$

$$M_2^{-1} = (3 \times x) \bmod 3 = 1$$

Step 4 : The solution to the simultaneous equation is as follows :

$$x = (a_1 \times M_1 \times M_1^{-1} + a_2 \times M_2 \times M_2^{-1}) \bmod 15$$

$$= (2 \times 5 \times 2 + 3 \times 3 \times 3) \bmod 15 = 47 \bmod 15 = 2$$

Que 2.18. Explain the Chinese Remainder Theorem with example. How Chinese remainder theorem provide the security to online information sharing transactions.

AKTU 2018-19, Marks 10

OR

Explain Chinese remainder theorem with example.

AKTU 2016-17, Marks 10

Answer

Chinese remainder theorem : Refer Q. 2.15, Page 2–12D, Unit-2.

Security to online information sharing transaction :

1. Chinese remainder theorem enables end-to-end transport layer security between WAP clients and servers located across the wired internet.
2. It uses secret sharing, which consist of distributing a set of shares in the form of congruence, among the group of people who all together can recover that secret share.

Que 2.19. Find the values of x for the following sets of Congruence using the Chinese remainder theorem.

$$X = 2 \pmod 3$$

$$X \equiv 1 \pmod 4$$
$$X \equiv 3 \pmod 5$$

AKTU 2015-16, Marks 15

Answer

$$X = 2 \pmod 3$$
$$X = 1 \pmod 4$$
$$X = 3 \pmod 5$$
$$M = m_1 \times m_2 \times m_3$$
$$M = 3 \times 4 \times 5 = 60$$
$$M_1 = 60/3 = 20$$
$$M_2 = 60/4 = 15$$
$$M_3 = 60/5 = 12$$
$$M_1^{-1} = 20^{-1} \bmod 3$$
$$= 20^{\phi(3)-1} \bmod 3$$
$$= 20^{2-1} \bmod 3$$
$$= 20 \bmod 3$$
$$= 2$$
$$M_2^{-1} = 15^{-1} \bmod 4$$
$$= 15^{\phi(4)-1} \bmod 4$$
$$= 15^{1-1} \bmod 4$$
$$= 15^0 \bmod 4$$
$$= 1 \bmod 4$$
$$= 1$$
$$M_3^{-1} = 12^{-1} \bmod 5$$
$$= 12^{\phi(5)-1} \bmod 5$$
$$= 12^3 \bmod 5$$
$$= 1728 \bmod 5$$
$$= 3$$

$$X = (a_1 \times M_1 \times M_1^{-1} + a_2 \times M_2 \times M_2^{-1} + a_3 \times M_3 \times M_3^{-1}) \bmod 60$$
$$X = ((2 \times 20 \times 2) + (1 \times 15 \times 1) + (3 \times 12 \times 3)) \bmod 60$$
$$X = (80 + 15 + 108) \bmod 60$$
$$X = (203) \bmod 60$$
$$X = 23$$

PART-4

Discrete Logarithmic Problem, Principlas of Public Key CryptoSystems, RSA Algorithm, Security of RSA.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 2.20. **Write a short note on discrete logarithmic problems.**

Answer

1. Discrete logarithms are the set of congruence classes (1, ..., $p - 1$) under multiplication modulo, the prime p.
2. Let G be a finite cyclic group with n elements. We assume that the group is written multiplicatively.
3. Let b be a generator of G ; then every element g of G can be written in the form $g = b^k$ for some integer k.
4. Furthermore, any two such integers representing g will be congruent modulo n.
5. We can thus define a function $\log_b : G \rightarrow Z_n$ (where Z_n denotes the ring of integers modulo n) by assigning to g the congruence class of k modulo n.
6. This function is a group isomorphism, called the discrete logarithm to base b.

   For example, consider $(Z_{17})^{\times}$. To compute 3^4 in this group, we first compute $3^4 = 81$, and then we divide 81 by 17, obtaining a remainder of 13.

   Thus $3^4 = 13$ in the group $(Z_{17})^{\times}$.

Que 2.21. **What is the principle of public-key cryptosystems ? Discuss the applications for public-key cryptosystems.**

AKTU 2015-16, Marks 10

Answer

Principle of public-key cryptosystem : The concept of public-key cryptography evolved from an attempt to solve the most difficult problems associated with symmetric encryption *i.e.*, (1) two communicants already share a key, which has been distributed to them and (2) the use of a key distribution center. The second problem negates the very essence of cryptography: the ability to maintain total secrecy over the communication.

Applications for public-key cryptosystem : The use of public key cryptosystems is classified into three categories :

a. **Encryption/decryption :** The sender encrypts a message with the recipient's public key.

b. **Digital signature :** The sender signs a message with its private key. Signing is achieved by a cryptographic algorithm applied to the message or to a small block of data that is a function of the message.

c. **Key exchange :** Two sides cooperate to exchange a session key. Several different approaches are possible, involving the private key(s) of one or both parties.

Que 2.22. **Describe RSA algorithm, encryption and decryption function. In RSA, given $e = 07$ and $n = 3$. Encrypt the message "ME" using 00 to 25 for letters A to Z.**

AKTU 2014-15, Marks 05

Answer

RSA algorithm :

1. RSA is a public key encryption algorithm, named for its inventors (Rivest, Shamir and Adleman).
2. The RSA algorithms is based on the mathematical part that it is easy to find and multiply large prime numbers together, but it is extremely difficult to factor their product.

Key Generation :

1. Select two prime numbers p and q such that $p \neq q$
2. Calculate $n = p \times q$
3. Calculate $\phi(n) = (p - 1)(q - 1)$
4. Select integer e such that gcd $(\phi(n), e) = 1$; $1 < e < \phi(n)$
5. Calculate $d = e^{-1}$ (mod $\phi(n)$)
6. Public key $PU = \{e, n\}$
7. Private key $PR = \{d, n\}$

Encryption :

Calculate ciphertext $C = M^e \bmod n$.

Decryption :

Calculate plaintext $M = C^d \bmod n$.

Numerical :

1. Translate the numbers into letters : $M = 12$ and $E = 4$
2. Encrypt each block M using, $C \equiv M^7 \pmod 3$
3. For $M = 12$

$$\begin{aligned} C &= 12^7 \pmod 3 \\ &= 12^4 \times 12^3 \pmod 3 \\ &= (12^2)^2 \times 12^2 \times 12 \pmod 3 \\ &= 0 \end{aligned}$$

For $E = 4$

$$C = E^7 \pmod 3$$

$= 4^7 \pmod 3$

$= 4 \pmod 3$

$= 1$

∴ The encrypted ciphertext is : 0 and 1.

Que 2.23. **Explain RSA algorithm. Perform encryption and decryption using RSA algorithm for $p = 11, q = 13, e = 7, m = 9$.**

AKTU 2015-16, Marks 15

OR

Explain RSA using example. **AKTU 2016-17, Marks 10**

Answer

RSA algorithm :

1. The RSA algorithm is asymmetric key cryptographic algorithm.
2. The RSA algorithm is based on the mathematical fact that it is easy to find and multiply large prime numbers together, but it is extremely difficult to factor their product.
3. The private and public keys in RSA are made up of 100 or more digits prime numbers.
4. The real challenge in RSA is the selection and generation of the public and private keys.
5. The RSA algorithm is shown as :
   a. Choose two large prime numbers p and q.
   b. Calculate $n = p \times q$.
   c. Select the public key (*i.e.*, the encryption key) e such that it is not a factor of $(p - 1)$ and $(q - 1)$.
   d. Select the private key (*i.e.*, the decryption key) d such that the following equation is true :
   $$(d \times e) \bmod (p-1) \times (q-1) = 1$$
   e. For encryption, calculate the cipher text C from the plain text M as follows :
   $$C = M^e \bmod n$$
   f. Send C as the cipher text to the receiver.
   g. For decryption, calculate the plain text C from the cipher text C as follows :
   $$M = C^d \bmod n$$

Numerical :

Step 1 : $p = 11, q = 13$

Step 2 : $n = p \times q = 11 \times 13 = 143$

Step 3 : Calculate

$$\phi(n) = (p-1)(q-1)$$

$$= (11-1)(13-1) = 10 \times 12 = 120$$

Step 4 : Determine d such that de ≡ 1 (mod 160)

$$d = e^{-1} \text{ mod } 160$$

Using extended Euclidean algorithm we calculate d.

q	r_1	r_2	r	t_1	t_2	t
17	120	7	1	0	1	– 17
7	7	1	0	1	– 17	120
	1	0		– 17	120	

$$= -17 \text{ mod } 120$$

$$d = 103$$

Public key = {7, 143}

Private key = {103, 143}

Encryption $(C) = M^e \text{ (mod } n)$

$$M = 9$$

$$C = 9^7 \text{ mod } 143$$

$$= [(9^4 \text{ mod } 143) \times (9^2 \text{ mod } 143)$$

$$(9^1 \text{ mod } 143)] \text{ mod } 143$$

$$= (126 \times 81 \times 9) \text{ mod } 143$$

$$= 91854 \text{ mod } 143$$

$$= 48$$

Decryption $(M) = 13^{103} \text{ mod } 143$

Que 2.24. **Discuss public key cryptosystem. Explain RSA algorithm with suitable steps. Let $p = 17$, $q = 11$, $e = 7$ and d = 23. Calculate the public key and private key and show encryption and decryption for plain text $M = 88$ by using RSA algorithm.**

AKTU 2017-18, Marks 10

Answer

Public key cryptosystem : Refer Q. 2.21, Page 2–16D, Unit-2.

RSA algorithm : Refer Q. 2.23, Page 2–18D, Unit-2.

Numerical :

Step 1 : $p = 17, q = 11$

Step 2 : $n = p \times q = 17 \times 11 = 187$

Step 3 : Calculate $\phi(n) = (p-1)(q-1) = 16 \times 10 = 160$

Step 4 : $d = 23$ and $e = 7$

Public key is {7, 187}

Private key is {23, 187}

Encryption : Ciphertext is

$C = M^e \bmod n = 88^7 \bmod 187 = (88^2 \bmod 187)\,(88^5 \bmod 187)$

$= [77 \times (77 \times 77) \times 88] \bmod 187 = 11$

$C = 11$

Decryption : Plaintext is

$M = C^d \bmod n = 11^{23} \bmod 187 = (11^5 \bmod 187)\,(11^{18} \bmod 187)$

$= [44 \times (44 \times 44 \times 44)\,(11^3 \bmod 187)] \bmod 187$

$= [44^4 \times 22] \bmod 187 = 88$

Que 2.25. **What are the advantage and disadvantage of RSA ?**

Answer

Advantages :

1. **Convenience :** It solves the problem of distributing the key for encryption.
2. **Provides message authentication :** Public key encryption allows the use of digital signatures which enables the recipient of a message to verify that the message is from a particular sender.
3. **Detection of tampering :** The use of digital signatures in public key encryption allows the receiver to detect if the message was altered in transit. A digitally signed message cannot be modified without invalidating the signature.
4. **Provides non-repudiation :** Digitally signing a message is related to physically signing a document. It is an acknowledgement of the message and thus, the sender cannot deny it.

Disadvantages :

1. **Public keys should/must be authenticated :** No one can be absolutely sure that a public key belongs to the person it specifies and so everyone must verify that their public keys belong to them.
2. **Slow :** Public key encryption is slow compared to symmetric encryption. Not feasible for use in decrypting bulk messages.
3. **Uses more computer resources :** It requires a lot more computer supplies compared to single-key encryption.
4. **Widespread security compromise is possible :** If an attacker determines a person's private key, his or her entire messages can be read.
5. **Loss of private key may be irreparable :** The loss of a private key means that all received messages cannot be decrypted.

Que 2.26. **What are the securities of RSA ? Perform encryption and decryption using RSA algorithm for $p = 17$, $q = 11$, $e = 7$, $m = 88$.**

AKTU 2015-16, Marks 10

Answer

Three possible approaches and securities of the RSA algorithm are :

1. **Brute force :** This involves trying all possible private keys.
   a. The defense against the brute force approach is to use a large key space.
2. **Mathematical attacks :** There are several approaches used for factoring the product of two primes.
   a. The defense against mathematical attacks is to use factoring performance as a benchmark against which to evaluate the security of RSA.
3. **Timing attacks :** These depend on the running time of the decryption algorithm. Counter-measures that can be used, includes the following :
   a. **Constant exponentiation time :** Ensure that all exponentiation take the same amount of time before returning a result. This is a simple fix but does degrade performance.
   b. **Random delay :** Better performance could be achieved by adding a random delay to the exponentiation algorithm to confuse the timing attack.
   c. **Blinding :** Multiply the ciphertext by a random number before performing exponentiation. This process prevents the attacker from knowing what ciphertext bits are being processed inside the computer and therefore prevents the bit-by-bit analysis essential to the timing attack.

Numerical :

Step 1 : $p = 17$, $q = 11$

Step 2 : $n = p \times q = 17 \times 11 = 187$

Step 3 : Calculate $\phi(n) = (p-1)(q-1)$

$$= 16 \times 10 = 160$$

Step 4 : Determine d such that $de \equiv 1 \pmod{160}$

$$d = e^{-1} \bmod 160 \quad \text{taking } e = 7$$

Using extended Euclidean algorithms we calculate d.

q	r_1	r_2	r	t_1	t_2	t
22	160	7	6	0	1	–22
1	7	6	1	1	–22	23
6	6	1	0	–22	23	–160
	1	0		23	–160	

$\therefore \quad d = 23$

Public key = {7, 187}

Private key = {23, 187}

11 to be kept secret.

Encryption : $C = M^e \pmod n$

Given : $M = 88$

$C = 88^7 \bmod 187$

$= [(88^4 \bmod 187) \times (88^2 \bmod 187)$
$(88^1 \bmod 187)] \bmod 187$

$= (132 \times 77 \times 88) \bmod 187 = 11$

Decryption : $M = 11^{23} \bmod 187$

$= [(11^1 \bmod 187) \times (11^2 \bmod 187)$
$\times (11^4 \bmod 187) \times (11^8 \bmod 187)$
$\times (11^8 \bmod 187)] \bmod 187$

$= (11 \times 121 \times 55 \times 33 \times 33) \bmod 187 = 88.$

Que 2.27. **Differentiate between DES and AES.**

Answer

S. No.	Basis for Comparison	DES (Data Encryption Standard)	AES (Advanced Encryption Standard)
1.	Basic	Data block is divided into two halves.	Data block is processed as a single matrix.
2.	Principle	DES work on Feistel cipher structure.	AES works on substitution and permutation principle.
3.	Plaintext	Plaintext is of 64 bits	Plaintext can be of 128,192, or 256 bits.
4.	Key size	DES in comparison to AES has smaller key size.	AES has larger key size as compared to DES.
5.	Rounds	16 rounds	10 rounds for 128-bit algo, 12 rounds for 192-bit algo, 14 rounds for 256-bit algo.
6.	Rounds Names	Expansion Permutation, XOR, S-box, P-box, XOR and Swap.	Subbytes, Shiftrows, Mix columns, Addroundkeys.
7.	Security	DES has a smaller key which is less secure.	AES has large secret key which is more secure.
8.	Speed	DES is comparatively slower.	AES is faster.

VERY IMPORTANT QUESTIONS

Following questions are very important. These questions may be asked in your SESSIONALS as well as UNIVERSITY EXAMINATION.

Q. 1. Define group field and finite field of the form $GF(p)$.

Ans. Refer Q. 2.1.

Q. 2. State the Advanced Encryption Standard (AES). Also provide the functioning of AES.

Ans. Refer Q. 2.7.

Q. 3. Illustrate the concept of Chinese Remainder Theorem. By using Chinese Remainder Theorem solve the simultaneous congruence $X = 2 \bmod P$ for all $P \in (3, 5, 7)$.

Ans. Refer Q. 2.15.

Q. 4. Explain the Chinese Remainder Theorem with example. How Chinese remainder theorem provide the security to online information sharing transactions.

Ans. Refer Q. 2.18.

Q. 5. What is the principle of public-key cryptosystems ? Discuss the applications for public-key cryptosystems.

Ans. Refer Q. 2.21.

Q. 6. Describe RSA algorithm, encryption and decryption function. In RSA, given $e = 07$ and $n = 3$. Encrypt the message "ME" using 00 to 25 for letters A to Z.

Ans. Refer Q. 2.22.

Q. 7. What are the securities of RSA ? Perform encryption and decryption using RSA algorithm for $p = 17$, $q = 11$, $e = 7$, $m = 88$.

Ans. Refer Q. 2.26.

☺☺☺

3

UNIT

Message Authentication Codes

CONTENTS

PART-1

Message Authentication Codes, Authentication Requirements, Authentication Functions, Message Authentication code.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 3.1. **Discuss the message authentication codes. Also give the use of authentication requirement in MAC.**

AKTU 2018-19, Marks 10

Answer

Message Authentication Code :

1. A cryptographic Message Authentication Code (MAC) is a short piece of information used to authenticate a message.
2. A MAC algorithm accepts as input a secret key and an arbitrary length message to be authenticated, and outputs a MAC (sometimes known as a tag).
3. The MAC value protects both message's data integrity as well as its authenticity, by allowing verifiers (who also possess the secret key) to detect any change to the message content.
4. MAC is written as :

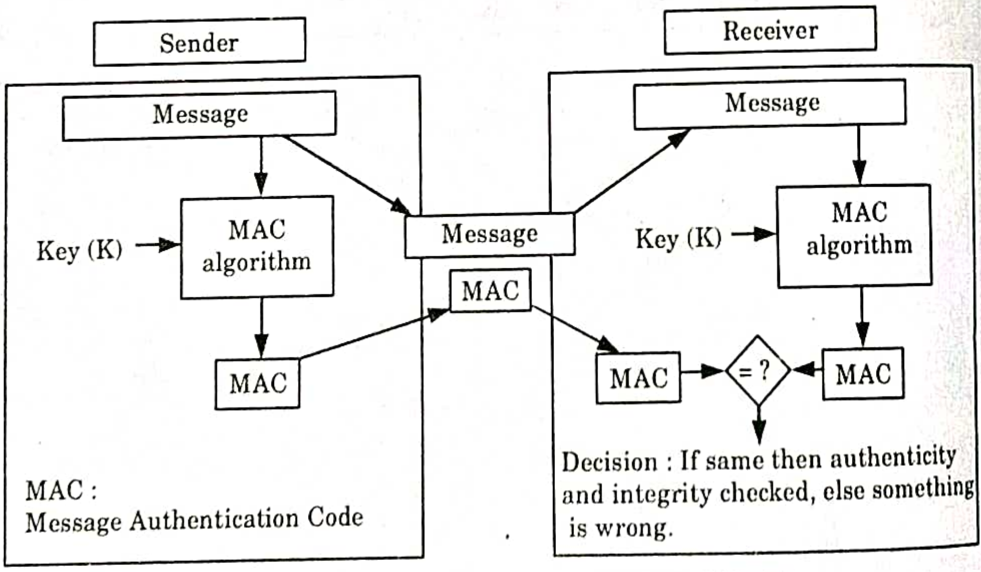

Sender
Receiver
Message
Key (K)
MAC algorithm
MAC
Message
MAC
Message
Key (K)
MAC algorithm
MAC
= ?
MAC
MAC :
Message Authentication Code
Decision : If same then authenticity and integrity checked, else something is wrong.

Fig. 3.1.1. Message Authentication Code.

$$MAC = C(K, M)$$

where M is a variable length message, K is the secret key shared only by sender and the receiver, and C(K, M) is the fixed length authenticator.

Use of authentication requirement in MAC : Authentication requirement in MAC is used to verify the integrity of a message *i.e.*, whether the message is from the authorized sender or not.

Que 3.2. What types of attacks are addressed by message authentication ?

Answer

Types of attacks that are addressed by message authentication are :

1. **Masquerade :**
   a. This attack happens when the messages from a fraud source are put into the network.
   b. This attack also includes the fake acknowledgements corresponding to the received or failed messages by some other entity except the intended recipient.
2. **Modification of the message :**
   a. This attack involves making certain modifications in the contents of the captured message or changing the sequence of messages being transmitted between the communicating parties.
3. **Timing modification :**
   a. This attack involves delaying or replaying the messages being transmitted.
   b. The term 'replay' means capturing a copy of the message sent by the original sender and retransmitting it later to bring about an unauthorized result.
   c. In a connection-oriented application, the entire session can be delayed or replayed, whereas in a connection-less application, the individual messages can be delayed or replayed.

Que 3.3. Why message authentication is required ? Discuss working of MAC with suitable block diagram. Also discuss HMAC & CMAC in detail.

AKTU 2017-18, Marks 10

Answer

Message authentication is required to protect both message's data integrity as well as authenticity.

Working of MAC : Let us assume that the sender A wants to send a message M to a receiver B, as shown in Fig. 3.3.1.

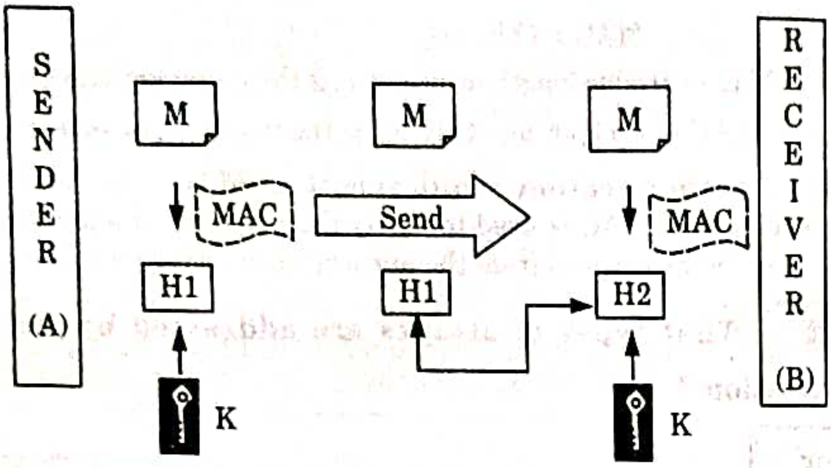


Fig. 3.3.1. Message Authentication Code (MAC).

1. A and B share a symmetric (secret) key K, which is not known to anyone else. Sender 'A' calculates the MAC H1 by applying key K to the message M.
2. A then sends the original message M and the MAC H1 to B.
3. When B receives the message, B also uses K to calculate its own MAC H2 over M.
4. B now compares H1 with H2. If the two match, B concludes that the message M has not been changed during transit. However, if H1 do not match H2, B rejects the message, realizing that the message was changed during transit.

HMAC :

1. HMAC (Hash-based Message Authentication Code) has been chosen as a mandatory security implementation for the Internet Protocol (IP) security and is also used in the Secure Socket Layer (SSL) protocol, widely used on the Internet.
2. The fundamental idea behind HMAC is to reuse the existing message digest algorithm, such as MD5 or SHA-1.
3. HMAC treats the message digest as a black box.
4. It uses the shared symmetric key to encrypt the message digest, which produces the output MAC.

CMAC :

1. Cipher-based Message Authentication Codes (CMAC) are the tools used for calculating message authentication codes using a block cipher coupled with a secret key.
2. CMAC is used to verify both the integrity and authenticity of a message.
3. In CMAC, the message is divided into *N* blocks, each *m* bits long. The size of the CMAC is *n* bits.
4. If the last block is not *m* bits, it is padded with a 1-bit followed by enough 0-bits to make it *m* bits. The first block of the message is encrypted with the symmetric key to create an *m*-bit block of encrypted data.

5. This block is XORed with the next block and the result is encrypted again to create a new *m*-bit block.

Que 3.4. **What are the requirements of a Message Authentication Code (MAC) ? Discuss the logical structure, components and algorithmic steps of MD5 algorithm.**

AKTU 2014-15, Marks 10

OR

Discuss MD-5 algorithm with all required steps and suitable block diagram.

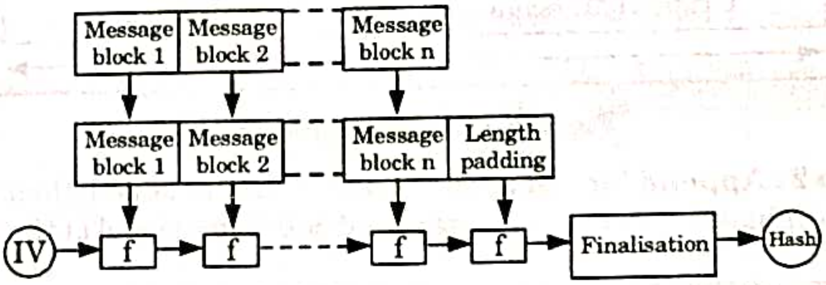
AKTU 2017-18, Marks 10

Answer

Requirements for MACs : The MAC function should satisfy the following requirements :

1. If an opponent observes M and C(K, M), it should be computationally infeasible for the opponent to construct a message M' such that C(K, M') = C(K, M).
2. C(K, M) should be uniformly distributed in the sense that for randomly chosen messages, M and M', the probability that C(K, M) = C(K, M') is 2^n, where n is the number of bits in the MAC.
3. Let M' be equal to some known transformation on M that is, M' = f(M). For example, f may involve inverting one or more specific bits. In that case, Pr[C(K, M) = C(K, M')] = 2^{-n}.

Logical structure of MD5 algorithm :



1. The one-way compression function *f* transforms two fixed length inputs to an output of the same size as one of the input.
2. The algorithm starts with an initial value, the initialization vector (IV). The IV is a fixed value algorithm.
3. For each message block, the compression function *f* takes the result so far, combines it with the message block, and produces an intermediate result.
4. The last block is padded with zeros as needed and bits representing the length of the entire message are appended.
5. The last result is then fed through a finalisation function.
6. The finalisation function compresses a bigger internal state into a smaller output hash size.

Components of MD5 algorithm :

1. **Buffer :** MD5 uses a buffer that is made up of four words that are each 32 bits long. These words are called A, B, C and D.
2. **Table :** MD5 uses a table K that has 64 elements. Element number i is indicated as K_i.
3. **Four auxiliary functions :** MD5 uses four auxiliary functions that each take as input three 32-bit words and produce as output one 32-bit word. They apply the logical operators AND, OR, NOT and XOR to the input bits.
4. **Blocks processing :** The contents of the four buffers (A, B, C and D) are mixed with the words of the input, using the four auxiliary functions (F, G, H and I). There are four rounds, each involves 16 basic operations.

Algorithmic steps of MD5 :

Step 1 : Padding : The first step in MD5 is to add padding bits to the original message. The aim of this step is to make the length of the original message equal to a value 64 bits, but less than an exact multiple of 512.

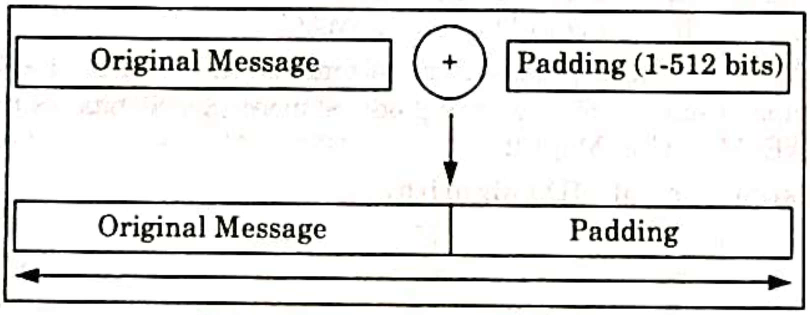


Fig. 3.4.1. Padding process.

Step 2 : Append length : After padding bits are added, then calculate the original length of the message and add it to the end of the message.

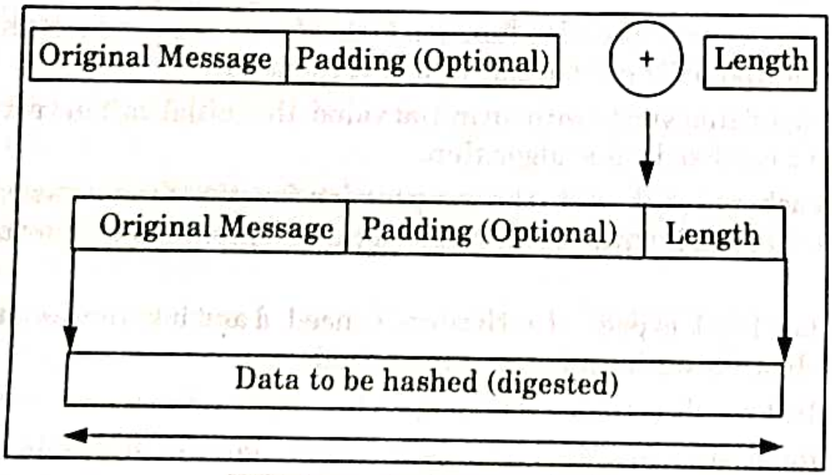


Fig. 3.4.2. Append length.

Step 3 : Divide the input into 512-bit blocks : We divide the input message into blocks, each of length 512-bits.

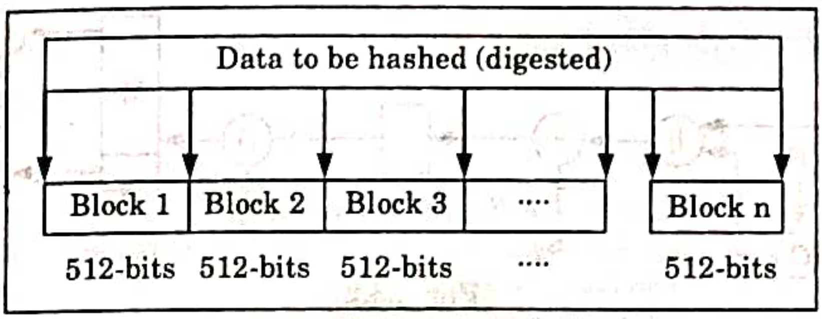


Fig. 3.4.3. Data is divided into 512-bit blocks.

Step 4 : Initialize chaining variables : In this step, four variables (called as chaining variables) are initialized. They are called as *A*, *B*, *C* and *D*. Each of these is a 32-bit number.

Step 5 : Process blocks : After all the initializations main algorithm is executed :

a. Copy the four chaining variables into four corresponding variables, *a*, *b*, *c* and *d*. Thus, we have $a = A$, $b = B$, $c = C$ and $d = D$,

b. Divide the current 512-bit block into 16 sub-block.

c. We have four rounds. In each round, we process all the 16 sub-blocks belonging to a block. The inputs to each round are : (i) all the 16 sub-blocks, (ii) the variables *a*, *b*, *c* and *d* (iii) some constants, designated as *t*.

Que 3.5. **Discuss the basic use of message authentication code with suitable diagrams.**

AKTU 2016-17, Marks 10

Answer

Basic uses of Message Authentication Code (MAC) are :

1. **Message authentication :** It provide authentication but not confidentiality because the message as a whole is transmitted in the clear. Confidentiality can be provided by performing message encryption either after or before the MAC algorithm.

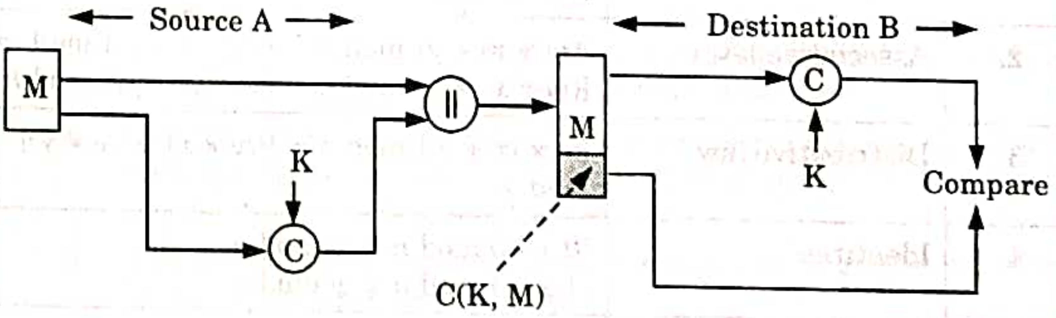


Fig. 3.5.1.

2. **Message authentication and confidentiality (Authentication tied to plaintext) :** It uses two separate key each of which is shared by

the sender and the receiver. The MAC is calculated with the message as input and is then concatenated to the message. The entire block is then encrypted.

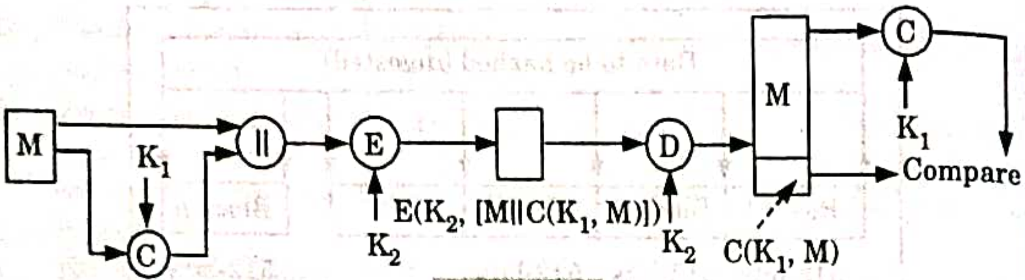


Fig. 3.5.2.

3. **Message authentication and confidentiality (Authentication tied to ciphertext) :** The message is encrypted and then MAC is calculated using the resulting ciphertext and is concatenated to the ciphertext to form transmitted block.

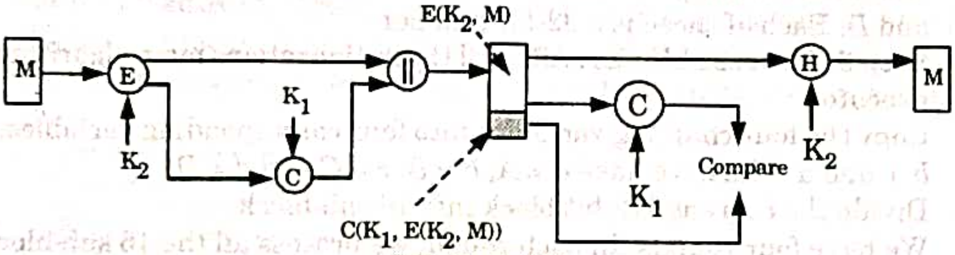


Fig. 3.5.3.

Que 3.6. **What are the properties of modular arithmetic operation ? What are the requirements of Message Authentication Code (MAC) ? List and explain them.** **AKTU 2015-16, Marks 10**

Answer

Properties of modular arithmetic operation :

S. No.	Property	Expression
1.	Commutative laws	$(w + x) \bmod n = (x + w) \bmod n$ $(w \times x) \bmod n = (x \times w) \bmod n$
2.	Associative laws	$[(w + x) + y] \bmod n = [w + (x + y)] \bmod n$ $[(w \times x) \times y] \bmod n = [w \times (x \times y)] \bmod n$
3.	Distributive law	$[w \times (x + y)] \bmod n = [(w \times x) + (w \times y)] \bmod n$
4.	Identities	$(0 + w) \bmod n = w \bmod n$ $(1 \times w) \bmod n = w \bmod n$
5.	Additive inverse $(-w)$	For each $w \in Z_n$, there exists z such that $w + z \equiv 0 \bmod n$

Requirements for MACs : Refer Q. 3.4, Page 3–5D, Unit-3.

Que 3.7. **Write the objectives of HMAC. Describe the HMAC algorithms.** **AKTU 2016-17, Marks 10**

Answer

Objective of HMAC are :

1. To use available hash functions without modifications.
2. To allow for easy replaceability of the embedded hash function in case faster or more secure hash functions are found or required.
3. To preserve the original performance of the hash function without incurring a significant degradation.
4. To use and handle keys in a simple way.

HMAC algorithm :

1. Append zeros to the left end of K to create a b-bit string K^+.
2. XOR K^+ with ipad to produce the b-bit block S_i.
3. Append M to S_i.
4. Apply H to the stream generated in step 3.
5. XOR K^+ with opad to produce the b-bit block S_o.
6. Appends the hash result from step 4 to S_o.
7. Apply H to the stream generated in step 6 and output the result.

Where, K = Secret key

K^+ = K padded with zeros on the left so that the result is b bits in length

ipad = 00110110 repeated $b/8$ times

opad = 01011100 repeated $b/8$ times

M = Message input

H = Embedded hash function

Que 3.8. **Discuss the security of HMAC.**

Answer

1. The security of HMAC depends on the cryptographic strength of the embedded hash function, the size of secret key used and the length of the message digest produced.
2. The probability of attacking HMAC successfully is equal to either of the following attacks on the embedded hash function :
   a. The intruder can calculate the output of compression function without having the knowledge of IV (Initalization Vector), which is selected at random and kept secret.
   b. The intruder determines the collisions in the hash function even if the IV is secret and random.
3. The intruder selects a random value of n bits (*i.e.* the length of the message digest produced) and uses it in place of IV.

4. The intruder needs to determine two messages, M_1 and M_2, such that when the hash function H is applied on them, they yield the same output, that is, $H(M_1) = H(M_2)$.
5. The intruder can attack MD5 by selecting some set of messages and generating the corresponding hash codes to determine the collisions.
6. For a 128-bit hash code in MD5, this requires observing 264 blocks generated using the same key. The use of MD5 is acceptable to HMAC as far as speed is concerned.

PART-2

Hash Functions, Birthday Attacks, Security of Hash Function.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 3.9. What is hash function ? Discuss SHA-512 with all required steps, round function and block diagram.

AKTU 2017-18, Marks 10

Answer

Hash function :

1. A cryptographic hash function is a transformation that takes an input and returns a fixed-size string, which is called the hash value.
2. A hash value h is generated by a function H of the form :

$$h = H(M)$$

where M is the variable length message and H(M) is the fixed length hash value.

3. The hash value is appended to the message at the source at a time when message is assumed or known to be correct.
4. The receiver authenticates the message by recomputing the hash value.
5. The ideal hash function has three main properties :
   a. It is extremely easy to calculate a hash for any given data.
   b. It is extremely difficult to calculate a text that has given hash.
   c. It is extremely unlikely that two different messages, however close, will have the same hash.

Working of Secure Hash Algorithm (SHA) : The algorithm takes as input a message with maximum length of less than 2^{128} bits and produces as output a 512-bit message digest. The input is processed in 1024-bit blocks. The processing consists of following steps :

Step 1 : Padding : The first step in SHA is to add padding to the end of the original message in such a way that the length of the message is 64-bits short of a multiple of 512.

Step 2 : Append length : The length of the message excluding the length of the padding is calculated and appended to the end of the padding as a 64-bit block.

Step 3 : Divide the input into 512-bit blocks : The input message is divided into blocks, each of length 512-bits. These blocks become the input to the message digest processing logic.

Step 4 : Initialize chaining variables : Five chaining variables *A* through *E* are initialized. In SHA, we want to produce a message digest of length 160-bits. Therefore, we need to have five chaining variables.

Step 5 : Process blocks : Main algorithm is executed in process block.

Round Functions :

1. The round function computes a new value for variable A and shifts all working variable once per round.
2. The computation for variable A is a five operand addition modulo 2^{32} where the operands depend on all input words, the round-dependent constant K_t, and the current message word W_t.

Block diagram of SHA-512 :

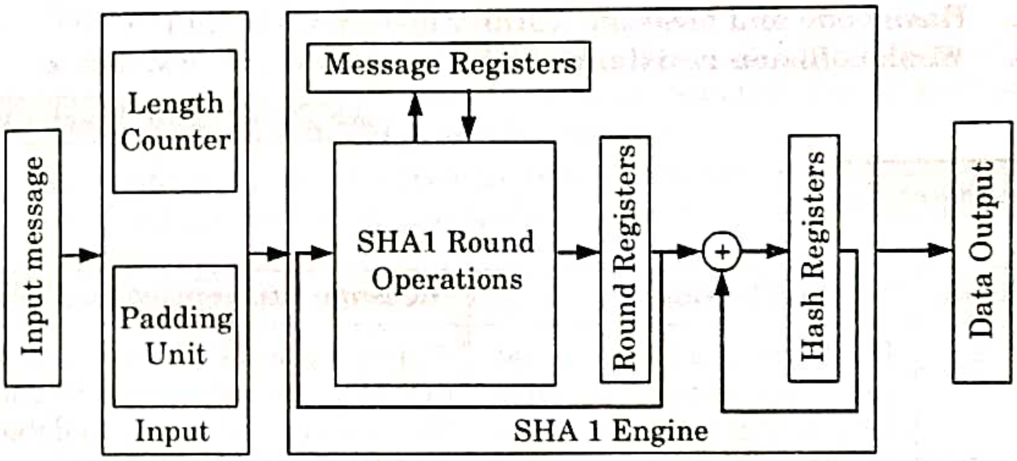


Fig. 3.9.1.

1. The core is composed of two main units, the SHA1 Engine and the padding unit.
2. The SHA1 Engine applies the SHA1 loops on a single 512-bit message block, while the padding unit splits the input message into 512-bit blocks and performs the message padding on the last block of the message.
3. The processing of one 512-bit block is performed in 82 clock cycles and the bit-rate achieved is 6.24 Mbps / MHz on the input of the SHA1 core.

Que 3.10. What characteristics (requirements) are needed in secure hash function ?

Answer

Characteristics (requirements) of secure hash function :

1. The hash function should be applicable on a block of data of any size.
2. The output produced by the hash function should always be of fixed length.
3. For any given message or block of data, it should be easier to generate the hash code.
4. Given a hash code, it should be nearly impossible to determine the corresponding message or block of data.
5. Given a message or block of data, it should not be computationally feasible to determine another message or block of data generating the same hash code as that of the given message or block of data.
6. No two messages or blocks of data, even being almost similar, should be likely to have the same hash code.

Que 3.11. Differentiate between the following :

a. Hash code and Message Authentication Code (MAC)
b. Weak collision resistance and Strong collision resistance

AKTU 2014-15, Marks 10

Answer

a.

S. No.	Hash code	Message Authentication Code
1.	Hash code is a function that takes message of variable length and returns a fixed length code.	A message authentication code is a cryptographic checksum on data that uses a session key to detect modification of the data.
2.	Hash code can have many numbers of inputs *i.e.*, (m_1, m_2, m_3 ...).	MAC requires two input *i.e.*, a message and a secret key.
3.	Hash code is used for indexing and retrieving items in hashing.	MAC is used for authentication and verification of received message.

b.

S. No.	Weak collision resistance	Strong collision resistance
1.	It is the property that, for a given values of h, it is infeasible to find $y = x$ with $H(y) = H(x)$.	It is the property that, it is infeasible to find any pair (x, y) such that $H(x) = H(y)$.
2.	It is bound to a particular input.	It can be applied to any two arbitrary inputs.
3.	Brute force attack takes 2^n way to break weak collision resistance.	Brute force attack takes $2^{n/2}$ ways to break strong collision resistance.

Que 3.12. **Describe birthday attack against any hash function. Give the mathematical basis of the attack.**

AKTU 2014-15, Marks 10

Answer

Birthday attack against hash function :

1. Suppose that a 64-bit hash code is used.
2. If an encrypted hash code C is transmitted with the corresponding unencrypted message M, then an opponent would find an M' such that $H(M') = H(M)$ to substitute another message.
3. The source, A, is prepared to sign a message by appending the appropriate m-bit hash code and encrypting that hash code with A's private key.
4. The opponent generates $2^{m/2}$ variations on the message, which convey some meaning. He prepares an equal number of messages, all of which are variations on the fraudulent message to be substituted for the real one.
5. The two sets of messages are compared to find a pair of messages that produces the same hash code. The probability of success is greater than 0.5. If no match is found, additional messages are generated until a match is found.
6. The opponent offers the valid variation to A for signature. This signature can then be attached to message for transmission to the intended recipient. As the two variations have the same hash code, they will produce the same signature.

Mathematical basis of the attack :

1. Given a hash function H, with n possible outputs and a specific value $H(x)$, if H is applied to k random inputs. Hence, the probability that atleast one input y satisfies $H(y) = H(x)$ is 0.5.

2. For a single value of y, the probability that $H(y) = H(x)$ is just $1/n$.
3. Conversely, the probability that $H(y) {}^{1} H(x)$ is $[1 - (1/n)]$.
4. If we generate k random values of y, then the probability that none of them match is just the product of the probabilities that each individual value does not match, or $[1 - (1/n)]^k$.
5. Thus, the probability that there is atleast one match is $1 - [1 - (1/n)]^k$.
6. The binomial theorem can be stated as follows :

$$(1 - a)^k = 1 - ka + \frac{k(k-1)}{2!}a^2 - \frac{k(k-1)(k-2)}{3!}a^3 \ldots$$

7. For very small values of a, this can be approximated as $(1 - ka)$. Thus, the probability of atleast one match is approximated as $1 - [1 - (1/n)^k \approx 1 - [1 - (k/n)] = k/n$. For a probability of 0.5, we have $k = n/2$.

Que 3.13. **Write a short note on the properties of cryptographic hash function that impact the security of password storage.**

Answer

1. **Non-reversibility (one-way function) :** A good hash function should make it very hard to reconstruct the original password from the output.
2. **Diffusion (avalanche effect) :** A change in one bit of the original password should result in change to half the bits of its hash.
3. **Determinism :** A given password must always generate the same hash value or enciphered text.
4. **Collision resistance :** It should be hard to find two different passwords that hash to the same enciphered text.
5. **Non-predictable :** The hash value should not be predictable from the password.

PART-3

Secure Hash Algorithm (SHA) Digital Signatures : Digital Signatures, Elgamal Digital Techniques, Digital Signature Standard (DSS), Proof of Digital Signature Algorithm.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 3.14. **What do you understand from hash functions ? Discuss the working of Secure Hash Algorithm (SHA) in message authentication.**

AKTU 2018-19, Marks 10

Answer

Hash function : Refer Q. 3.9, Page 3–10D, Unit-3.

Working of Secure Hash Algorithm (SHA) : The algorithm takes as input a message with maximum length of less than 2^{128} bits and produces as output a 512-bit message digest. The input is processed in 1024-bit blocks. The processing consists of following steps :

Step 1 : Padding : The first step in SHA is to add padding to the end of the original message in such a way that the length of the message is 64 bits short of a multiple of 512. The padding is always added, even if the message is already 64 bits short of a multiple of 512.

Step 2 : Append length : The length of the message excluding the length of the padding is calculated and appended to the end of the padding as a 64-bit block.

Step 3 : Divide the input into 512-bit blocks : The input message is divided into blocks, each of length 512 bits. These blocks become the input to the message digest processing logic.

Step 4 : Initialize chaining variables : Five chaining variables *A* through *E* are initialized. In SHA, we want to produce a message digest of length 160 bits. Therefore, we need to have five chaining variables.

Step 5 : Process blocks : Main algorithm is executed in process block.

Que 3.15. Differentiate between SHA-1 and MD5 algorithm.

Answer

S. No.	SHA-1 algorithm	MD5 algorithm
1.	It generates a message digest of 160 bits.	It generates a message digest of 128 bits.
2.	It uses little-endian scheme	It uses big-endian scheme
3.	In this scheme, the most significant byte of a 32-bit word is stored in the low-address byte position.	The least significant byte of a 32-bit word is stored in the low-address byte position.
4.	Slower in operation than MD5.	Faster in operation than SHA-1.
5.	It is not vulnerable to cryptanalytic attack.	It is vulnerable to cryptanalytic attack.
6.	It is more secure than MD5.	It is less secure as compared to SHA-1.

Que 3.16. **Write the Digital Signature Algorithm (DSA) of Digital Signature Standard. What is the implication if same *K* (secret per message) is used to sign two different message using DSA ?**

AKTU 2014-15, Marks 10

Answer

Digital Signature Algorithm (DSA) : DSA is an asymmetric encryption algorithm that works on two different key *i.e.*, one public and one private to produce digital signature.

1. The sender generates a random number k, which is less than q.
2. The sender now calculates :
   a. $r = (g^k \bmod p) \bmod q$
   b. $s = (K^{-1}(H(m) + xr)) \bmod q$

   The values r and s are the signatures of the sender.
3. The sender sends these values to the receiver. To verify the signature, the receiver calculates :

   $w = s^{-1} \bmod q$

   $u1 = (H(m) * w) \bmod q$

   $u2 = (rw) \bmod q$

   $v = ((g^{u1^*} y^{u2}) \bmod p) \bmod q$

   If $v = r$,the signature is said to be verified. Otherwise, it is rejected.

   where,

   p = A prime number of length L bits.

   q = A 160-bits prime factor of $(p - 1)$

   $g = h^{(p-1)/q} \bmod p$,

   x = A number less than q.

   $y = g^x \bmod p$.

   H = Message Digest algorithm.

If same secret (k1, k2) is used for signing two different messages, it will generate two different signatures (r1, s1) and (r1, s2) :

1. s1 = k1^{-1}(h1k2 + d(r1 + r2))
2. s2 = k1^{-1}(h2k2 + d(r1 + r2))

   where h1 = SHA512(m1) and h2 = SHA512(m2)
3. k1s1 – k1s2 = h1k2 + dr – h2k2 – dr
4. k1(s1 – s2) = k2(h1 – h2) .
5. We cannot obtain k1, k2 from this equation and so this scheme is more secure than original ECDSA (Elliptical Curve Digital Signature Algorithm) scheme.

Que 3.17. **Explain the digital signatures. Also give a detail description of Elgamal digital signature techniques.**

AKTU 2018-19, Marks 10

OR

Explain Elgamal digital signature scheme.

AKTU 2016-17, Marks 10

Answer

Digital signatures :

1. Digital signature is a mathematical scheme used for verifying the authenticity of digital message or documents.
2. Digital signature uses three algorithms :
   a. **Key generation :** This algorithm selects a private key uniformly at random from a set of possible private keys. Output of this algorithm is private key and its corresponding public key.
   b. **Signing algorithm :** It produce signature by using message and private key.
   c. **Signature verifying algorithm :** For a given message, signature and public key, either accepts or rejects the messages claim to authenticity.
3. Fig. 3.17.1 shows the concept of digital signature

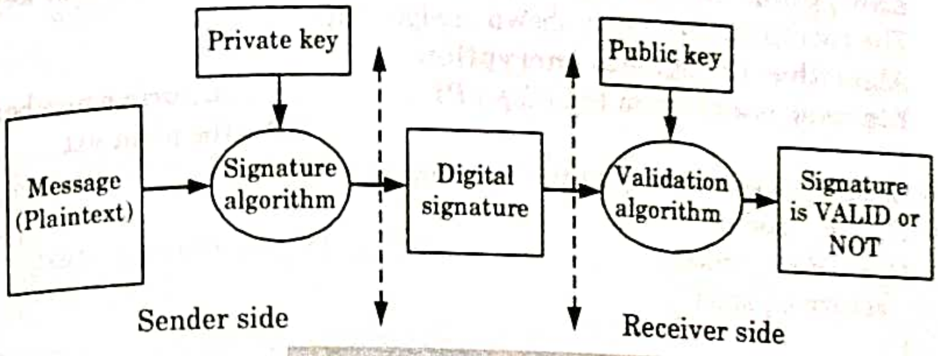


Fig. 3.17.1. Digital signature.

Elgamal digital signature techniques :

1. The Elgamal technique is a public key algorithm, which can be used for both; digital signatures as well as encryption.
2. Its security is based on the difficulty of computing discrete logarithms in a finite field.
3. To generate a key pair, first select a prime number p and two random numbers g and x, so that both g and x are less than p. Then find out $y = g^x \bmod p$. The public key becomes y, g and p. Both g and p can be shared in a group of users. The private key is x.
4. For encrypting a plain text message M, first select a random number k such that k is relatively prime to $p - 1$. Then :

$$a = g^k \bmod p$$
$$b = y^k M \bmod p$$

5. Here, $M = (ax + kb) \bmod (p - 1)$. Then the pair (a, b) becomes the cipher text. Note that it is double the size of the plain text. To decrypt (a, b) to

find out the plain text M, calculate $M = b/a^x \bmod p$.

Que 3.18. **What do you understand by Elgamal encryption system ? Explain its encryption and decryption ?**

AKTU 2017-18, Marks 10

Answer

1. In cryptography, the Elgamal encryption system is an asymmetric key encryption algorithm for public key cryptography which is based on the Diffie-Hellman key agreement.
2. Elgamal encryption is used in PGP (Pretty Good Privacy) and other cryptosystems. Elgamal encryption can be defined over any cyclic group G.
3. Its security depends upon the difficulty of a certain problem in G related to computing discrete logarithms.
4. Elgamal encryption consists of three components : The key generator, the encryption algorithm and the decryption algorithm.

Encryption : Anyone can send a message to user using his public key. The encryption process is shown in algorithm 1.

Algorithm 1 : Elgamal encryption

```
Elgamal_encryption ($e_1$, $e_2$, $p$ , $P$)            // $p$ is the prime number
{                                                      // $P$ is the plaintext
Select a random integer $r$ in the group $G = < Z_p^*, \times >$
$C_1 \leftarrow e_1^r \bmod p$
$C_2 \leftarrow (P \times e_2^r) \bmod p$                 // $C_1$ and $C_2$ are the ciphertexts
  return $C_1$ and $C_2$
}
```

Decryption : User can use algorithm 2 to decrypt the ciphertext message received.

Algorithm 2 : Elgamal decryption

```
Elgamal_decryption ($d, p, C_1 , C_2$) // $C_1$ and $C_2$ are the ciphertexts
{
 $P \leftarrow [C_2 (C_1^d)^{-1} \bmod p]$              // $P$ is the plaintext
                return $P$                   // $p$ is the prime number
```

Que 3.19. **Explain digital signature. Discuss signing & verifying process of Digital Signature Algorithm (DSA) in detail with suitable steps.**

AKTU 2017-18, Marks 10

Answer

Digital signature : Refer Q. 3.17, Page 3–16D, Unit-3.

Signing : Signing algorithm is use to produce signature by using messages private key.

1. Generate a random per-message value k where $0 < k < q$.

alculate $r = (g^k \bmod p) \bmod q$.

alculate $s = (k^{-1}(H(m) + x^*r)) \bmod q$.

here, p and q are prime numbers

and x are random number.

ecalculate the signature in the unlikely case that $r = 0$ or $s = 0$.

he signature is (r, s), where r and s are secret key.

erifying : Verifying algorithm is use to either accept or reject the essage claim to authenticity.

eject the signature if either $0 < r < q$ or $0 < s < q$ is not satisfied.

alculate $w = (s')^{-1} \bmod q$.

alculate $u1 = (H(m)\,;\,w) \bmod q$.

alculate $u2 = (r'w) \bmod q$.

alculate $v = ((g^{u1}y^{u2}) \bmod p) \bmod q$.

he signature is valid if $v = r'$

vhere $v = ((g^{(H(m')w) \bmod q}\ y^{r'w \bmod q)} \bmod p) \bmod q$

$H(m)$ = hash of m using SHA-1

M', r', s' = received versions of m, r, s.

3.20. What are the properties and requirements for a digital ature ?

wer

erties of digital signature :

It must be able to verify the author, the date and time of the signature.

It must be able to authenticate the contents of the message at the time of the signature.

There must be third (trusted) party who can verify the digital signature to resolve disputes between the sender and receiver.

uirements for a digital signature :

The signature must be in the form of a bit pattern and relative to the message being signed.

The signature must contain information that is unique to the sender, so that forgery and denial can be avoided.

The process of creating, recognizing and verifying the digital signature must also be comparatively easy.

A high computational effort must be required to forge a digital signature.

The copy of a digital signature must be retained in storage mechanism.

e 3.21. Explain the variants of digital signatures ?

Answer

Variants of digital signature are :

1. **Timestamped signature :**
   a. Timestamped digital signatures include a timestamp value in order to prevent replay attack.
   b. In a replay attack, the documents can be replayed by a third party.
2. **Blind signature :**
   a. Blind signature is used when the sender does not want to reveal the contents of the message to the signer and just wishes get the message signed by the signer.
   b. Blind signatures are used in situations where the signer message authors are completely different parties.
   c. Blind signatures scheme can be implemented by using a number of public-key digital signature schemes such as RSA and DSS.
3. **Undeniable digital signature :**
   a. This scheme is a non-self-authenticating signature scheme in which no signatures can be verified without the signer's cooperation and notification.
   b. This scheme has three components :
      i. **Signing algorithm :** This allows the signer to sign a message.
      ii. **Verification (or confirmation) protocol :** This allows the signer to limit the users who can verify his or her signature.
      iii. **Disavowal (or denial) protocol :** Since the verification process requires the involvement of the signer, it is quite possible that the signer can freely decline the request of the verifier. This protocol prevents the signer from proving that a signature is invalid when it is valid and vice versa.

Que 3.22. **Explain the proof of digital signature algorithm.**

Answer

To prove the algorithm, we have to show that $V_c = S_1$.

As we know that :

$$\begin{aligned} V_c &= [(e_1^y * e_2^z) \bmod p] \bmod q \\ &= [(e_1^{[h(M)w) \bmod q} * e_2(s_1W) \bmod q] \bmod p \bmod q \\ &= [(e_1^{[h(M)w] \bmod q} * e_1(dS_1w) \bmod q) \bmod p\ ] \bmod q \\ &= [(e_1^{[h(M) + ds_1]\, w \bmod q)} {}^{\bmod p}] \bmod p] \bmod q \\ &= [(e_1^{[h(M) + dS_1]k[1/h(M) + dS_1)] \bmod q)} \bmod p] \bmod q \end{aligned}$$

Using, $w = (S_2^{-1}) \bmod q$ and $S_2 = k[1/(h\,(M) + dS_1)] \bmod q)$

$$\begin{aligned} &= [(e_1^{k \bmod q}) \bmod p\ ] \bmod q \\ &= (e_1^k \bmod p) \bmod q\ = S_1 \end{aligned}$$

Hence, proved

where, e_1, e_2, p, q are public key of sender.

$S_{1,} S_2$ are digital signature.

$h(M)$ is hash of message M.

w, y and z are intermediate variable.

VERY IMPORTANT QUESTIONS

Following questions are very important. These questions may be asked in your SESSIONALS as well as UNIVERSITY EXAMINATION.

Q. 1. Why message authentication is required ? Discuss working of MAC with suitable block diagram. Also discuss HMAC & CMAC in detail.

Ans. Refer Q. 3.3.

Q. 2. What are the requirements of a Message Authentication Code (MAC) ? Discuss the logical structure, components and algorithmic steps of MD5 algorithm.

Ans. Refer Q. 3.4.

Q. 3. Differentiate between the following :

a. Hash code and Message Authentication Code (MAC)

b. Weak collision resistance and Strong collision resistance

Ans. Refer Q. 3.11.

Q. 4. What do you understand from hash functions ? Discuss the working of Secure Hash Algorithm (SHA) in message authentication.

Ans. Refer Q. 3.14.

Q. 5. Describe birthday attack against any hash function. Give the mathematical basis of the attack.

Ans. Refer Q. 3.12.

Q. 6. Write the Digital Signature Algorithm (DSA) of Digital Signature Standard. What is the implication if same K (secret per message) is used to sign two different message using DSA ?

Ans. Refer Q. 3.16.

Q. 7. What do you understand by Elgamal encryption system ? Explain its encryption and decryption ?

Ans. Refer Q. 3.18.

☺☺☺

4

UNIT

Key Management and Distribution

CONTENTS

PART-1

Key Management and Distribution : Symmetric Key Distribution Diffie-Hellman Key Exchange, Public Key Distribution.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

)ue 4.1. What is key management ? Also explain the functions of ey management.

nswer

Key management refers to the collection of processes used for the generation, storage, installation, transcription, recording, change, disposition, and control of keys that are used in cryptography.

It is essential for secure ongoing operation of any cryptosystem.

The various functions of key management are :

a. **Generation :** This process involves the selection of a key that is used for encrypting and decrypting the messages.

b. **Distribution :** This process involves all the efforts made in carrying the key from the point where it is generated to the point where it is to be used.

c. **Installation :** This process involves getting the key into the storage of the device or the process that needs to use this key.

d. **Storage :** This process involves maintaining the confidentiality of stored or installed keys while preserving the integrity of the storage mechanism.

e. **Change :** This process involves ending with the use of the key and starting with the use of another key.

f. **Control :** This process refers to the ability to implement a directing or restraining influence over the content and use of the key.

ıe 4.2. Differentiate between symmetric and asymmetric key ptography.

Answer

S. No.	Symmetric-key cryptography	Asymmetric-key cryptography
1.	It uses a single key for both encryption and decryption of data.	It uses two different keys—public key for encryption and private key for decryption.
2.	Both the communicating parties share the same algorithm and the key.	Both the communicating parties should have atleast one of the matched pair of keys.
3.	The processes of encryption and decryption are very fast.	The encryption and decryption processes are slower as compared to symmetric-key cryptography.
4.	Key distribution is a big problem.	Key distribution is not a problem.
5.	The size of encrypted text is same or less than the original text.	The size of encrypted text is more than the size of the original text.

Que 4.3. **Describe Diffie-Hellman key exchange algorithm. Users *A* and *B* use the Diffie-Hellman key exchange technique a common prime $q = 83$ and a primitive root $\alpha = 13$.**

i. If user A has private key 5 what is *A*'s public key ?

ii. If user *B* has private key 12, what is *B*'s public key ?

iii. What is the shared key ?

AKTU 2014-15, Marks 10

OR

Explain Diffie-Hellman key exchange.

AKTU 2016-17, Marks 10

OR

What is Diffie-Hellman key exchange in key management ?

AKTU 2018-19, Marks 10

Answer

Diffie-Hellman key exchange algorithm :

1. Diffie-Hellman key exchange (D-H) is a specific method of exchanging keys implemented within the field of cryptography.

2. The Diffie-Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel.
3. This key can then be used to encrypt subsequent communications using a symmetric key cipher.
4. The symmetric (shared) key in the Diffie-Hellman protocol is $K = G^{xy} \bmod N$.
5. The steps used in Diffie-Hellman key exchange are as follows :
   a. Sender chooses a large random number x such that $0 \le x \le N - 1$ and calculates $R_1 = G^x \bmod N$.
   b. Receiver chooses another large random number y such that $0 \le y \le N - 1$ and calculates $R_2 = G^y \bmod N$.
   c. Sender sends R_1 to receiver. Note that sender does not send the value of x; he sends only R_1.
   d. Receiver sends R_2 to sender. Again, note that receiver does not send the value of y, he sends only R_2.
   e. Sender calculates $K = (R_2)^x \bmod N$.
   f. Receiver also calculates $K = (R_1)^y \bmod N$.
6. K is the symmetric key for the session.
7. Receiver has calculated $K = (R_1)^y \bmod N = (G^x \bmod N)^y \bmod N = G^{xy} \bmod N$. Sender has calculated $K = (R_2)^x \bmod N = (G^y \bmod N)^x \bmod N = G^{xy} \bmod N$.
8. Both have reached the same value without receiver knowing the value of x and without sender knowing the value of y as shown in Fig. 4.3.1.

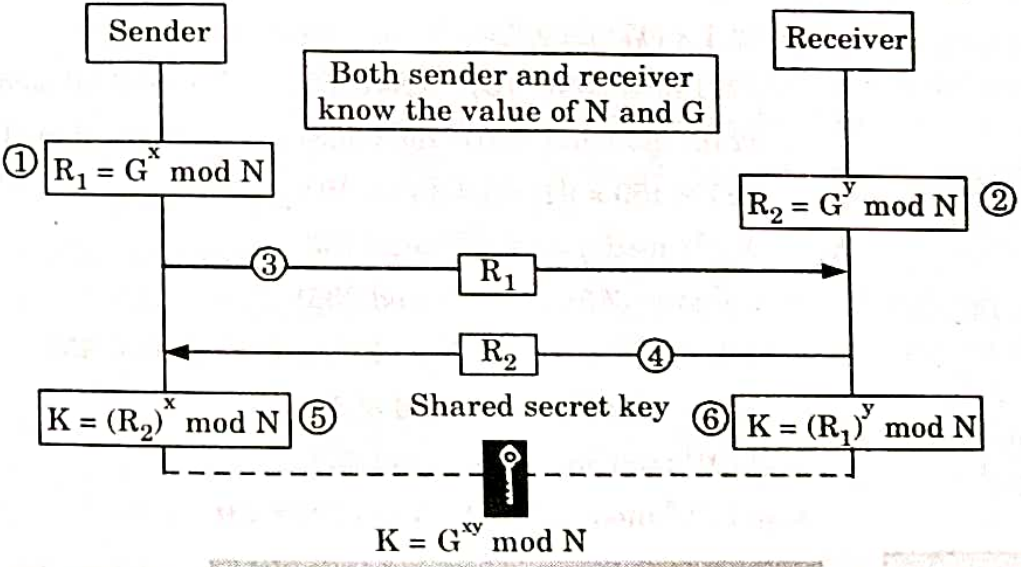


Fig. 4.3.1. Diffie-Hellman key exchange.

Numerical : Given : Common prime $q = 83$,
Primitive root $\alpha = 13$

i. $Y_A = 13^5 \bmod 83 = 34$
ii. $Y_B = 13^{12} \bmod 83 = 65$
iii. $K = 65^5 \bmod 83 = 10$

Que 4.4. **Discuss Diffie Hellman key exchange method. Let $q = 353, \alpha = 3, X_A = 97$ and $X_B = 233$. Then compute Y_A, Y_B, K_A & K_B using Diffie-Hellman.**

AKTU 2017-18, Marks 10

Answer

Diffie-Hellman key exchange : Refer Q. 4.3, Page 4–3D, Unit-4.

Numerical :

$$q = 353 \qquad \alpha = 3$$

$$X_A = 97 \qquad X_B = 233$$

Secret key

$$Y_A = 3^{97} \bmod 353$$
$$= [(3^{20} \bmod 353)^4 \times 3^{17} \bmod 353] \bmod 353$$
$$= (73 \times 73 \times 73 \times 73 \times 55) \bmod 353 = 40$$
$$Y_B = 3^{233} \bmod 353 = (3^{20} \bmod 353)\,(3^{213} \bmod 353)$$
$$= [73 \times 3^{212}\,(3^{20} \bmod 353)^{10} \times 3^{13} \bmod 353)]$$
$$= [(73^{11} \bmod 353) \times 175 \times 73] \bmod 353$$
$$= [((21)^2 \bmod 353 \times 73) \times 175 \times 73] \bmod 353$$
$$= (88 \times 175 \times 73) \bmod 353 = 47$$

Now, we calculate symmetric key

$$K_A = (Y_B)^{X_A} \bmod q = (47)^{97} \bmod 353 = 201 \times (47^{92} \bmod 353)$$
$$= [201 \times (47^5 \bmod 353)^{18} \times 47^2 \bmod 353] \bmod 353$$
$$= [(201 \bmod 353)^{16}\,(201^2 \bmod 353) \times 47^2 \bmod 353] \bmod 353$$
$$= [(218^4 \bmod 353)\,(201^2 \bmod 353)\,(47^2 \bmod 353)] \bmod 353$$
$$= (217 \times 159 \times 91) \bmod 353 = 191$$
$$K_B = (Y_A)^{X_B} \bmod q = (40)^{233} \bmod 353$$
$$= (40^7 \bmod 353) \times (40^{226} \bmod 353)$$
$$= [119 \times (40^7 \bmod 353)^{32} \times (40^2 \bmod 353)] \bmod 353$$
$$= [119 \times (119)^{32} \times 188] \bmod 353$$
$$= [119^{33} \bmod 353 \times 188] \bmod 953$$
$$= [((119)^6 \bmod 353) \times 188] \bmod 353 = 0$$

Que 4.5. **In the Diffie-Hellman key exchange algorithm, let the prime number be 353 and one of its primitive root be 3. Let the users *A* and *B* select their secret keys $X_A = 97$ and $X_B = 235$. Compute :**

i. The public keys of A and B

ii. The common secret key

Answer

Given :

$$p = 353$$
$$q = 3$$
$$X_A = 97$$
$$X_B = 233$$

i. Public key of *A*

$$Y_A = q^{X_A} \bmod p$$
$$\Rightarrow 3^{97} \bmod 353$$
$$\Rightarrow 40$$

Public key of *B*

$$Y_B = q^{X_B} \bmod p$$
$$\Rightarrow 3^{233} \bmod 353$$
$$\Rightarrow 248$$

ii. Common secret key

$$K = (Y_B)^{X_A} \bmod 353$$
$$\Rightarrow (248)^{97} \bmod 353$$
$$\Rightarrow 160$$

Que 4.6. **Describe various schemes used for public key distribution.**

Answer

Schemes used for the distribution of public keys are as follows :

1. **Public announcement :**
   a. The main focus of public-key encryption is that the public key should be public; that is, a user can send his or her public key to any other user of broadcast it to a large community.
   b. The main problem is that of forgery. That is, anyone can forge the key while it is being transmitted.
2. **Public directory :**
   a. Public directory is a dynamic directory the name and public key entry for each user is maintained and distributed by some trusted authority.
   b. This approach assumes that the public key of the authority is known to everyone, however the corresponding private key is known only to the authority.
   c. Each user has to register his or her public key with the directory authority.
   d. The user can replace its existing key with a new one as per his or her choice.

3. **Public-key authority :**

a. In public directory scheme, if the private key of the authority is stolen, then it may result in loss of data.

b. Thus, to achieve stronger security for public-key distribution, a tighter control needs to be provided over the distribution of public keys from the directory.

c. It this case, a central authority maintains the dynamic directory of the public keys of all the users. The user knows only the public key of the authority, while the corresponding private key is secret to the authority.

PART-2

X.509 Certificates, Public Key Infrastructure, Authentication Applications : Kerberos.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 4.7. **What is digital certificate ? Give the format of X.509 certificate showing the important elements of the certificate. How is an X.509 certificate revoked ?**

AKTU 2014-15, Marks 10

OR

Discuss X.509 digital certificate format. What is its significance in cryptography ?

AKTU 2017-18, Marks 10

OR

Explain X.509 in detail.

AKTU 2016-17, Marks 10

Answer

Digital certificates :

1. A digital certificate is a digital file that certifies the identity of an individual or even a router seeking access to computer-based information.

2. It is issued by a Certification Authority (CA) and serves the same purpose as a driver's license or a passport.

Format of X.509 certificate :

The general format of a X.509 digital certificate is shown in Fig. 4.7.1.

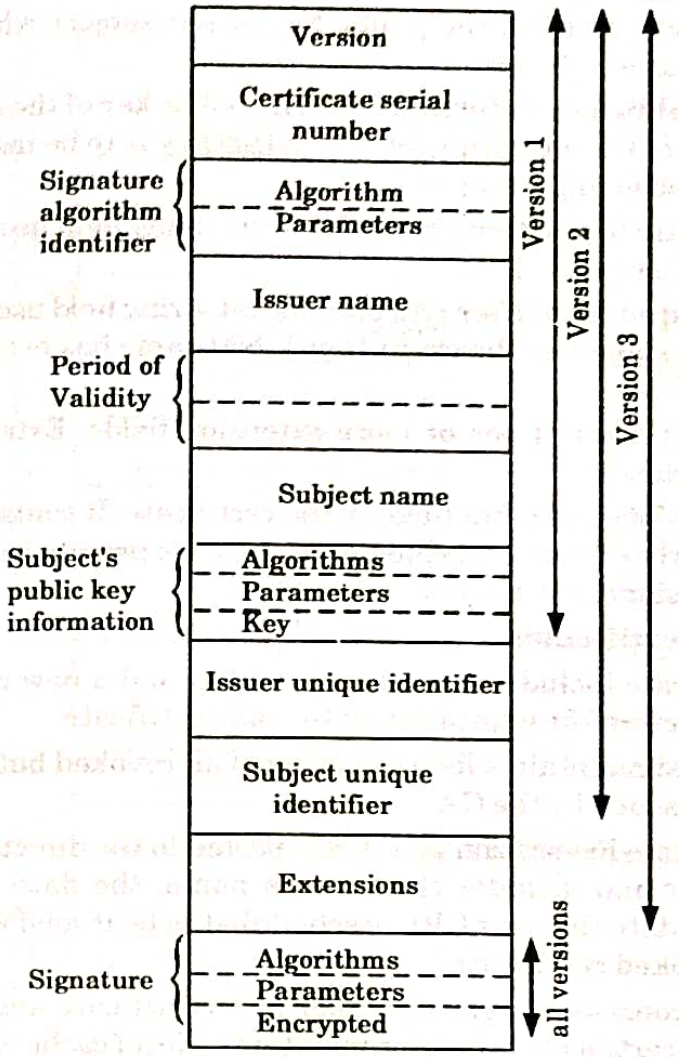


Fig. 4.7.1. X.509 format.

1. **Version :** Differentiates among successive versions of the certificate format; the default is version 1. If the Issuer Unique Identifier or Subject Unique Identifier are present, then the value must be version 2. If one or more extensions are present, the version must be version 3.

2. **Serial number :** It is a unique integer value within the issuing CA (Certification Authority), that is unambiguously associated with this certificate.

3. **Signature algorithm identifier :** This algorithm is used to sign the certificates together with any associated parameters.

4. **Issuer name :** X.500 name of the CA that created and signed the certificate.

5. **Period of validity :** Consist of two dates : the first and last on which the certificate is valid.

6. **Subject name :** The name of the user to whom this certificate refers. This certificate certifies the public key of the subject who holds the corresponding private key.
7. **Subject's public key information :** The public key of the subject, plus an identifier of the algorithm for which this key is to be used, together with any associated parameters.
8. **Issuer unique identifier :** An optional bit string field used to identify uniquely the issuing CA.
9. **Subject unique identifier :** An optional bit string field used to identify uniquely the subject in the event that X.500 name has been reused for different entities.
10. **Extensions :** A set of one or more extension fields. Extensions were added in version 3.
11. **Signature :** Cover all other fields of the certificate. It contains the hash code of the other fields encrypted with the CA's private key. This field includes the signature algorithm identifier.

Revocation of certificates :

1. Each certificate includes a period of validity and a new certificate is issued just before the expiration of the old certificate.
2. Each CA must maintain a list consisting of all revoked but not expired certificates issued by the CA.
3. Each Certificate Revocation List (CRL) posted to the directory is signed by the issuer and includes the issuer's name, the date the list was created, the date the next CRL is scheduled to be issued and an entry for each revoked certificate.
4. Each entry consists of serial number of a certificate and revocation date for that certificate. The user maintains a local cache of certificates and lists or revoked certificates.

Significance of digital certificate in cryptography :

1. It is used to verify the authenticity of sender.
2. It ensures the important variable of trust and integrity.
3. It helps to encrypt sensitive information.

Que 4.8. **Discuss public key infrastructure.**

Answer

1. A PKI (Public Key Infrastructure) is a set of hardware, software, people, policies and procedures needed to create, manage, store, distribute and revoke PKCs based on public-key cryptography.
2. The principle objective for developing PKI is to enable secure, convenient, and efficient acquisition of public keys.
3. Fig. 4.8.1 shows the interrelationship among the key elements of the PKI model.

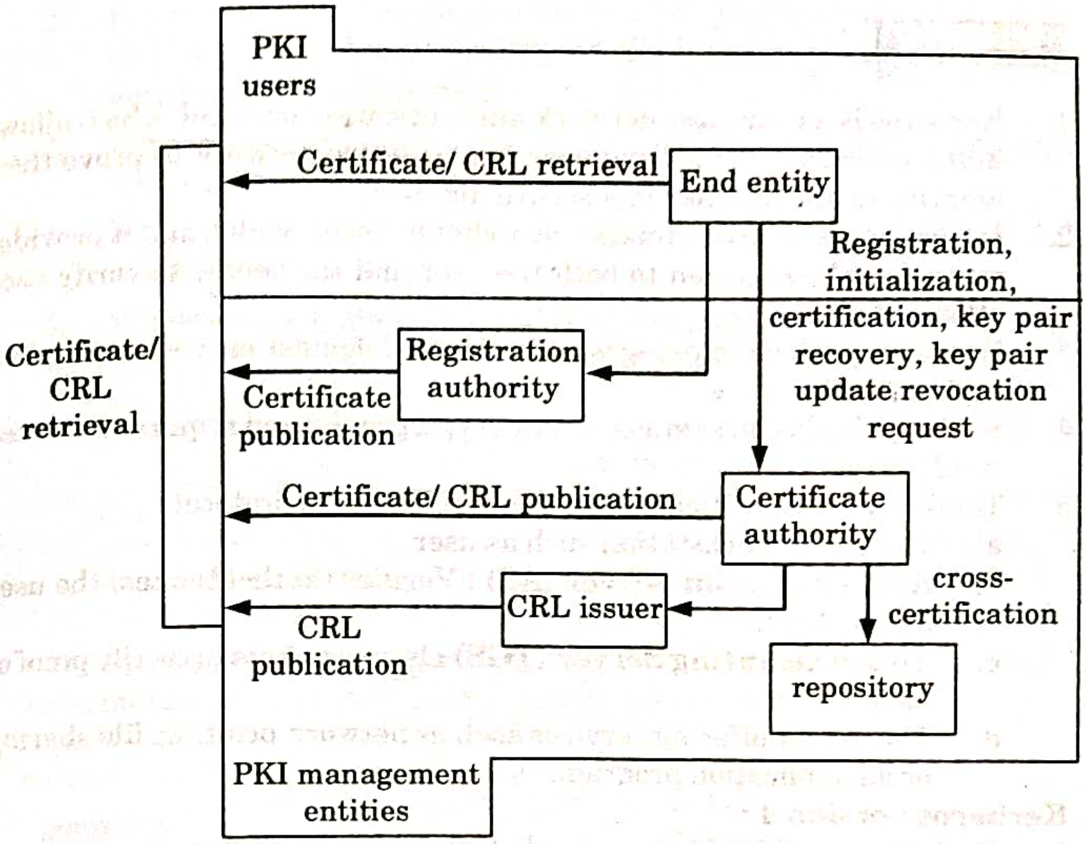

PKI users
Certificate/ CRL retrieval
End entity
Registration, initialization, certification, key pair recovery, key pair update revocation request
Certificate/ CRL retrieval
Registration authority
Certificate publication
Certificate/ CRL publication
Certificate authority
cross-certification
CRL issuer
CRL publication
repository
PKI management entities

Fig. 4.8.1. PKI architectural model.

These elements are :

a. **End entity :** It is used to validate digital signatures their certification path from a known public key of a trusted CA.

b. **Certificate Authority (CA) :** It is used to issue and revoke public-key cryptography.

c. **Registration Authority (RA) :** It is used to validate the binding between public keys and certificate holder identities.

d. **CRL issuer :** An optional component that a CA can delegate to publish CRLs.

e. **Repository :** It is used to store and make available certificates and Certificate Revocation Lists (CRLs).

PKI management functions : PKI identifies a number of management functions that potentially need to be supported by management protocols :

1. Registration
2. Initialization
3. Certification
4. Key-pair recovery
5. Key pair update
6. Revocation request
7. Cross certification

Que 4.9. **What is Kerberos ? Discuss Kerberos version 4 in detail.**

AKTU 2015-16, Marks 10

AKTU 2017-18, Marks 10

Answer

1. Kerberos is a computer network authentication protocol, which allows individuals communicating over a non-secure network to prove their identity to one another in a secure manner.
2. Its designers aimed primarily at a client-server model, and it provides mutual authentication to both the user and the server to verify each other's identity.
3. Kerberos protocol messages are protected against eavesdropping and replay attacks.
4. Kerberos builds on symmetric key cryptography and requires a trusted third party.
5. There are four entities involved in the Kerberos protocol :
   a. The client workstation such as user.
   b. **Authentication Server (AS) :** Verifies (authenticates) the user during login.
   c. **Ticket Granting Server (TGS) :** Issues tickets to certify proof of identity.
   d. The server offering services such as network printing, file sharing or an application program.

Kerberos version 4 :

1. Kerberos version 4 is the extended version of Kerberos.
2. It uses DES encryption to authenticate a user when logging into the system.
3. This version contains four entities :
   a. **Client (C) :** An entity which wants to make use of any service hosted on a server.
   b. **Server (S) :** An entity which hosts different services which client request for.
   c. **Authentication Server (AS) :** Authentication server knows the password of all user and stores them in a centralized database.
   d. **Ticket :** Ticket allows client to communicate over a non-secure network to prove their identity to one another in a secure manner.

Que 4.10. **Explain the full-service Kerberos environment ? What are the principle differences between version 4 and version 5 of Kerberos ?**

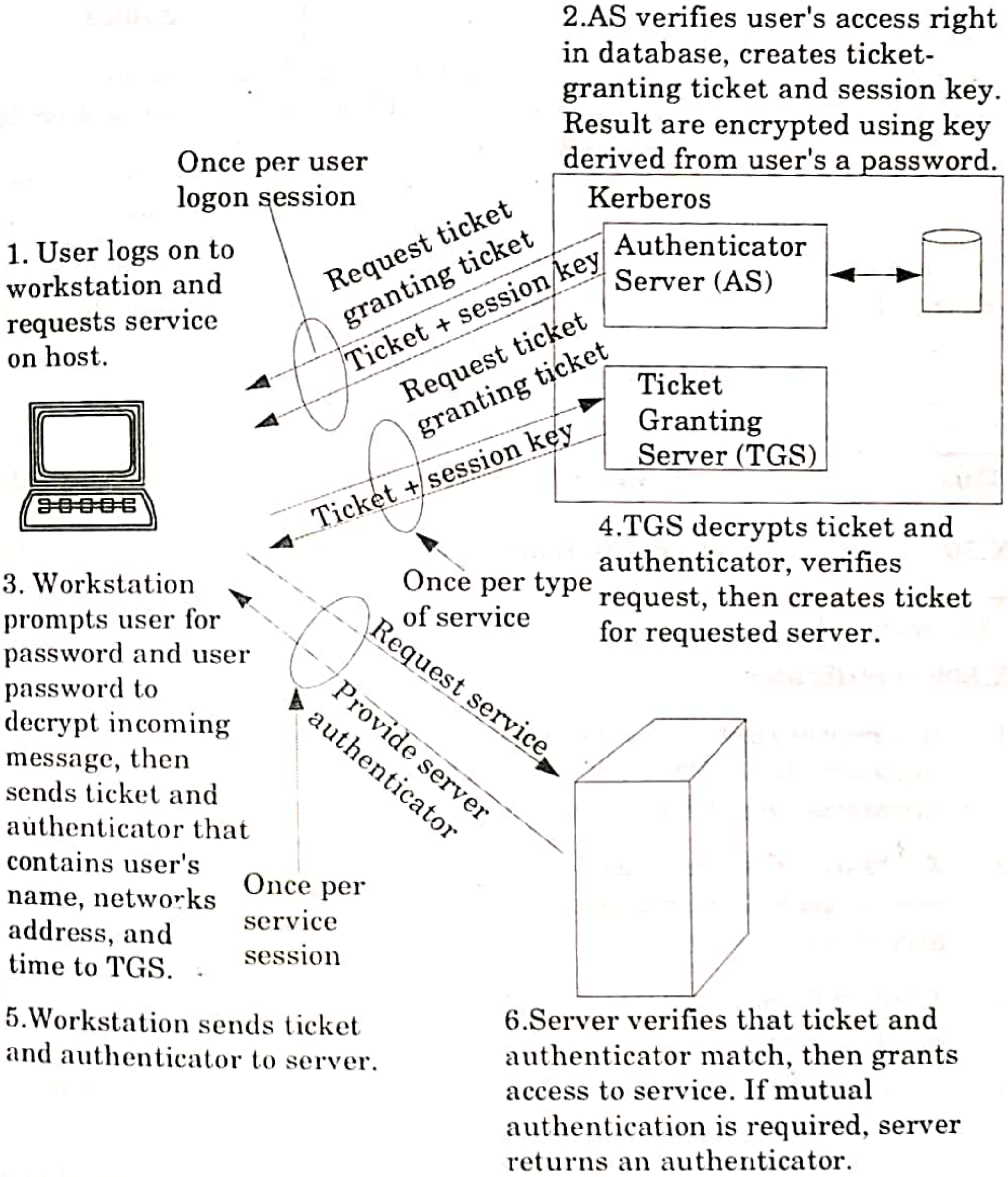
AKTU 2014-15, Marks 10

Answer

Full-service Kerberos environment :

1. Kerberos is a computer network authentication protocol, which allows individuals communicating over a non-secure network to prove their identity to one another in a secure manner.

2. Its designers aimed primarily at a client-server model, and it provides mutual authentication – both the user and the server verify each other's identity.
3. Kerberos protocol messages are protected against eavesdropping and replay attacks.
4. Kerberos builds on symmetric key cryptography and requires a trusted third party.
5. Windows 2000, Mac OS X and Red Hat Linux 4 use Kerberos.



2.AS verifies user's access right in database, creates ticket-granting ticket and session key. Result are encrypted using key derived from user's a password.

1. User logs on to workstation and requests service on host.

3. Workstation prompts user for password and user password to decrypt incoming message, then sends ticket and authenticator that contains user's name, networks address, and time to TGS.

4.TGS decrypts ticket and authenticator, verifies request, then creates ticket for requested server.

5.Workstation sends ticket and authenticator to server.

6.Server verifies that ticket and authenticator match, then grants access to service. If mutual authentication is required, server returns an authenticator.

Once per user logon session
Kerberos
Authenticator Server (AS)
Request ticket granting ticket
Ticket + session key
Request ticket granting ticket
Ticket Granting Server (TGS)
Ticket + session key
Once per type of service
Request service
Provide server authenticator
Once per service session

Fig. 4.10.1. Overview of kerberos.

Difference :

Parameters	Kerberos Versions 4	Kerberos Versio
Encryption algorithm used	DES only	DES and ot encryptions
Ticket lifetime	5 min units, Maximum = 1280 minutes	Start and end tim arbitrary
Message byte ordering	Tagged message with ordering	Abstract syn notation on ba encoding rules.
Password attack	Initial request is clear and use it for offline attack.	Need to send pre-authentication d
Two times encryption	Supported	Not supported
Session keys Hierarchy of realms	Replay risk using repeated ticket limits to pairs	Sub session key or only transition allow

Que 4.11. **Discuss X.509 certificates in detail. What is the rol X.509 certificates in cryptography ?** **AKTU 2018-19, Marks**

Answer

X.509 certificates :

1. In cryptography, X.509 is an ITU-T standard for a Public K Infrastructure (PKI) for single sign-on and Privilege Managem Infrastructure (PMI).
2. X.509 specifies, standard formats for public key certificates, certific revocation lists, attribute certificates and a certification path validati algorithm.
3. X.509 defines a framework for the provision of authentication servic by the X.500 directory to its user.
4. X.509 certificates is based on the use of public key cryptography ar digital signatures.
5. The standard does not dictate the use of a specific algorithm bu recommends RSA.

6. X.509 certificates format is used in S/MIME, IP security and SET.

Role of X.509 certificates in cryptography :

1. To verify that a public key belong to the user, computer or service identify contained within the certificate.
2. To validate the identity of encrypted data.

PART-3

Electronic Mail Security : Pretty good Privacy (PGP), S/MIME.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 4.12. **What is electronic mail security ? Provide the application of Pretty Good Privacy (PGP) in transaction authentication.** **AKTU 2018-19, Marks 10**

Answer

Electronic mail (email) security :

1. Email security refers to the collective measures used to secure the access and content of an email account or service.
2. It allows an individual or organization to protect the overall access to one or more email addresses/accounts.
3. Email security is a term that encompasses multiple techniques used to secure an email service.
4. It also implements firewall and software-based spam filtering applications to restrict unsolicited, untrustworthy and malicious email messages from delivery to a user's inbox.
5. SSL, TLS refers to the standard protocol used to secure email transmission.
6. Transport Layer Security (TLS), provide a way to encrypt a communication channel between two computers over the internet.

Application of PGP :

1. PGP provides secure encryption of documents and data files that even advanced super computers are not able to "crack".

2. For authentication, PGP employs the RSA public-key encryption scheme and the MD5, a one-way hash function to form a digital signature that assures the receiver that an incoming messages is authentic (that it comes from the alleged send and that it has not been altered).

Que 4.13. **How E-mail security is achieved ? Discuss S/MIME with suitable steps and block diagram.**

AKTU 2017-18, Marks 10

OR

Explain PGP and S/MIME.

AKTU 2016-17, Marks 10

Answer

PGP helps to achieve E-mail security.

PGP :

1. PGP (Pretty Good Privacy) is an encryption algorithm that provides cryptographic privacy and authentication for data communication.
2. PGP uses a combination of public-key and conventional encryption to provide security services for electronic mail message and data files.
3. PGP provides five services related to the format of messages and data files : authentication, confidentiality, compression, e-mail compatibility and segmentation.

S/MIME :

1. A secure version of MIME, S/MIME (Secure/Multipurpose Internet Mail Extensions), is used to support encryption of email messages.
2. It is based on the MIME standard and provides the security services for electronic messaging applications : authentication, message integrity and data security.
3. S/MIME uses public key cryptography to sign and encrypt E-mail.
4. Every participant has two keys :
   a. A private key, which is kept secret
   b. A public key, which is available to everyone
5. The following steps are taken in order to create a signed message :
   a. The user writes the message as clear-text.
   b. The message digest is being calculated using SHA-1 or MD5.

c. The message digest is being encrypted using the signer's private key (DSS or RSA).

ncrypted message :

- An encrypted message is sent by *A* to *B* and can only be read by *B*.
- This is ensured by encrypting the message using *B*'s public key, which is available to everyone.
- However, only *B* can decrypt the message, because only he owns his private key.

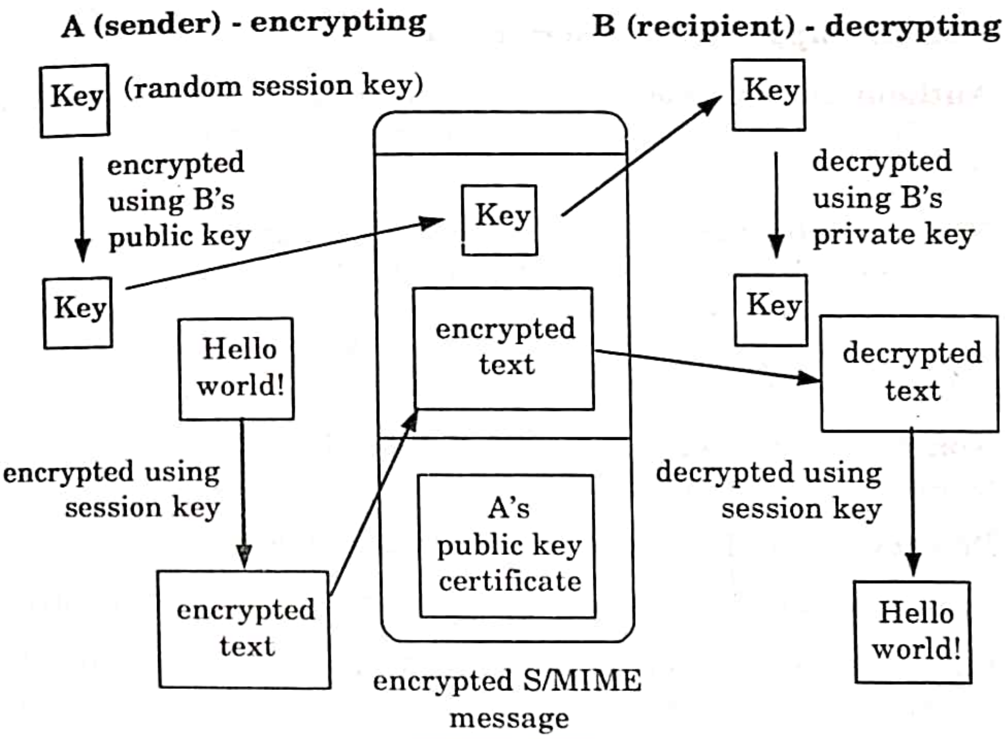

A (sender) - encrypting
B (recipient) - decrypting
Key
(random session key)
encrypted using B's public key
Key
Hello world!
encrypted using session key
encrypted text
Key
encrypted text
A's public key certificate
encrypted S/MIME message
Key
decrypted using B's private key
Key
decrypted text
decrypted using session key
Hello world!

Fig. 4.13.1.

4. To enhance the performance, S/MIME implementation is done as :
   a. The message is not encrypted using *B*'s public key but encrypted using a randomly created symmetric session key.
   b. The temporary session key is being encrypted using *B*'s public key. Therefore, only *B* can retrieve the session key and thus decrypt the original message.

Que 4.14. **Enlist various services supported by S/MIME. Explain how S/MIME supports these services. What is the purpose of content type field in MIME header ?**

AKTU 2014-15, Marks 10

Answer

S/MIME provides the following cryptographic security services :

1. Authentication
2. Message integrity
3. Non-repudiation of origin (using digital signatures)
4. Privacy
5. Data security (using encryption)

S/MIME supports these services as :

1. **Authentication :** For authentication, S/MIME uses a hierarchical certificate authorization model and use certificates based on X.509 standard.
2. **Message integrity :** To supports message integrity S/MIME encrypts the message by using a symmetric cipher, whose key is protected using the recipient's public key. Since a message encrypted in this way can only be decrypted with the recipient's private key, it cannot be read by anyone other than the intended recipient.
3. **Non-repudiation of origin :** S/MIME uses digital signature to ensure non-repudiation of origin.
4. **Privacy :** S/MIME uses encryption to ensure privacy.
5. **Data security :** S/MIME uses encryption to ensure data security.

Purpose of content-type field in MIME header : The purpose of the content-type field is to describe the data contained in the body so that the receiving user can pick an appropriate mechanism to present the data to the user, or otherwise deal with the data in an appropriate manner.

Que 4.15. Discuss the steps that are followed for the transmission and reception of PGP messages.

Answer

The PGP messages are transmitted from the sender to receiver using following steps :

1. If signature is required, the hash code of the uncompressed plaintext message is created and encrypted using the sender's private key.

2. The plaintext message and the signature are compressed using the ZIP compression algorithm.
3. The compressed plaintext message and compressed signature are encrypted with a randomly generated session key to provide confidentiality. The session key is then encrypted with the recipient's public key and is added to the beginning of the message.
4. The entire block is converted to radix-64 format.

On receiving the PGP message, the receiver follows the following steps :

1. The entire block is first converted back to binary format.
2. The recipient recovers the session key using his or her private key, and then decrypts the message with the session key.
3. The decrypted message is then decompressed.
4. If the message is signed, the receiver needs to verify the signature. For this, he or she computes a new hash code and compares it with the received hash code. If they match, the message is accepted; otherwise, it is rejected.

Que 4.16. **Discuss the functionality of S/MIME.**

Answer

The basic functionality of S/MIME are :

1. **Enveloped data :** S/MIME supports enveloped data, which consists of the message containing any type of contents in encrypted form and the encryption key encrypted with receiver's public key.
2. **Signed data :** This consists of the message digest encrypted using the sender's private key. This signed message can only be viewed by the receivers who have S/MIME capability.
3. **Clear-signed data :** This functionality is similar to the signed data that allows the receivers to view the contents of the message even if they do not have S/MIME capability. However, they cannot verify the signature.
4. **Signed and enveloped data :** In this, S/MIME allows nesting of signed-only and encrypted-only entities, so that the encrypted data can be signed, and signed or clear-signed data can be encrypted.

Q. 1. Explain Diffie-Hellman key exchange.

Ans. Refer Q. 4.3.

Q. 2. Discuss Diffie Hellman key exchange method. Le $q = 353, \alpha = 3, X_A = 97$ and $X_B = 233$. Then compute Y_A, Y_B, K_A & K_B using Diffie Hellman.

Ans. Refer Q. 4.4.

Q. 3. What is digital certificate ? Give the format of X.509 certificate showing the important elements of the certificate. How is an X.509 certificate revoked ?

Ans. Refer Q. 4.7.

Q. 4. What is Kerberos ? Discuss Kerberos version 4 in detail.

Ans. Refer Q. 4.9.

Q. 5. Explain the full-service Kerberos environment ? What are the principle differences between version 4 and version 5 of Kerberos ?

Ans. Refer Q. 4.10.

Q. 6. How E-mail security is achieved ? Discuss S/MIME with suitable steps and block diagram.

Ans. Refer Q. 4.13.

Q. 7. What is electronic mail security ? Provide the application of Pretty Good Privacy (PGP) in transaction authentication.

Ans. Refer Q. 4.12.

5

UNIT

IP Security

CONTENTS

PART-1

IP Security : Architecture, Authentication Header, Encapsulating Security Payloads, Combining Security Association, Key Management.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 5.1. **Explain internet protocol security in detail.**

AKTU 2018-19, Marks 10

Answer

1. IP Security (IPSec) is a collection of protocols designed by the Internet Engineering Task Force (IETF) to provide security for a packet at the network layer.
2. IPSec is a capability that can be added to either version of the Internet Protocol (IPv4 or IPv6), by means of additional headers.
3. IPSec encompasses three functional areas : authentication, confidentiality, and key management.
   a. The authentication mechanism assures that a received packet was transmitted by the party identified as the source in the packet header.
   b. The confidentiality facility enables communicating nodes to encrypt messages to prevent eavesdropping by third party.
   c. The key management facility is concerned with the secure exchange of keys.
4. IPSec has two modes of operation :
   a. **Transport mode :** It is the default mode of IPSec which provide end-to-end security. It can secure communication between a client and a server.
   b. **Tunnel mode :** Tunnel mode is used between two routers, between a host and a router, or between a router and a host. It is used when either the sender or the receiver is not a host.
5. IPSec uses two protocols for message security :
   a. **Authentication Header (AH) :** Covers the packet format and general issues related to the use of AH for packet authentication.

b. **Encapsulating Security Payload (ESP) :** Covers the packet format and general issues related to the use of the ESP for packet encryption and, optionally, authentication.

Que 5.2. **Write a short note on the applications of IP security.**

Answer

Applications of IPSec are :

1. **Secure remote Internet access :** Using IPSec, we can make a local call to our Internet Service Provider (ISP) so as to connect to our organization's network in a secure manner from our home or hotel.
2. **Secure branch office connectivity :** Rather than subscribing to an expensive borrow line for connecting its branches across cities/countries an organization can set up an IPSec-enabled network to securely connect all its branches over the Internet.
3. **Set up communication with other organizations :** IPSec allows connectivity between various branches of an organization, and it can also be used to connect the networks of different organizations together in a secure and inexpensive fashion.

Que 5.3. **What are the advantages of IPSec ?**

Answer

Advantages of IPSec are :

1. IPSec is transparent to the end users. There is no need for user training, key revocation.
2. When IPSec is configured to work with a firewall, it becomes the only entry-exit point for all traffic making it extra secure.
3. IPSec works at the network layer. Hence, no changes are needed to the upper layers *i.e.*, application and transport.
4. When IPSec is implemented in a firewall or a router, all the outgoing and incoming traffic gets protected. However, the internal traffic does not have to use IPSec. Thus, it does not add any overheads for the internal traffic.
5. IPSec can allow traveling staff to have secure access to the corporate network.
6. IPSec allows interconnectivity between branches/offices in a very inexpensive manner.

Que 5.4. **Explain the ESP format. What is anti-replay service ?**

AKTU 2016-17, Marks 10

Answer

Encapsulating Security Payload : The encapsulating security payload provides confidentiality services, including confidentiality of message contents and limited traffic flow confidentiality.

ESP format :

Fig. 5.4.1 shows the format of an ESP packet. It contains the following fields :

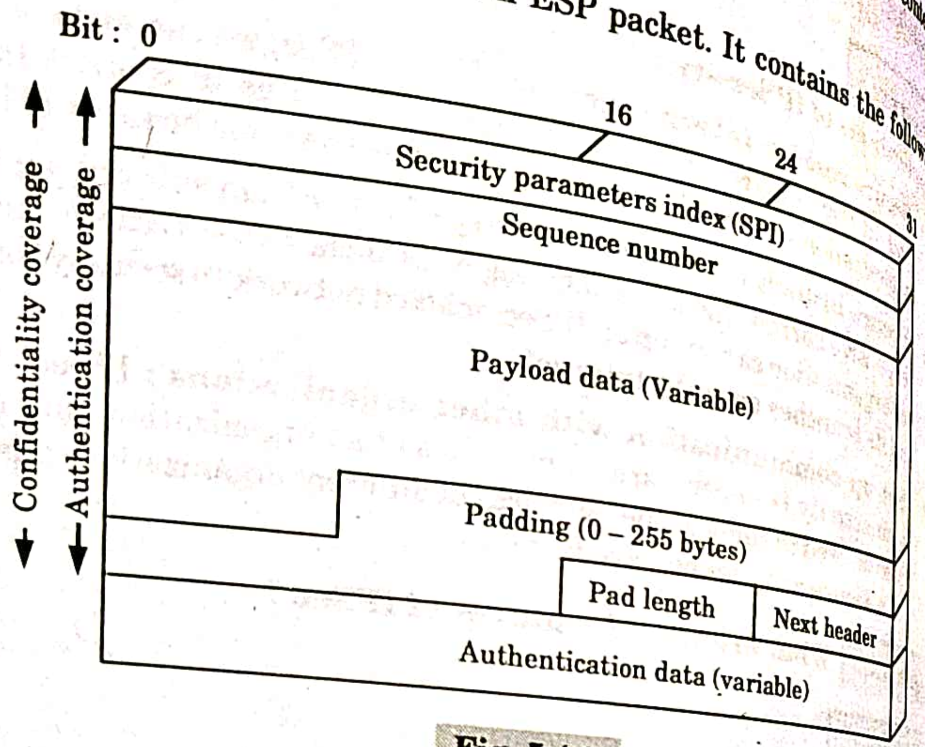


Fig. 5.4.1.

1. **Security parameters index (32 bits) :** Identifies a security association.
2. **Sequence number (32 bits) :** A monotonically increasing counter value, this provides an anti-replay function.
3. **Payload data (variable) :** This is a transport-level segment (transport mode) or IP packet (tunnel mode) that is protected by encryption.
4. **Padding (0-255 bytes) :** Padding field is used to expand the plaintext to the required length.
5. **Pad length (8 bits) :** Indicates the number of pad bytes immediately preceding this field.
6. **Next header (8 bits) :** Identifies the type of data contained in the payload data field by identifying the first header in that payload.
7. **Authentication data (variable) :** A variable-length field that contains the integrity check value computed over the ESP packet minus the authentication data field.

Anti-replay service :

1. A replay attack is one in which an attacker obtains a copy of an authenticated packet and later transmits it to the intended destination.

2. The receipt of duplicate, authenticated IP packets may disrupt service in some way or may have some other undesired consequence. The sequence number field is designed to thwart such attacks.

Que 5.5. **Describe briefly operations of ESP transport and ESP tunnel mode.**

Answer

The operation of the ESP transport mode :

1. At the sender's end, the block of data containing the ESP trailer and the entire transport layer segment is encrypted and the plain text of this block is replaced with its corresponding cipher text to form the IP packet. Authentication is appended, if selected. This packet is now ready for transmission.
2. The packet is routed to the destination. The intermediate routers need to take a look at the IP header as well as any IP extension headers, but not at the cipher text.
3. At the receiver's end, the IP header and any plain text IP extension headers are examined. The remaining portion of the packet is then decrypted to retrieve the original plain text transport layer segment.

The operation of the ESP tunnel mode :

1. At the sender's end, the sender prepares an inner IP packet with the destination address as the internal destination. This packet is pre-fixed with an ESP header and then the packet and ESP trailer are encrypted and authentication data is added. A new IP header is added to the start of this block. This forms the outer IP packet.
2. The outer packet is routed to the destination firewall. Each intermediate router needs to check and process the outer IP header, along with any other outer IP extension headers.
3. At the receiver's end, the destination firewall processes the outer IP header plus any extension headers and recovers the plain text from the cipher text. The packet is then sent to the actual destination host.

Que 5.6. **Explain the header format for an ISAKMP message.**

Answer

1. Internet Security Association and Key Management Protocol (ISAKMP) is designed to carry messages for Internet key exchange in IPSec.
2. It defines procedures and formats for establishing, maintaining and deleting information regarding security associations.
3. An ISAKMP message consists of an ISAKMP header followed by one or more payloads.
4. This entire block is encapsulated inside a transport segment.

5. The header format for an ISAKMP message shown in Fig. 5.6.1 consists of the following fields :

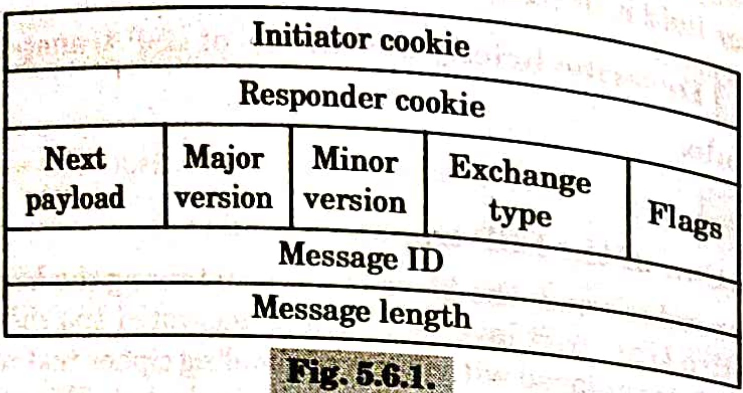


Fig. 5.6.1.

a. **Initiator cookie :** This is a 64-bit field defining the cookie of the entity that initiates the SA establishment, notification or deletion.

b. **Responder cookie :** This is a 64-bit field defining the cookie of the entity responding to the initiator. This field contains the value 0 in the first message sent by the initiator.

c. **Next payload :** This is an 8-bit field indicating the type of the first payload of the message.

d. **Major version :** This is a 4-bit field indicating the major ISAKMP version as used in the current exchange. The current value of this field is 1.

e. **Minor version :** This is a 4-bit field indicating the minor ISAKMP version as used in the current exchange. The current value of this field is 0.

f. **Exchange type :** This is an 8-bit field indicating the type of exchange that is being carried by the ISAKMP packets.

g. **Flags :** This is an 8-bit field indicating the specific set of options for ISAKMP exchange. Each bit in this field defines a single option.

h. **Message ID :** This is a 32-bit field specifying a unique ID for message.

i. **Message length :** This is a 32-bit field specifying the total length of the packet (including the header and all payloads) in octets.

Que 5.7. **Differentiate between transport mode and tunnel mode.**

Answer

S. No.	Transport mode	Tunnel mode
1.	Provides protection primarily for upper-layer protocols.	Provides protection to the entire IP packet.
2.	Typically used for end-to-end communication between two hosts.	Used when one or both ends of a security association (SA) are a security gateway.
3.	ESP in transport mode encrypts and optionally authenticates the IP payload but not the IP header.	ESP in tunnel mode encrypts and optionally authenticates the entire inner IP packet, including the inner IP header.
5.	AH in transport mode authenticates the IP payload and selected portions of the IP header.	AH in tunnel mode authenticates the entire inner IP packet and selected portions of the outer IP header.

Que 5.8. **Explain the concept of Security Association (SA) in IPSec. What is the use of ISAKMP protocol in IPSec ?**

AKTU 2014-15, Marks 10

Answer

Concept of security association in IPSec :

1. Security association is a one-way relationship between a sender and a receiver that affords security services to the traffic carried on it.
2. If a peer relationship is needed, for two-way secure exchange, then two security associations are required.
3. Security services are afforded to an SA for the use of AH (Authentication Header) or ESP (Encapsulating Security Payload), but not both.
4. A security association is uniquely identified by three parameters :
   i. **Security Parameters Index (SPI) :** A bit string is assigned to this SA and has local significance only. The SPI is carried in AH and ESP headers to enable the receiving system to select the SA under which a received packet will be processed.

ii. **IP destination address :** Currently, only unicast addresses are allowed; this is the address of the destination endpoint of the SA, which may be an end user system or a network system such as a firewall or router.

iii. **Security protocol identifier :** This indicates whether the association is an AH or ESP security association.

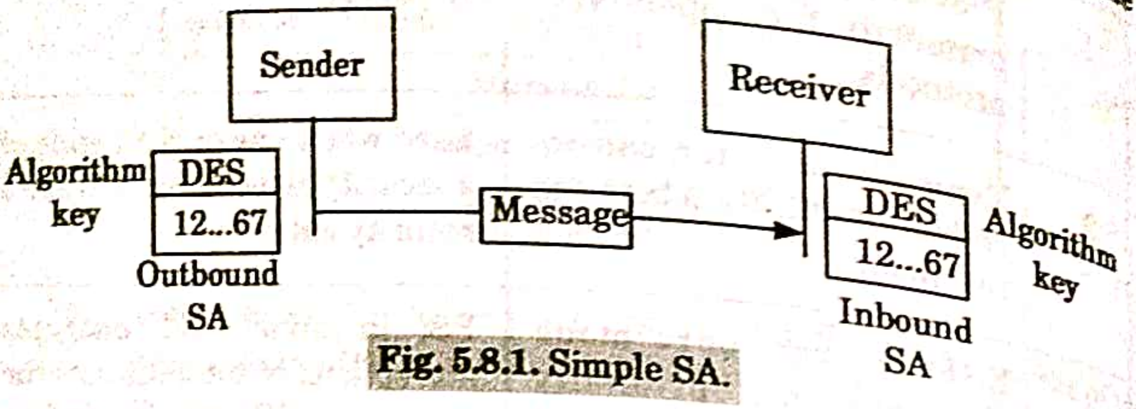


Fig. 5.8.1. Simple SA.

Use of ISAKMP : Internet Security Association and Key Management Protocol (ISAKMP) is use for negotiating, establishing, modification and deletion of SAs and related parameters.

Que 5.9. **Explain the Authentication Header (AH) protocol.**

Answer

1. The Authentication Header (AH) protocol is used to provide source authentication, and also to ensure the integrity of the payloads being carried in the IP packets.
2. The authentication feature allows the receiver to authenticate the sender, and accept or reject packets, accordingly. In addition, it prevents the address spoofing attacks.
3. The integrity feature ensures that the contents of the IP packets are not altered during transmission.
4. This protocol is based on the Message Authentication Code (MAC), which implies that the two parties must share a secret key.
5. Message digest is created with the help of a hash function and a symmetric key.
6. The message digest is then inserted into the AH. This AH is finally placed in the appropriate location as per the mode used (transport or tunnel).

Que 5.10. **Discuss authentication header format.**

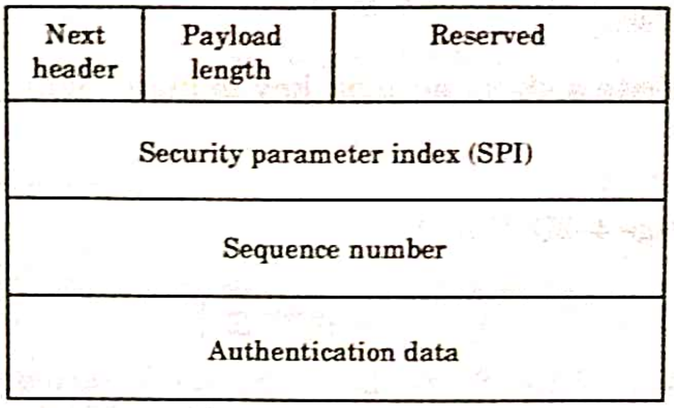


Fig. 5.10.1. Authentication header format.

Answer

The various fields of the AH are :

1. **Next header :** This is an 8-bit field that specifies the type of header.
2. **Payload length :** This is an 8-bit field that specifies the length of the AH in 32-bit words.
3. **Reserved field :** This is a 16-bit field that has been kept reserved for future use.
4. **Security Parameter Index (SPI) :**
   a. This is a 32-bit field that uniquely identifies the security associations for the traffic to which the IP datagram belongs.
   b. It plays the role of a virtual circuit identifier.
   c. This field is used in combination with the source and destination addresses, as well as the IPSec protocol used (AH or ESP).
5. **Sequence number :**
   a. This is a 32-bit field that contains a monotonically increasing number (a counter) that specifies the ordering of the IP datagrams.
   b. The sequence number is capable of preventing the replay attacks.
   c. The sender must always transmit this field, but the receiver need not always act upon it.
6. **Authentication data :**
   a. This is a variable length field that contains the authentication data, called the Integrity Check Value (ICV) for the datagram.

b. For IPv4 datagrams, this value must be an integral multiple of 32, and for IPv6, this value must be an integral multiple of 64.

c. The ICV is generated by applying a hash function to the whole IP datagram.

Que 5.11. **Write a short note on key management.**

Answer

Refer Q. 4.1, Page 4–2D, Unit-4.

PART-2

Introduction to Secure Socket Layer, Secure Electronic Transaction (SET), System Security : Introductory Idea of Intrusion, Intrusion Detection, Viruses and Related Threats, Firewalls.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 5.12. **Explain SSL with its architecture.**

Answer

1. The Secure Socket Layer (SSL) protocol provides exchange of information between a web browser and a web server in a secure manner.
2. Its main aim is to provide entity authentication, message integrity and confidentiality.
3. SSL is an additional layer located between the application layer and the transport layer of the TCP/IP protocol suite. All the major web browsers support SSL.

SSL architecture : The higher layer protocols include handshake protocol, change cipher spec protocol and alert protocol. The lower layer includes the SSL record protocol, which is used for providing various basic security services to the higher layer protocols. HTTP, which enables the web browser to interact with the web server, can work on the top of SSL.

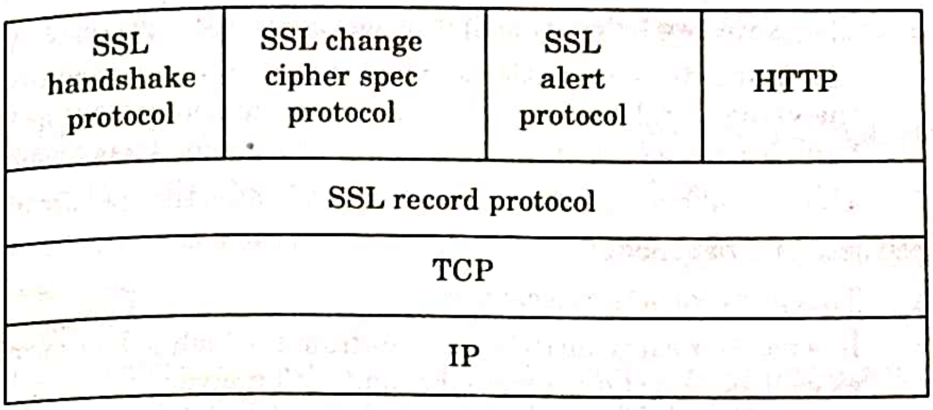


Fig. 5.12.1.

1. **Handshake protocol :**
   a. This protocol allows authentication between the server and the client.
   b. It allows the server and the client to negotiate on an encryption and MAC algorithm, and cryptographic keys to be used for encrypting the data in an SSL record.
   c. In this protocol, several messages are exchanged between the server and the client.
2. **Change cipher spec protocol :**
   a. The change cipher spec is the simplest protocol that is used to signal that the cryptographic secrets are ready for use.
   b. This protocol consists of only one message, which consists of a single byte with the value.
   c. This value causes the pending state to be changed to the active state.
   d. The pending state is the one in which two communicating parties keep track of the parameters and secrets.
   e. The active state is the one in which the two parties use these parameters and secrets to sign/verify or encrypt/decrypt the messages.
   f. The change cipher spec protocol is responsible for moving values between the pending state and active state.
3. **Alert protocol :**
   a. This protocol is used to signal errors or any abnormal conditions to the nodes.
   b. It enables the nodes to exchange the error or warning information.
   c. The type of message associated with alert protocol is the alert message.

d. There are two bytes in each message of the alert protocol.

e. The first byte conveys the severity of the error. It can take either the value 1 or 2, where 1 indicates warning and value 2 indicates fatal. In case of fatal error, the connection is immediately terminated.

f. The second byte contains a code that indicates the specific alert.

4. **SSL record protocol :**

a. This protocol acts as a carrier.

b. It is used for carrying the messages from the higher-layer protocols as well as data coming from the application layer.

c. It receives the data to be transmitted from the application layer.

Que 5.13. **Discuss Secure Electronic Transaction (SET).**

AKTU 2016-17, Marks 10

OR

Write short note on SET.

AKTU 2017-18, Marks 05

OR

Explain Secure Electronic Transaction (SET) in internet protocol security in detail.

AKTU 2018-19, Marks 10

Answer

1. Secure Electronic Transaction (SET) is a standard protocol for securing credit card transactions over insecure networks, *i.e.*, the internet.
2. SET is not a payment system but rather a set of security protocols and formats that enables users to employ the existing credit card payment infrastructure on an open network in a secure fashion.
3. SET is based on X.509 certificates with several extensions.
4. SET makes use of cryptographic techniques such as digital certificates and public key cryptography to allow parties to identify themselves to each other and exchange information securely.
5. SET uses a blinding algorithm that lets merchants to substitute a certificate for a user's credit card number.
6. This allows traders to credit funds from client's credit cards without the need of the credit card numbers.
7. The purpose of the SET protocol is to establish payment transactions. It provides confidentiality of payment and ordering information, and ensures the integrity of all transmitted data.
8. SET creates a protocol that neither depends on transport security mechanisms nor prevents their use.

9. It facilitates and encourage interoperatability among software and network providers.

Que 5.14. **Who are the participants in SET (Secure Electronic Transaction) system ? Describe in brief the sequence of events that are required for a transaction.** **AKTU 2014-15, Marks 10**

Answer

Secure Electronic Transaction (SET) is a standard protocol for securing credit card transactions over insecure networks *i.e.*, the internet.

Following are the participants in the SET system :

1. **Cardholder :**
   a. In the electronic environment, consumers and corporate purchasers interact with merchants over the internet.
   b. A cardholder is an authorized holder of a payment card that has been issued by an issuer.
2. **Merchant :**
   a. A merchant is a person or organization that has goods or services to sell to the cardholder. These goods and services are offered via a website or by electronic mail.
   b. A merchant that accepts payments cards must have a relationship with an acquirer.
3. **Issuer :** This is the financial institution that provides the cardholder with the payment card.
4. **Acquirer :**
   a. The acquirer provides authorization to the merchant that given card account is active and the proposed purchase does not exceed the credit limit.
   b. The acquirer also provides electronic transfer of payments to the merchant's account.
5. **Payment gateway :**
   a. The payment gateway act as an interface between SET and the existing bank card payment networks for authorization and payment functions.
   b. The merchant exchange SET messages with the payment gateway over the internet, while the payment gateway has connection to the acquirer's financial processing system.
6. **Certification Authority (CA) :** This is an entity that is trusted to issue X.509 public key certificates for cardholders, merchants and payment gateways.

Following are the sequence of events that are required fo transaction :

1. **The customer opens an account :** The customer obtains a cre card account with a bank that supports electronic payment and SE
2. **The customer receives a certificate :**
   a. After suitable verification of identity, the customer receives X.509 digital certificate, which is signed by the bank.
   b. The certificate verifies the customer's RSA public key and i expiration date. It also establishes a relationship between t customer's key pair and his credit card.
3. **Merchant have their own certificates :**
   a. A merchant who accepts a certain brand of card must be possession of two certificates for two public keys owned by th merchant : one for signing messages, and one for key exchang
   b. The merchant also needs a copy of the payment gateway's publ key certificate.
4. **The custoner places an order :** In this process, the customer senc a list of items to be purchased to merchant, who returns an order forı containing the list of items, their price, a total price and an orde number.
5. **The merchant is verified :** In addition to the order form, the merchar sends a copy of its certificate, so that the customer can verify that he i dealing with a valid store.
6. **The order and payment are sent :** The customer sends both th order and payment information to the merchant, along with th customer's certificate.
7. **The merchant requests payment authorization :** The merchan sends the payment information to the payment gateway, requestin authorization that the customer's available credit is sufficient for thi purchase.
8. **The merchant confirms the order :** The merchant send confirmation of the order to the customer.
9. **The merchant provides the goods or service :** The merchant ship the goods or provides the service to the customer.

Que 5.15. **How SET achieves its objectives.**

Answer

Following steps are taken by SET to achieve its objectives :

1. The SET software prepares the Payment Information (PI) on the cardholder's computer exactly in the same way as it happens in any Web-based payment system.

2. The cardholder's computer creates a one-time session key.
3. Using this one-time session key, the cardholder's computer encrypts the payment information.
4. The cardholder's computer wraps the one-time session key with the public key of the payment gateway to form a digital envelope.
5. It then sends the encrypted payment information (Step 3) and the digital envelope (Step 5) together to the merchant.

Que 5.16. **What do mean by system security ? Also discuss viruses and related threats to system security ?**

AKTU 2018-19, Marks 10

Answer

System security : System security refers to the process and methodologies involved in keeping information confidential, available and assuring its integrity.

Viruses :

1. A virus is a piece of program code that attaches itself to host program and execute when the host program runs. It can then infect other programs in that computer or in another computer in a same network.
2. Usually viruses cause damage to computer and network systems to the extent that it can be repaired assuming that the organization deploys good backup and recovery procedures.
3. During its lifetime, a virus goes through four phases :
   a. **Dormant phase :** In this phase, the virus is idle. It gets activated based on certain action or event. This is optional phase.
   b. **Propagation phase :** In this phase, a virus copies itself and each copy starts creating more copies of self, thus propagating the virus.
   c. **Triggering phase :** A dormant virus moves into this phase when the action / event for which it was waiting is initiated.
   d. **Execution phase :** This is the actual work of the virus, which could be harmless or destructive.

Related threats to system security : Following are the related threats to system security :

1. **Worms :**
   a. Worms are the piece of code that replicates itself again and again. Worms are different from viruses in terms of implementation.
   b. A virus modifies a program, however a worm does not modify a program.

c. A worm replicates itself so much that ultimately the computer or the network on which the worm resides become very slow, finally coming to a halt.

d. Thus, the basic purpose of worm is to consume system resources to make system unusable.

2. **Trojan horse :**

a. A Trojan horse is a hidden piece of code, which allows attacker to obtain or reveal some confidential information about a computer or a network.

b. Trojan horse could attach to the code of login screen.

c. When user enters user id and password, the Trojan could capture these details and send this information to attacker. Then attacker can use this information to gain access to the system.

3. **Logic bombs :**

a. Logic bombs are the codes embedded in host program that are executed when a predefined event occurs.

b. These bombs display a message to the user and occur at a time when either the user is accessing the internet or making use of a word processor application.

c. The logic bomb initiation is a four-step process :

i. Attacker implants the logic bomb.

ii. Victim reports the installation.

iii. Attacker sends the attack message.

iv. Victim does as the logic bomb dictates.

4. **Mail bombing :**

a. A mail bombing is a type of e-mail attack that is also a denial of service (DoS).

b. Attacker routes large quantities of e-mail messages to the target.

c. By sending large e-mails, attackers can take advantage of poorly configured e-mail systems on the internet and trick them into sending many e-mails to an address chosen by the attacker.

5. **Trapdoor :**

a. A trapdoor or a backdoor is a secret means of access to a computer program that bypasses security mechanisms.

b. The trapdoor is the code that recognizes some special sequence of input or is triggered by being run from a certain user ID or by an unlikely sequence of events.

Que 5.17. **What are the different security threats ? What is firewall ?**

AKTU 2016-17, Marks 10

OR

Write a short note on firewall.

AKTU 2017-18, Marks 05

Answer

Security threats : Refer Q. 5.16, Page 5–15D, Unit-5.

Firewall :

1. A firewall defines a single choke point that keeps unauthorized users out of the protected network, prohibits potentially vulnerable services from entering or leaving the network, and provides protection from various kinds of IP spoofing and routing attacks.
2. The use of a single choke point simplifies security management because security capabilities are consolidated on a single system or set of systems.
3. A firewall provides a location for monitoring security-related events. Audits and alarms can be implemented on the firewall system.
4. A firewall is a convenient platform for several Internet functions that are not security related. These include a network address translator, which maps local addresses to Internet addresses, and a network management function that audits or logs Internet usage.
5. A firewall can serve as the platform for IPSec. Using the tunnel mode capability the firewall can be used to implement virtual private networks.

Que 5.18. **What are the types of firewall ? Explain them.**

AKTU 2014-15, Marks 10

Answer

A firewall is a single point defense between two networks. A firewall is a specialized version of a routers and a combination of packet filters and application gateway.

Following are the types of firewall :

1. **Packet filtering firewall :**
   a. Packet filtering firewall is a firewall technique used to control network access by monitoring outgoing and incoming packets.

b. Packet filtering firewall allows packet to pass or halt based on the source and destination Internet Protocol (IP) address, Protocols and ports.

2. **Circuit level firewall :**

a. A circuit level firewall creates a circuit between a client and a server without knowing the service required.

b. A circuit level firewall does not require special proxy-client applications.

3. **Application-level firewall :**

a. An application-level firewall is a host computer running software known as a proxy server.

b. A proxy server is an application that controls the traffic between two networks.

c. When using an application-level firewall the intranet and the internet are not physically connected.

4. **Stateful firewall :**

a. A stateful firewall is a network that tracks the operating state and characteristics of network connections traversing it.

b. The firewall is configured to distinguish valid packets for different types of connections.

Que 5.19. **List some limitations of firewalls.**

Answer

1. A firewall provides effective security to the internal network if it is configured as the only entry-exit point in the organization.
2. If there are multiple entry-exit points in the organization and firewall is implemented at just one of them, then the incoming or outgoing traffic may bypass the firewall. This makes the internal network susceptible to attack through the points where the firewall has not been implemented.
3. A firewall is designed to protect against outside attacks. However, it does not have any mechanism to protect against internal threats such as an employee of a company who unknowingly helps an external attacker.
4. The firewall does not provide protection against any virus-infected program or files being transferred through the internal network. This is because it is almost impossible to scan all the files entering in the network for viruses.
5. To protect the internal network against virus threats, a separate virus detection and removal strategy should be used.

Que 5.20. **What are the advantages and disadvantages of application-level gateway ?**

Answer

Advantages :

1. The entire communication between the internal and external network happens only through the application gateways. This protects the internal IP addresses from the external network.
2. The use of application gateways provides transparency between the users and the external network.
3. They understand and implement high-level protocols such as HTTP and FTP.
4. They support functions such as user authentication, caching, auditing and logging.
5. They can process and manipulate the packet data.
6. Strong user authentication can be enforced with application gateways.

Disadvantages :

1. Each new network service requires a number of proxy services to be added. Thus, application-level gateways are not scalable.
2. The addition of proxy services causes client applications to be modified.
3. Application gateways operate at a slower speed. Thus network performance degrades.
4. As they rely on operating system, they are vulnerable to the bugs in the system.

Que 5.21. **What do you understand by trusted system ? Explain the concept of reference monitor.** **AKTU 2014-15, Marks 10**

Answer

1. A trusted system is a computer and operating system that can be verified to implement a given security policy.
2. Trusted system are build upon a TCB (Trusted Computing Base) which contains all of the elements of the system responsible for supporting the security policy and isolation of objects on which the protection is based.
3. The focus of a trusted system is access control. A general model of access control as exercised by a file or database management system is that of an access matrix.

4. The basic elements of the model are as follows :
   a. **Subject :** An entity capable of accessing objects.
   b. **Object :** Anything to which access is controlled.
   c. **Access right :** The way in which an object is accessed by a subject.
5. An access matrix is usually sparse and is implemented by decomposition in one of two ways. The matrix may be decomposed by columns, yielding access control lists.
6. Thus, for each object, an access control list notes users and their permitted access right. The access control list may contain a default, or public entry.

Reference monitor :

1. The reference monitor is a controlling element in the hardware and operating system of a computer that regulates the access of subjects to objects on the basis of security parameters of the subject and object.
2. The reference monitor has access to a file, known as the security kernel database, that note the access privileges and the protection attributes of each object.
3. The reference monitor enforces the security rules (no read up, no write down) and has the following properties :
   a. **Complete mediation :** The security rules are enforced on every access, not just.
   b. **Isolation :** The reference monitor and database are protected from unauthorized modification.
   c. **Verifiability :** The reference monitor's correctness must be provable.
4. The requirement for complete mediation means that every access to data within main memory and on disk and tape must be mediated.
5. The requirement for isolation means that it must not be possible for an attacker, to change the logic of the reference monitor.

Que 5.22. **What are the advantages and disadvantage of packet-filtering router firewall ?**

Answer

Advantages :

1. They are simple, since a single rule is enough to indicate whether to allow or deny the packet.
2. They are transparent to the users *i.e.*, the users need not know the existence of packet filters.
3. They operate at a fast speed as compared to other techniques.

4. The client computers need not be configured specially while implementing packet-filtering firewalls.
5. They protect the IP addresses of internal hosts from the outside network.

Disadvantages :

1. They are unable to inspect the application layer data in the packets and thus, cannot restrict access to FTP services.
2. It is a difficult task to set up the packet-filtering rules correctly.
3. They lack support for authentication and have no alert mechanisms.
4. Being stateless in nature, they are not well suited to application layer protocols.

Que 5.23. **What are the advantage and disadvantage of circuit-level gateway ?**

Answer

Advantages :

1. They operate at a faster speed as compared to application-level gateways.
2. They offer more security than packet filters.
3. They are not subject to IP address spoofing attacks.
4. They perform Network Address Translation (NAT) by changing source node IP address to its own and, thus, protecting internal host IP addresses from the external network.

Disadvantages :

1. They are unable to perform security checks on higher-level protocols.
2. They can restrict access only to TCP protocol subsets.
3. They have only a confined audit event generation capability.

Que 5.24. **Write a short note on intrusion detection.**

AKTU 2017-18, Marks 05

Answer

1. Intrusion detection refers to the process of identifying attempts to penetrate a system and gain unauthorized access.
2. An intrusion detection system is a Software/Hardware designed to detect unwanted attempts at accessing of target application or system.
3. If an intrusion is detected quickly enough, the intruder can be identified and ejected from the system before any damage is done or any data are compromised.

4. Even if the detection is not sufficiently time to preempt the intruder, tl sooner that the intrusion is detected, the less the amount of damage a more quickly recovery can be achieved.
5. An effective intrusion detection system can serve as a deterrent intrusions.
6. Intrusion detection enables the collection of information about intrusi techniques that can be used to strengthen the intrusion preventi facility.

Que 5.25. **Briefly describe the two approaches for intrusi detection.**

Answer

Two approaches for intrusion detection are :

1. **Statistical anomaly detection :** In this category, the behaviour legitimate users is evaluated over some time interval. It can be achiev by two way :
   a. **Threshold detection :**
      i. In threshold detection, thresholds are defined for all users a group, and the total number of events that are attributed the user are measured against these threshold values.
      ii. The number of events is assumed to round upto a number tl is most likely to occur, and if the event count exceeds t number, then intrusion is said to have occurred.
   b. **Profile-based detection :**
      i. In profile-based detection, profiles for all users are creat and then matched with available statistical data to find ou any unwanted action has been performed.
      ii. A user profile contains several parameters. Therefore, char in a single parameter is not a sign of alert.
2. **Rule-based detection :** In this category, certain rules are applied the actions performed by the users. It is classified into two types :
   a. **Anomaly-based detection :**
      i. In anomaly-based detection, the usage patterns of users collected, and certain rules are applied to check any deviat from the previous usage patterns.
      ii. The collected patterns are defined by the set of rules tl includes past behaviour patterns of users, programs, privileg time-slots, terminals, etc.

iii. The current behaviour patterns of the user are matched with the defined set of rules to check whether there is any deviation in the patterns.

b. **Penetration identification :**

i. In penetration identification, an expert system is maintained that looks for any unwanted attempts.

ii. This system also contains rules that are used to identify the suspicious behaviour and penetrations that can exploit known weaknesses.

Que 5.26. **Differentiate between SSL and SET.**

Answer

Issue	SSL	SET
Main objective	To allow exchange of data in an encrypted form	To support e-commerce related payment mechanisms.
Certification	The certificates are exchanged between the two parties.	A trusted third party certifies all the parties involved in the communication process.
Authentication	The authentication mechanism is not very strong.	The authentication mechanism is very strong.
Risk of merchant fraud	It is prone in merchant fraud as financial data is provided to the merchant.	It is free from this fraud as financial data is given to the payment gateway only.
Risk of customer fraud	It is prone to this kind of fraud as the customer can refuse to pay later; there is no mechanism that can prevent such kind of fraud.	The payment instructions are digitally signed by the customer. Thus, there is less chance of such fraud.
Action in case of customer fraud	Merchant is responsible if a customer later refuses to pay.	Payment gateway is responsible in case of customer fraud.
Practical usage	High.	Less.

VERY IMPORTANT QUESTIONS

Following questions are very important. These questions may be asked in your SESSIONALS as well as UNIVERSITY EXAMINATION.

Q. 1. Explain internet protocol security in detail.

Ans. Refer Q. 5.1.

Q. 2. Explain the ESP format. What is anti-replay service ?

Ans. Refer Q. 5.4.

Q. 3. Explain the concept of Security Association (SA) in IPSec. What is the use of ISAKMP protocol in IPSec ?

Ans. Refer Q. 5.8.

Q. 4. Discuss Secure Electronic Transaction (SET).

Ans. Refer Q. 5.13.

Q. 5. Who are the participants in SET (Secure Electronic Transaction) system ? Describe in brief the sequence of events that are required for a transaction.

Ans. Refer Q. 5.14.

Q. 6. What do mean by system security ? Also discuss viruses and related threats to system security ?

Ans. Refer Q. 5.16.

Q. 7. What are the types of firewall ? Explain them.

Ans. Refer Q. 5.18.

Q. 8. Write a short note on intrusion detection.

Ans. Refer Q. 5.24.

☺☺☺

1 UNIT

Introdution (2 Marks Questions)

1.1. What do you mean by cryptography ?

AKTU 2018-19, Marks 02

Ans. Cryptography is defined as the conversion of data into a scrambled code that can be decrypted and sent across a public or private network. It is the science and art of creating secret codes.

1.2. What are the different factors on which cryptography depends ?

AKTU 2017-18, Marks 02

Ans. Following are the different factors on which cryptography depends :

1. Plaintext
2. Encryption algorithm
3. Ciphertext
4. Decryption algorithm

1.3. What are the different security attacks ?

AKTU 2016-17, Marks 02

OR

What is security attack ? Discuss its various types.

AKTU 2017-18, Marks 02

Ans. Security attack is defined as an attempt to gain unauthorized access to information resource or services or to cause harm to information system. Following are the two types of security attacks :

1. **Passive attacks :** Passive attacks are those attacks where the attacker indulges in monitoring of data transmission.
2. **Active attacks :** Active attacks are those attacks where the attackers attempt to make change to data.

1.4. Distinguish between an active and passive attack.

AKTU 2015-16, Marks 02

Ans.

S. No.	Active attack	Passive attack
1.	Access and modify information.	Access information.
2.	System is harmed.	No harm to system.
3.	Easy to detect than prevent.	Difficult to detect than prevent.
4.	Threat to integrity, availability.	Threat to confidentiality.

1.5. What are different security mechanism ?

AKTU 2016-17, Marks 02

Ans. Different security mechanisms are :

i. Encipherment
ii. Data integrity
iii. Digital signature
iv. Traffic padding
v. Routing control
vi. Notarization
vii. Access control

1.6. Specify two differences between procedural and object oriented language.

AKTU 2015-16, Marks 02

Ans.

S. No.	Procedural language	Object-oriented language
1.	It executes series of procedures sequentially.	It executes through the approach of collection of objects.
2.	This is a top-down programming approach.	This is a bottom-up programming approach.

1.7. What type of security goals are used in cryptography ?

AKTU 2015-16, Marks 02

Ans. Types of security goals used in cryptography are :

1. To protect the confidentiality of data
2. To preserve the integrity of data
3. To promote the availability of data for authorized use

1.8. Define block cipher.

AKTU 2018-19, Marks 02

Ans. A block cipher is defined as a symmetric key cipher where a group of plaintext symbols are encrypted together to create a group of ciphertext of same size.

1.9. What is stream cipher ? **AKTU 2015-16, Marks 02** **AKTU 2018-19, Marks 02**

Ans. A stream cipher is defined as a symmetric key cipher where encryption and decryption are done on one symbol at a time.

1.10. What is cryptanalysis ? **AKTU 2017-18, Marks 02**

Ans. Cryptanalysis is the decryption and analysis of codes, ciphers or encrypted text.

1.11. Discuss linear and differential cryptanalysis. **AKTU 2017-18, Marks 02**

Ans. **Linear cryptanalysis :** Linear cryptanalysis is a known plaintext attack in which the attacker studies probabilistic linear relations between parity bits of the plaintext, the ciphertext, and the secret key.

Differential cryptanalysis : Differential cryptanalysis is a general form of cryptanalysis applicable primarily to block ciphers, but also to stream ciphers and cryptographic hash functions where the attackers studies of how differences in the information input that can affect the resultant difference at the output.

1.11. Define data integrity.

Ans. Data integrity is designed to protect data from modification, insertion, deletion and replacing by any entity. It can be applied to a stream of message, a single message or a selected position within a message.

1.12. What do you mean by Avalanche effect ?

Ans. Avalanche effect is defined as the effect where a small change in either the plaintext or the key should produce a significant change in the ciphertext *i.e.*, a change in one bit of plaintext produces change in many bit of the ciphertext.

1.13. Discuss double and triple DES. **AKTU 2017-18, Marks 02**

Ans. **Double DES :** In double DES, we use two instances of DES ciphers for encryption and two instances of reverse ciphers for decryption. Each instances use a different key. The size of the key is 112-bits.

Triple DES : In triple DES, three stages of DES are used for encryption and decryption of messages. This increases the security of DES.

☺☺☺

2 UNIT

Advanced Encryptio Standar (2 Marks Questions

2.1. Discuss group and ring with suitable axioms.

AKTU 2017-18, Marks 0

Ans. **Group :** A group (*G*), denoted by {G, •}, is a set of elements wi a binary operation '•' that satisfies following four properties :

1. **Closure :** $c = a \bullet b$
2. **Associativity :** $(a \bullet b) \bullet c = a \bullet (b \bullet c)$
3. **Identity :** $e \bullet a = a \bullet e = a$.
4. **Inverse :** $a \bullet a' = a' \bullet a = e$.

Ring : A ring *R*, denoted by {*R*, +, ×}, is a set of elements with t binary operations, called addition and multiplication, such that f all *a*, *b*, *c* in *R* the following axioms are obeyed :

1. **Closure under multiplication :** If *a* and *b* belong to *R*, then *ab* also in *R*.
2. **Associativity of multiplication :** $a(bc) = (ab)c$ for all *a*, *b*, *c* in
3. **Distributive laws :**

$$a(b + c) = ab + ac \text{ for all } a, b, c \text{ in } R$$
$$(a + b)\, c = ac + bc \text{ for all } a, b, c \text{ in } R$$

4. **Commutative of multiplication :** $ab = ba$ for all *a*, *b* in *R*.
5. **Multiplicative identity :** There is an element 1 in *R* such that

$$a1 = 1a \text{ for all } a \text{ in } R.$$

6. **No zero divisors :** If *a*, *b* belong to *R* and $ab = 0$, then either $a =$ or $b = 0$.

2.2. Write down the properties of modular arithmet operations.

Ans. **Modular arithmetic exhibits the following properties :**

1. $[(a \bmod n) + (b \bmod n)] \bmod n = (a + b) \bmod n$
2. $[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$
3. $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$

2.3. Define relatively prime numbers ?

Ans. Two integers *a* and *b* are relatively prime if gcd $(a, b) = 1$. Tl integers $a_1, a_2, ..., a_n$ are pair-wise relatively prime if g $(a_i, a_j) = 1$, whenever $1 \leq i < j \leq n$.

2.4. Describe primality testing in brief.

Ans. A primality testing is an algorithm used for determining whether an input number is prime. This algorithms is divided into two categories :

i. Deterministic algorithm

ii. Divisibility algorithm

2.5. What are the requirements for the use of a public key certificates scheme ? **AKTU 2015-16, Marks 02**

Ans. Requirements for the use of a public key certificates scheme are :

1. Any participant can read a certificate to determine the name and public key of the certificate's owner.
2. Any participant can verify that the certificate originated from the certificate authority and is not fake.
3. Only the certificate authority can create and update certificates.
4. Any participant can verify the currency of the certificate.

2.6. Explain field with example. **AKTU 2016-17, Marks 02**

Ans. Field : A field F, denoted by {F, +, ×}, is a set of elements with two binary operations, called addition and multiplication, such that for all a, b, c in F the following axioms are obeyed :

1. F is an integral domain.
2. **Multiplicative inverse :** For each a in F, except 0, there is an element a^{-1} in F such that $aa^{-1} = (a^{-1})\, a = 1$.

   For example : Rational numbers, real numbers and complex numbers are the examples of field.

2.7. Find GCD (1970, 1066) by using Euclid's algorithm.

AKTU 2017-18, Marks 02

Ans. gcd (1970, 1066) = gcd (1066, 1970 mod 1066)
= gcd (1066, 904) = gcd (904, 1066 mod 904)
= gcd (904, 162) = gcd (162, 904 mod 162)
= gcd (162, 94) = gcd (94, 162 mod 94)
= gcd (94, 68) = gcd (68, 94 mod 68)
= gcd (68, 26) = gcd (26, 68 mod 26)
= gcd (26, 16) = gcd (16, 26 mod 16) = gcd (16, 10)
= gcd (10, 16 mod 10) = gcd (10, 6) = gcd (6, 10 mod 6)
= gcd (6, 4) = gcd (4, 6 mod 4) = gcd (4, 2) = gcd (2, 4 mod 2)
= gcd (2, 0) = 2

2.8. Compute the value of 5^{17} mod 11 and 11^{17} mod 5.

AKTU 2017-18, Marks 02

Ans. **5^{17} mod 11 :**

$= (5^2 \text{ mod } 11)\,(5^{15} \text{ mod } 11)$

$= [3 \times (5^2 \text{ mod } 11)^7 \times (5 \text{ mod } 11)] \text{ mod } 11$

$= [3 \times 3^7 \times 5] \text{ mod } 11 = 3$

11^{17} mod 5 :

$= (11^2 \text{ mod } 5)\,(11^{15} \text{ mod } 5) = [1 \times (11^2 \text{ mod } 5)^7 \times (11 \text{ mod } 5)] \text{ mod } 5$

$= [1 \times 1^7 \times 1] \text{ mod } 5 = 1$

2.9. Find the value of Euler's Totient Number $\phi(88)$.

AKTU 2017-18, Marks 02

Ans. $\phi(88) = \phi(11 \times 4 \times 2) = (11 - 1) \times (4 - 1) \times (2 - 1)$

$= 10 \times 3 \times 1 = 30$

2.10. Give the ingredients of public key encryption scheme.

Ans. **Ingredients of public key encryption scheme are :**

i. Plain text
ii. Encryption algorithm
iii. Public and private keys
iv. Ciphertext
v. Decryption algorithm

2.11. Define AES.

Ans. Advanced Encryption Standard (AES) is a symmetric-key block cipher that operates on a data block of 128-bits, and comprises several rounds for encryption and decryption.

2.12. What do you mean by RSA ?

Ans. RSA is asymmetric cryptography algorithm where the encryption key is public and it is different from the decryption key which is kept secret.

☺☺☺

3

UNIT

Message Authentication Codes (2 Marks Questions)

3.1. What is message authentication code ?

AKTU 2015-16, Marks 02

AKTU 2016-17, Marks 02

Ans. A cryptographic Message Authentication Code (MAC) is a short piece of information used to authenticate a message. A MAC algorithm accepts as input a secret key and an arbitrary length message to be authenticated, and produces MAC as output.

3.2. What are the types of attacks addressed by MAC ?

Ans. The types of attacks that are addressed by message authentication are :

1. Masquerade
2. Modification of the message
3. Timing modification

3.3. What requirements should a digital signature scheme satisfy ? **AKTU 2015-16, Marks 02**

Ans. Following are the requirements for digital signature are :

1. The signature must be a bit pattern that depends on the message being signed.
2. The signature must use some information unique to the sender, to prevent both forgery and denial.
3. Production of digital signature must be easy.

3.4. Explain briefly the two different approaches of digital signature. **AKTU 2015-16, Marks 02**

Ans. Two different approaches of digital signature are :

1. **RSA :** RSA is used for encryption and decryption.
2. **DSA :** DSA (Digital Signature Algorithm) is used for signing/ verification.

3.5. Define hash algorithm. **AKTU 2018-19, Marks 02**

Ans. A hash algorithm is a function that converts a data string of variable length into a numeric output string of fixed length. Hash algorithms are designed to be collision-resistant, hence there is a very low probability that the same string would be created for different data.

3.6. Give the general form of a hash function.

Ans. A hash value h is generated by a function H of the form :

$$h = H(\mathrm{M})$$

where M is the variable length message and H(M) is the fixed length hash value.

3.7. What is DSS in cryptography ? **AKTU 2018-19, Marks 02**

Ans. Digital Signature Standard (DSS) is a standard that defines methods for digital signature generation and can be used for protection of binary data, verification and validation of digital signatures.

3.8. Describe birthday attack. **AKTU 2018-19, Marks 02**

OR

What is Birthday attack ? **AKTU 2017-18, Marks 02**

Ans. A birthday attack is a type of cryptographic attack that exploits the mathematics behind the birthday problem in probability theory. This attack can be use to exploit the communication between two parties.

3.9. What are the objectives for HMAC ?

Ans. **Objectives for HMAC are :**

i. To use without modifications, available hash functions.

ii. To use and handle keys in a simple way.

3.10. Write down the security services provided by a digital signature.

Ans. **Security services provided by digital signature are :**

i. Message Authentication

ii. Message Integrity

iii. Non-repudiation

iv. Confidentiality

3.11. What are the drawbacks of digital signature ?

Ans. **Drawbacks of digital signature are :**

i. Association of digital signature and trusted time stamping.

ii. Non-repudiation.

3.12. What is Elgamal encryption ?

Ans. The Elgamal encryption system is a public-key cryptosystem based on the concept of Diffie-Hellman key agreement.

3.13. Name different attacks on Elgamal algorithm.

Ans. Different attacks on Elgamal algorithm are :

1. Modulus attack
2. Known-plaintext attack

☺☺☺

4 UNIT

Key Management and Distribution (2 Marks Questions)

4.1. Define symmetric key cryptography.

Ans. Symmetric key cryptography is a shared secret key between two parties. It is more efficient for enciphering large messages. Its strength rests with the key distribution technique.

4.2. What is an authenticated Diffie-Hellman key agreement ?

AKTU 2015-16, Marks 02

Ans. Authenticated Diffie-Hellman key agreement is the building block for establishing secure session keys in security systems. Authenticated key agreement aims at simultaneously providing authentication of communicating parties.

4.3. Write down the use of Diffie-Hellman algorithm.

Ans. Diffie-Hellman algorithm is used to encrypt subsequent communications using a symmetric key cipher. It provides the basis for a variety of authenticated protocols and is used to provide perfect forward secrecy in transport layer security's modes.

4.4. What are the advantage of Diffie-Hellman algorithm ?

Ans. Advantages of the Diffie-Hellman algorithm are :

1. Secret keys are generated as and when required.
2. No pre-existing infrastructure is required for key exchange.

4.5. What are the limitations of Diffie-Hellman algorithm ?

Ans. Limitations of Diffie-Hellman algorithm are :

1. It does not provide any information regarding the identities of the users exchanging the key.
2. It is vulnerable to man-in-the-middle-attack.
3. It involves a lot of computation.

4.6. Define S/MIME. **AKTU 2015-16, Marks 02**

Ans. S/MIME is a standard for public key encryption and signing of MIME data. S/MIME (Secure Multi-Purpose Internet Mail

Extensions) is a secure method of sending e-mail that uses the RSA encryption system.

4.7. What is Kerberos ? **AKTU 2016-17, Marks 02**

Ans. Kerberos is a computer network authentication protocol, which allows individuals communicating over a non-secure network to prove their identity to one another in a secure manner.

4.8. What do you mean by mail security ?

AKTU 2018-19, Marks 02

OR

What do you mean by e-mail security ?

AKTU 2018-19, Marks 02

OR

Explain e-mail security. **AKTU 2016-17, Marks 02**

Ans. Mail security refers to the collective measures used to secure the access and content of an email account or service. It allows an individual or organization to protect the overall access to one or more email addresses/accounts.

4.9. Write down the different ways the public key can be distributed.

Ans. Different ways the public key can distributed are :

i. Public announcement

ii. Publically available directory

iii. Public key authority

4.10. Define public-key authority.

Ans. In public-key authority, central authority maintains a dynamic directory of public keys of all participants. Each participant reliably knows a public key for the authority, with only the authority knowing the corresponding private key.

4.11. What are public key certificates ?

Ans. Public key certificate define as the certificate used by participants to exchange keys without contacting a public-key authority in a reliable way as if the keys were obtained directly from a public-key authority.

4.12. What do you understand by Pretty Good Privacy algorithm ?

Ans. PGP is an encryption algorithm that provides cryptographic privacy and authentication for data communication.

4.13. Give the services provided by PGP.

Ans. **Service provided by PGP :**

i. Authentication
ii. Confidentiality
iii. Compression
iv. Segmentation and Reassembly
v. Signature component
vi. Message component

4.14. Differentiate between public key and private key.

AKTU 2016-17, Marks 0

AKTU 2018-19, Marks 0

Ans.

S. No.	Public key	Private key
1.	It is use to encrypt the message.	It is use to decrypt the messag
2.	Distributed freely and openly.	Protected by owner.
3.	It is used to verify signatures.	It is used to sign signatures.

☺☺☺

5

UNIT

IP Security (2 Marks Questions)

5.1. What is IP security ? **AKTU 2016-17, Marks 02**

Ans. IP Security (IPSec) is a collection of protocols designed by the Internet Engineering Task Force (IETF) to provide security for a packet at the network layer.

5.2. Explain intrusion detection. **AKTU 2016-17, Marks 02**

OR

Explain intrusion detection in brief. **AKTU 2018-19, Marks 02**

Ans.

1. Intrusion detection refers to the process of identifying attempts to penetrate a system and gain unauthorized access.
2. An intrusion detection system is a Software/Hardware designed to detect unwanted attempts at accessing of target application or system.

5.3. Differentiate between virus and firewalls. **AKTU 2016-17, Marks 02**

Ans.

S. No.	Virus	Firewalls
1.	A software that is capable of copying itself and has a harmful effect of corrupting the system.	It is a hardware/software security based network security system that prevents unauthorized access between computer programs.
2.	Its inspection capability is limited to techniques imposed by the antivirus vendor.	Its inspection capability is based on a pre-defined set of networks protocols.

5.4. What are the functional areas of IPsec ?

Ans. Functional areas of IPSec are :

i. Authentication
ii. Confidentiality
iii. Key management

5.5. What are the services provided by IPSec ?

Ans. Services provided by IPSec are :

i. Access control
ii. Connectionless integrity
iii. Data origin authentication
iv. Confidentiality
v. Limited traffic flow confidentiality

5.6. Describe briefly the concept of security association.

Ans. A security association is a contact between two parties to create a secure channel between them. Each of them stores the value of the key in a variable and the name of the encryption / decryption algorithm in another.

5.7. What do you understand by Security Association Database (SAD) ?

Ans. Security Association Database is a standard storage area which is used by communicating parties for storing the SA information.

5.8. Write down the list of information associated with the ESP protocol.

Ans. Information associated with the ESP protocol :

i. Encryption algorithm
ii. Authentication algorithm
iii. Keys
iv. Key lifetime
v. Initiator vectors

5.9. Describe briefly the security policy database.

Ans. Security policy database specifies the policies that determine the disposition of all IP traffic inbound or outbound from a host or a security gateway.

5.10. Give a list of main entities in SET.

Ans. There are four main entities in SET :

i. Card holder (customer)
ii. Merchant (web server)
iii. Merchant's Bank (payment gateway, acquirer)
iv. Issuer (cardholder's bank)

5.11. Describe briefly the purpose of SET protocol.

Ans. **Purpose of SET protocol are :**

i. Provide confidentiality of payment and ordering information.

ii. It facilitates and encourages interoperability among software and network providers.

iii. It ensures the integrity of all transmitted data.

5.12. What are the major transactions supported by SET ?

Ans. The major transactions supported by SET are purchase request, payment authorization and payment capture.

5.13. What do you mean by audit record ?

Ans. An audit record is a tool used in introduction detection. Audit records are used to track the actions performed by users. If any user tries to get unauthorized access in a network, then traces of such actions can be detected in these records, so the appropriate measures can be taken.

5.14. What are honeypots ?

Ans. Honeypots are the traps that are designed to attract the potential intruders and, thus, track their activities.

5.15. What do you mean by malicious software ?

Ans. Malicious softwares are the programs that generate threats to the computer system and stored data. They could be in the form of viruses, worms, Trojan horses, logic bombs and zombic programs.

☺☺☺

B.Tech.

(SEM. VII) ODD SEMESTER THEORY EXAMINATION, 2014-15

CRYPTOGRAPHY & NETWORK SECURITY

Time : 3 Hours **Max. Marks : 100**

Note : (1) Attempt **all** questions.
(2) All questions carry equal marks.

1. Attempt any **four** parts : (5 × 4 = 20)

a. **Explain Feistel encryption and decryption algorithms. What is the difference between diffusion and confusion ?**

Ans. Refer Q. 1.15, Page 1–12D, Unit-1.

b. **Compare and contrast substitution techniques with transposition techniques under classical encryption.**

Ans. Refer Q. 1.5, Page 1–5D, Unit-1.

c. **What is the most security-critical component of DES round function ? Give a brief description of this function.**

Ans. Refer Q. 1.19, Page 1–17D, Unit-1.

d. **What is the difference between block cipher and stream cipher ? What are the different modes of block cipher operation ? Explain any one of them.**

Ans. Refer Q. 1.25, Page 1–22D, Unit-1.

e. **What is the idea behind meet-in-middle attack ? How it can be avoided in 3 DES ?**

Ans. Refer Q. 1.21, Page 1–19D, Unit-1.

f. **The hill cipher uses the following key for enciphering the message.**

$$K = \begin{pmatrix} 3 & 2 \\ 5 & 7 \end{pmatrix}$$

Obtain the decryption key to be used for deciphering the cipher text.

Ans. Refer Q. 1.8, Page 1–7D, Unit-1.

2. Attempt any **four** parts : **(5 × 4 = 20)**

a. **Describe RSA algorithm, encryption and decryption function. In RSA, given $e = 07$ and $n = 3$. Encrypt the message "ME" using 00 to 25 for letters A to Z.**

Ans. Refer Q. 2.22, Page 2–17D, Unit-2.

b. **Write the pseudocode for Miller-Rabin primality testing. Test whether 61 is prime or not using the same Miller-Rabin test.**

Ans. Refer Q. 2.14, Page 2–11D, Unit-2.

c. **Describe the Fermat's little theorem. Using Fermat's theorem, find the value of 3^{201} mod 11.**

Ans. Refer Q. 2.9, Page 2–8D, Unit-2.

d. **Define ring and field. Give an example of ring which is not a field.**

Ans. Refer Q. 2.3, Page 2–3D, Unit-2.

e. **Illustrate the concept of Chinese Remainder Theorem. By using Chinese Remainder Theorem solve the simultaneous congruence $X = 2 \bmod P$ for all $P \in (3, 5, 7)$.**

Ans. Refer Q. 2.15, Page 2–12D, Unit-2.

f. **Describe Diffie-Hellman key exchange algorithm. Users A and B use the Diffie-Hellman key exchange technique a common prime $q = 83$ and a primitive root $\alpha = 13$.**

i. **If user A has private key 5 what is A's public key ?**

ii. **If user B has private key 12, what is B's public key ?**

iii. **What is the shared key ?**

Ans. Refer Q. 4.3, Page 4–3D, Unit-4.

3. Attempt any **two** parts : **(10 × 2 = 20)**

a. **Write the Digital Signature Algorithm (DSA) of Digital Signature Standard. What is the implication if same K (secret per message) is used to sign two different message using DSA ?**

Ans. Refer Q. 3.16, Page 3–16D, Unit-3.

b. **What are the requirements of a Message Authentication Code (MAC) ? Discuss the logical structure, components and algorithmic steps of MD5 algorithm.**

Ans. Refer Q. 3.4, Page 3–5D, Unit-3.

c. i. **Differentiate between the following :**

a. **Hash code and Message Authentication Code (MAC)**

b. Weak collision resistance and Strong collision resistance

Ans. Refer Q. 3.11, Page 3–12D, Unit-3.

ii. Describe birthday attack against any hash function. Give the mathematical basis of the attack.

Ans. Refer Q. 3.12, Page 3–13D, Unit-3.

4. Attempt any two parts : **(10 × 2 = 20)**

a. Enlist various services supported by S/MIME. Explain how S/MIME supports these services. What is the purpose of content type field in MIME header ?

Ans. Refer Q. 4.14, Page 4–16D, Unit-4.

b. What is digital certificate ? Give the format of X.509 certificate showing the important elements of the certificate. How is an X.509 certificate revoked ?

Ans. Refer Q. 4.7, Page 4–7D, Unit-4.

c. Explain the full-service Kerberos environment ? What are the principle differences between version 4 and version 5 of Kerberos ?

Ans. Refer Q. 4.10, Page 4–11D, Unit-4.

5. Attempt any two parts : **(10 × 2 = 20)**

a. Explain the concept of Security Association (SA) in IPSec. What is the use of ISAKMP protocol in IPSec ?

Ans. Refer Q. 5.8, Page 5–7D, Unit-5.

b. Who are the participants in SET (Secure Electronic Transaction) system ? Describe in brief the sequence of events that are required for a transaction.

Ans. Refer Q. 5.14, Page 5–13D, Unit-5.

c. i. What are the types of firewall ? Explain them.

Ans. Refer Q. 5.18, Page 5–17D, Unit-5.

ii. What do you understand by trusted system ? Explain the concept of reference monitor.

Ans. Refer Q. 5.21, Page 5–19D, Unit-5.

☺☺☺

B.Tech

(SEM. VII) ODD SEMESTER THEORY EXAMINATION, 2015-16

CRYPTOGRAPHY & NETWORK SECURITY

Time : 3 Hours **Max. Marks : 100**

SECTION – A

Note : Attempt all parts. All parts carry equal marks. Write answer of each parts in short : **(2 × 10 = 20)**

1. a. Specify two differences between procedural and object oriented language.

Ans. Refer Q. 1.6, Page SQ–2D, Unit-1, Two Marks Questions.

b. What is a stream cipher ?

Ans. Refer Q. 1.9, Page SQ–3D, Unit-1, Two Marks Questions.

c. What is an authenticated Diffie-Hellman key agreement ?

Ans. Refer Q. 4.2, Page SQ–10D, Unit-4, Two Marks Questions.

d. Distinguish between an active and passive attack.

Ans. Refer Q. 1.4, Page SQ–1D, Unit-1, Two Marks Questions.

e. What are Message Authentication Codes (MACs) ?

Ans. Refer Q. 3.1, Page SQ–7D, Unit-3, Two Marks Questions.

f. What requirements should a digital signature scheme satisfy ?

Ans. Refer Q. 3.3, Page SQ–7D, Unit-3, Two Marks Questions.

g. What type of security goals are used in cryptography ?

Ans. Refer Q. 1.7, Page SQ–2D, Unit-1, Two Marks Questions.

h. Define S/MIME.

Ans. Refer Q. 4.6, Page SQ–10D, Unit-4, Two Marks Questions.

i. What are the requirements for the use of a public key certificates scheme ?

Ans. Refer Q. 2.5, Page SQ–5D, Unit-2, Two Marks Questions.

j. Explain briefly the two different approaches of digital signature.

Ans. Refer Q. 3.4, Page SQ–7D, Unit-3, Two Marks Questions.

SECTION – B

Note : Attempt any **five** questions from this section : **(10 × 5 = 50)**

2. What are the properties of modular arithmetic operation ? What are the requirements of Message Authentication Code (MAC) ? List and explain them.

Ans. **Properties of modular arithmetic operation :** Refer Q. 2.4, Page 2–3B, Unit-2.

Requirements of message authentication code : Refer Q. 3.5, Page, Unit-3.

3. Encrypt the message "THIS IS AN EXERCISE" using Playfair Cipher with key = DOLLARS.

Ans. Refer Q. 1.9, Page 1–8D, Unit-1.

4. What is Kerberos ? Discuss Kerberos version 4 in detail.

Ans. Refer Q. 4.9, Page 4–10D, Unit-4.

5. Define the Chinese remainder theorem. Find the values of x for the following sets of Congruence using the Chinese remainder theorem.

$X = 2 \bmod 7$ and $X = 3 \bmod 9$.

Ans. Refer Q. 2.16, Page 2–13D, Unit-2.

6. What are the securities of RSA ? Perform encryption and decryption using RSA algorithm for $p = 17$, $q = 11$, $e = 7$, $m = 88$.

Ans. Refer Q. 2.26, Page 2–20D, Unit-2.

7. What is the principle of public-key cryptosystems ? Discuss the applications for public-key cryptosystems.

Ans. Refer Q. 2.21, Page 2–16D, Unit-2.

8. What are the properties of modular arithmetic operation ?

Ans. Refer Q. 2.4, Page 2–3D, Unit-2.

9. Define group field and finite field of the form $GF(p)$.

Ans. Refer Q. 2.1, Page 2–2D, Unit-2.

SECTION – C

Note : Attempt any **two** questions from this section : **(15 × 2 = 30)**

10. Find the values of x for the following sets of Congruence using the Chinese remainder theorem.

$$X = 2 \pmod 3$$
$$X = 1 \pmod 4$$
$$X = 3 \pmod 5$$

Ans. Refer Q. 2.19, Page 2–14D, Unit-2.

11. Explain RSA algorithm. Perform encryption and decryption using RSA algorithm for $p = 11$, $q = 13$, $e = 7$, $m = 9$.

Ans. Refer Q. 2.23, Page 2–18D, Unit-2.

12. Draw block diagram of DES encryption. Also, discuss the strengths of DES.

Ans. Refer Q. 1.18, Page 1–16D, Unit-1.

☺☺☺

B.Tech.

(SEM. VII) ODD SEMESTER THEORY EXAMINATION, 2016-17

CRYPTOGRAPHY & NETWORK SECURITY

Time : 3 Hours **Max. Marks : 100**

Note : Attempt **all** sections. If required any missing data; then choose suitably.

Section-A

1. Attempt **all** questions in brief. (2 × 10 = 20)

a. **What are the different security attacks ?**

Ans. Refer Q. 1.3, Page SQ–1D, Unit-1, Two Marks Questions.

b. **Explain field with example.**

Ans. Refer Q. 2.6, Page SQ–5D, Unit-2, Two Marks Questions.

c. **What is message authentication code ?**

Ans. Refer Q. 3.1, Page SQ–7D, Unit-3, Two Marks Questions.

d. **Explain intrusion detection.**

Ans. Refer Q. 5.2, Page SQ–13D, Unit-5, Two Marks Questions.

e. **Differentiate between virus and firewalls.**

Ans. Refer Q. 5.3, Page SQ–13D, Unit-5, Two Marks Questions.

f. **Explain e-mail security.**

Ans. Refer Q. 4.8, Page SQ–11D, Unit-4, Two Marks Questions.

g. **Differentiate between public key and private key.**

Ans. Refer Q. 4.14, Page SQ–12D, Unit-4, Two Marks Questions.

h. **What are the different security mechanisms ?**

Ans. Refer Q. 1.5, Page SQ–2D, Unit-1, Two Marks Questions.

i. **What is Kerberos ?**

Ans. Refer Q. 4.7, Page SQ–11D, Unit-4, Two Marks Questions.

j. **What is IP security ?**

Ans. Refer Q. 5.1, Page SQ–13D, Unit-5, Two Marks Questions.

Section-B

2. Attempt any **three** of the following. **(10 × 3 = 30)**

a. i. What is ideal block cipher ?

Ans. Refer Q. 1.12, Page 1–10D, Unit-1.

ii. Explain Shannon principle of confusion and diffusion.

Ans. Refer Q. 1.14, Page 1–11D, Unit-1.

b. Explain Chinese remainder theorem with example.

Ans. Refer Q. 2.18, Page 2–14D, Unit-2.

c. Discuss the basic use of message authentication code with suitable diagrams.

Ans. Refer Q. 3.5, Page 3–7D, Unit-3.

d. Explain Diffie-Hellman key exchange.

Ans. Refer Q. 4.3, Page 4–3D, Unit-4.

e. What are the different security threats ? What is firewall ?

Ans. Refer Q. 5.17, Page 5–17D, Unit-5.

Section-C

3. Attempt any **one** part of the following. **(10 × 1 = 10)**

a. Explain DES with diagram.

Ans. Refer Q. 1.17, Page 1–15D, Unit-1.

b. Explain different block cipher mode of operation.

Ans. Refer Q. 1.25, Page 1–22D, Unit-1.

4. Attempt any **one** part of the following : **(10 × 1 = 10)**

a. State and prove Euler theorem.

Ans. Refer Q. 2.10, Page 2–9D, Unit-2.

b. Explain RSA using example.

Ans. Refer Q. 2.23, Page 2–18D, Unit-2.

5. Attempt any **one** part of the following : **(10 × 1 = 10)**

a. Write the objectives of HMAC. Describe the HMAC algorithms.

Ans. Refer Q. 3.7, Page 3–9D, Unit-3.

b. Explain Elgamal digital signature scheme.

Ans. Refer Q. 3.17, Page 3–16D, Unit-3.

6. Attempt any **one** part of the following : **(10 × 1 = 10)**

a. **Explain PGP and S/MIME.**

Ans. Refer Q. 4.13, Page 4–15D, Unit-4.

b. **Explain X.509 in detail.**

Ans. Refer Q. 4.7, Page 4–7D, Unit-4.

7. Attempt any **one** part of the following : **(10 × 1 = 10)**

a. **Explain the ESP format. What is anti-replay service ?**

Ans. Refer Q. 5.4, Page 5–3D, Unit-5.

b. **Discuss Secure Electronic Transaction (SET).**

Ans. Refer Q. 5.13, Page 5–12D, Unit-5.

☺☺☺

B.Tech.

(SEM. VII) ODD SEMESTER THEORY EXAMINATION, 2017-18

CRYPTOGRAPHY & NETWORK SECURITY

Time : 3 Hours **Max. Marks : 100**

Note : 1. Attempt **all** Sections. If required any missing data; then choose suitably.

SECTION-A

1. Attempt **all** questions in brief. **(2 × 10 = 20)**

a. **Find GCD (1970, 1066) by using Euclid's algorithm.**

Ans. Refer Q. 2.7, Page SQ–5D, Unit-2, Two Marks Questions.

b. **What are the different factors on which cryptography depends ?**

Ans. Refer Q. 1.2, Page SQ–1D, Unit-1, Two Marks Questions.

c. **Compute the value of 5^{17} mod 11 and 11^{17} mod 5.**

Ans. Refer Q. 2.8, Page SQ–5D, Unit-2, Two Marks Questions.

d. **Find the value of Euler's Totient Number $\phi(88)$.**

Ans. Refer Q. 2.9, Page SQ–6D, Unit-2, Two Marks Questions.

e. **What is cryptanalysis ?**

Ans. Refer Q. 1.10, Page SQ–3D, Unit-1, Two Marks Questions.

f. **Discuss linear and differential cryptanalysis.**

Ans. Refer Q. 1.11, Page SQ–3D, Unit-1, Two Marks Questions.

g. **What is Birthday attack ?**

Ans. Refer Q. 3.8, Page SQ–8D, Unit-3, Two Marks Questions.

h. **Discuss double and triple DES.**

Ans. Refer Q. 1.13, Page SQ–3D, Unit-1, Two Marks Questions.

i. **Discuss group and ring with suitable axioms.**

Ans. Refer Q. 2.1, Page SQ–4D, Unit-2, Two Marks Questions.

B.Tech.

(SEM. VII) ODD SEMESTER THEORY EXAMINATION, 2018-19

CRYPTOGRAPHY & NETWORK SECURITY

Time : 3 Hours **Max. Marks : 100**

Note : 1. Attempt **all** Sections. If required any missing data; then choose suitably.

SECTION-A

1. Attempt **all** questions in brief. **(2 × 10 = 20)**

a. Define block cipher.

Ans. Refer Q. 1.8, Page SQ–2D, Unit-1, Two Marks Questions.

b. What do you mean by cryptography ?

Ans. Refer Q. 1.1, Page SQ–1D, Unit-1, Two Marks Questions.

c. Define hash algorithm.

Ans. Refer Q. 3.5, Page SQ–7D, Unit-3, Two Marks Questions.

d. What is stream cipher ?

Ans. Refer Q. 1.9, Page SQ–3D, Unit-1, Two Marks Questions.

e. Differentiate between public key and private key.

Ans. Refer Q. 4.14, Page SQ–12D, Unit-4, Two Marks Questions.

f. Explain intrusion detection in brief.

Ans. Refer Q. 5.2, Page SQ–13D, Unit-5, Two Marks Questions.

g. What do you mean by mail security ?

Ans. Refer Q. 4.8, Page SQ–11D, Unit-4, Two Marks Questions.

h. What is DSS in cryptography ?

Ans. Refer Q. 3.7, Page SQ–8D, Unit-3, Two Marks Questions.

i. What do you mean by email security ?

Ans. Refer Q. 4.8, Page SQ–11D, Unit-4, Two Marks Questions.

j. Describe birthday attack.

Ans. Refer Q. 3.8, Page SQ–8D, Unit-3, Two Marks Questions.

SECTION-B

2. Attempt any **three** of the following : **(10 × 3 = 30)**

a. **Draw the block diagram of DES algorithm. Also explain its functionality.**

Ans. Refer Q. 1.17, Page 1–15D, Unit-1.

b. **What is prime and relative prime numbers in cryptography and network security ?**

Ans. Refer Q. 2.5, Page 2–4D, Unit-2.

c. **Discuss the message authentication codes. Also give the use of authentication requirement in MAC.**

Ans. Refer Q. 3.1, Page 3–2D, Unit-3.

d. **What is Diffie-Hellman key exchange in key management ?**

Ans. Refer Q. 4.3, Page 4–3D, Unit-4.

e. **Explain internet protocol security in detail.**

Ans. Refer Q. 5.1, Page 5–2D, Unit-5.

SECTION-C

3. Attempt any **one** part of the following : **(10 × 1 = 10)**

a. **List the strength of DES in brief. Also explain the triple DES.**

Ans. Refer Q. 1.20, Page 1–18D, Unit-1.

b. **What is the Shannon's theory of confusion and diffusion in terms of information security ?**

Ans. Refer Q. 1.14, Page 1–11D, Unit-1.

4. Attempt any **one** part of the following : **(10 × 1 = 10)**

a. **State the Advanced Encryption Standard (AES). Also provide the functioning of AES.**

Ans. Refer Q. 2.7, Page 2–6D, Unit-2.

b. **Explain the Chinese Remainder Theorem with example. How Chinese remainder theorem provide the security to online information sharing transactions.**

Ans. Refer Q. 2.18, Page 2–14D, Unit-2.

5. Attempt any **one** part of the following : **(10 × 1 = 10)**

a. **What do you understand from hash functions ? Discuss the working of Secure Hash Algorithm (SHA) in message authentication.**

Ans. Refer Q. 3.14, Page 3–14D, Unit-3.

b. **Explain the digital signatures. Also give a detail description of Elgamal digital signature techniques.**

Ans. Refer Q. 3.17, Page 3–16D, Unit-3.

6. Attempt any **one** part of the following : (10 × 1 = 10)

a. **Discuss X.509 certificates in detail. What is the role of X.509 certificates in cryptography ?**

Ans. Refer Q. 4.11, Page 4–13D, Unit-4.

b. **What is electronic mail security ? Provide the application of Pretty Good Privacy (PGP) in transaction authentication.**

Ans. Refer Q. 4.12, Page 4–14D, Unit-4.

7. Attempt any **one** part of the following : (10 × 1 = 10)

a. **Explain Secure Electronic Transaction (SET) in internet protocol security in detail.**

Ans. Refer Q. 5.13, Page 5–12D, Unit-5.

b. **What do mean by system security ? Also discuss viruses and related threats to system security ?**

Ans. Refer Q. 5.16, Page 5–15D, Unit-5.

☺☺☺

B. Tech.
(SEM. VII) ODD SEMESTER THEORY EXAMINATION, 2019-20
CRYPTOGRAPHY AND NETWORK SECURITY

Time : 3 Hours **Max. Marks : 70**

Note : Attempt all sections. If require any missing data; then choose suitably.

Section-A

1. Attempt **all** questions in brief. **(2 × 7 = 14)**

a. Explain active and passive attack.

Ans. Refer Q. 1.3, Page SQ–1D, Unit-1, Two Marks Questions.

b. State Fermat's theorem.

Ans. Refer Q. 2.9, Page 2–8D, Unit-2.

c. Specify the benefits of IPSec.

Ans. Benefits of IPsec :

1. Reduced key negotiation overhead and simplified maintenance by supporting the Internet Key Exchange (IKE) protocol.
2. Good compatibility.
3. Encryption on a per-packet rather than per-flow basis.

d. Determine the GCD (24561, 17892) using Euclid's Algorithm.

Ans. Refer Q. 2.7, Page SQ–5D, Unit-2, Two Marks Questions.

Answer : GCD (24561, 17892) = 9

e. Why is trapdoor one way function used ?

Ans. Trapdoor one way function is used for single transfer of information from one user to another.

f. Explain role of compression function in hash function.

Ans. A compression function takes two fixed size input, a chainir and a message and returns a fixed size value.

g. What are the services provided by the PGP ?

Ans. Refer Q. 4.13, Page SQ–12D, Unit-4, Two Marks Questior

Section-B

2. Attempt any **three** of the following : **(7**

a. Perform encryption and decryption using hill cip the following message PEN and key ACTIVATED.

Ans. Plaintext : PEN

Key : ACTIVATED

$$\text{Key } (K) = \begin{bmatrix} 0 & 2 & 19 \\ 8 & 21 & 0 \\ 19 & 4 & 3 \end{bmatrix}$$

Plaintext (*P*) is represented in vector form as $\begin{bmatrix} 15 \\ 4 \\ 13 \end{bmatrix}$

$$C = KP \bmod 26$$

$$= \begin{bmatrix} 0 & 2 & 19 \\ 8 & 21 & 0 \\ 19 & 4 & 3 \end{bmatrix} \begin{bmatrix} 15 \\ 4 \\ 13 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 255 \\ 204 \\ 340 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 21 \\ 22 \\ 2 \end{bmatrix} = \text{VWC}$$

For plaintext PEN, ciphertext is VWC.

b. Explain MD5 processing of a single 512 bit block.

Ans. Refer Q. 3.4, Page 3–5D, Unit-3.

**c. Analyze various types of virus and its counter mea

Ans. **Various types of virus :**

1. **Parasitic virus :** This virus attaches itself to executable files and keeps replicating whenever the infected file is executed, the virus looks for other executable files to attach itself and spread.
2. **Memory-resident virus :** This virus first attaches itself to an area of the main memory and then infects every executable program.
3. **Boot sector virus :** This virus infects the master boot record of disk and spread on the disk when operating system starts booting the computer.
4. **Stealth virus :** This virus has intelligence built-in, which prevent anti-virus software program from detecting it.
5. **Polymorphic virus :** A virus that keeps its signature on every execution making it very difficult to detect.
6. **Metamorphic virus :** In addition to changing its signature like a polymorphic virus, this type of virus keeps rewriting itself every time, making its detection even harder.

In order to counter measure the threats of virus the user should :

1. Install antivirus applications.
2. Often get the scanned and analyzed data drive.
3. Gaining basic knowledge about the way virus work.
4. Installing basic internet security applications.

d. Explain triple DES and its applications.

Ans. **Triple DES :** Refer Q. 1.20, Page 1–18D, Unit-1.

Application : Triple DES is used in PGP and S/MIME.

e. State and prove the chinese remainder theorem. What are the last two digit of 49^{19} ?

Ans. **Chinese remainder theorem :** Refer Q. 2.15, Page 2–12D, Unit-2.

Numerical :

Let $X = 49^{19}$

Dividing 19 by 4 *i.e.*, 19 mod 4

$= 3$

$X = 49^3$

$= 117649$

Hence, last two digit is 49.

Section-C

3. Attempt any **one** part of the following : **(7 × 1 = 7)**

a. **Explain Elliptic curve cryptography with an example.**

Ans.

1. Elliptical Curve Cryptography (ECC) is a public key encryption technique based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys.
2. This technology can be used in conjunction with most public key encryption methods, such as RSA, and Diffie-Hellman.
3. ECC generates keys through the properties of the elliptic curve equation.
4. An elliptical curve can simply illustrated as a set of points defined by the following equation :

$$y^2 = x^3 + ax + b$$

5. Based on the values given to a and b, this will determine the shape of the curve.
6. Elliptical curve cryptography uses these curves over finite fields to create a secret that only the private key holder is able to unlock.
7. The larger the key size, the larger the curve, and the harder the problem is to solve.

Example : The following procedure allows Aditya and Anjana to securely exchange the value of a point on an elliptic curve, although neither of them initially knows the value of the point :

1. Aditya and Anjana agree on a finite field F_q, an elliptic curve E/F_q, and a point $P \in E(F_q)$.
2. Aditya selects a secret integer a and computes the point $A = [a] P \in E(F_q)$.
3. Anjana selects a secret integer b and computes the point $B = [b] P \in E(F_q)$.
4. Aditya and Anjana exchange the values of A and B over a possibly insecure communication line.
5. Aditya computes $[a] B$ and Anjana computes $[b] A$. They have now shared the value of the point $[ab] P$.

b. **Find the secret key shared between user A and user B using Diffie-Hellman algorithm for the following :**

$q = 353$, α(primitive root) $= 3$, $X_A = 45$ and $X_B = 50$.

Ans. Refer Q. 4.5, Page 4–5D, Unit-4.

Answer : $Y_A = 3^{45} \bmod 353 = 143$

$$Y_B = 3^{50} \bmod 353 = 155$$
$$K = 197$$

4. Attempt any **one** part of the following : **(7 × 1 = 7)**

a. Explain SHA2 in detail with diagram.

Ans. Refer Q. 3.9, Page 3–10D, Unit-3.

b. Explain the concept of digital signature algorithm with key generation and verification in detail.

Ans. **Digital signature algorithm :** Refer Q. 3.17, Page 3–16D, Unit-3.

Key generation : Key generation has two phases :

1. **Parameter generation :** The first phase is a choice of algorithm parameter which may be shared between different users of the system :
   i. Choose an approved cryptographic hash function H with output length H bits. If H is greater than the modulus length N, only the leftmost N bits of the hash output are used.
   ii. Choose a key length L. The original DSS constrained to be a multiple of 64 between 512 and 1024 inclusive.
   iii. Choose the modulus length N such that $N < L$ and $N \leq H$.
   iv. Choose an N-bit prime q.
   v. Choose an L-bit prime p such that $p - 1$ is a multiple of q.
   vi. Choose an integer h randomly from $\{h... (p-2)\}$.
   vii. Compute $g = h^{(p-1)/q} \bmod p$. This modular exponentiation can be computed efficiently even if the values are large.
   viii. The algorithm parameters are (p, q, g). These may be shared between different users of the system.
2. **Per-user keys :** Given a set of parameters, the second phase computes the key pair for a single user :
   i. Choose an integer x randomly from $\{1...(p-1)\}$.
   ii. Compute $y = g^x \bmod p$.

   Where x is the private key and y is the public key.

   Verifying : Refer Q. 3.19, Page 3–18D, Unit-3.

5. Attempt any **one** part of the following : **(7 × 1 = 7)**

a. Explain Secure Electronic Transaction (SET) protocol with their components.

Ans. **SET :** Refer Q. 5.13, Page 5–12D, Unit-5.

Components : Refer Q. 5.14, Page 5–13D, Unit-5.

b. Explain IDS in detail with suitable example.

Ans.

1. An Intrusion Detection System (IDS) is a network security technology originally built for detecting vulnerability exploits against a target application or computer.
2. Intrusion Prevention Systems (IPS) extended IDS solutions by adding the ability to block threats in addition to detecting them and has become the dominant deployment option for IDS/IPS technologies.
3. An IDS needs only to detect threats and as such is placed out-of-band on the network infrastructure, *i.e.*, it is not in the true real-time communication path between the sender and receiver of information.
4. IDS solutions will often take advantage of a SPAN (Switched Port Analyzer) port to analyze a copy of the inline traffic stream.
5. The IDS monitors traffic and report its results to an administrator, but cannot automatically take action to prevent a detected exploit from taking over the system.

Example of IDS :

1. Car alarms
2. Fire detectors
3. House alarms
4. Surveillance systems

6. Attempt any **one** part of the following : **(7 × 1 = 7)**

a. Explain in detail about S/MIME.

Ans. Refer Q. 4.13, Page 4–15D, Unit-4.

b. Explain briefly about the architecture and certification mechanism in Kerberos.

Ans. **Architecture of Kerberos :** Refer Q. 4.10, Page 4–11D, Unit-4.

Certification in Kerberos :

1. Kerberos is the authentication protocol. In this protocol user passwords are not used to authenticate with individual services; rather, it uses encrypted tickets generated by a Key Distribution Center (KDC).
2. The KDC offers authentication and ticket-granting services.

3. These mechanisms serve two ticket types to clients *i.e.*, ticket-granting and individual service tickets.
4. The TGT is used to request service tickets, which are used to access individual applications.

Ticket format :

1. Kerberos tickets are ASN.1 encoded and contain a ticket block encrypted using the long-term key of the authentication service (*i.e.*, the KDC master key) or an individual service principal (such as a network service or application).
2. Fig. 1 summarizes kerberos ticket structure, which is encrypted by the KDC using either the authentication service key (in the case of a TGT) or a particular service principal key (in the case of a service ticket).

Start/End/Max/Renew	: 14/07/2014 00 : 26 : 09 ; 14/07/2014 10 : 46 : 09 ; 21/07/2014 00 : 46 : 09
Service Name (02)	: krbtgt : CHOCOLATE.LOCAL ; @CHOCOLATE.LOCAL :
Target Name (02)	: krbtget : CHOCOLATE ; @CHOCOLATE.LOCAL :
Client Name (01)	: Administrator : @CHOCOLATE.LOCAL (CHOCOLATE)
Flags 40e10000	: name_canno initial : renewable ; forwardable
Session Key	: 0 × 00000012

Fig. 1. Kerberos ticket format.

Table 1 lists individual kerberos ticket fields. The first three fields are plaintext (so that the client can cache and manage the ticket), and the remaining ticket block is encrypted.

Table 1. Kerberos ticket fields.

Field	Description
Version number	Kerberos version used by the ticket format
Realm	Name of the realm (domain) that issued the ticket
Server name	The target service principal name and realm
Flags	Options for the ticket (forwardable, renewable, invalid, etc.)

Key	The session key used to encrypt subsequent messages
Client realm	The realm of the requester
Client name	The principal name of the requester
Transited	A first of Kerberos realms if cross-realm authentication is used
Authentication time	The timestamp of the initial authentication event
Start time	The time from which the ticket is valid
End time	The expiry time for the ticket
Renew until	The optional time until which the ticket can be renewed
Client address	Optional list of addresses from which the ticket can be used
Authorization data	Authorization data for the client. This contains the PAC data structure defining the username, domain, and SID values; within MIT Kerberos, this field contains restrictions that should be enforced

7. Attempt any **one** part of the following : **(7 × 1 = 7)**

a. Explain public key infrastructure in detail.

Ans. Refer Q. 4.8, Page 4–9D, Unit-4.

b. Discuss authentication header and ESP in detail with their packet format.

Ans. **Authentication header :** Refer Q. 5.9, Page 5–8D, Unit-5.
ESP : Refer Q. 5.4, Page 5–3D, Unit-5.

☺☺☺

B.Tech.

(SEM. VII) ODD SEMESTER THEORY EXAMINATION, 2020-21

CRYPTOGRAPHY AND NETWORK SECURITY

Time : 3 Hours **Max. Marks : 70**

Note : Attempt **all** sections. If require any missing data; then choose suitably.

SECTION-A

1. Attempt **all** questions in brief. **(2 × 7 = 14)**

a. What do you mean Brute Force Attack ?

Ans. In cryptography, a brute-force attack consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing correctly. The attacker systematically checks all possible passwords and passphrases until the correct one is found.

b. Define CIA ?

Ans. CIA, these three letters stand for confidentiality, integrity, and availability, otherwise known as the CIA triad. Together, these three principles form the cornerstone of any organization's security infrastructure; in fact, they (should) function as goals and objectives for every security program.

c. Define the concept of Confusion and Diffusion ?

Ans. Confusion is employed for making uninformed cipher text whereas Diffusion is employed for increasing the redundancy of the plain text over the foremost a part of the cipher text to create it obscure. The stream cipher solely depends on confusion, or else, diffusion is employed by each stream and block cipher.

d. Find all the primitive roots of 11.

Ans. The primitive roots are 2, 6, 7, 8 (mod 11).

e. Find gcd (24140, 16762) using Euclid's algorithm ?

Ans. Gcd (24140, 16762) = Gcd (16762, 24140 mod 16762)
Gcd (16762, 7378) = Gcd (7378, 16762 mod 7378)
Gcd (7378, 2006) = Gcd (2006, 7378 mod 2006)
Gcd (2006, 1360) = Gcd (1360, 2006 mod 1360)
Gcd (1360, 646) = Gcd (646, 1360 mod 546)
Gcd (646, 68) = Gcd (68, 646 mod 68)
Gcd (68, 34) = Gcd (34, 68 mod 64)
Gcd (34, 0) = 34

f. List out the services provided by the Digital Signature.

Ans. Refer Q. 3.10, Page SQ–8D, Unit-3, Two Marks Question.

g. What are the five principal services provided by PGP ?

Ans. Refer Q. 4.13, Page SQ–12D, Unit-4, Two Marks Question.

SECTION-B

2. Attempt any **three** of the following : (7 × 3 = 21)

a. Explain the Security Attacks with Example.

Ans. Refer Q. 1.1, Page 1–2D, Unit-1.

b. Explain the Structure of DES Algorithm and define the role of Feistel cipher in DES in detail.

Ans. **DES :** Refer Q. 1.17, Page 1–15D, Unit-1.

Role of Feistel cipher in DES :

1. Many ciphers have been created based upon the Feistel structure, the most famous of these is the Data Encryption Standard (DES). DES was based off of the original Lucifer cipher developed by Feistel and Coppersmith.
2. DES uses the Feistel cipher structure with 16 rounds of processing.
3. DES uses a Feistel cipher to achieve confusion and diffusion of bits from the plaintext to the ciphertext.
4. As in any Feistel cipher, the DES round function swaps the left and right side of the inputs, and applies the F function during one of the swaps. That is,

   i. $L_{i+1} = R_i$ ii. $R_{i+1} = L_i \wedge F(R_i)$
5. Like all other Feistel ciphers, the process for decryption in DES follows the exact same steps as encryption.
6. Due to its Feistel structure and uncomplicated logic, DES is relatively easy to implement.

c. Explain symmetric and asymmetric cryptography with the help of diagrammatic representation. And how-to symmetric cryptography is different from asymmetric cryptography.

Ans. **Symmetric Cryptography :**

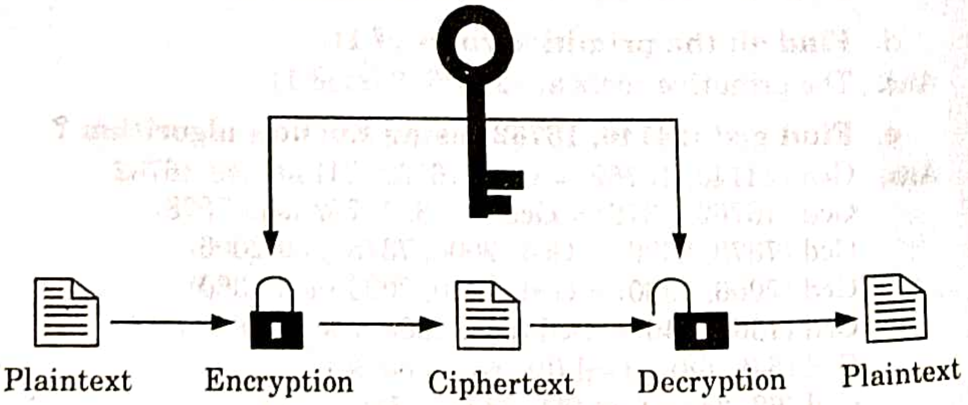


Fig. 1. Symmetric cryptography.

i. In symmetric cryptography, the same key is used for both encrypting and decrypting messages.

ii. Because the entire mechanism is dependent on keeping the key a shared secret it does not scale well.

iii. Symmetric cryptography algorithms can use either block ciphers or stream ciphers.

iv. With block ciphers, a number of bits are encrypted as a single unit. For instance, AES uses a block size of 128 bits with options for three different key lengths - 128, 192, or 256 bits.

v. Although there are key management issues with symmetric encryption, it's faster and functions without a lot of overheads on network or CPU resources. Therefore, it's often used in combination with asymmetric encryption.

Asymmetric Cryptography :

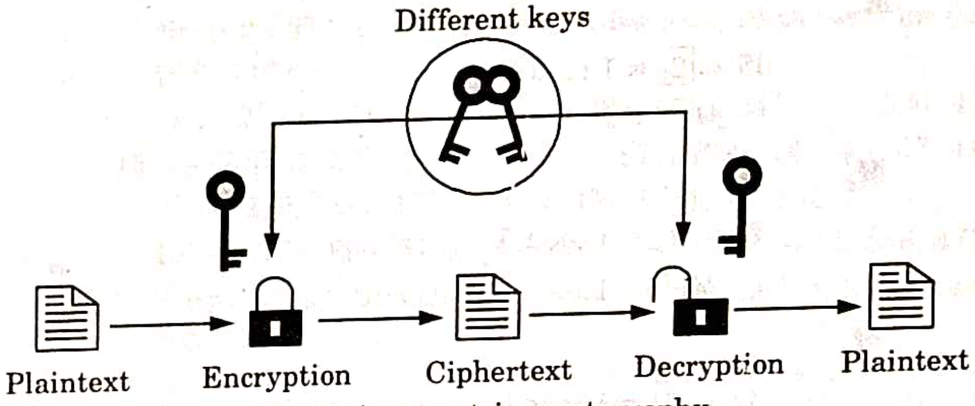


Fig. 2. Asymmetric cryptography.

i. Asymmetric cryptography uses a pair of related keys - a public and a private key.

ii. The public key, which is accessible to everyone, is what's used to encrypt a plaintext message before sending it.

iii. To decrypt and read this message, you need to hold the private key. The public and the private keys are mathematically related, but the private key cannot be derived from it.

iv. In asymmetric cryptography the private key is only shared with the key's initiator since its security needs to be maintained.

v. Asymmetric cryptography is a more complicated process so the time required is greater. However, it offers a higher level of security since the private key is not meant to be shared and is kept a secret.

vi. It is a considerably more scalable technique.

Difference : Refer Q. 4.2, Page 4–2D, Unit-4.

d. State Chinese remainder theorem and find *X* for the given set of congruent equations using CRT: *X* = 2 (mod 3), *X* = 3 (mod 5), *X* = 2 (mod 7).

Ans. Refer Q. 2.15, Page 2–12D, Unit-2.

Numerical :

$$X = 2 \pmod 3$$

$$X = 3 \pmod 5$$
$$X = 2 \pmod 7$$
$$a_1 = 2, a_2 = 3, a_3 = 2$$
$$m_1 = 3, m_2 = 5, m_3 = 7$$

Step 1 : $M = 3 \times 5 \times 7 = 105$

Step 2 : $M_1 = 105/3 = 35$

$M_2 = 105/5 = 21$

$M_3 = 105/7 = 15$

Step 3 : Finding the multiplicative inverse

$$M_1 \times M_1^{-1} \equiv 1 \bmod 3$$
$$M_2 \times M_2^{-1} \equiv 1 \bmod 5$$
$$M_3 \times M_3^{-1} \equiv 1 \bmod 7$$

Therefore,

M_1^{-1}

$$35 \times \boxed{2} \equiv 1 \bmod 3$$
$$M_1^{-1} = 2$$

M_2^{-1}

$$21 \times \boxed{1} \equiv 1 \bmod 5$$
$$M_2^{-1} = 1$$

M_3^{-1}

$$15 \times \boxed{1} \equiv 1 \bmod 7$$
$$M_3^{-1} = 1$$

Step 4 : $x = (2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1) \bmod 1$

$x = (140 + 63 + 30) \bmod 105$

$x = 233 \bmod 105$

$x = 23$

e. Describe RSA algorithm. Suppose alice and bob uses public key cryptosystem using RSA, the two prime no $P = 13$ and $q = 17$ and $e = 7$ the find out the decryption k d and Perform the encryption and decryption of t message "CRYPTOGRAPHY" Using 00 to 25 for letters A Z.

Ans. RSA : Refer Q. 2.23, Page 2–18D, Unit-2.

Numerical :

Step 1 : $p = 13, \; q = 17$

Step 2 : $n = p \times q$

$= 13 \times 17 = 221$

Step 3 : Calculate $\phi(n)$

$$\phi(n) = (p - 1)(q - 1)$$
$$= (13 - 1)(17 - 1) = 12 \times 16 = 192$$

Step 4 : Determined d

$$de \equiv 1 \pmod{192}$$
$$d = e^{-1} \bmod 192$$

q	r_1	r_2	r	t_1	t_2	t
27	192	7	1	0	1	– 27
7	7	1	0	1	– 27	126
	1	0		– 27	126	

$d = -27 \bmod 126$ $\quad(\because \quad 126 - 27 = 99)$

$= 99$

Encryption and decryption of 'CRYPTOGRAPHY' :

Step 1 :	C	R	Y	P	T	O	G	R	A	P	H	Y
	2	17	24	15	19	14	6	17	0	15	7	24

Step 2 : The next step is to raise each of these numbers to the power of $e = 7$.

i.e., $2^7 \rightarrow (128)$, $17^7 \rightarrow (410, 338, 673)$, $24^7 \rightarrow (4, 586, 471, 424)$, $15^7 \rightarrow (170, 859, 375)$, $19^7 \rightarrow (893, 871, 739)$, $14^7 \rightarrow (105, 413, 504)$, $6^7 \rightarrow (279, 936)$, $17^7 \rightarrow (410, 338, 673)$, $0^7 \rightarrow 0$, $15^7 \rightarrow (170, 859, 375)$, $7^7 \rightarrow (823, 543)$, $24^7 \rightarrow (4, 586, 471, 424)$

Step 3 : Then find the remainders when each of these numbers is divided by $n = 221$.

$(2^7 \rightarrow 128)$, $(17^7 \rightarrow 17)$, $(24^7 \rightarrow 80)$, $(15^7 \rightarrow 76)$, $(19^7 \rightarrow 111)$, $(14^7 \rightarrow 40)$, $(6^7 \rightarrow 150)$, $(17^7 \rightarrow 17)$, $(0^7 \rightarrow 0)$, $(15^7 \rightarrow 76)$, $(7^7 \rightarrow 97)$, $(24^7 \rightarrow 80)$

Therefore, the encrypted message to be sent is :

128 17 80 76 111 40 150 17 0 76 97 80

For decryption, we use '*d*' instead of '*e*' :

Step 1 : Starting with the encrypted message :

128 17 80 76 111 40 150 17 0 76 97 80

Step 2 : Raising each number to the power $d = 99$

$(128^{99} \rightarrow 4.109481\text{E} + 208)$, $(17^{99} \rightarrow 6.522937\text{E} + 121)$,
$(80^{99} \rightarrow 2.546295\text{E} + 188)$, $(76^{99} \rightarrow 1.586886\text{E} + 186)$,
$(111^{99} \rightarrow 3.068845\text{E} + 202)$, $(40^{99} \rightarrow 4.017345\text{E} + 158)$,
$(150^{99} \rightarrow 2.710408\text{E} + 215)$, $(17^{99} \rightarrow 6.522937\text{E} + 121)$,
$(0^{99} \rightarrow 0)$, $(76^{99} \rightarrow 1.586886\text{E} + 186)$, $(97^{99} \rightarrow 4.90232\text{E} + 196)$,
$(80^{99} \rightarrow 2.546295\text{E} + 188)$

Step 3 : Finding the remainders when each number is divided by $n = 221$.

$(128^{99} \rightarrow 23)$, $(17^{99} \rightarrow 76)$, $(80^{99} \rightarrow 60)$, $(76^{99} \rightarrow 67)$

$(111^{99} \rightarrow 156)$, $(40^{99} \rightarrow 180)$, $(150^{99} \rightarrow 113)$, $(17^{99} \rightarrow 76)$

$(0^{99} \rightarrow 0)$, $(76^{99} \rightarrow 67)$, $(97^{99} \rightarrow 138)$, $(80^{99} \rightarrow 60)$

Therefore,
The original message is
23 76 60 67 156 180 113 76 23 76 60 67 156 180 113 76 0 67 138 60

SECTION-C

3. Attempt any one part of the following : (7 × 1 = 7)

a. **Explain Block modes of operation and also explain the Electronic Code Book (ECB) mode is not a secured mode of encryption and highlight the problems with this mode.**

Ans. **Block cipher modes of operation :** Block cipher is an encryption algorithm that takes a fixed size of input say b bits and produces a ciphertext of b bits again. If the input is larger than b bits it can be divided further. For different applications and uses, there are several modes of operations for a block cipher.

ECB is not a secured mode of encryption and its problems :

1. ECB is the simplest and weakest, because repeating plaintext generates repeating ciphertext. As a result, anyone can easily derive the secret keys to break the encryption and decrypt the ciphertext. ECB may also leave obvious plaintext patterns in the resulting ciphertext.
2. ECB uses simple substitution rather than an initialization vector or chaining, this is its biggest drawback. Two identical blocks of plaintext result in two correspondingly identical blocks of ciphertext, making it cryptologically weak.
3. ECB is not good to use with small block sizes—say, for blocks smaller than 40 bits—and identical encryptinn modes. In small block sizes some words and phrases may be reused often in the plaintext. This means that the ciphertext may carry (and betray) patterns from the same plaintext, and the same repetitive part-blocks of ciphertext can emerge.

b. **Give a real-life example where both confidentiality and integrity are needed. Explain why encryption alone does not provide integrity of information.**

Ans. Confidentiality and Integrity are needed simultaneously in many applications. The most common example I can think of is the SSL handshake. Here the need for integrity arises for the fact that the client has to make sure that the server's certificate has not been tampered with.

SSL : Refer Q. 5.12, Page 5–10D, Unit-5.

Encryption alone does not provide integrity of information : Encryption is the process of scrambling data so that it can't be unscrambled without access to a key and knowledge of the algorithm. It does not guarantee that the data hasn't changed; only that it's been kept private. Only those with access to the right key can unscramble the data.

4. Attempt any one part of the following : **(7 × 1 = 7)**

a. **Compare Substitution and Transposition techniques.**

Ans. Refer Q. 1.5, Page 1–5D, Unit-1.

b. **Encrypt the following using play fair cipher using the keyword : MONARCHY. "SWARAJ IS MY BIRTH RIGHT". Use *X* as blank space.**

Ans. Matrix :

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/ J	K
L	P	Q	S	T
U	V	W	X	Z

SW AR AJ IS MY BI RT HR IG HT SW: Is in different row and column

Therefore s=>Q w=>X

AR : In same Row. Therefore A=>R R=>M

AJ: In same column. Therefore A=>B J=>S

IS : In same column. Therefore I=>s S=>x

My : In different row and column M=>N y=>c

BI : In same column B=>I I=>s

RT : In same column R=>d t=>z

HR : In different row and column H=>d R=>o

IG : In same Row i=>k g=>I

HT In different row and column H=>D T=>P

therefore : SWARAJ IS MY BIRTH RIGHT is written as QXRMBS SX NC ISDZD OKIDP

5. Attempt any one part of the following : **(7 × 1 = 7)**

a. **Define Primality Test and also explain Miller Rabin Algorithm using base 2 to test whether the number 341 is composite or not ?**

Ans. Primality Test : Refer Q. 2.12, Page 2–10D, Unit-2.

Miller-Rabin algorithm : Refer Q. 2.13, Page 2–10D, Unit-2.

Numerical :

Let $n = 341$

Calculate $n - 1 = 340$

$= 85 \times 2 \times 2$

we have $2^{85} = 32 \neq 1$

$2^{170} = 1 \neq -1$

Hence, 341 fails the Miller-Rabin test for base 2. Consequently, 341 is composite number.

b. **Explain AES algorithm. What is the difference between the AES decryption algorithm and the DES algorithm ?**

Ans. ASE : Refer Q. 2.7, Page 2–6D, Unit-2.

Difference : Refer Q. 2.27, Page 2–22D, Unit-2.

6. Attempt any one part of the following : (7 × 1 = 7)

a. **Explain the Kerberos protocol for key distribution? Explain the functionality of each step.**

Ans. Kerberos : Refer Q. 4.9, Page 4–10D, Unit-4.

Functionality of each step :

Following are the component of kerberos :

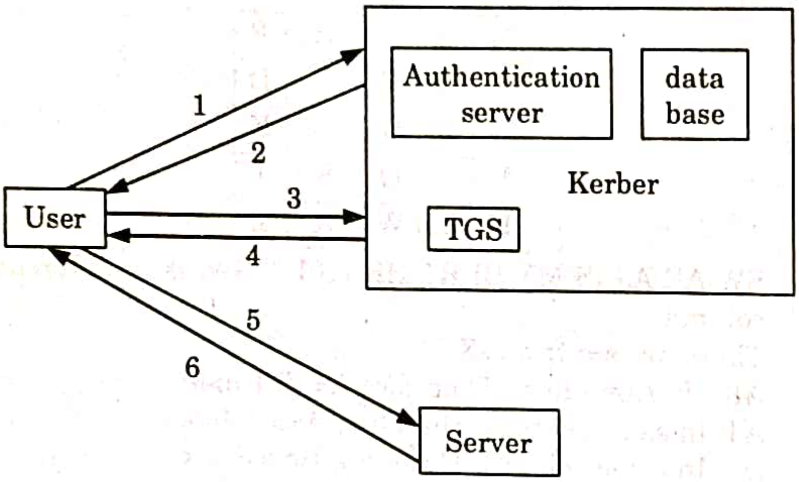


Fig. 3.

1. **Authentication Server (AS) :** The Authentication Server performs the initial authentication and ticket for Ticket Granting Service.

Database : The Authentication Server verifies access rights of users in database.

Ticket Granting Server (TGS) : The Ticket Granting Server issues the ticket for the Server.

Step 1 : User logon and request services on host. Thus user requests for ticket-granting-service.

Step 2 : Authentication Server verifies user's access right using database and then gives ticket-granting-ticket and session key. Results are encrypted using Password of user.

Step 3 : Decryption of message is done using the password then send the ticket to Ticket Granting Server. The Ticket contains authenticators like user name and network address.

Step 4 : Ticket Granting Server decrypts the ticket send by User and authenticator verifies the request then creates the ticket for requesting services from the Server.

Step 5 : User sends the Ticket and Authenticator to the Server.

Step 6 : Server verifies the Ticket and authenticators then generate the access to the service. After this User can access the services.

b. **How does worms and viruses compare? Describe the components of the virus and how does it protect from anti-virus software's ?**

Ans. **Comparison :**

S. No.	Worms	Viruses
1.	A Worm is a form of malware that replicates itself and can spread to different computers via network.	A Virus is a malicious executable code attached to another executable file which can be harmless or can modify or delete data.
2.	The main objective of worms is to eat the system resources.	The main objective of viruses is to modify the information.
3.	It doesn't needs a host to replicate from one computer to another.	It requires a host for spreading.
4.	It is less harmful as compared.	It is more harmful.
5.	Worms can be detected and removed by the Antivirus and firewall.	Antivirus software is used for protection against viruses.
6.	Worms can be controlled by remote.	Viruses can't be controlled by remote.
7.	Worms are executed via weaknesses in the system.	Viruses are executed via executable files.
8.	Internet worms, Instant messaging worms, Email worms, File sharing worms, Internet relay chat (IRC) worms are different types of worms.	Boot sector virus, Direct Action virus, Polymorphic virus, Macro virus, Overwrite virus, File Infector virus are different types of viruses
9.	Examples of worms include Morris worm, storm worm, etc.	Examples of viruses include Creeper, Blaster, Slammer, etc.
10.	It does not need human action to replicate.	It needs human action to replicate.
11.	Its spreading speed is faster.	Its spreading speed is slower as compared.

Components of a virus :

1. Fig. 4 shows the various components of a computer virus.

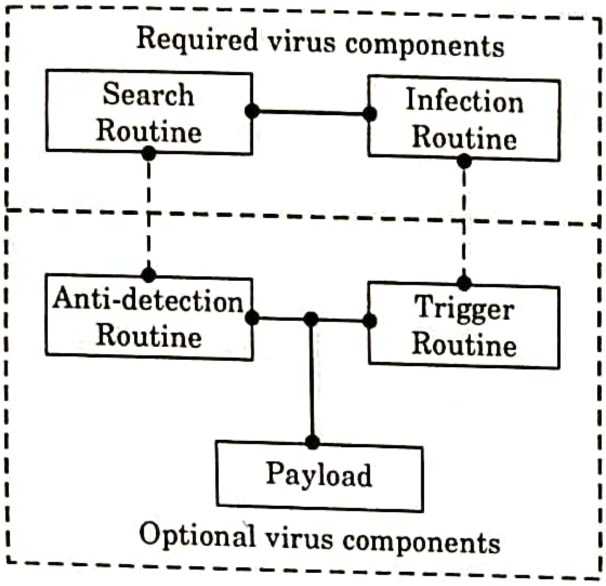


Fig. 4. Virus components.

2. All viruses have some basic common components.
3. All viruses have a search routine and an infection routine.
4. The search routine is responsible for locating new files, disk space, or RAM to infect.
5. The second component of a virus, infection routine, is responsible for copying the virus and attaching it to a suitable host.
6. Most viruses also contain a payload. The purpose of the payload routine might be to erase the hard drive or display a message to the monitor.
7. Many viruses might also have an antidetection routine. Its goal is to help make the virus more stealth-like and avoid detection.
8. Finally, there is the trigger routine. Its goal is to launch the payload at a given date and time.
9. A virus protects itself from antivirus software by using the antidetection routine.

7. Attempt any one part of the following : **(7 × 1 = 7)**

a. What do you mean by SHA1 algorithm ? What basic arithmetical and logical functions are used in SHA ?

Ans. Secure Hash Algorithm 1 (SHA-1) :

1. SHA-1 produces a 160-bit hash value or message digests from the inputted data (data that requires encryption), which resembles the hash value of the MD5 algorithm.

2. It uses 80 rounds of cryptographic operations to encrypt and secure a data object.
3. Some of the protocols that use SHA-1 include :
   i. Transport Layer Security (TLS)
   ii. Secure Sockets Layer (SSL)
   iii. Pretty Good Privacy (PGP)
   iv. Secure Shell (SSH)
   v. Secure/Multipurpose Internet Mail Extensions (S/MIME)
   vi. Internet Protocol Security (IPSec)
4. SHA-1 is commonly used in cryptographic applications and environments where the need for data integrity is high.
5. It is also used to index hash functions and identify data corruption and checksum errors.

Arithmetical and logical functions used in SHA :

The following arithmetical and logical functions are used in SHA :

Arithmetical functions : add, modBit-Ops Left circular shift
Logical functions : AND, OR, NOT and XOR

b. Explain in detail about S/MIME and what is difference between S/MIME and PGP.

Ans. **S/MIME :** Refer Q. 4.13, Page 4–15D, Unit-4.

S. No.	PGP	S/MIME
1.	It is designed for processing the plain texts.	While it is designed to process email as well as many multimedia files.
2.	PGP is less costly as compared to S/MIME.	While S/MIME is comparatively expensive.
3.	PGP is good for personal as well as office use.	While it is good for industrial use.
4.	PGP is less efficient than S/MIME.	While it is more efficient than PGP.
5.	It depends on user key exchange.	Whereas it relies on a hierarchically valid certificate for key exchange.
6.	PGP is comparatively less convenient.	While it is more convenient than PGP due to the secure transformation of all the applications.

7.	PGP contains 4096 public keys.	While it contains only 1024 public keys.
8.	PGP is the standard for strong encryption.	While it is also the standard for strong encryption but has some drawbacks.
9.	PGP is also used in VPNs.	While it is not used in VPNs, it is only used in email services.
10.	PGP uses Diffie-Hellman digital signature.	While it uses Elgamal digital signature.

☺☺☺