CS8792-CRYPTOGRAPHY AND NETWORK SECURITY

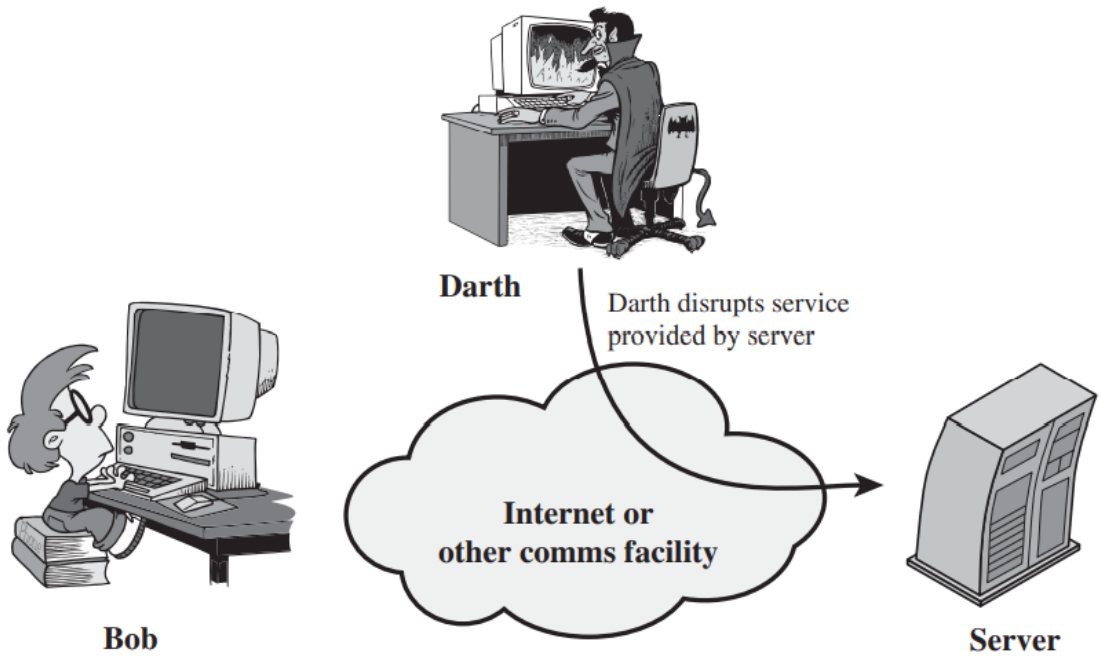
UNIT-I: INTRODUCTION

1.What is meant by Denial of Service [DoS]attack? Is it Active Attack or Passive Attack?[Nov/Dec 2021]

The **denial of service** ***prevents or inhibits*** the normal **use or management of communications facilities.**

Example

An entity may suppress ***all messages directed to a particular destination.***



Denial of service

- It is an **Active Attack**
- Active attacks involve ***some modification of the data stream or the creation of a false stream*** and
- Denial of Service (DoS) can be category of **ActiveAttack**.

2. Let message = "Anna", and k = 3, find the ciphertext using Caesar.[Nov/Dec 2021]

Caesar algorithm

C = E (p,k) = (p+k) mod 26

Let us assign a numerical equivalent to each letter:

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

C=E(A,3)=(0+3)mod 26=d
C=E(N,3)=(13+3)mod 26=16 mod 26=q

Cipher text =dqqd

3.Differentiate active and passive attacks[Apr/May 2019]

On the basis of	Active Attack	Passive attack
Definition	In active attacks, the attacker intercepts the connection and efforts to modify the message's content.	In passive attacks, the attacker observes the messages, then copy and save them and can use it for malicious purposes.
Modification	In an active attack, the attacker modifies the actual information.	In passive attacks, information remains unchanged.
Types	Active attacks involve (i)Masquerade, (ii)Modification of message (iii) Replay (iv) Denial of service.	(i)Release of message contents (ii)traffic analysis
	Easy to detect	Difficult to detect

4.Specify the components of encryption algorithm[Apr/May 2019]

The main components of an encryption system are: \

(1) plaintext (not encrypted message), (2) encryption algorithm (works like a locking mechanism to a safe),

(3) key (works like the safe's combination), and

(4) ciphertext (produced from plaintext message by encryption key).

5.Distinguish between attack and threat?[Nov/Dec 2018]

Threat[2-marks]

A ***potential for violation of security***, because of

(1). Circumstances, (2). Capability, (3). Action or event that **break security** and **cause harm.**
Threat is possible that might ***create Vulnerability***.

Attack[2-marks].

It is an intelligent act that is a deliberate attempt to
(1). **Avoid security services and (2). Violate the security policy of a system.**

6.Calculate the cipher text for the following using one time pad cipher(Perfect secrecy or Vernam Cipher)

Plain Text:ROCK

Keyword:BOTS

Answer

Each **new message** requires **a new key of the same length** as the **new message**.
Such a scheme, known as ***a one-time pad, is unbreakable***.
It produces **random output** that bears **no statistical *relationship*** to the **plaintext.**

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Plain Text	R(17)	O(14)	C(2)	K(10)
Keyword	B(1)	O(14)	T(19)	S(18)
Sum (PT+K)	18	28	21	28
If Sum >25 then 26-sum	S	C(2)	V	C(2)

Cipher Text :SCVC

Vernam Cipher

- One-time pad (OTP), also called Vernam-cipher or the perfect cipher, is a crypto algorithm where plaintext is combined with a random key.
- The key is at least as long as the message or data that must be encrypted.
- Each key is used only once, and both sender and receiver must destroy their key after use.
- There should only be two copies of the key: one for the ***sender*** and one for the ***receiver***.

Vernam Cipher

1. assign a number to each character of the Plain-Text, like (a = 0, b = 1, c = 2, … z = 25). As per given table.

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12
n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

2. Assign a number to each character of the plain-text and the key according to alphabetical order.

Plain Text	I	A	M	A	N	I	N	D	I	A	N
	8	0	12	0	13	8	13	3	8	0	13
Key	A	N	T	I	P	A	K	I	S	T	A
	0	13	19	8	15	0	10	8	18	19	0

3. Add both the number (Corresponding plain-text character number and Key character number).

Plain Text	I	A	M	A	N	I	N	D	I	A	N
	8	0	12	0	13	8	13	3	8	0	13
Key	A	N	T	I	P	A	K	I	S	T	A
	0	13	19	8	15	0	10	8	18	19	0
SUM (P.T. + Key)	8	13	31	8	28	8	23	11	26	19	13

4. Subtract the number from 26 if the added number is grater than 26. otherwise left it. Assign alphabets of numbers, it produce cipher text.

Plain Text	I	A	M	A	N	I	N	D	I	A	N
	8	0	12	0	13	8	13	3	8	0	13
Key	A	N	T	I	P	A	K	I	S	T	A
	0	13	19	8	15	0	10	8	18	19	0
SUM (P.T. + Key)	8	13	31	8	28	8	23	11	26	19	13
SUM – 26 (if SUM > 25)	8	13	5	8	2	8	23	11	0	19	13
Cipher Text	I	N	F	I	C	I	X	L	A	T	N

Cipher Text:INFICIXLATN

7.Define Brute-force attack.

The attacker tries every possible key on a piece of cipher text until an intelligible translation into plaintext is obtained.

On average, half of all possible keys must be tried to achieve success

8.Give an example each for substitution and transposition ciphers.

Or

Define the two basic building blocks of encryption techniques

https://www.youtube.com/watch?v=OWeqP65Ixg8&list=PLzQqHxFtQGydze3lo22YC12IGfL0irVFs&index=15

comparison of substitution and transposition technique

Substitution technique	**Transposition technique**
Changes its identity but retain its position.	Changes its position but retain its identity.
Simple process.	Complex than substitution technique.
Easy to crack the code.	Difficult to crack the code.
Unauthorized users can easily access the data.	Difficult for intruders to access the information.
The time complexity of Encryption and decryption is less.	**The time complexity of Encryption and decryption is high.**
Example: Caesar cipher	Example: Columnar transposition cipher. **Rail fence Cipher**

9. List out the problems of one time pad?[Nov /Dec 2011]

It makes the problem of making large quantities of random keys.

- It also makes the problem of key distribution and protection

10. Define: Replay attack.

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

11.What is the difference between a mono alphabetic and a poly alphabetic cipher?

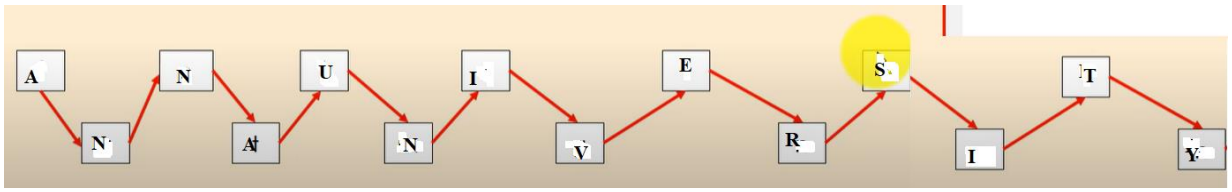
No	Poly Alphabetic	Mono Alphabetic
1	It is more secure in compare to mono-alphabetic.	It is less secure in compare to poly-alphabetic.
2	More than one alphabets are used to substitution.	One single fixed alphabets are used to substitution.
3	In this method, the substitution rule changes continuously from letter to letter according to the elements of the encryption key.	In this method, same substitution rule is used for each substitution.
4	In this method, any one alphabets substitute with different alphabets using Vigenère table.	In this method, for a particular alphabet, only one substitution can be used.

12.Convert the given text "annauniversity" into cipher text using rail fence technique.

Rail Fence Technique

It involves ***writing plain text as a sequence of Diagonals*** and then reading it Row-by-Row to produce cipher text

It is an ***example of transposition***



Cipher text

ANUIESTNANVRIY

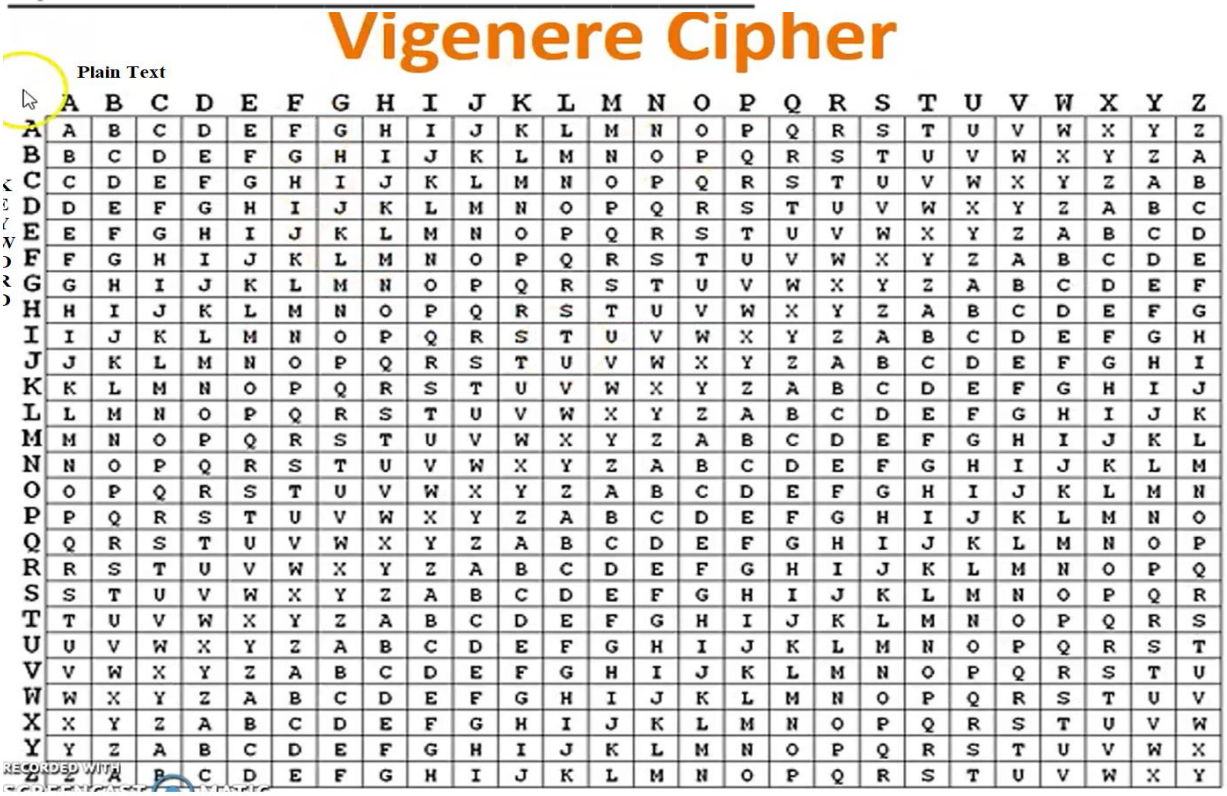
13,Define steganography

Methods of hiding the existence of a message or other data.This is different than cryptography, which hides the meaning of a message but does not hide the message itself.

14. Encrypt the plaintext tobeornottobe using the vigenere cipher for the key value Now.

n	O	w	N	o	w	n	o	W	n	o	w	n
t	O	b	E	o	r	n	o	T	t	o	b	e
g	C	x	R	c	n	a	c	P	g	c	x	r

Key	N	O	W	N	O	W	N	O	W	N	O	W	N
plaintext	t	o	b	e	o	r	n	o	t	t	o	b	e
ciphertext	G	C	X	R	C	N	A	C	P	G	C	X	R



Example

Encrypt the plaintext *welcome to anna university* using the Vigenere cipher for the key value *security*.

Solution

Key	S	E	C	U	R	I	T	Y	S	E	C	U	R	I	T	Y	S	E	C	U	R	I	T
plaintext	w	e	l	c	o	m	e	t	o	a	n	n	a	u	n	i	v	e	r	s	i	t	y
ciphertext	O	I	N	W	F	U	X	R	G	E	P	H	R	C	G	G	N	I	T	M	Z	B	R

15. Explain the avalanche effect. [NOV 2007][Nov 2013][MAY 2016]

If there is a **small change in either the plaintext or the key** should **produce a significant <u>chanige</u>** in **the cipher text**. A change in one of the bit of the plaintext or one bit of the key should produce a change in many bits of the cipher text.

16. What are the two approaches to attacking a cipher?[NOV 2007]

The two to attack a cipher are:

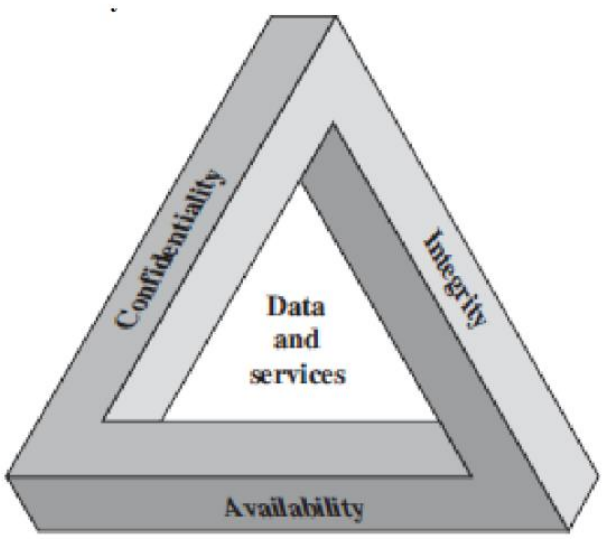
- Cryptanalysis
- Brute-force attack

17.Why is asymmetric cryptography bad for huge data? Specify the reason. (APRIL/MAY 18)

Asymmetric encryption uses **two separate keys** and **more complex *algorithms*** in the encryption and decryption process, which makes it ***<u>slower for encrypting and decrypting large amounts of data.</u>***

18.What are the key principles of security?

Three key objectives of the computer security are **confidentially, integrity and availability**.



1.Confidentiality-Only the intended receiver can understand the information.

Ensures that the information in a computer system and transmitted information are accessible only by authorized parties.

(i)Data confidentiality – assures that private or confidential information is not made available or disclose(make known) to unauthorized individuals.

(ii)Privacy:-

It assures that individuals control what information related to them may be collected and stored.

It also assures that information may be disc by whom and to whom.

2.Integrity [2-marks]

Ensures that only authorized parties are able to modify the stored information and transmitted information.

(i).Data integrity -assures that information and programs are changed only in a

specified and authorized manner.

(ii).System integrity:-

Assures that system performs to proposed functions in an undamaged manner. Free from purposed unauthorized manipulate of the system.

3.Availability-assures that system works promptly and service is not denied to

authorized Users

19.What are the two basic functions used in the encryption algorithm?

1.Substitution 2.Transposition

1.Substitution

In which each element in the plaintext is mapped into another element.

2.Transposition

In which elements in the plaintext are rearranged .No information is lost.

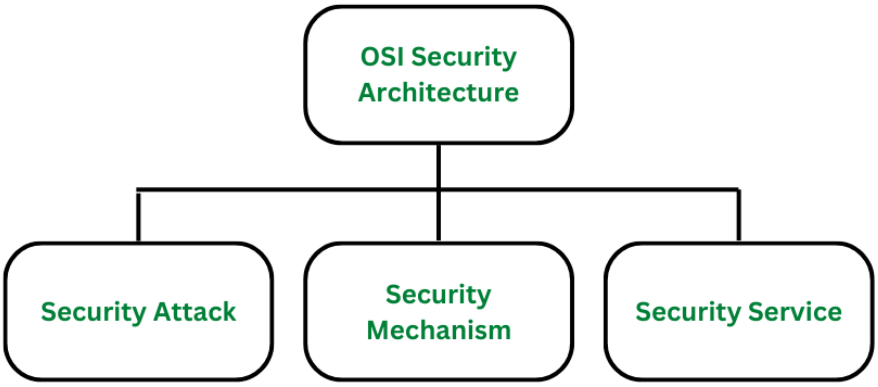
20.List the entities that are to be kept secret in conventional encryption techniques?

Secret Key and encryption algorithm

Part B Questions

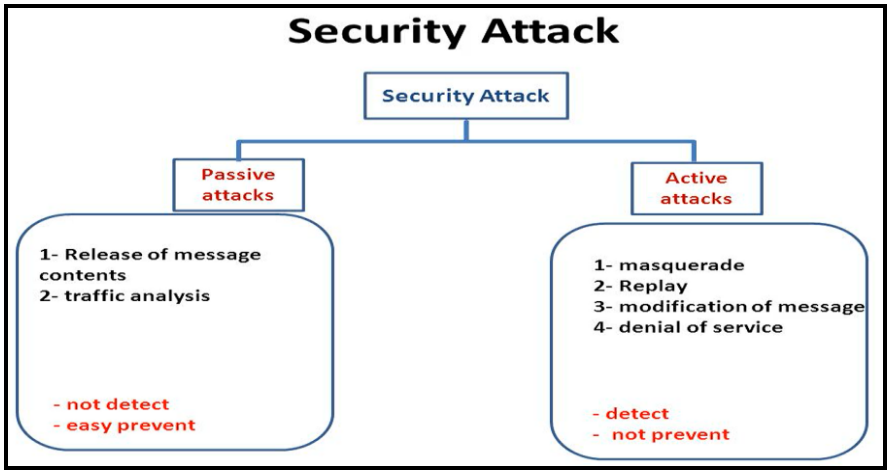
1.(i)Explain OSI Security Architecture model with neat diagram[Nov /Dec 2016]

The **OSI security architecture focuses** on **security attacks, mechanisms, and services**



Definition of ***security attacks, mechanisms, and services***

Threat and Attack –Definition And Difference



(i)Security Attack

Types

1.Passive Attack 2.Active Attack

1.Active Attack

Definition

Types

(i)Masquerade, (ii)Modification of message (iii) Replay (iv) Denial of service.

1.Passive Attack

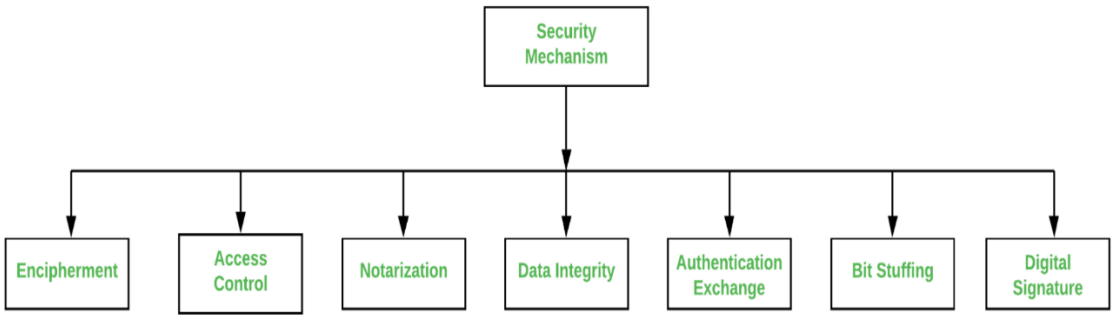
Definition

Types

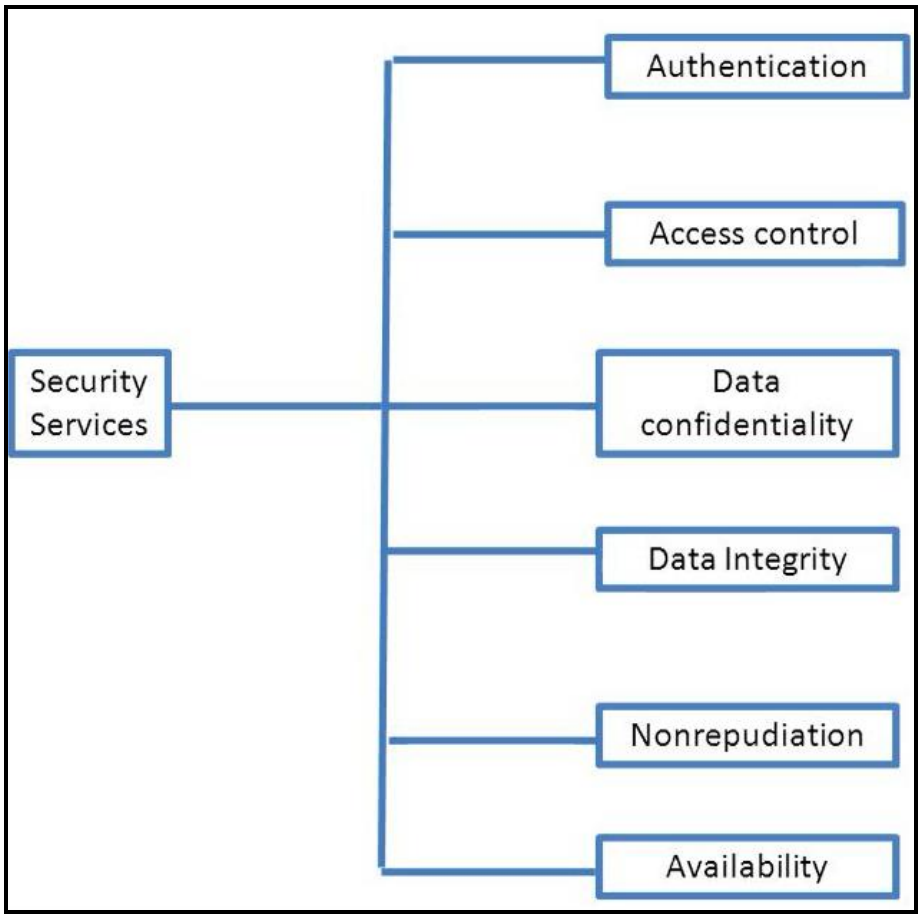
- ❖ Release of message contents
- ❖ Traffic analysis

Difference between Active Attack and passive Attack

(ii)Describe the various security mechanism



Security Services



2.Encrypt the following using play fair cipher using the keyword "MONARCHY."

SWARAJ IS MY BIRTH RIGHT" Use X for blank spaces.(Nov/Dec 17)

SWARAJ IS MY BIRTH RIGHT" Use X for blank spaces. (Nov/Dec 17)

The best known multiple letter encryption cipher is the playfair, which treats digrams in the plaintext as single units and translates these units into cipher text digrams. The playfair algorithm is based on the use of 5x5 matrix of letters constructed using a keyword.

Let the keyword be "monarchy" .

The matrix is constructed by

- Filling in the letters of the keyword from left to right and from top to bottom
- Duplicates are removed
- Remaining unfilled cells of the matrix is filled with remaining alphabets in alphabetical order.

The matrix is 5x5. It can accommodate 25 alphabets. To accommodate the 26th alphabet I and J are counted as one character.

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

Rules for encryption

- Repeating plaintext letters that would fall in the same pair are separated with a filler letter such as 'x'.
- Two plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row circularly following the last. For example, ar is encrypted as RM.
- Two plaintext letters that fall in the same column are each replaced by the letter beneath, with the top element of the column circularly following the last. For example, mu is encrypted as CM.
- Otherwise, each plaintext letter in a pair is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter. Thus, hs becomes BP and ea becomes IM (or JM, as the encipherer wishes).

Keyword

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

Plain Text: SWARAJ IS MY BIRTH RIGHT

Insert X in Blank Spaces: SW AR AJ XI SX MY XB IR TH XR IG HT

SW – QX [Different row different column]
AR - RM [Same Row]
AJ - BS [Same column]
XI - AS [Same column]
SX - XA [Same column]
MY - NC [Different row different column]
XB – AI or AJ [Same column]
IR – AK [Different row different column]
TH – DP [Different row different column]
XR – AZ [Different row different column]
IG – KI or KJ [Same row]
HT – DP [Different row different column]

Plain Text Pairs	SW	AR	AJ	XI	SX	MY	XB	IR	TH	XR	IG	HT
Rule No	5	3	4	4	4	5	4	5	5	5	3	5
Cipher Text Encryption Process	QX	RM	BS	AS	XA	NC	AI	AK	DP	AZ	KI	DP

Cipher Text QX RM BS AS XA NC AI AK DP AZ KI DP

3.Describe
(i)Play fair Cipher
(ii)Railfence Cipher
(iii)Vignere Cipher

Answer

(i)Play fair Cipher

- Definition
- Algorithm
- Example
- Result →Plain Text
  - Cipher etxt

ii)Railfence Cipher

- Definition
- Algorithm
- Example

iii)Vignere Cipher

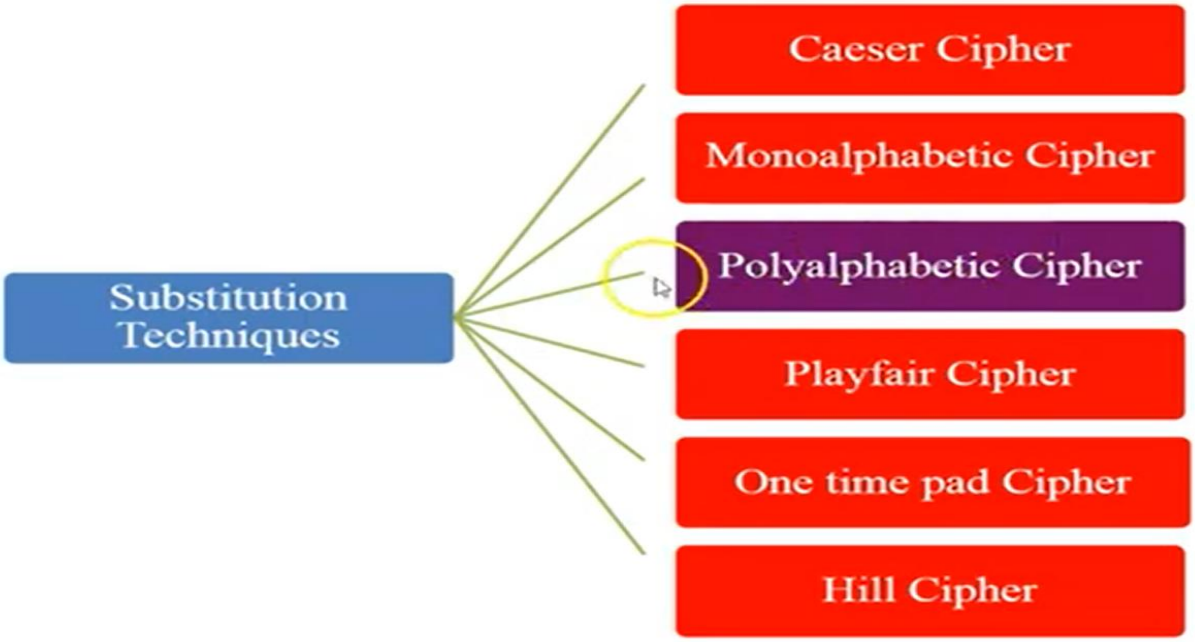
- Definition
- Algorithm
- Table

❖ Example

4.Explain classical encryption techniques with symmetric cipher and Hill Cipher model?

There are basically two types of symmetric cipher :

- ❑ Substitution Cipher
- ❑ Transposition Cipher



5.(i)What is steganography?Describe the various techniques used in Steganography?

- ❖ Definition
- ❖ Example
- ❖ Techniques used
  - o Character Marking
  - o Invisible links
  - o Pin Punctures
  - o Type written correction ribbon
- ❖ Advantages and disadvantages

(ii)What is monoalphabetic cipher?Examine how it differs from Caesar Cipher?

Monoalphabetic cipher is **one where each symbol in plain text is mapped to a fixed symbol in cipher text**.

In Caesar cipher, it can see that it is simply for a hacker to crack the key as Caesar cipher supports only 25 keys in all. This pit is covered by utilizing Monoalphabetic cipher. **In Monoalphabetic cipher, the substitute characters symbols supports a random permutation of 26 letters of the alphabet**. 26!

Caesar Cipher

- Definiton
- Example

Drawbacks

Easy to break because the key size is fixed.

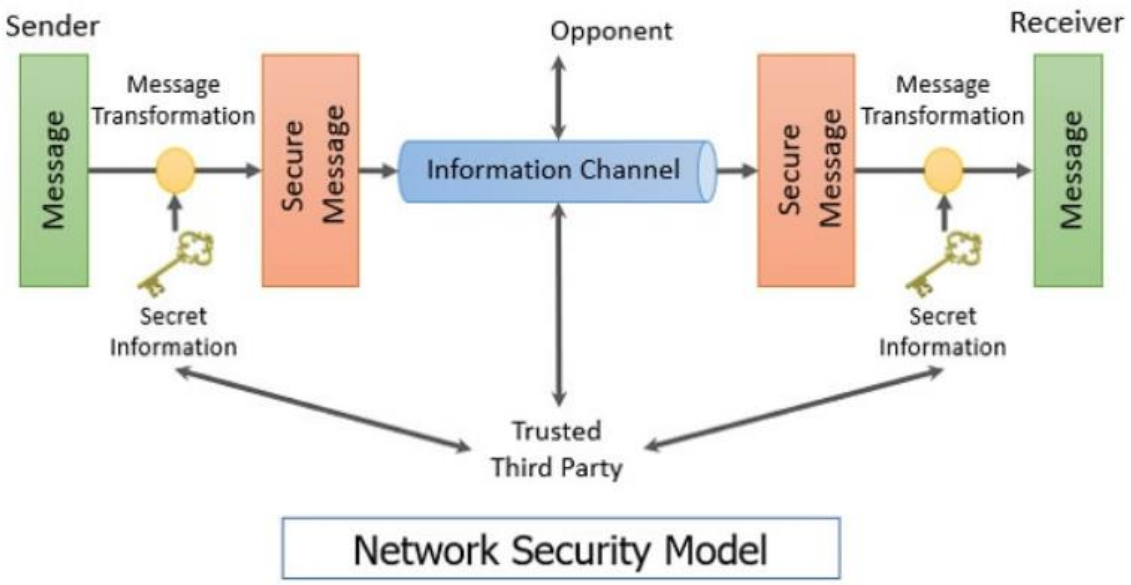
C=(PT+3)MOD 26

MonaAlphabetic Cipher

- Why Mona alphabetic cipher
- Example
- Difference
- Drawbacks

C=(PT+K)MOD 26

6.Explain the network security model and its importance with a neat block diagram?



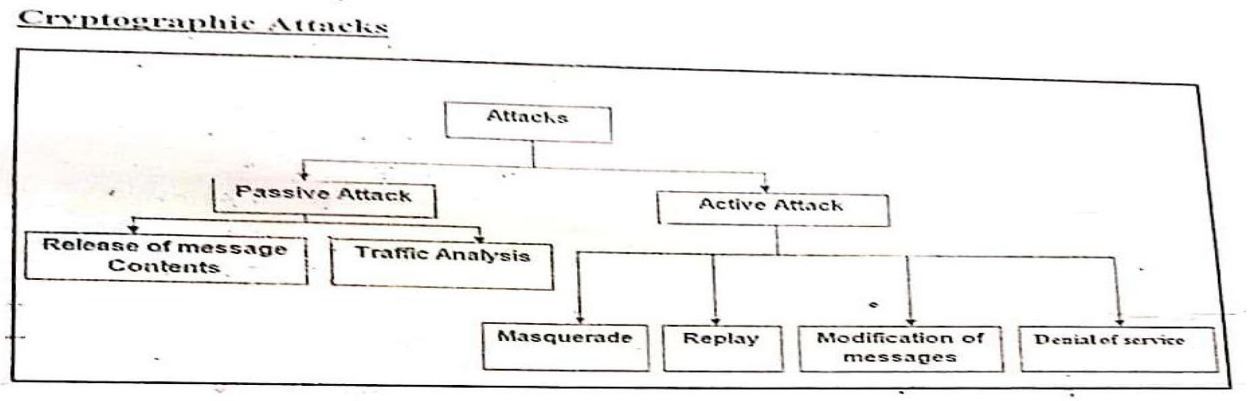
- Two Components for providing Network Security Model
  - Security related transformation
  - Security information
- Trusted Third party
- Responsibility of trusted third party

- Four basic task to design a particular security service
- Network Access Security Model
- Two types of Threats
- Security Mechanisms
  - Major Procees of Secuirty Mechanisms
    - Gate Keeper
    - Variety of internal Controls

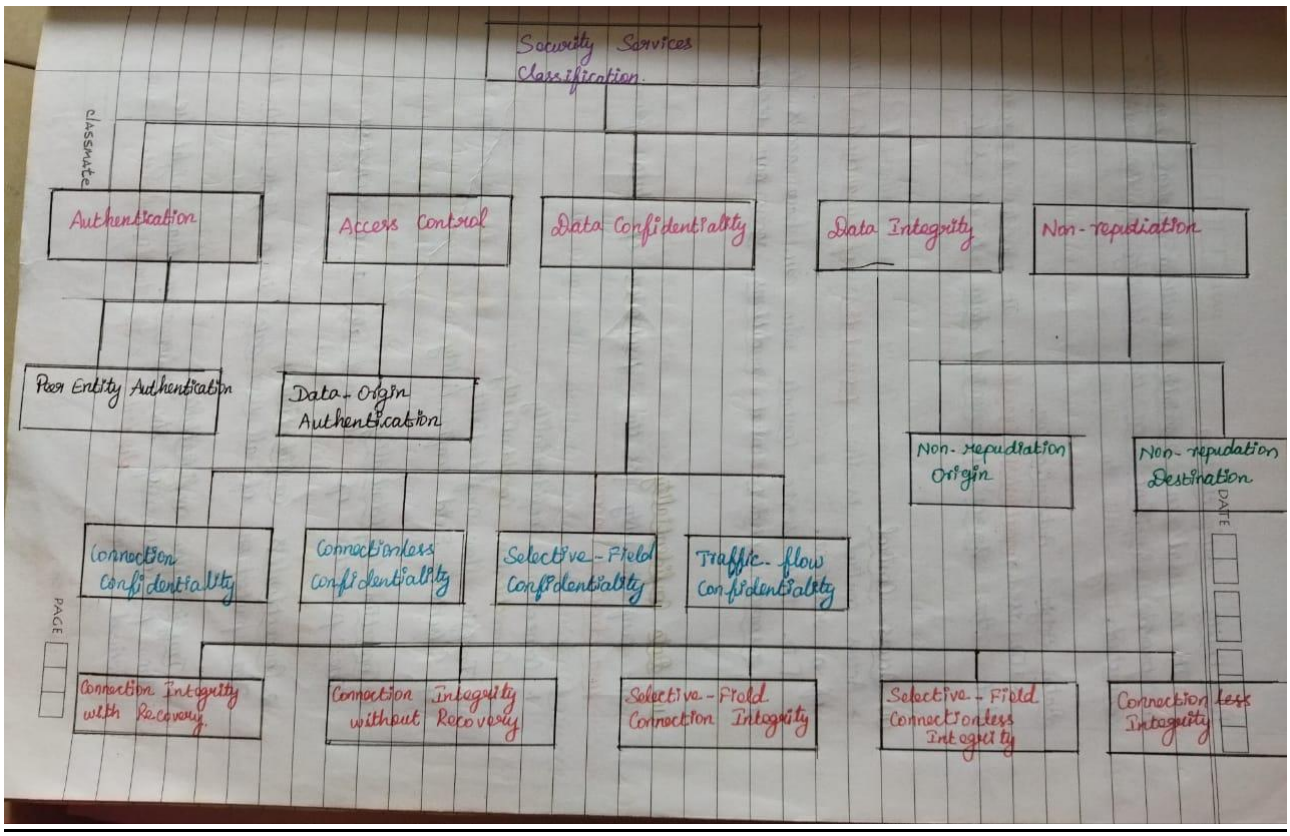
7.Write a note on different types of security attacks and services in detail?

Security attacks

Definition



Security Services



8.Demonstrate encryption and decryption process in hill cipher. Consider m = "sh" and key = hill".

Define Hill Cipher

- Hill Cipher is **polyalphabetic** substitution techniques.

- Hill Cipher can work seamlessly with **digraphs (two-letter blocks), trigraphs (three-letter blocks), or any multiple-sized blocks** for building a uniform cipher.
- Hill Cipher is based on a **mathematical topic of linear Algebra** and t**he sophisticated use of matrices** in general, as well as rules for **modulo arithmetic**

Hill Cipher can work seamlessly **with digraphs (two-letter blocks), trigraphs (three-letter blocks)**, or any ***multiple-sized blocks for building a uniform cipher***.

Encryption

Step1

Remove the punctuation marks or space in the given plain text

Step 2:Group the plaintext into pairs

If we have odd number of letters then repeat the last letter

If **key is 2x2 matrix** ,then the plaintext is **divided into 2 characters**

If **key is 3x3 matrix** ,then the plaintext is **divided into 3 characters**

Step 3: Replace **each letters** by the number corresponding to its position in the alphabet

Step 4: Convert each pair of letters into plaintext vectors

Step 5:Convert the plaintext vectors into ciphertext vectors

5.1 **Multiply the key matrix** by the **plain text vector**.

5.2 **Replace** each new vector by its **modulo 26**

Step 6: Convert each entry in the ciphertext vector into its corresponding position in the alphabet

Step 7:Align the letters in a single line without spaces.

Encryption

m = sh
key = hill

a	b	c	d	e	f	g	h	i	j	k	l	m	n
0	1	2	3	4	5	6	7	8	9	10	11	12	13

o	p	q	r	s	t	u	v	w	x	y	z
14	15	16	17	18	19	20	21	22	23	24	25

Encryption

s = 18
h = 7

hill
h → 7 i → 8
l → 11 l → 11

$$\text{keyword} = \begin{pmatrix} H & I \\ L & L \end{pmatrix} = \begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}$$

$$\text{Message} = \begin{pmatrix} S \\ h \end{pmatrix} = \begin{pmatrix} 18 \\ 7 \end{pmatrix}$$

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}\begin{pmatrix} 18 \\ 7 \end{pmatrix} = \begin{pmatrix} 7\times18+8\times7 \\ 18\times11+11\times7 \end{pmatrix} = \begin{pmatrix} 182 \\ 275 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 0 \\ 15 \end{pmatrix} = \begin{pmatrix} A \\ P \end{pmatrix}$$

$\boxed{\text{sh} = \text{ap}}$

classmate

PAGE

Decryption

Step 1: Find the Multiplicative Inverse of the Determinant

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc$$

$$\begin{vmatrix} 7 & 8 \\ 11 & 11 \end{vmatrix} = 77 - 88 = -11 = 15 \bmod 26 = 15$$

$$dd^{-1} = 1 \bmod 26$$
$$15 \times 7 = 1 \bmod 26$$

Step 2: Find the adjacent matrix.

$$\text{adj} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

$$\text{adj} \begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} = \begin{pmatrix} 11 & -8 \\ -11 & 7 \end{pmatrix} = \begin{pmatrix} 11 & 18 \\ 15 & 7 \end{pmatrix}$$

Step 3: Multiply the multiplicative Inverse of the Determinant

$$7 \times \begin{pmatrix} 11 & 8 \\ 15 & 7 \end{pmatrix} = \begin{pmatrix} 77 & 126 \\ 165 & 49 \end{pmatrix} \bmod 26 = \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix}$$

$$K^{-1} = \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix}$$

$$\begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix} \begin{pmatrix} A \\ P \end{pmatrix} = \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix} \begin{pmatrix} 0 \\ 15 \end{pmatrix} = \begin{pmatrix} 25 \times 0 + 22 \times 15 \\ 1 \times 0 + 23 \times 15 \end{pmatrix}$$

$$= \begin{pmatrix} 330 \\ 345 \end{pmatrix} \bmod 26 = \begin{pmatrix} 18 \\ 7 \end{pmatrix} = \begin{pmatrix} S \\ h \end{pmatrix}$$

classmate PAGE

Decryption

Step 1

$P = K^{-1} C \bmod 26$

Step 2

$$K^{-1} = \frac{1}{|d|} \text{Adj}(K)$$

Now find the multiplicative inverse of the determinant.

ie., $d\,d^{-1} \equiv 1 \bmod 26$

So first find the determinant of the matrix : $d = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = |ad - bc|$

To remove the negative sign, add 26 to negative numbers.

So we get $\begin{bmatrix} 6 & -3+26 \\ -3+26 & 2 \end{bmatrix} = \begin{bmatrix} 6 & 23 \\ 23 & 2 \end{bmatrix}$

Now multiply this with the multiplicative inverse of determinant.

So $9 * \begin{bmatrix} 6 & 23 \\ 23 & 2 \end{bmatrix} = \begin{bmatrix} 54 & 207 \\ 207 & 18 \end{bmatrix}$

Now find its modulo 26.

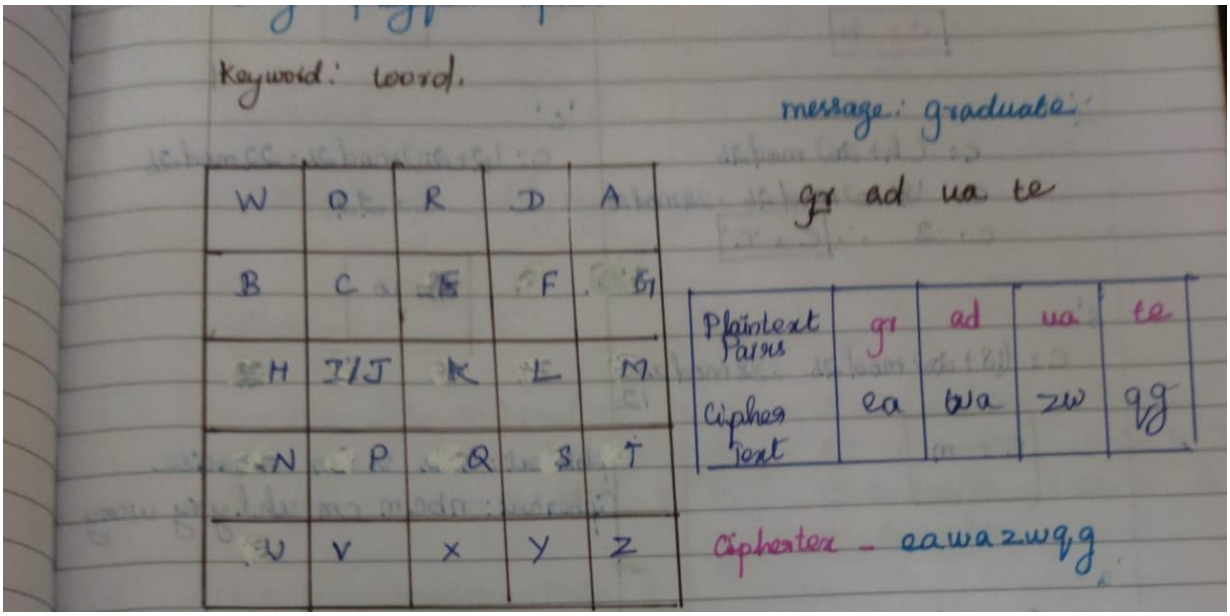
ie., $= \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix}$ → This is the decryption key K^{-1}

Encryption	Decryption
$c_1 = (k_{11}p_1 + k_{12}p_2 + k_{13}p_3) \bmod 26$ $c_2 = (k_{21}p_1 + k_{22}p_2 + k_{23}p_3) \bmod 26$ $c_3 = (k_{31}p_1 + k_{32}p_2 + k_{33}p_3) \bmod 26$	$P = K^{-1}C \bmod 26$ where K^{-1} is inverse of K i.e., $K^{-1}K = 1 \bmod 26$
$\begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix} = \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} \begin{pmatrix} p_1 \\ p_2 \\ p_3 \end{pmatrix} \bmod 26$ $C = KP \bmod 26$	**Example** $K = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$ $K^{-1} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix}$

9. Let message = "graduate", Key = "word", find ciphertext using playfair cipher.

Answer

Algorithm for play fair cipher



10.Encrypt the message "this is an exercise using additive cipher with key =20.Ignore the space between words .Decrypt the message to get the original plaintext.

or

Encrypt the message "this is an exercise" using additive cipher with key = 20. Ignore the space between words. Decrypt the message to get the original plaintext.(6 Marks)

Answer

C=E(K,P)=(P+K) mod 26

Let us assign a numerical equivalent to each letter:

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

Original Message: thisisanexercise Key: 20

Now, let's encrypt each letter with numbering and calculations:

1. 't' (19) + 20 = 39 % 26 = 13 -> 'n'
2. 'h' (7) + 20 = 27 % 26 = 1 -> 'b'
3. 'i' (8) + 20 = 28 % 26 = 2 -> 'c'
4. 's' (18) + 20 = 38 % 26 = 12 -> 'm'
5. 'i' (8) + 20 = 28 % 26 = 2 -> 'c'
6. 's' (18) + 20 = 38 % 26 = 12 -> 'm'

7. 'a' (0) + 20 = 20 % 26 = 20 -> 'u'
8. 'n' (13) + 20 = 33 % 26 = 7 -> 'h'
9. 'e' (4) + 20 = 24 % 26 = 24 -> 'y'
10. 'x' (23) + 20 = 43 % 26 = 17 -> 'r'
11. 'e' (4) + 20 = 24 % 26 = 24 -> 'y'
12. 'r' (17) + 20 = 37 % 26 = 11 -> 'l'
13. 'c' (2) + 20 = 22 % 26 = 22 -> 'w'
14. 'i' (8) + 20 = 28 % 26 = 2 -> 'c'
15. 's' (18) + 20 = 38 % 26 = 12 -> 'm'
16. 'e' (4) + 20 = 24 % 26 = 24 -> 'y'

Encrypted Message: "nbcmucrhwcmy"

Now, let's decrypt the message by reversing the process:

1. 'n' (13) - 20 = -7 -> 't' (19)
2. 'b' (1) - 20 = -19 -> 'h' (7)
3. 'c' (2) - 20 = -18 -> 'i' (8)
4. 'm' (12) - 20 = -8 -> 's' (18)
5. 'c' (2) - 20 = -18 -> 'i' (8)
6. 'm' (12) - 20 = -8 -> 's' (18)
7. 'u' (20) - 20 = 0 -> 'a' (0)
8. 'h' (7) - 20 = -13 -> 'n' (13)
9. 'y' (24) - 20 = 4 -> 'e' (4)
10. 'r' (17) - 20 = -3 -> 'x' (23)
11. 'y' (24) - 20 = 4 -> 'e' (4)
12. 'l' (11) - 20 = -9 -> 'r' (17)
13. 'w' (22) - 20 = 2 -> 'c' (2)
14. 'c' (2) - 20 = -18 -> 'i' (8)
15. 'm' (12) - 20 = -8 -> 's' (18)
16. 'y' (24) - 20 = 4 -> 'e' (4)

Decrypted Message: "thisisanexercise"

So, the original plaintext is indeed "this is an exercise."

11.Perform Encyption and decryption using Hill Cipher for the following Messsage :PEN and Key:ACTIVATED

1. Perform Encryption and decryption using Hill cipher for the following Message : PEN and key : ACTIVATED

Sol:

Encryption:

$$C = KP \bmod 26$$

$$\begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix} = \begin{pmatrix} 0 & 2 & 19 \\ 8 & 21 & 0 \\ 19 & 4 & 3 \end{pmatrix} \begin{pmatrix} p_1 \\ p_2 \\ p_3 \end{pmatrix} \bmod 26$$

$$\begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix} = \begin{pmatrix} 0 & 2 & 19 \\ 8 & 21 & 0 \\ 19 & 4 & 3 \end{pmatrix} \begin{pmatrix} 15 \\ 4 \\ 13 \end{pmatrix} \bmod 26$$

$$\begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix} = \begin{pmatrix} 0\times 15 + 2\times 4 + 19\times 13 \\ 8\times 15 + 21\times 4 + 0\times 13 \\ 19\times 15 + 4\times 4 + 3\times 13 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 255 \\ 204 \\ 340 \end{pmatrix} \bmod 26$$

$$\begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix} = \begin{pmatrix} 21 \\ 22 \\ 2 \end{pmatrix} \rightarrow \begin{pmatrix} V \\ W \\ C \end{pmatrix}$$

cipher text = VWC

Decryption:

$$P = K^{-1} C \mod 26$$

$$K^{-1} = \frac{1}{|K|} \text{adj } K$$

$$|K| = \begin{pmatrix} 0 & 2 & 19 \\ 8 & 21 & 0 \\ 19 & 4 & 3 \end{pmatrix} \mod 26$$

$$\Rightarrow \left(0\left[(21\times3)-(4\times0)\right] - 2\left[(8\times3)-(19\times0)\right] + 19\left[(8\times4)-(19\times21)\right]\right)$$

$$\Rightarrow \left[-2(24) + 19(32-399)\right] \mod 26$$

$$\Rightarrow \left[-48 + 19(-367)\right] \mod 26$$

$$\Rightarrow \left[-48 - 6973\right] \mod 26$$

$$\Rightarrow -7021 \mod 26$$

$$|K| \Rightarrow 25$$

$$\text{adj } K = \begin{pmatrix} +\begin{vmatrix} 21 & 0 \\ 4 & 3 \end{vmatrix} & -\begin{vmatrix} 8 & 0 \\ 19 & 3 \end{vmatrix} & +\begin{vmatrix} 8 & 21 \\ 19 & 4 \end{vmatrix} \\ -\begin{vmatrix} 2 & 19 \\ 4 & 3 \end{vmatrix} & +\begin{vmatrix} 0 & 19 \\ 19 & 3 \end{vmatrix} & -\begin{vmatrix} 0 & 2 \\ 19 & 4 \end{vmatrix} \\ +\begin{vmatrix} 2 & 19 \\ 21 & 0 \end{vmatrix} & -\begin{vmatrix} 0 & 19 \\ 8 & 0 \end{vmatrix} & +\begin{vmatrix} 0 & 2 \\ 8 & 21 \end{vmatrix} \end{pmatrix}^T$$

$$= \begin{pmatrix} 63 & -24 & -367 \\ 70 & -361 & 38 \\ -399 & 152 & -16 \end{pmatrix}^T$$

$$\text{adj } K = \begin{pmatrix} 63 & 70 & -399 \\ -24 & -361 & 152 \\ -367 & 38 & -16 \end{pmatrix}$$

$$K^{-1} = \frac{1}{|K|} \text{adj } K$$

$$K^{-1} = 25^{-1} \begin{pmatrix} 63 & 70 & -399 \\ -24 & -361 & 152 \\ -367 & 38 & -16 \end{pmatrix}$$

$$= 25 \begin{pmatrix} 63 & 70 & -399 \\ -24 & -361 & 152 \\ -367 & 38 & -16 \end{pmatrix} \mod 26$$

$$= \begin{pmatrix} 1575 & 1750 & -9975 \\ -600 & -9025 & 3800 \\ -9175 & 950 & -400 \end{pmatrix} \bmod 26$$

$$K^{-1} = \begin{pmatrix} 15 & 8 & 9 \\ 24 & 23 & 4 \\ 3 & 14 & 16 \end{pmatrix}$$

$$P = K^{-1} C \bmod 26$$

$$\begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} = \begin{pmatrix} 15 & 8 & 9 \\ 24 & 23 & 4 \\ 3 & 14 & 16 \end{pmatrix} \begin{pmatrix} 21 \\ 22 \\ 2 \end{pmatrix} \bmod 26$$

$$\begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} = \begin{pmatrix} 15\times21 + 8\times22 + 9\times2 \\ 24\times21 + 23\times22 + 4\times2 \\ 3\times21 + 14\times22 + 16\times2 \end{pmatrix} \bmod 26$$

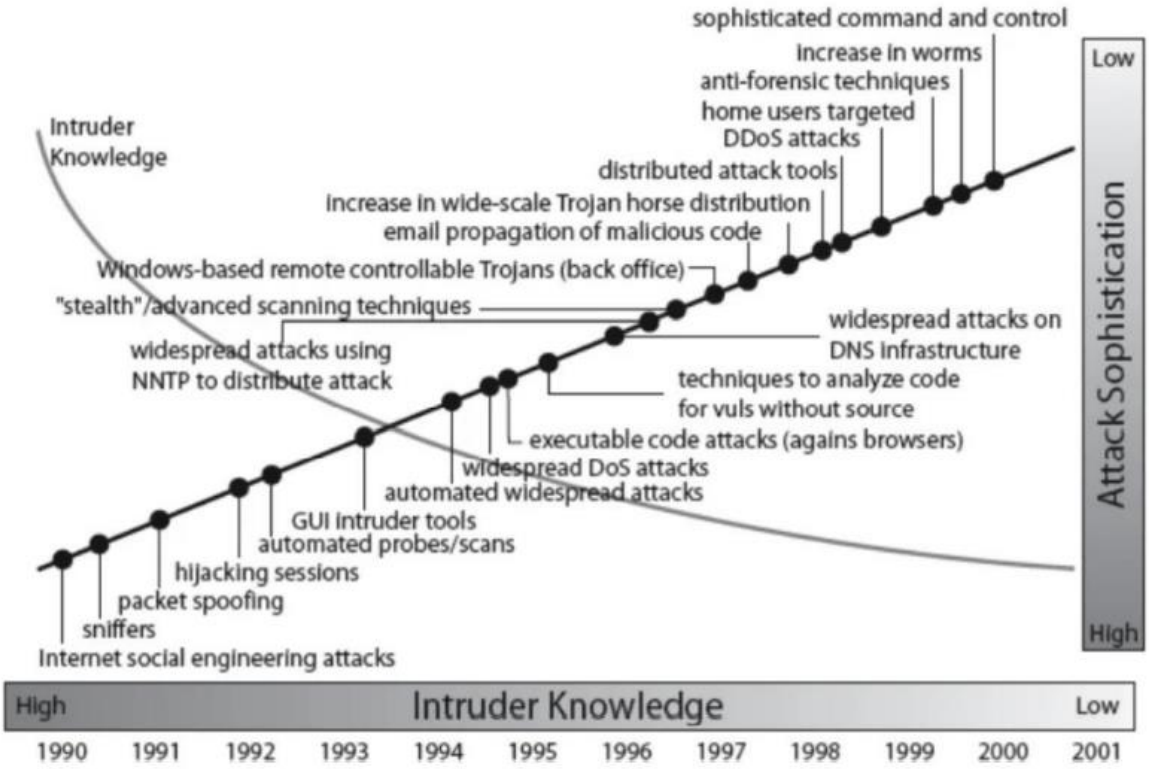
$$= \begin{pmatrix} 509 \\ 1018 \\ 403 \end{pmatrix} \bmod 26$$

$$\begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} = \begin{pmatrix} 15 \\ 4 \\ 13 \end{pmatrix} = \begin{pmatrix} P \\ E \\ N \end{pmatrix}$$

plain text = PEN

Study the following Questions Also

1.Security Trends



2.Need for Security at Multiple levels

3.Security polices

Four Types of Policies 1.Cryptography and compliance 2.Use of Encryption 3.Managing electronic keys 4.Using and receiving digital signatures

4.Foundation of Modern Cryptography

Perfect Security

Information Theory

Product Crypto Systems

(i)Perfect Security

Definition

Steps

(i)Encyprtion/Decryption Rules

(ii)Probabilities of messages

(iii)Probabilities of keys

(iv)Shannon's Theorem

(ii)Information Theory

Entropy

Properties of Entropy

(iii) Product Crypto Systems

Definition

Diagram

5.List out any two di-gram, two tri-gram. Shortly describe the application of di-gram and tri-gram in cryptography.(5 Marks)

Di-grams and Tri-grams:

Di-grams:

Example 1: "TH" is a di-gram.

Example 2: "IN" is another di-gram.

Tri-grams:

Example 1: "THE" is a tri-gram.

Example 2: "AND" is another tri-gram.

Applications in Cryptography:

1.Frequency Analysis

Di-grams and tri-grams are used in frequency analysis, which is a technique in cryptanalysis (the study of breaking codes) to decipher encrypted messages. In natural languages like English, certain di-grams and tri-grams occur more frequently than others. Cryptanalysts can use this information to make educated guesses about the substitution patterns used in simple ciphers like the Caesar cipher

2.Text Scoring

Di-grams and tri-grams are also used in text scoring systems for cryptographic algorithms like the Vigenère cipher. By analyzing the frequencies of di-grams and tri-grams in the decrypted text, one can assign a score to different decryption keys. Keys that produce decrypted text with di-grams and tri-grams that closely resemble those found in the expected language (e.g., English) are considered more likely to be the correct key. This helps automated decryption processes.

6. Outline any four types of cryptanalysis attack and explain with neat sketches?How this attack is made possible?

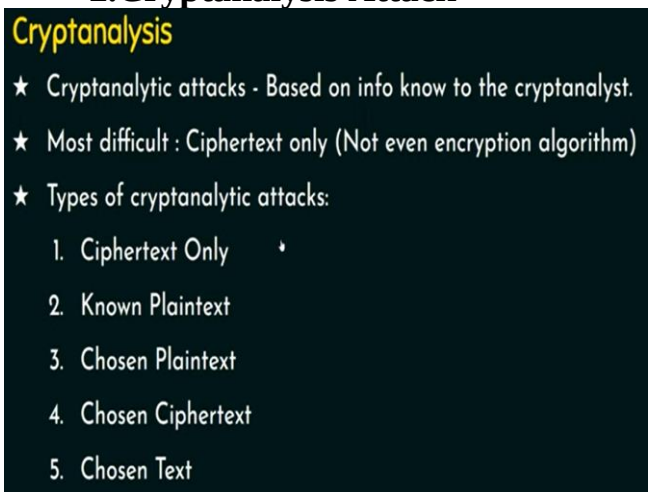
Cryptanalysis is the art and science of breaking cryptographic systems. There are various types of cryptanalysis attacks, each with its own techniques and methods

1.Brute Force Attack:

Explanation: In a brute force attack, the attacker tries every possible combination of keys until the correct one is found. This method is often used when the encryption key space is relatively small**.**

How it's made possible: The attacker systematically generates and tests each possible key until the correct one is discovered.

2.Cryptanalysis Attack



Type of Attack	Known to cryptanalyst
Ciphertext Only	★ Encryption Algorithm ★ Ciphertext
Known Plaintext	★ Encryption Algorithm ★ Ciphertext ★ One or more PT-CT pairs formed with secret key
Chosen Plaintext	★ Encryption Algorithm ★ Ciphertext ★ PT message chosen by cryptanalyst, together with its CT generated with the secret key
Chosen Ciphertext	★ Encryption Algorithm ★ Ciphertext ★ CT chosen by cryptanalyst, together with its corresponding decrypted PT generated with the secret key
Chosen Text	★ Chosen Plaintext and Chosen Ciphertext

Part C Questions

Discuss examples from real life, where the following security objectives are needed

i) Confidentiality. (5)

ii) Integrity. (5)

iii) Non-repudiation. (5)

Suggest suitable security mechanisms to achieve them:

Answer

Confidentiality:

Confidentiality is a security objective that ensures that sensitive information is protected from unauthorized access or disclosure.

It involves keeping data secret and only accessible to those who have the proper authorization to view or use it. The goal is to prevent unauthorized individuals or entities from gaining access to confidential information.

Example

Healthcare Records: In the healthcare industry, patient records must be kept confidential. Unauthorized access to medical records can lead to privacy breaches

and identity theft. Security mechanisms such as access controls, encryption, and strong authentication can help maintain confidentiality.

Integrity:

It ensures that data remains unchanged and unaltered during storage, transmission, or processing**.**

Example

Financial Transactions: In the financial sector, the integrity of transactions is critical. Transaction logs, hashing algorithms, and audit trails help detect and prevent unauthorized or malicious changes to financial data.

Non-Repudiation

It prevents an individual or entity from denying the authenticity or legitimacy of a message, transaction, or action they have taken. It provides proof that a specific communication or transaction occurred and that the parties involved cannot later claim they were not responsible for it. Non-repudiation is often achieved through the use of digital signatures and cryptographic techniques to create a verifiable record of actions or communications.

Example

Digital Signatures: In electronic contracts or agreements, digital signatures provide non-repudiation. When a document is signed with a digital certificate, the signer cannot deny their involvement.

CS8792-CRYPTOGRAPHY AND NETWORK SECURITY

UNIT-2: SYMMETRIC CRYPTOGRAPHY

1.Find gcd(2740, 1760) using Euclidean Algorithm(Nov/Dec 2016)

Step-by-step explanation:

Euclidean algorithm for GCD

GCD (a , b) ; $a \geq b > 0$

a = 2740

b = 1760

Euclid's formula;

A = b(q) + r ; [q = quotient and r = remainder]

2740 = 1760 (1) + 980

again by taking a = 1760 and b = 980

1760 = 980 (1) + 780

similarly, we have to continue till we get r as 0

980 = 780(1) + 200

780 = 200 (3) + 180

200 = 180(1) + 20

180 = 20 (9) + 0

Now as the r = 0 ,

∴ 20 is the GCD of (2740,1760)

2.Find gcd(1970,1000) using Euclidean Algorithm

To find the greatest common divisor (GCD) of 1970 and 1000 using the Euclidean algorithm with the formula GCD(a, b) = GCD(b, a mod b), you can follow these steps:

GCD(1970, 1000) = GCD(1000, 1970 % 1000)

GCD(1000, 970) = GCD(970, 1000 % 970)

GCD(970, 30) = GCD(30, 970 % 30)

GCD(30, 10) = GCD(10, 30 % 10)

GCD(10, 0)

Since the remainder has become 0, we can stop. The GCD of 1970 and 1000 is 10, which is the last non-zero remainder in the Euclidean algorithm process.

So, GCD(1970, 1000) = 10.

3.Determine the gcd(24140,16762)using Euclid's Algorithm

The **formula GCD(a, b) = GCD(b, a mod b),** you can follow these steps:

GCD(24140, 16762) = GCD(16762, 24140 % 16762)

GCD(16762, 7378) = GCD(7378, 16762 % 7378)

GCD(7378, 2006) = GCD(2006, 7378 % 2006)

GCD(2006, 363) = GCD(363, 2006 % 363)

GCD(363, 170) = GCD(170, 363 % 170)

GCD(170, 23) = GCD(23, 170 % 23)

GCD(23, 3) = GCD(3, 23 % 3)

GCD(3, 2) = GCD(2, 3 % 2)

GCD(2, 1) = GCD(1, 2 % 1)

GCD=2

4.Find gcd(21,300) using Euclid's Algorithm

To find the greatest common divisor (GCD) of 21 and 300 using the Euclidean algorithm with the formula GCD(a, b) = GCD(b, a mod b), you can follow these steps:

GCD(21, 300) = GCD(300, 21 mod 300)

GCD(300, 21) = GCD(21, 300 mod 21)

GCD(21, 15) = GCD(15, 21 mod15)

GCD(15, 6) = GCD(6, 15 mod6)

GCD(6, 3) = GCD(3, 6 mod 3)

GCD(3, 0)

At this point, the remainder becomes 0, so we can stop. The last non-zero remainder is 3.

So, GCD(21, 300) = 3.

5.Find gcd(45,6)using Euclidean algorithm.

To find the greatest common divisor (GCD) of 45 and 6 using the Euclidean algorithm with the following formula:

GCD(a, b) = GCD(b, amod b)

Let's apply this formula step by step:

GCD(45, 6) = GCD(6, 45 % 6)

GCD(6, 3) = GCD(3, 6 % 3)

GCD(3, 0)

Since the second number becomes 0, we have our result:

GCD(45, 6) = 3

So, the **GCD of 45 and 6 is 3.**

6.Brief the strength of Triple DES

Triple DES with 2 Keys

- It uses ***three stages of DES*** for ***encryption and decryption***.
- The 1st, 3rd stage use ***K1 key and 2nd stage use K2 key***.
- To make ***triple DES compatible with single DES***, the middle stage uses decryption in the encryption side and encryption in the decryption side.
- It's much stronger than double DES.
- The function follows an encrypt-decrypt-encrypt (EDE) sequence

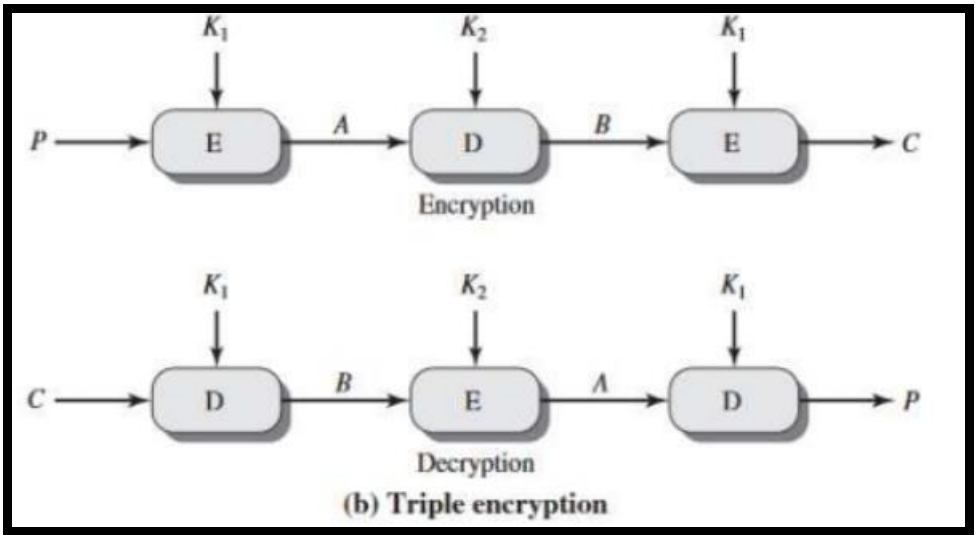
The function follows an encrypt-decrypt-encrypt (EDE) sequence.

$$C = E(K_1, D(K_2, E(K_1, P)))$$

$$P = D(K_1, E(K_2, D(K_1, C)))$$

By the use of triple DES with 2-key encryption, it raises the cost of the meet-in-the-middle attack to 2^{112}

It has the drawback of requiring a key length of $56 \times 3 = 168$ bits which may be somewhat un wide.



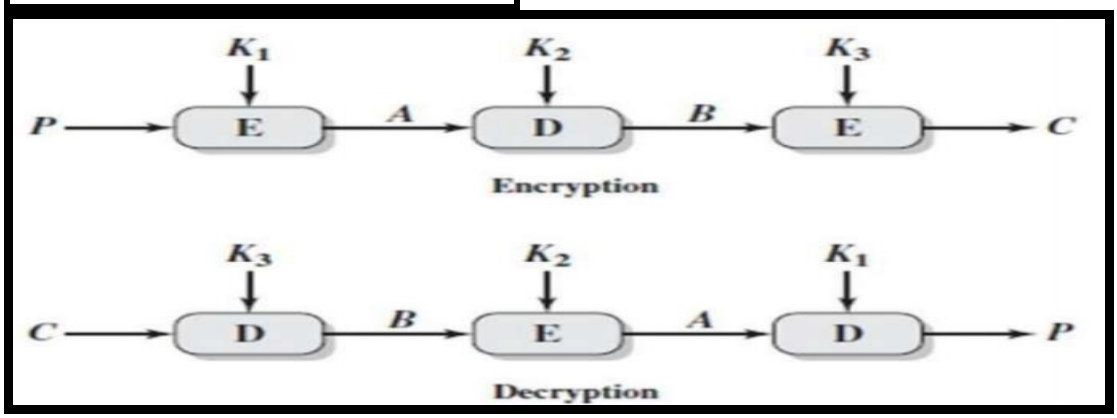
(b) Triple encryption

Triple DES with 3-key

Although the attacks just described appear impractical, anyone using two key 3DES
It uses three stages of DES for encryption and decryption. The 1st, use K_1key and 2nd stage use K_2 key and 3rd stage k3 key

Three-key 3DES has ***<u>an effective key length of 168 bits</u>*** and is defined as

$$C = E(K_3, D(K_2, E(K_1, P)))$$



7.State the difference between private key and public key Algorithm

Private Key	Public Key
The key is kept secret by two people.	One key is publicly available while the other remains secret.
Once lost, the file will become unusable.	There's no possibility of loss since one of the requirements is a public key.
It is commonly used to protect disk drives and other data storage devices.	It is commonly used to secure web sessions and emails.
It is a form of symmetrical encryption.	It is a form of asymmetrical encryption.
It is faster since only one key is needed.	It is slower since two keys are required.

8.Give the five modes of operation of block cipher

Block Cipher Modes of Operation

Mode	Description	Typical Application
Electronic Codebook (ECB)	Each block of 64 plaintext bits is encoded independently using the same key.	• Secure transmission of single values (e.g., an encryption key)
Cipher Block Chaining (CBC)	The input to the encryption algorithm is the XOR of the next 64 bits of plaintext and the preceding 64 bits of ciphertext.	• General-purpose block-oriented transmission • Authentication
Cipher Feedback (CFB)	Input is processed *s* bits at a time. Preceding ciphertext is used as input to the encryption algorithm to produce pseudorandom output, which is XORed with plaintext to produce next unit of ciphertext.	• General-purpose stream-oriented transmission • Authentication
Output Feedback (OFB)	Similar to CFB, except that the input to the encryption algorithm is the preceding encryption output, and full blocks are used.	• Stream-oriented transmission over noisy channel (e.g., satellite communication)
Counter (CTR)	Each block of plaintext is XORed with an encrypted counter. The counter is incremented for each subsequent block.	• General-purpose block-oriented transmission • Useful for high-speed requirements

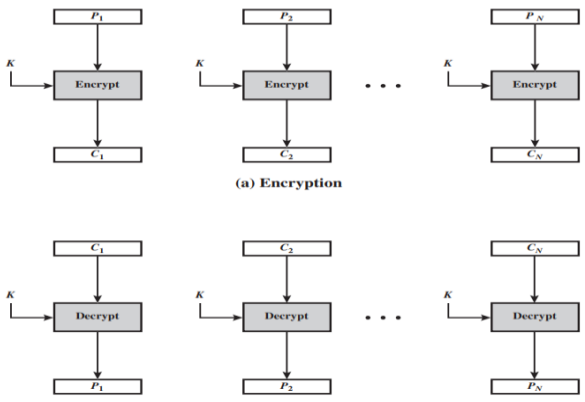


Figure Electronic Codebook (ECB) Mode

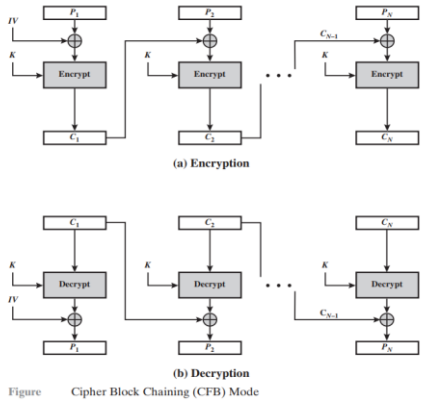


Figure Cipher Block Chaining (CFB) Mode

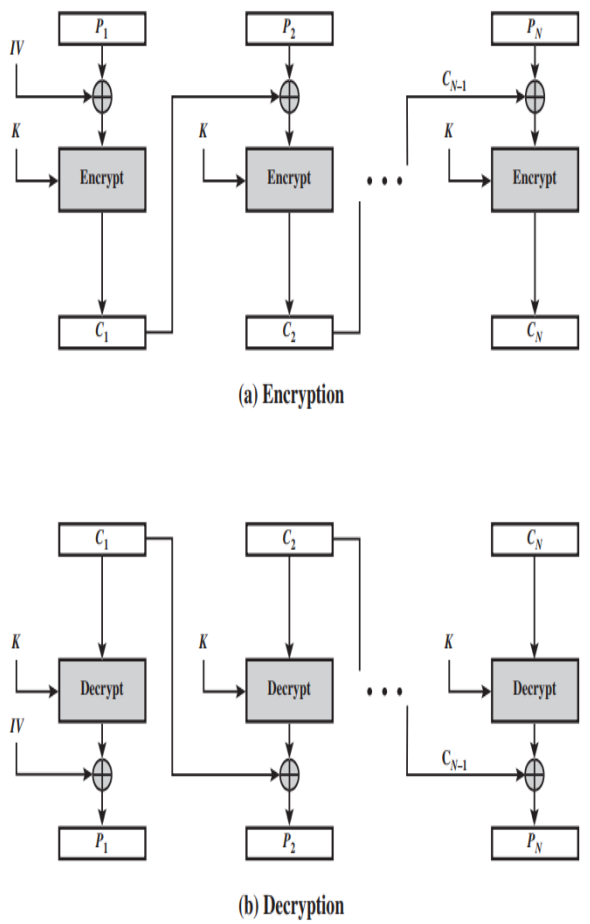


Figure Cipher Block Chaining (CFB) Mode

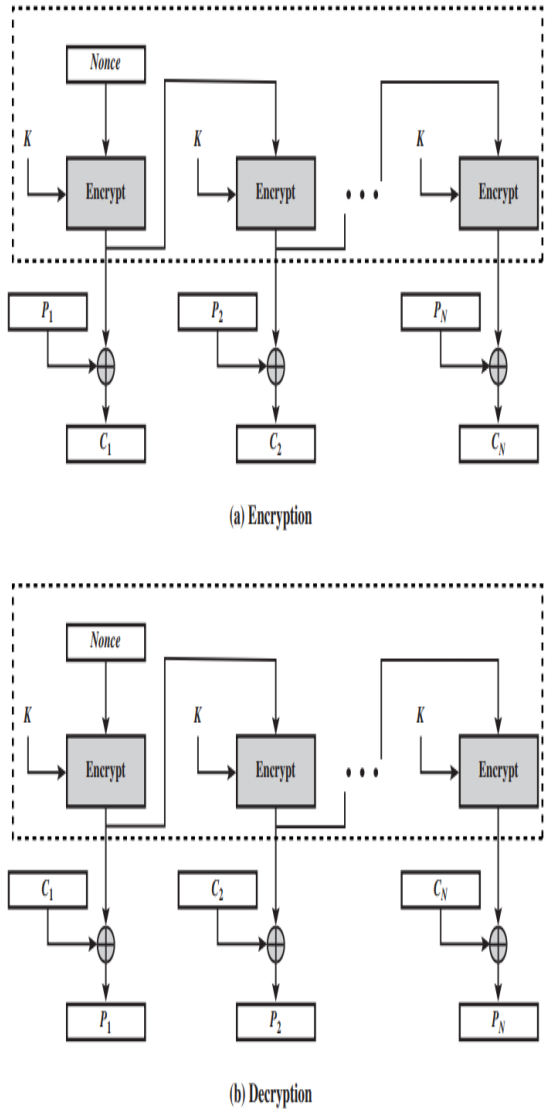


Figure Output Feedback (OFB) Mode

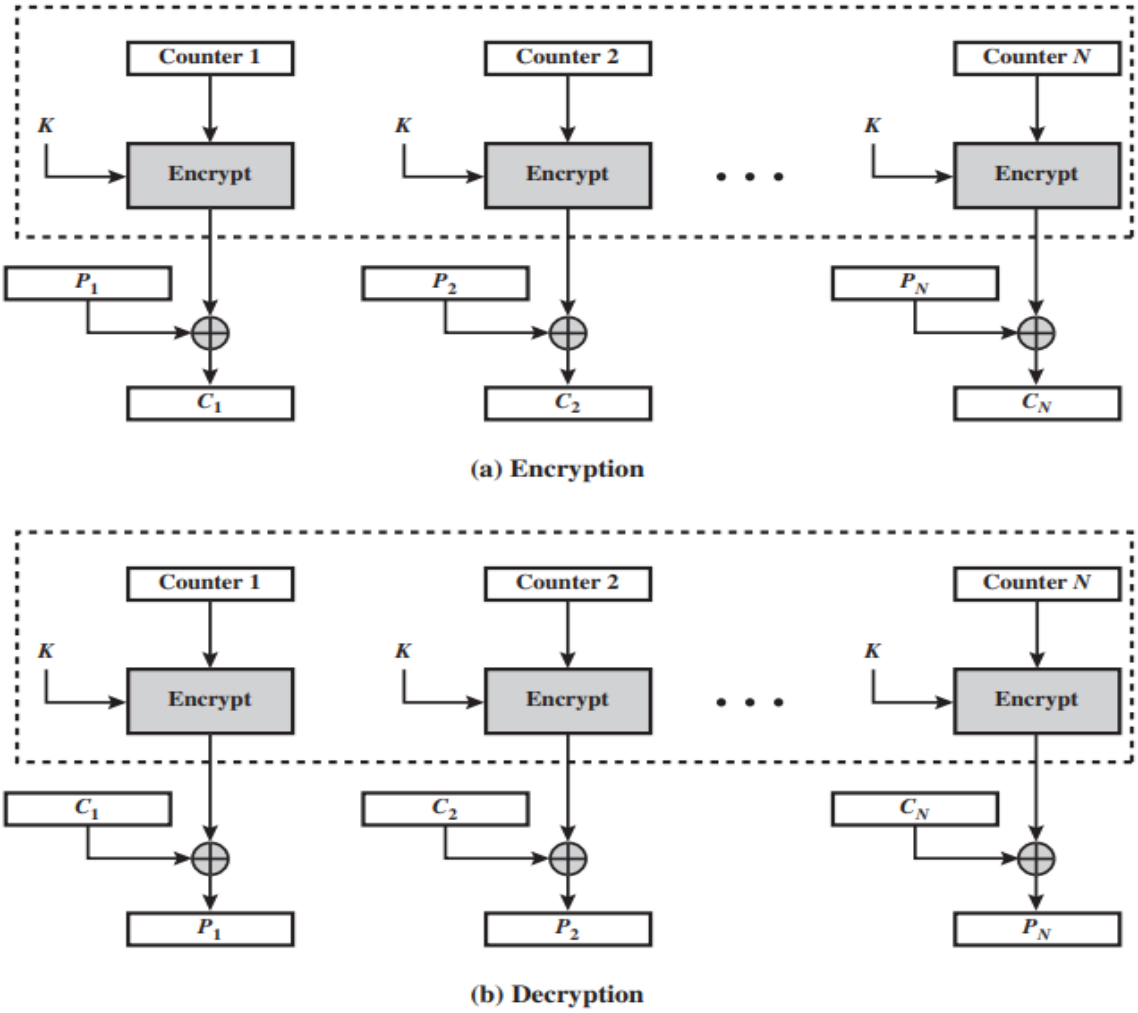


Figure Counter (CTR) Mode

9.List the parameters (block size,key size and no of rounds) for the three AES versions.

- The algorithm is referred to as **AES-128, AES-192, orAES-256,** depending on the **key length.**

Key Size (words/bytes/bits)	4/16/128	6/24/192	8/32/256
Plaintext Block Size (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Number of Rounds	10	12	14
Round Key Size (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Expanded Key Size (words/bytes)	44/176	52/208	60/240

10.**What are the primitive operations used in RC4?**

The primitive operation used in RC4 is bit wise Exclusive-OR (XOR) operation.

11.Compare DES and AES

AES	DES

AES	DES
AES stands for ***Advanced Encryption Standard***	DES stands for ***Data Encryption Standard***.
AES allows the data length (plain text size) of 128, 192, and 256 bits.	Data encryption standard takes 64-bit plaintext as input and creates 64-bit Ciphertext i.e. it encrypts data in a block of size 64-bits per block.
AES divide plaintext into 16 bytes (128-bit) blocks and treats each block as a 4×4 State array and supporting three different key lengths, 128, 192. and 256 bits.	In DES plaintext message is divided into size 64-bit block each and encrypted using the 56-bit key at the initial level.
The number of rounds is 10, which is for the case when the encryption key is 128 bits long. (As mentioned earlier, the number of rounds is 12 when the key is 192 bits and 14 when the key is 256.)	The left plaintext and right plaintext goes through 16 rounds of encryption process along with 16 different keys for each round.
AES was designed by Vincent Rijmen and Joan Daemen.	DES was designed by IBM.
AES is faster.	DES is comparatively slower.
AES has a large secret key comparatively hence, more secure.	DES has a smaller key which is less secure.
Subbytes, Shiftrows, Mix columns, Addroundkeys.	Expansion Permutation, Xor, S-box, P-box, Xor, and Swap.
10 rounds for 128-bit algo 12 rounds for 192-bit algo 14 rounds for 256-bit algo	16 Ounds

10.Define field and Ring in Number Theory?

Fields

A **field** F, sometimes denoted by $\{F, +, \times\}$, 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.

(A1–M6) F is an integral domain; that is, F satisfies axioms A1 through A5 and M1 through M6.

(M7) Multiplicative inverse: For each a in F, except 0, there is an element a^{-1} in F such that $aa^{-1} = (a^{-1})a = 1$.

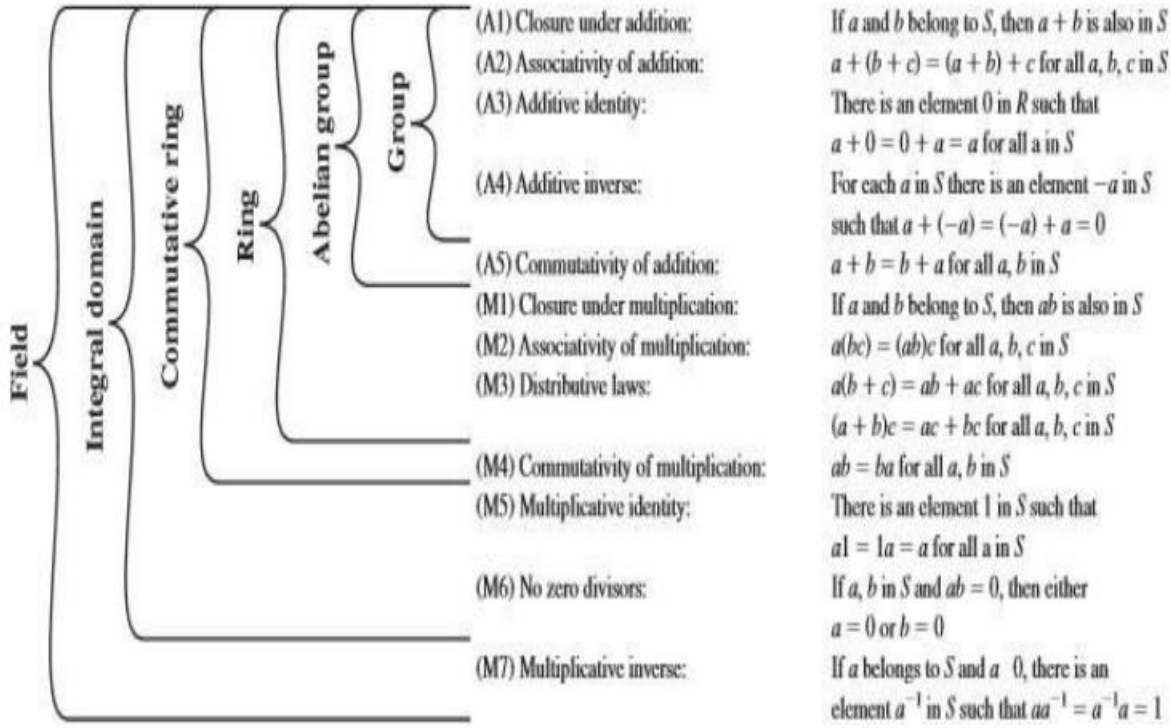


Figure 2.2 Groups, Ring and Field

Ring

A **ring** R, sometimes denoted by $\{R, +, \times\}$, is a set of elements with two binary operations, called *addition* and *multiplication*,[6] such that for all a, b, c in R the following axioms are obeyed.

(A1–A5) R is an abelian group with respect to addition; that is, R satisfies axioms A1 through A5. For the case of an additive group, we denote the identity element as 0 and the inverse of a as $-a$.

(M1) Closure under multiplication: If a and b belong to R, then ab is also in R.

(M2) Associativity of multiplication: $a(bc) = (ab)c$ for all a, b, c in R.

(M3) Distributive laws: $a(b + c) = ab + ac$ for all a, b, c in R.
$(a + b)c = ac + bc$ for all a, b, c in R.

11.List the entities that are to be kept secret in conventional encryption techniques

Two main requirements are needed **for secure use of conventional encryption**:

(i). A **strong encryption algorithm** is needed. It is desirable that the algorithm should be in such a way that, even the attacker who knows the algorithm and has access to one or more cipher texts would be unable to decipher the ciphertext or figure out the key.

(ii).The **secret key** must be distributed among the sender and receiver in a very secured way. If in any way the key is discovered and with the knowledge of algorithm, all communication using this key is readable.

The important point is that the ***security of conventional encryption*** depends on the **secrecy of the key**, not ***the secrecy of the algorithm*** i.e. it is not necessary to keep the algorithm secret, but only ***the key is to be kept secret***

12.What is the residues of 6 when n=8

When the integer a is divided by the integer n, **the remainder r** is referred to as the **residue**.

Equivalently, **r=a mod n**.

6 divided by 8 equals 0 with a remainder of 6.

So, the residue of 6 when n = 8 is 6.

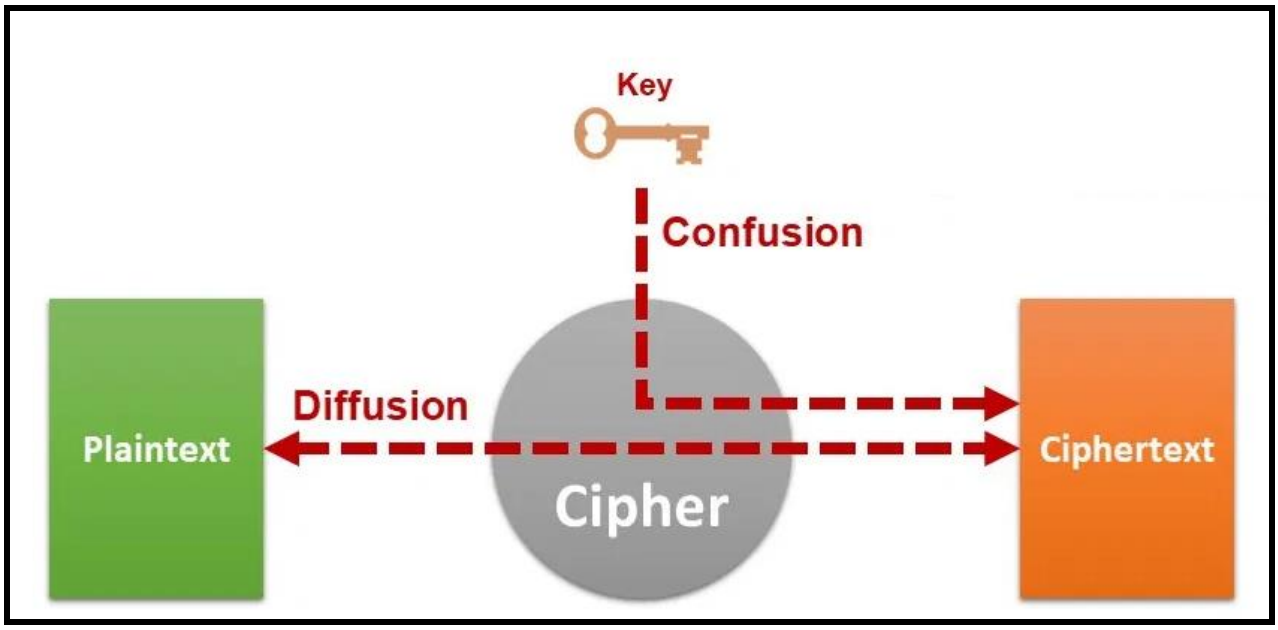
13. Write down the purpose of the S-Boxes in DES?

S-boxes are ***non-linear transformations*** of a few input bits that **provide confusion.**

14. Define : Diffusion.

Diffusion

- If any of the ***characters in the plaintext is changed***,then simultaneously ***several characters of the ciphertext should also be changed.***
- It is a **classical transposition cipher**.
- Note:**Diffusion** hides the relation between the **ciphertext and plaintext**.
- **P-box or transposition cipher**
- **Confusion**
  - In Confusion **each character of ciphertext** depends on a **different part of a key**.
  - In confusion **the key does not directly** related to **ciphertext.**
  - It is a classical **substitution cipher.**
  - Note:**Confusion** hides the relation between the **ciphertext and key**.
  - **S-box or Substitution cipher**



15. Define : Primality test. ?

A **primality test** is an algorithm **for determining whether an input number is prime**.

16.Why modular arithmetic has been used in cryptography?

Modular arithmetic allows us to easily create groups, rings and fields which are fundamental building blocks of most modern public-key cryptosystems.

17.State the difference between conventional encryption and public-key encryption

Table 9.2 Conventional and Public-Key Encryption

Conventional Encryption	Public-Key Encryption
Needed to Work: 1. The same algorithm with the same key is used for encryption and decryption. 2. The sender and receiver must share the algorithm and the key. *Needed for Security:* 1. The key must be kept secret. 2. It must be impossible or at least impractical to decipher a message if no other information is available. 3. Knowledge of the algorithm plus samples of ciphertext must be insufficient to determine the key.	*Needed to Work:* 1. One algorithm is used for encryption and decryption with a pair of keys, one for encryption and one for decryption. 2. The sender and receiver must each have one of the matched pair of keys (not the same one). *Needed for Security:* 1. One of the two keys must be kept secret. 2. It must be impossible or at least impractical to decipher a message if no other information is available. 3. Knowledge of the algorithm plus one of the keys plus samples of ciphertext must be insufficient to determine the other key.

18.Define primitive root

primitive root If r and n are relatively prime integers with $n > 0$ and if $\phi(n)$ is the least positive exponent m such that $r^m \equiv 1 \bmod n$, then r is called a primitive root modulo n.

19. What are the disadvantages of double DES?

The disadvantages of double DES is Meet in the middle Attack

Double DES results in a ***mapping that is not equivalent to a single DES*** encryption. But there is a way ***to attack this scheme***, one that does not depend on any particular property of DES but that will work against any block encryption cipher. The algorithm, known as a **meet-in-the-middle attack**

22.Find GCD(21,300) using Euclid's Algorithm

20.What is the Meet in the Middle Attack?

Definition

- This attack involves **encryption from one end and decryption from other end** and then matching the results in the middle is called as ***Meet in the Middle attack***
- This attack requires knowing **some plain text and cipher text pairs**

21. List AES Evaluation criteria?

Three categories of criteria were as follows

(i)Security (ii)Cost (iii)Algorithm and Implementation characteristics

22.List important design considerations for a stream cipher.

- The **encryption sequence** should have a **large period**.
- The **key stream** should approximate the **properties of a true random number stream as close as** possible.
- The output of the **pseudorandom number generator** is conditioned on the value of the input key.

23.Compare linear and differential cryptanalysis?

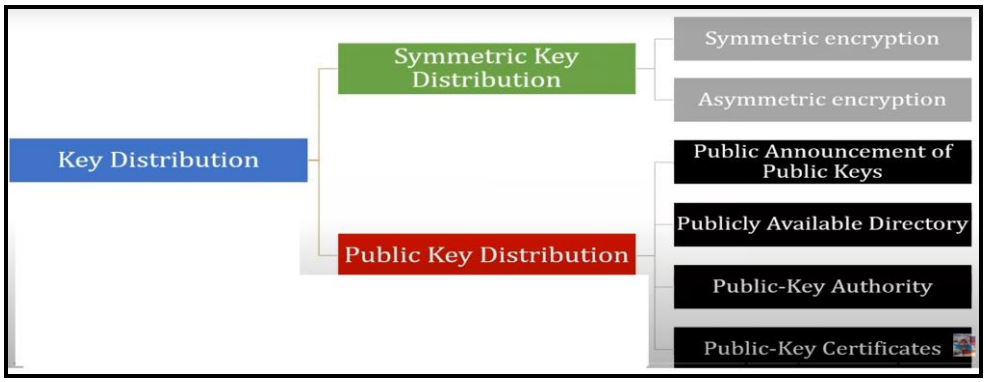
Linear Cryptanalysis and Differential Cryptanalysis are two different techniques used in the field of cryptanalysis to break cryptographic systems.

Here's a comparison of these techniques in a tabular format:

	Linear Cryptanalysis	Differential Cryptanalysis
Primary Objective	Find linear relationships between the plaintext, ciphertext, and key bits	Find the differences (differentials) in plaintext, ciphertext, or key bits
Type of Attack	Statistical attack	Statistical attack
Target Cryptosystems	Generally used for symmetric-key block ciphers (e.g., DES)	Primarily used for symmetric-key block ciphers (e.g., DES)

	Linear Cryptanalysis	Differential Cryptanalysis
Basis of Attack	Based on linear equations	Based on the differences (differentials) between plaintexts and ciphertexts
Core Concept	Explores the correlation between bits using linear approximations	Explores how small input differences propagate through the encryption process
Attack Complexity	Generally requires a lot of known plaintext-ciphertext pairs	Typically requires fewer known plaintext-ciphertext pairs compared to linear cryptanalysis
Key Recovery	Tries to recover the secret key used for encryption	Tries to recover the secret key used for encryption
Attack Difficulty	Often considered more challenging and computationally intensive	Can be more efficient and require fewer resources compared to linear cryptanalysis
Resistance to Attacks	Cryptosystems designed with low linear approximation probability are more resistant	Cryptosystems designed with low differential probability are more resistant
Historical Significance	Linear cryptanalysis played a significant role in breaking DES	Differential cryptanalysis played a significant role in breaking DES
Practical Applicability	May not always be applicable due to its computational demands	Often used for practical attacks on symmetric-key ciphers, especially when plaintext-ciphertext pairs are limited

24.What are the various ways to distribute the keys?



Part B Questions

1.Draw the functionality diagram (functionality in one round) of DES with number of bits in each flow of data. (8)
[or]
Describe DES algorithm with neat diagram and explain the steps.
Answer

DES Definition

Steps

i)Initial permutation
(ii)16 fiestal rounds
(iii)Swapping /left-right swap
(iv)Final Permutation /Inverse Initial Permutation

2.11.2 Basic Structure

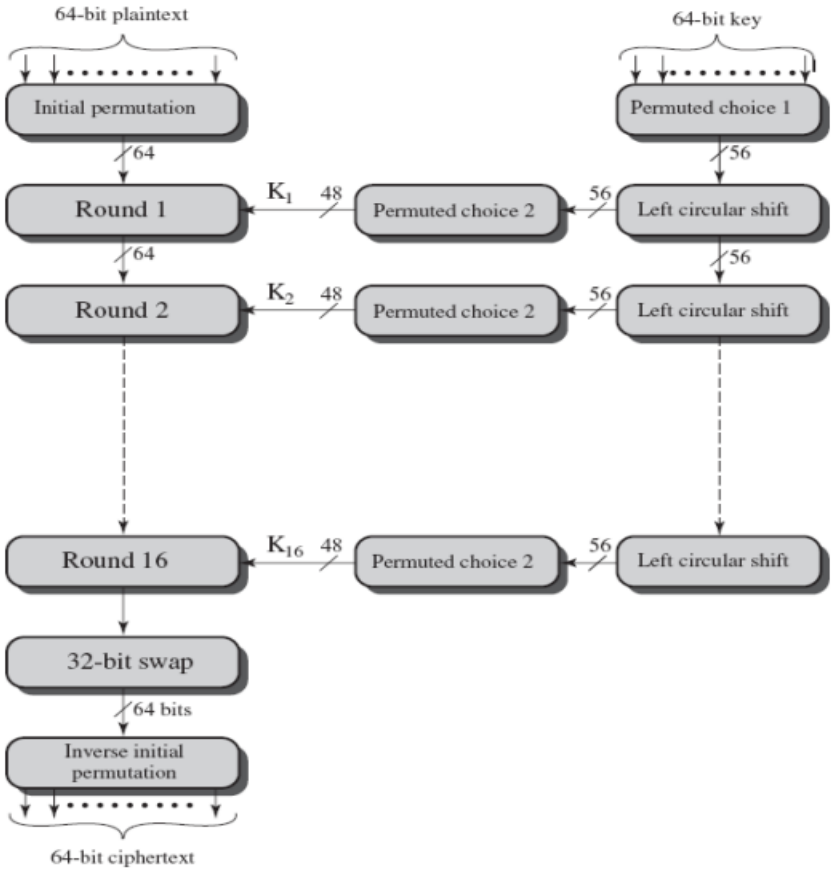


Figure 2.8 DES Encryption Algorithm

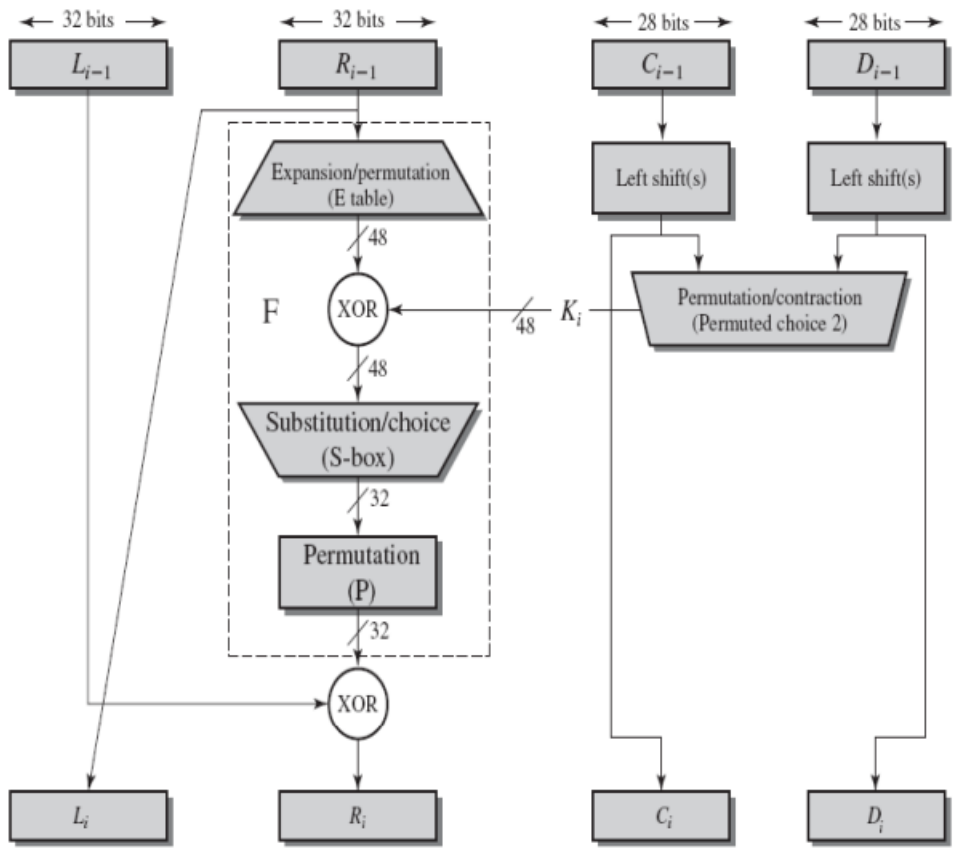


Figure 2.9 Single Round of DES Algorithm

Steps in Function Block

1.Expansion Permutation

2.Definition of S-Boxes

3.Permutation Function

4.Inverse Permutation

2.(b) (i) Explain with sample data: Four transformations in AES.

Or

What do you mean by AES Diagrammatically illustrate the structure of AES and describe the steps in AES encryption process with example.

The **first N - 1 round** consist of **four distinct transformation functions:**

(i)Sub Bytes,

(ii)Shift Rows,

(iii)Mix Columns, and

(iv)AddRoundKey.

(ii) In finite field arithmetic, $(x^6 + x^4 + x^2 + x + 1) + (x^7 + x + 1) = ?$

The Advanced Encryption Standard (AES) uses arithmetic in the finite field GF(2^8), with the irreducible polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$. Consider the two polynomials $f(x) = x^6 + x^4 + x^2 + x + 1$ and $g(x) = x^7 + x + 1$. Then

$$\begin{aligned} f(x) + g(x) &= x^6 + x^4 + x^2 + x + 1 + x^7 + x + 1 \\ &= x^7 + x^6 + x^4 + x^2 \end{aligned}$$

$$\begin{aligned} f(x) \times g(x) &= x^{13} + x^{11} + x^9 + x^8 + x^7 \\ &\quad + x^7 + x^5 + x^3 + x^2 + x \\ &\quad + x^6 + x^4 + x^2 + x + 1 \\ &= x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1 \end{aligned}$$

$$\begin{array}{r|l} & x^5 + x^3 \\ \hline x^8 + x^4 + x^3 + x + 1 & x^{13} + x^{11} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + 1 \\ & x^{13} + x^9 + x^8 + x^6 + x^5 \\ \hline & x^{11} + x^4 + x^3 \\ & x^{11} + x^7 + x^6 + x^4 + x^3 \\ \hline & x^7 + x^6 + 1 \end{array}$$

Therefore, $f(x) \times g(x) \bmod m(x) = x^7 + x^6 + 1$.

3. Explain the bitwise XOR operation which involved in RC4.

- Definition of Stream cipher

Stream cipher **encrypts plaintext one byte at a time**, although a stream cipher may be designed to operate on one bit at a time or on units larger than a byte at a time.

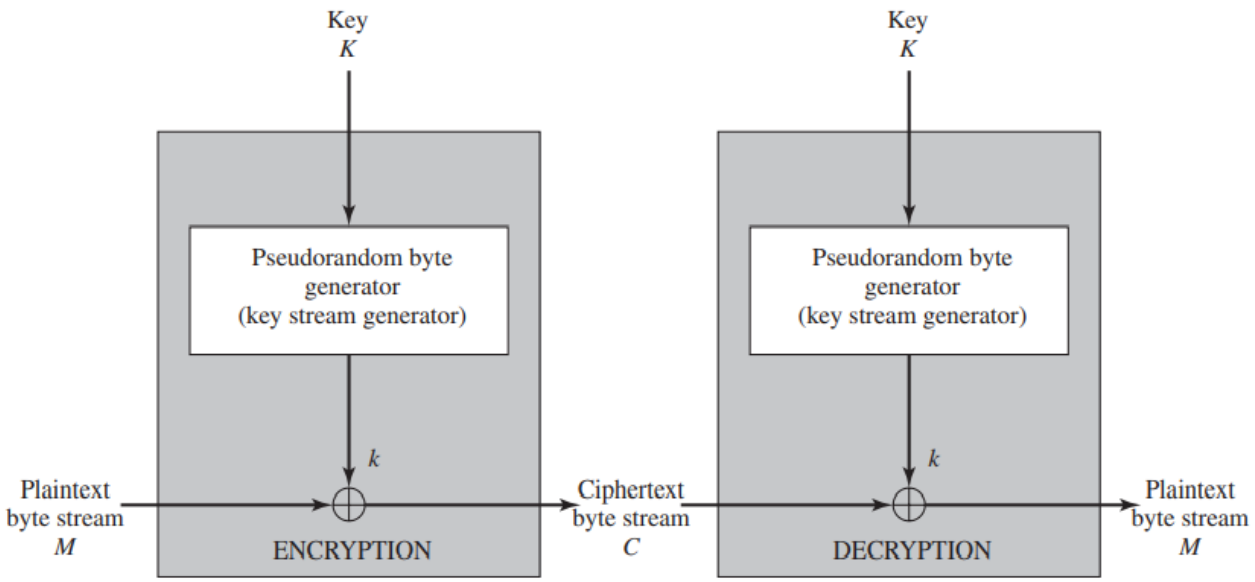


Figure Stream Cipher Diagram

- Figure 7.5 is a representative diagram of stream cipher structure.

- In this structure, **a key** is input to a **pseudorandom bit generator** that produces a stream of 8-bit numbers that are apparently random.
- The output of the generator, called **a keystream**, is combined **one byte at a time** with the plaintext stream using the bitwise exclusive-OR (XOR) operation.
- For example, if the next byte generated by the generator is 01101100 and the next plaintext byte is 11001100, then the resulting ciphertext byte is

```
  11001100  plaintext
⊕ 01101100  key stream
  10100000  ciphertext
```

Decryption requires the use of the same pseudorandom sequence:

```
  10100000  ciphertext
⊕ 01101100  key stream
  11001100  plaintext
```

The **stream cipher** is similar to the **one-time pad** .

Difference between onetimepad and Stream Cipher

The difference is that ***a one-time pad*** uses a ***genuine random number stream***, where as a ***stream cipher*** uses a **pseudorandom number stream.**

Note

Pseudorandom number

The set of values or elements that is statistically random, but it is derived from a known **starting point** and is typically **repeated over and over.**.

Design considerations for a stream cipher

List important design considerations for a stream cipher.

1.The encryption sequence should have a large period

- The **encryption sequence** should have **a large period**.
- A ***pseudorandom number generator*** uses a ***function that produces a deterministic stream of bits*** that **eventually repeats**.
- The ***longer the period of repeat*** the more difficult it will be to do cryptanalysis.
- This is essentially the same consideration that was discussed with reference to the Vigenère cipher, namely that ***the longer the keyword*** the ***more difficult the cryptanalysis.***

2.The ***keystream should approximate*** the **properties of a true random number stream** as close as possible.

- For example, there should be an **approximately equal number of 1s and 0s.**

- If the ***keystream is treated as a stream of bytes***, then all of the ***256 possible byte values*** should appear approximately equally often.
- The more **random-appearing the keystream** is, ***the more randomized the ciphertext*** is, making **cryptanalysis more difficult**.

3. The **output of the pseudorandom number generator** depends on **the value of the input key**.

To ***guard against brute-force attacks***, the ***key*** needs to be ***sufficiently long***.

The **same considerations that apply to block ciphers** are valid here. Thus, with current technology, **a key length of at least 128 bits is desirable**.

Cipher	Key Length	Speed (Mbps)
DES	56	9
3DES	168	3
RC2	Variable	0.9
RC4	Variable	45

Advantages of Stream Cipher

- With a properly designed pseudorandom number generator, a stream cipher can be as secure as a block cipher of comparable key length.
- **Stream ciphers** that ***do not use block ciphers*** as a building block are typically **faster and use far less code than do block ciphers**.
- For applications that require encryption/decryption of a stream of data, such as over a data communications channel or a browser/Web link, a stream cipher might be the better alternative.

Draw backs of Stream Cipher

- **Cryptanalysis** is easy
- If the two ciphertext streams are XORed together, the result is the XOR of the original plaintexts.
- If the ***plaintexts are text strings***, credit card numbers, or other byte streams with known properties, then cryptanalysis may be successful

- Initialization of S
- Stream Generation
- Strength of RC4

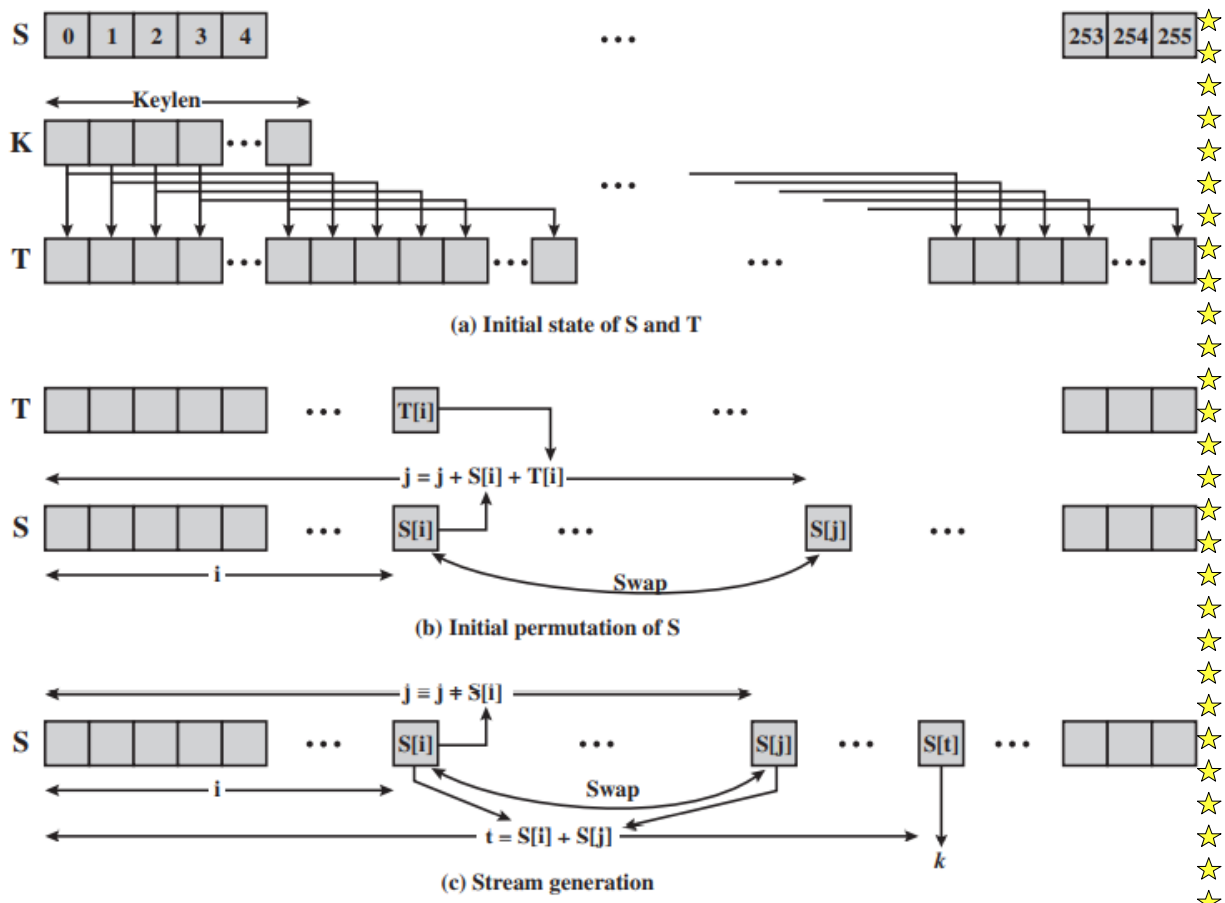


Figure 7.6 RC4

3.Demonstrate that the set of polynomials whose coefficients form a field is a ring.

In cryptography and algebraic structures, it's common to work with sets of polynomials whose coefficients come from a field. To demonstrate that the set of polynomials whose coefficients form a field is a ring, we need to show that it satisfies the properties of a ring, which are:

- Closure under addition.
- Closure under multiplication.
- Associativity of addition.
- Commutativity of addition.
- Existence of an additive identity.
- Existence of additive inverses.
- Associativity of multiplication.
- Distributive property.

Let's go through these properties step by step:

Assumption: We are working with a field F, which means F is a set with two binary operations, addition (+) and multiplication (*), such that F satisfies all the

field axioms (like commutativity, associativity, existence of additive and multiplicative identities, and existence of additive and multiplicative inverses).

Now, let R be the set of all polynomials with coefficients from F. Let's denote this set as R = F[x], where x represents an indeterminate.

Closure under Addition:

For any two polynomials f(x) and g(x) in F[x], their sum f(x) + g(x) is also a polynomial in F[x].

Therefore, F[x] is closed under addition.

Closure under Multiplication:

For any two polynomials f(x) and g(x) in F[x], their product f(x) * g(x) is also a polynomial in F[x].

Therefore, F[x] is closed under multiplication.

Associativity of Addition:

Addition of polynomials is associative, which follows from the associativity of addition in the field F.

Commutativity of Addition:

Addition of polynomials is commutative, which follows from the commutativity of addition in the field F.

Existence of an Additive Identity:

The zero polynomial, denoted as 0(x) or simply 0, serves as the additive identity. It's a polynomial with all coefficients equal to the additive identity (0) in the field F.

Existence of Additive Inverses:

For any polynomial f(x) in F[x], there exists a polynomial -f(x) such that f(x) + (-f(x)) = 0. This is because in a field, every element has an additive inverse.

Associativity of Multiplication:

Multiplication of polynomials is associative, which follows from the associativity of multiplication in the field F.

Distributive Property:

The distributive property holds for polynomials over a field. For any polynomials f(x), g(x), and h(x) in F[x], we have: f(x) * (g(x) + h(x)) = f(x) * g(x) + f(x) * h(x).

Since **the set of polynomials F[x] satisfies all the properties of a ring,** it is indeed a ring. This is a fundamental concept in algebraic structures used in cryptography, where polynomial rings over finite fields are often employed for various cryptographic algorithms and protocols.

4.Discuss the properties that are to be satisfied by Groups,Rings and Fields.

Groups

A **group** G, sometimes denoted by $\{G, \bullet\}$, is a set of elements with a binary operation denoted by $\bullet$ that associates to each ordered pair (a, b) of elements in G an element $(a \bullet b)$ in G, such that the following axioms are obeyed:[4]

(A1) Closure:	If a and b belong to G, then $a \bullet b$ is also in G.
(A2) Associative:	$a \bullet (b \bullet c) = (a \bullet b) \bullet c$ for all a, b, c in G.
(A3) Identity element:	There is an element e in G such that $a \bullet e = e \bullet a = a$ for all a in G.
(A4) Inverse element:	For each a in G, there is an element a' in G such that $a \bullet a' = a' \bullet a = e$.

If a ***group has a finite number of elements***, it is referred to as **a finite group,** and the ***order of the group*** is equal to the ***number of elements in the group***. Otherwise, the group is **an infinite group**.

A group is said to ***be abelian*** if it satisfies the following additional condition:

(A5) Commutative:	$a \bullet b = b \bullet a$ for all a, b in G.

Abelian Group

A group is said to ***be abelian*** if it satisfies the following additional condition:

(A5) Commutative:	$a \bullet b = b \bullet a$ for all a, b in G.

Cyclic Group

A **group is cyclic** if every **element of is a power** (is an integer) of a ***fixed element*** .

The element is said to ***generate the group or to be a generator of G***.

A cyclic group is always ***abelian and may be finite or infinite.***

Ring

A **ring** R, sometimes denoted by $\{R, +, \times\}$, is a set of elements with two binary operations, called *addition* and *multiplication*,[6] such that for all a, b, c in R the following axioms are obeyed.

(A1–A5) R is an abelian group with respect to addition; that is, R satisfies axioms A1 through A5. For the case of an additive group, we denote the identity element as 0 and the inverse of a as $-a$.

(M1) Closure under multiplication: If a and b belong to R, then ab is also in R.

(M2) Associativity of multiplication: $a(bc) = (ab)c$ for all a, b, c in R.

(M3) Distributive laws: $a(b + c) = ab + ac$ for all a, b, c in R.
$(a + b)c = ac + bc$ for all a, b, c in R.

A ring is said to be **commutative** if it satisfies the following additional condition:

(M4) Commutativity of multiplication: $ab = ba$ for all a, b in R.

Next, we define an **integral domain**, which is a commutative ring that obeys the following axioms.

(M5) Multiplicative identity: There is an element 1 in R such that $a1 = 1a = a$ for all a in R.

(M6) No zero divisors: If a, b in R and $ab = 0$, then either $a = 0$ or $b = 0$.

Fields

A **field** F, sometimes denoted by $\{F, +, \times\}$, 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.

(A1–M6) F is an integral domain; that is, F satisfies axioms A1 through A5 and M1 through M6.

(M7) Multiplicative inverse: For each a in F, except 0, there is an element a^{-1} in F such that $aa^{-1} = (a^{-1})a = 1$.

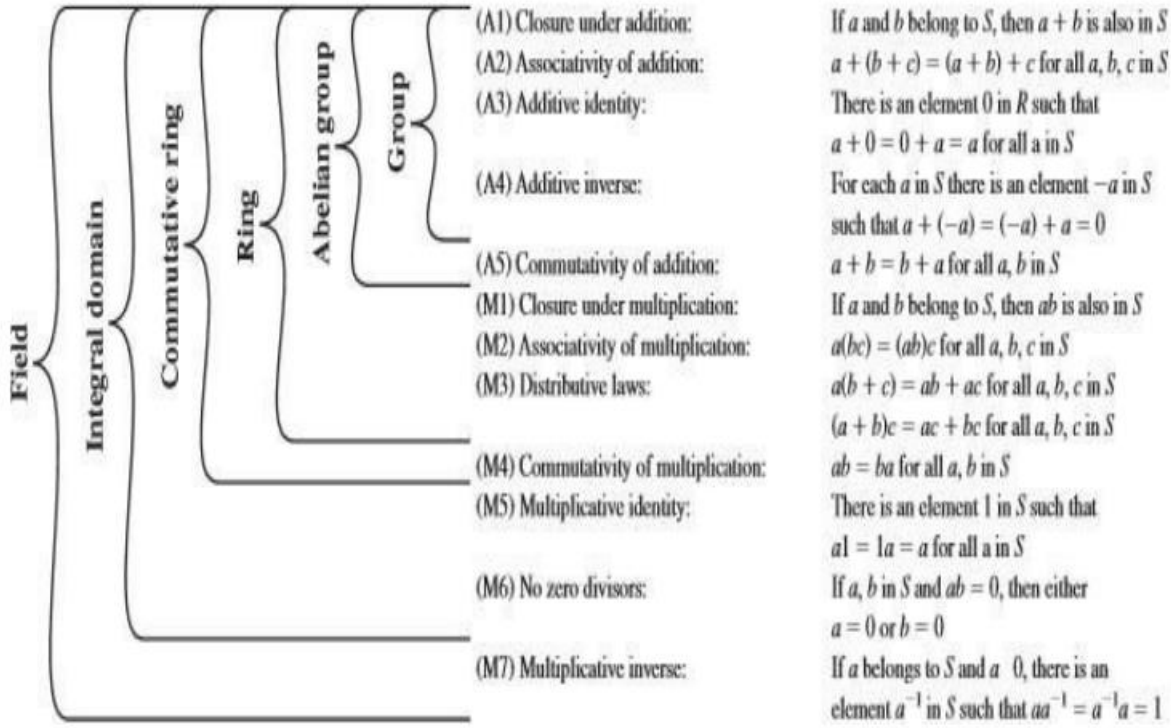


Figure 2.2 Groups, Ring and Field

5.For each of the following element of DES,indicate the comparable element in AES available

(i)XOR of subkey material with the input to the function.

<u>Adding the Key</u>

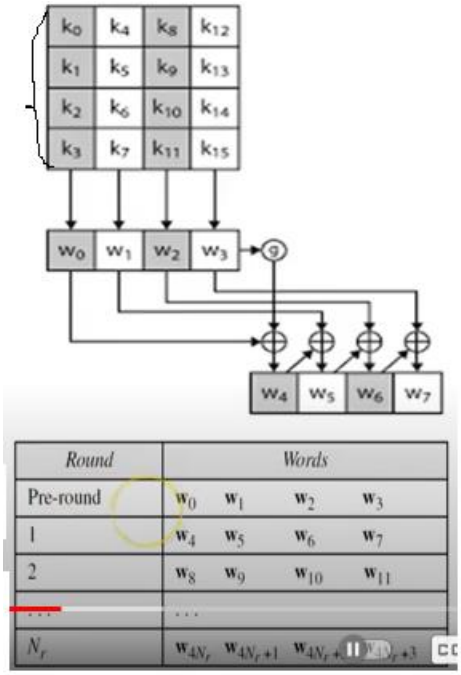
In this the **128 bits of State** are **bitwise XORed** with the ***<u>128bits of the round key.</u>***

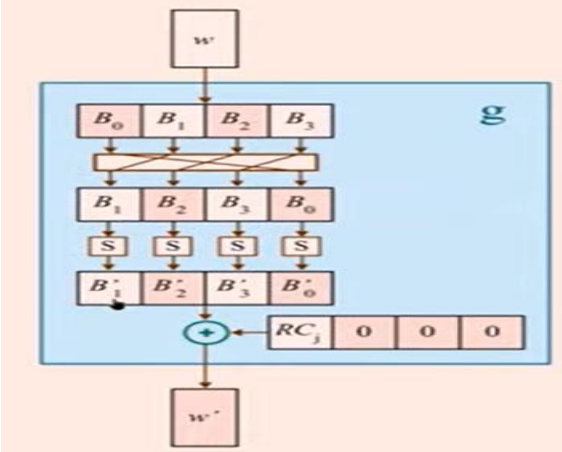
(ii)f Function-function g in Key expansion

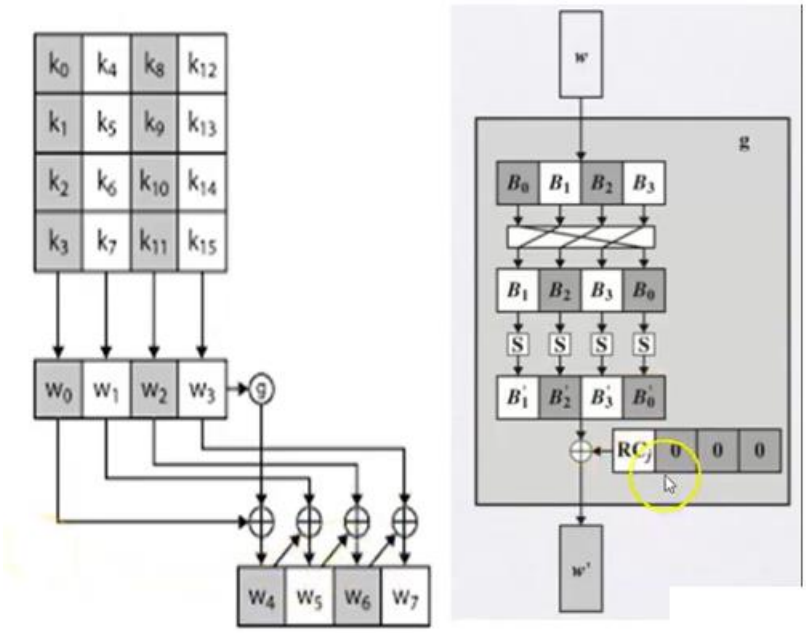
(iii)Permutation p –Mix Columns

(iv)Swapping of halves of the block

6.(i)Describe in detail the key generation in AES algorithm and its expansion format.





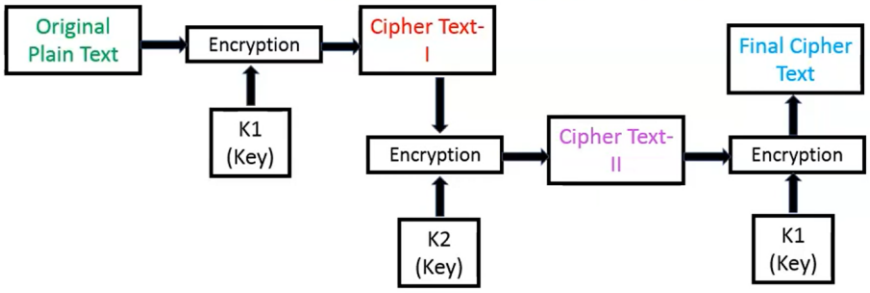


(ii)**Describe triple DES and its applications.**

Triple DES makes use of three stages of the DES algorithm, using ***a total of two or three distinct keys***

Triple DES with 2 keys (Encryption)

- Triple DES performs the same operation as double DES.
- Triple DES using two keys K1 & K2 while encrypting plain text.
- First it performs encryption on plaintext P, which is encrypted using K1 obtains first cipher text C1.
- Again this cipher text is encrypted using key K2 which obtain the second cipher text C2.
- Which is again encrypted using K1 & generate final cipher text C3.



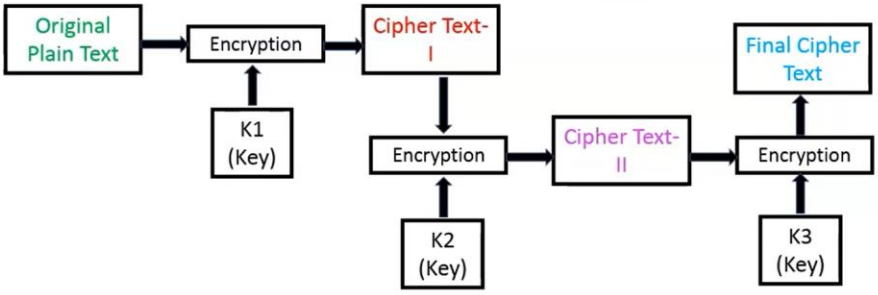
Mathematically triple DES (with 2 keys) encryption is represented as,

1. **C1 = E (K1, P)**
2. **C2 = E (K2, C1)**
   C2 = E (K2, E (K1, P))
3. **C3 = E (K1, C2)**
   C3 = E (K1, E (K2, C1))
   C3 = E (K1, E (K2, E (K1, P)))

Where, P = Plain text, K1 = Key – 1, K2 = Key – 2, C1 = first cipher text, C2 = second cipher te
C3 = Final cipher text, E = Encryption Process

Triple DES with 3 keys (Encryption)

- Triple DES performs the same operation as double DES.
- Triple DES using three keys K1, K2 & K3 while encrypting plain text.
- First it performs encryption on plaintext P, which is encrypted using K1 and obtains first cipher text C1.
- Again this cipher text is encrypted using key K2 which obtain the second cipher text C2.
- Which is again encrypted using K3 & generate final cipher text C3.



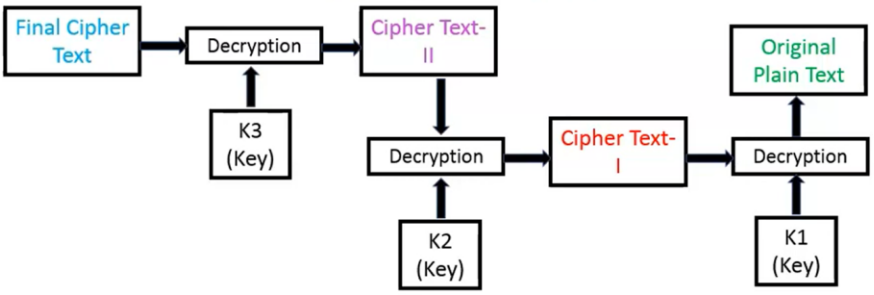
Mathematically triple DES (with 3 keys) encryption is represented as,

1. **C1 = E (K1, P)**
2. **C2 = E (K2, C1)**
   C2 = E (K2, E (K1, P))
3. **C3 = E (K3, C2)**
   C3 = E (K3, E (K2, C1))
   C3 = E (K3, E (K2, E (K1, P)))

Where, P = Plain text, K1 = Key – 1, K2 = Key – 2, K3 = Key – 3, C1 = first cipher text,

Triple DES with 3 keys (Decryption)

- Decryption of Triple DES is reverse of encryption.
- In triple DES decryption process final cipher text C3 decrypt using K3, result is cipher text C2.
- C2 will be decrypt with K2 and get C1 cipher text.
- Then C1 cipher text decrypt with K1 key and get original plain text P.



Mathematically triple DES (with 3 keys) decryption is represented as,

1. **C2 = D (K3, C3)**
2. **C1 = D (K2, C2)**
   C1 = D (K2, D (K3, C3))
3. **P = D (K1, C1)**
   P = D (K1, D (K2, C2))
   P = D (K1, D (K2, D (K3, C3)))

Where, P = Plain text, K1 = Key – 1, K2 = Key – 2, K3 = Key – 3, C1 = first cipher text, C2 = second cipher text, C3 = Final cipher text, D = Decryption Process

Applications

A number of Internet-based applications have adopted **three-key 3DES**, including **PGP and S/MIME**

6. Explain the Key Generation, Encryption and Decryption of SDES algorithm in detail

SIMPLIFIED DATA ENCRYPTION STANDARD (S-DES)

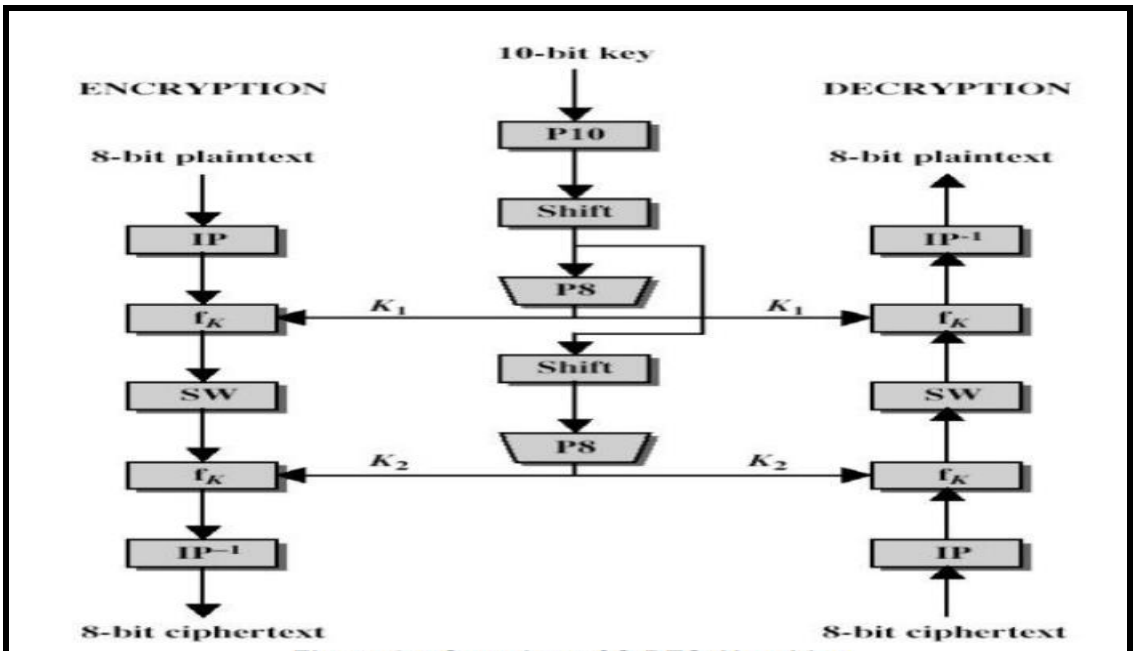


Figure 2.5 Overview of S-DES Algorithm

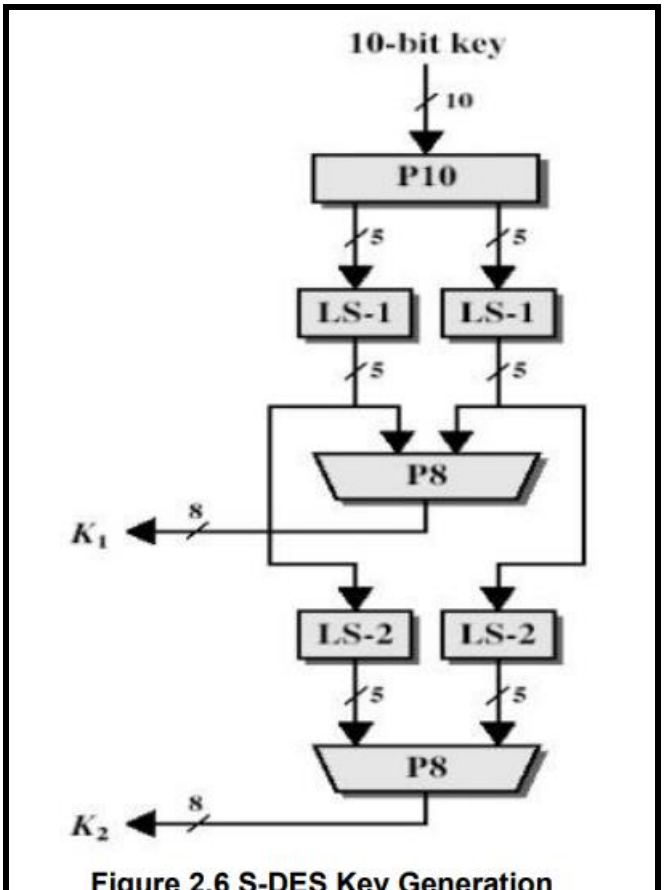


Figure 2.6 S-DES Key Generation

Other Questions

1.Block Cipher Modes of Operation

- Need of Modes of Block Cipher

(i)Electronic Code Book

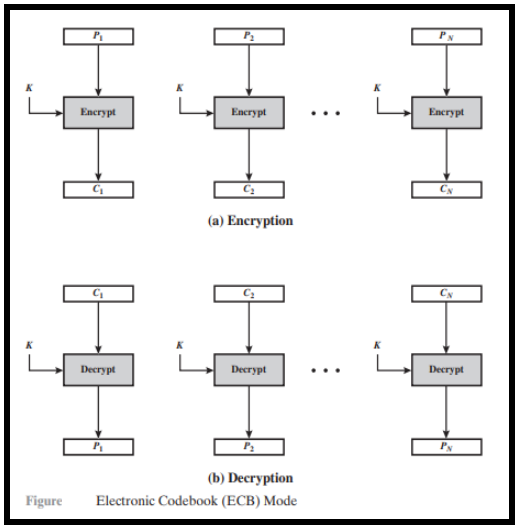


Figure Electronic Codebook (ECB) Mode

(ii) Cipher Block Chaining Mode

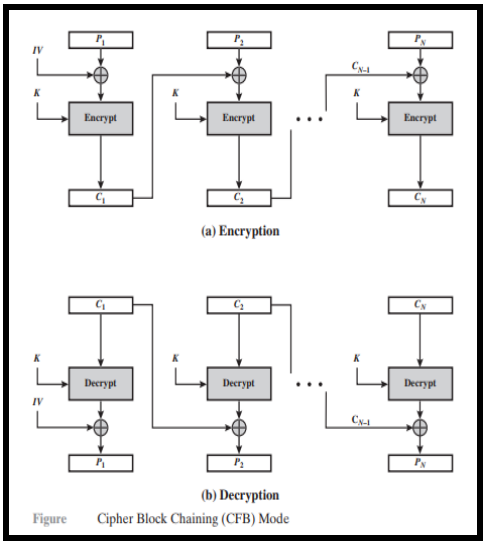


Figure Cipher Block Chaining (CFB) Mode

Advantages and Disadvantages of ECB

CIPHER FEEDBACK MODE[Stream Cipher Mode]

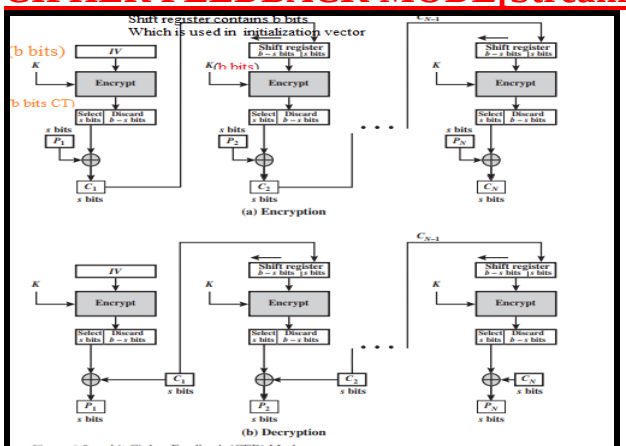


Figure 6.5 s-bit Cipher Feedback (CFB) Mode

Output Feedback Mode

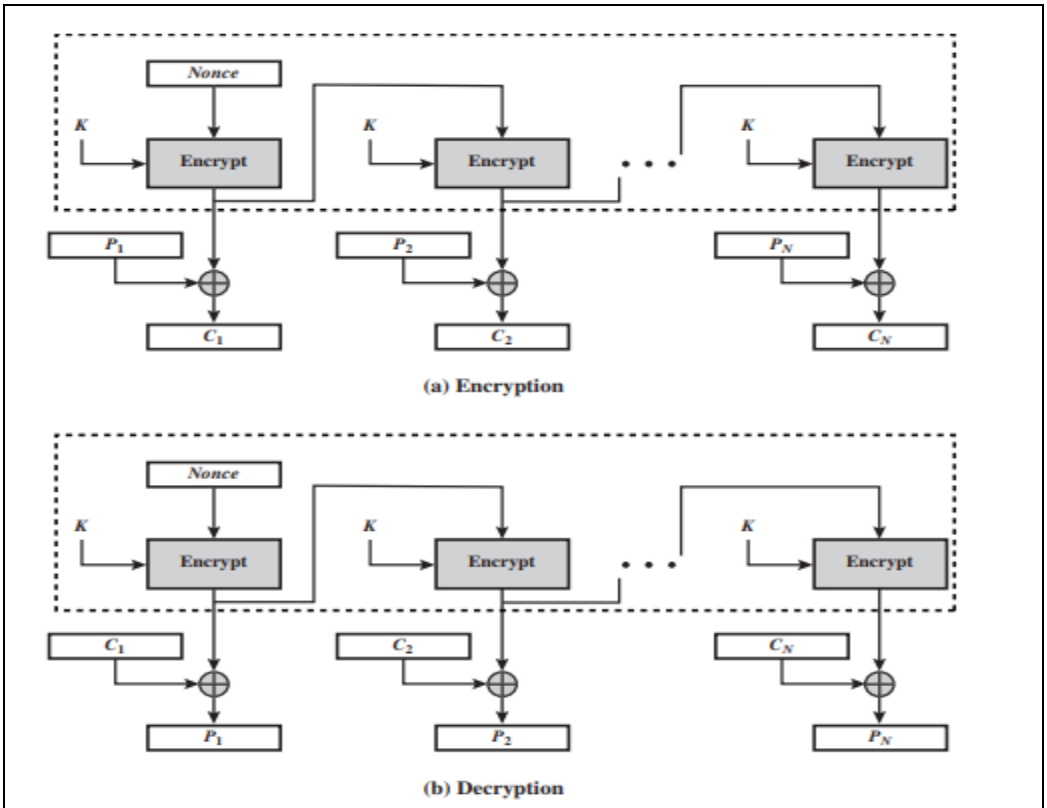


Figure 6.6 Output Feedback (OFB) Mode

COUNTER MODE

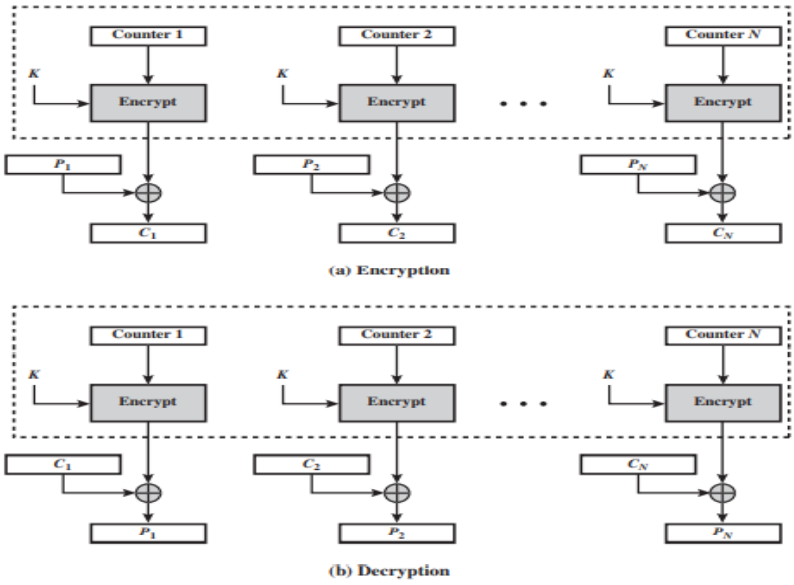


Figure 6.7 Counter (CTR) Mode

Table 6.1 Block Cipher Modes of Operation

Mode	Description	Typical Application
Electronic Codebook (ECB)	Each block of 64 plaintext bits is encoded independently using the same key.	• Secure transmission of single values (e.g., an encryption key)
Cipher Block Chaining (CBC)	The input to the encryption algorithm is the XOR of the next 64 bits of plaintext and the preceding 64 bits of ciphertext.	• General-purpose block-oriented transmission • Authentication
Cipher Feedback (CFB)	Input is processed *s* bits at a time. Preceding ciphertext is used as input to the encryption algorithm to produce pseudorandom output, which is XORed with plaintext to produce next unit of ciphertext.	• General-purpose stream-oriented transmission • Authentication
Output Feedback (OFB)	Similar to CFB, except that the input to the encryption algorithm is the preceding encryption output, and full blocks are used.	• Stream-oriented transmission over noisy channel (e.g., satellite communication)
Counter (CTR)	Each block of plaintext is XORed with an encrypted counter. The counter is incremented for each subsequent block.	• General-purpose block-oriented transmission • Useful for high-speed requirements

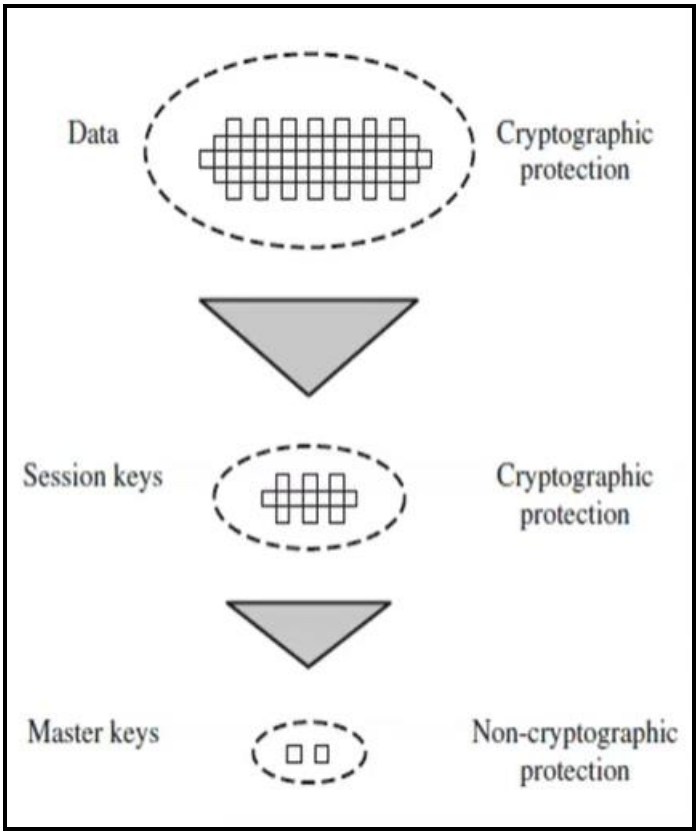
2.Design Principles of block cipher

- DES Design Criteria
  - Criteria for the S-boxes
  - Criteria for the permutation P
  - Number of Rounds
- Design of Function F
- Key Schedule Algorithm

3.Key Distribution in Symmetric Encryption

Key Distribution between two parties

Symmetric Key Distribution using Symmetric Encryption



- Key Distribution Scenario
- A transparent key control scheme

UNIT III PUBLIC KEY CRYPTOGRAPHY

1.User X and Y exchange the key using Diffie Hellman algorithm.Assume a=5 q=11 XA=2 XB=3..Find the value of YA,YB and k[Nov/Dec 2022]

In the Diffie-Hellman key exchange algorithm, two parties, X and Y, exchange public keys and then use each other's public keys to compute a shared secret key. Let's go step by step:

Given parameters:

- Prime modulus (q) = 11
- Primitive root (a) = 5
- Private key of X (XA) = 2
- Private key of Y (XB) = 3

1. Calculate the public key for X (YA):
   YA = (a^XA) % q
   YA = (5^2) % 11
   YA = 25 % 11
   YA = 3
2. Calculate the public key for Y (YB):
   YB = (a^XB) % q
   YB = (5^3) % 11
   YB = 125 % 11
   YB = 8

1. Calculate the shared secret key (k) by both X and Y:

   For X:

   kX = (YB^XA) % q

   kX = (8^2) % 11

   kX = 64 % 11

   kX = 9

   For Y:

   kY = (YA^XB) % q

   kY = (3^3) % 11

   kY = 27 % 11

   kY = 5

Now, X and Y both have the same shared secret key:

- kX = 9 (computed by X)
- kY = 5 (computed by Y)

The Diffie-Hellman key exchange is successful, and X and Y share the secret key "k," where k = 9 for X and k = 5 for Y.

2. What mathematical problem is behind security of the ElGamal cryptosystems [Nov/Dec 2022]

The security of the ElGamal cryptosystem is based on the difficulty of solving the **discrete logarithm problem (DLP**) in a finite field or elliptic curve group.

The mathematical problem at the core of ElGamal security is the discrete logarithm problem, and it plays a fundamental role in many public key cryptography systems.
Here's a brief overview of the discrete logarithm problem:
Discrete Logarithm Problem (DLP): Given a group G, a generator g of that group, and an element h in G, find the integer x such that **g^x = h**.
In other words, given h, find the exponent x that was used to compute h from the generator g.

2.For p = 11 and q = 19 and choose d = 17. Apply RSA algorithm where Cipher message = 80 and thus find the plain text

8. For p=11 and q=19 and choose d=19 and e=11 find the plain text where cipher message = 80. Find the plain text.

Given

$p = 11, \quad q = 19 \quad d = 19 \quad C = 80$

$n = p \times q = 11 \times 19 = 209$

$M = C^d \bmod n$

$M = 80^d \bmod 209$

$M = 80^{19} \bmod 209$

$80^{19} = 80^1 \times 80^2 \times 80^4 \times 80^8 \times 80^2$

$= 80 \times 6400 \times 40{,}960{,}000 \times 40{,}960{,}000 \times 40{,}960{,}000 \times 6400$

$80^1 \bmod 209 = 80$

$80^2 \bmod 209 = 130$

$80^4 \bmod 209 = 130 \times 130 = 180$

$80^8 \bmod 209 = 180 \times 180 = 5$

$M = 80 \times 130 \times 180 \times 180 \times 180$

$M = 144$

3.Find gcd(2740, 1760) using Euclidean Algorithm. by using formula gcd(a,b)

Find the greatest common divisor (GCD) of two numbers using the Euclidean algorithm

1. Start with $a = 2740$ and $b = 1760$.
2. Calculate $a \mod b$:
   $a \mod b = 2740 \mod 1760 = 980$
3. Now, set $a = b$ and $b = a \mod b$:
   $a = 1760$ and $b = 980$
4. Calculate $a \mod b$:
   $a \mod b = 1760 \mod 980 = 780$
5. Again, set $a = b$ and $b = a \mod b$:
   $a = 980$ and $b = 780$
6. Continue this process:
   $a \mod b = 980 \mod 780 = 200$
   $a = 780$ and $b = 200$
7. Repeat:
   $a \mod b = 780 \mod 200 = 180$
   $a = 200$ and $b = 180$
8. Repeat:
   $a \mod b = 200 \mod 180 = 20$
   $a = 180$ and $b = 20$
9. Repeat:
   $a \mod b = 180 \mod 20 = 0$
10. Now, a is 20, and b is 0. According to the algorithm, when b becomes 0, the GCD is the non-zero value of a. So, the GCD of 2740 and 1760 is 20.

Therefore, the GCD of 2740 and 1760 is indeed 20, as calculated using the Euclidean algorithm.

4. Using Fermat's theorem, check whether 19 is prime or not? Consider a is 7.

Fermat's Little Theorem states that if p is a prime number and a is an integer not divisible by p, then:

$$a^{p-1} \equiv 1 \pmod{p}$$

In other words, if a^{p-1} leaves a remainder of 1 when divided by p, then p is prime. However, if a^{p-1} does not leave a remainder of 1 when divided by p, then p is definitely not prime.

In your case, you want to check whether 19 is prime or not with $a = 7$. So, calculate $7^{18} \pmod{19}$:

$$7^{18} \equiv 1 \pmod{19}$$

Since 7^{18} leaves a remainder of 1 when divided by 19, according to Fermat's Little Theorem, 19 is a prime number.

So, 19 is indeed prime.

5. Find atleast two points lies in the elliptic curve y^2=x^3+2x+3(mod 5)

To find points on the elliptic curve $y^2 \equiv x^3 + 2x + 3 \pmod{5}$, you can try different values of x and calculate the corresponding y values. Remember that you need to check for residues modulo 5. Here are some values of x and their corresponding y values:

1. $x = 0$:
   $y^2 \equiv 0^3 + 2 \cdot 0 + 3 \equiv 3 \pmod{5}$
   There are no integers y such that $y^2 \equiv 3 \pmod{5}$.
2. $x = 1$:
   $y^2 \equiv 1^3 + 2 \cdot 1 + 3 \equiv 6 \equiv 1 \pmod{5}$
   So, $y = \pm 1$ are solutions.
3. $x = 2$:
   $y^2 \equiv 2^3 + 2 \cdot 2 + 3 \equiv 11 \equiv 1 \pmod{5}$
   Again, $y = \pm 1$ are solutions.

4. $x = 3$:
   $y^2 \equiv 3^3 + 2 \cdot 3 + 3 \equiv 30 \equiv 0 \pmod 5$
   So, $y = 0$ is a solution.
5. $x = 4$:
   $y^2 \equiv 4^3 + 2 \cdot 4 + 3 \equiv 75 \equiv 0 \pmod 5$
   Here, $y = 0$ is also a solution.

So, two points on the elliptic curve $y^2 \equiv x^3 + 2x + 3 \pmod 5$ are:

1. $(1, 1)$
2. $(2, 1)$

These are two points that lie on the curve modulo 5.

6.Find the gcd(68,8) using Euclidean Algorithm [Apr/May 2023]

$\mathrm{GCD}(a, b) = \mathrm{GCD}(b, a \mod b)$
In this case, $a = 68$ and $b = 8$, so:

$$\mathrm{GCD}(68, 8) = \mathrm{GCD}(8, 68 \mod 8)$$

Now, let's calculate $68 \mod 8$:

$$68 \mod 8 = 4$$

So, we have:

$$\mathrm{GCD}(68, 8) = \mathrm{GCD}(8, 4)$$

Now, we can continue applying the formula:

$$\mathrm{GCD}(8, 4) = \mathrm{GCD}(4, 8 \mod 4)$$

Calculate $8 \mod 4$:

$$8 \mod 4 = 0$$

$\mathrm{GCD}(4, 0)$

When you reach a remainder of 0, the GCD is the non-zero value from the previous step, which is 4.

So, $\mathrm{GCD}(68, 8) = 4$,

7.Find φ(21)(April /May 2023)

Answer

1. Prime Factorization of 21:

   $21 = 3 \times 7$

2. Euler's Totient Formula for Composite Numbers:

   For a positive integer n represented as a product of its prime factors as $n = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_k^{a_k}$, where $p_1, p_2, \ldots, p_k$ are distinct prime factors, you can calculate φ(n) using the formula:

   $\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_k}\right)$

   For 21, which is $21 = 3 \cdot 7$, you can calculate φ(21) as follows:

   $\varphi(21) = 21\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{7}\right) = 21 \cdot \frac{2}{3} \cdot \frac{6}{7} = 12$

So, φ(21) is equal to 12. There are 12 positive integers less than or equal to 21 that are coprime to 21.

8. Find the value of 7^8 mod 15 Using Euler's Theorem

Euler's Theorem states that if a and n are coprime (i.e., a and n have no common factors other than 1), then:

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

where $\phi(n)$ is Euler's totient function, which counts the number of positive integers less than n that are coprime to n.

In this case, you want to find the value of $7^8 \mod 15$. First, let's calculate $\phi(15)$:

$$15 = 3 \times 5$$

$$\phi(15) = 15\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 15 \times \frac{2}{3} \times \frac{4}{5} = 8$$

Now, using Euler's Theorem:

$$7^8 \equiv 1 \pmod{15}$$

Therefore, the value of $7^8 \mod 15$ is 1.

9.Find the multiplicative inverse of 313 in modulo 67

1. Use the Extended Euclidean Algorithm to find the greatest common divisor (GCD) of 313 and 67 while keeping track of coefficients:

   $313 = 4 \cdot 67 + 45$

   $67 = 1 \cdot 45 + 22$

   $45 = 2 \cdot 22 + 1$

2. Now, work backward to find the coefficients that satisfy the equation $313x + 67y = 1$:

   Starting with the last equation: $45 = 2 \cdot 22 + 1$

   Rewriting it as: $1 = 45 - 2 \cdot 22$

   Then using the equation $67 = 1 \cdot 45 + 22$:

   $1 = 45 - 2 \cdot (67 - 1 \cdot 45) = 3 \cdot 45 - 2 \cdot 67$

   Next, using the equation $313 = 4 \cdot 67 + 45$:

   $1 = 3 \cdot 45 - 2 \cdot 67 = 3 \cdot (313 - 4 \cdot 67) - 2 \cdot 67$

   Simplifying further:

   $1 = 3 \cdot 313 - 14 \cdot 67$

3. Now, notice that the coefficient of 313 is 3. Since we're looking for the multiplicative inverse of 313 modulo 67, we need the coefficient of 313 to be positive and less than 67. To achieve this, we can reduce 3 modulo 67:

   $3 \equiv 3 \pmod{67}$

So, the multiplicative inverse of 313 in modulo 67 is 3.

Reg

10.Write the difference between public key and private key crypto systems? (APR/MAY 2012&APR/MAY 2017)(Analysis)

S.NO	PRIVATE KEY	PUBLIC KEY
1.	Private key is faster than public key.	It is slower than private key.
2.	In this, the same key (secret key) and algorithm is used to encrypt and decrypt the message.	In public key cryptography, two keys are used, one key is used for encryption and while the other is used for decryption.
3.	In private key cryptography, the key is kept as a secret.	In public key cryptography, one of the two keys is kept as a secret.
4.	Private key is **Symmetrical** because there is only one key that is called secret key.	Public key is **Asymmetrical** because there are two types of key: private and public key.
5.	In this cryptography, sender and receiver need to share the same key.	In this cryptography, sender and receiver does not need to share the same key.
6.	In this cryptography, the key is private.	In this cryptography, public key can be public and private key is private.

11.State whether symmetric and asymmetric cryptographic algorithms need key exchange? (APR/MAY 2014)(Analysis)

- Key exchange is a method in cryptography by which cryptographic keys are exchanged between two parties, allowing use of a cryptographic algorithm.
- Symmetric encryption requires the sender and receiver to share a secret key.
- Asymmetric encryption requires the sender and receiver to share a public key.
- If the cipher is a symmetric key cipher, both will need a copy of the same key.
- If an asymmetric key cipher with the public/private key property, both will need the other's public key

12.What is the Fermat's theorem? (Nov/Dec 2017)? (Remember)

Fermat's theorem states the following: If p is prime and a is a positive integer not divisible by p, then

$$\boxed{a^{p-1} \equiv 1 \pmod{p}}$$

Uses of Fermat's Theorem

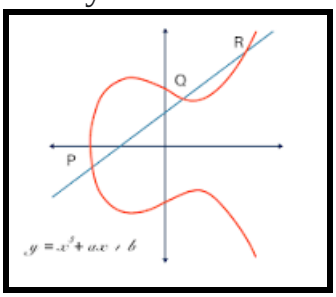
- This theorem is method of ***determining maxima and minima***: in one dimension, one can find ***extreme by simply computing the stationary points*** (by computing the zeros of the derivative), the non- differentiable points, and the boundary points, and then investigating this set to determine the extreme.

- One can do this either ***by evaluating the function at each point and taking the maximum, or by analyzing the derivatives*** further, using the first derivative test, the second derivative test, or the higher-order derivative test.
- In dimension above 1, one cannot use the first derivative test any longer, but the second derivative test and higher-order derivative test generalize.

13.Define Elliptic curve[Nov/Dec 2016]

It is a plane curve over a finite field which is made up of the points satisfying the equation: $\mathbf{y^2=x^3 + ax + b.}$

In this elliptic curve cryptography example, any point on the curve can be mirrored over the x-axis and the curve will stay the same.



14. Perform encryption for the plain text M=88 using the RSA algorithm with p=17 and q=11 e=7.[Nov/Dec 2017]

For this example, the keys were generated as follows.

1. Select two prime numbers, $p = 17$ and $q = 11$.
2. Calculate $n = pq = 17 \times 11 = 187$.
3. Calculate $\phi(n) = (p-1)(q-1) = 16 \times 10 = 160$.
4. Select e such that e is relatively prime to $\phi(n) = 160$ and less than $\phi(n)$; we choose $e = 7$.
5. Determine d such that $de \equiv 1 \pmod{160}$ and $d < 160$. The correct value is $d = 23$, because $23 \times 7 = 161 = (1 \times 160) + 1$; d can be calculated using the extended Euclid's algorithm (Chapter 4).

The resulting keys are public key $PU = \{7, 187\}$ and private key $PR = \{23, 187\}$. The example shows the use of these keys for a plaintext input of $M = 88$. For encryption, we need to calculate $C = 88^7 \bmod 187$. Exploiting the properties of modular arithmetic, we can do this as follows.

$$88^7 \bmod 187 = [(88^4 \bmod 187) \times (88^2 \bmod 187) \times (88^1 \bmod 187)] \bmod 187$$

$$88^1 \bmod 187 = 88$$

$$88^2 \bmod 187 = 7744 \bmod 187 = 77$$

$$88^4 \bmod 187 = 59{,}969{,}536 \bmod 187 = 132$$

$$88^7 \bmod 187 = (88 \times 77 \times 132) \bmod 187 = 894{,}432 \bmod 187 = 11$$

15.Difference between Conventional and Public Key Encryption

Table 9.2 Conventional and Public-Key Encryption

Conventional Encryption	Public-Key Encryption
Needed to Work: 1. The same algorithm with the same key is used for encryption and decryption. 2. The sender and receiver must share the algorithm and the key. *Needed for Security:* 1. The key must be kept secret. 2. It must be impossible or at least impractical to decipher a message if no other information is available. 3. Knowledge of the algorithm plus samples of ciphertext must be insufficient to determine the key.	*Needed to Work:* 1. One algorithm is used for encryption and decryption with a pair of keys, one for encryption and one for decryption. 2. The sender and receiver must each have one of the matched pair of keys (not the same one). *Needed for Security:* 1. One of the two keys must be kept secret. 2. It must be impossible or at least impractical to decipher a message if no other information is available. 3. Knowledge of the algorithm plus one of the keys plus samples of ciphertext must be insufficient to determine the other key.

18.State Euler's Theorem?[Apr/May 2018]

Euler's Theorem

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

$$a^{\phi(n)} \equiv 1 (\bmod n) \quad \textbf{(8.4)}$$

19. Perform encryption and decryption for the plain text M=8 using the RSA algorithm with p=7 and q=11 e=17.[Apr/May 2018]

P=7; q=11; e=17; M=8. (APRIL/ MAY 2018)

Soln:

n=pq

n=7*11=77

ö(n)=(p-1) (q-1) =6*10 = 60

e=17

d =27

C= M^e mod n

C = 8^{17} mod 77 = 57

M = C^d mod n = 57^{27} mod 77 = 8

20.Give the applications of public key crypto systems [Apr/May 2019]

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

- **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.
- **Key exchange:** Both sender & receiver cooperate to exchange a session key.

21. What Primality testing . Mention any three Primality testing methods

Primality testing method is a method to find and to prove whether the given number is prime number.

Methods

1. Native Algorithm

2. Fermat's Primality Test
3. Miller – Rabin Primality Test

22. what is Miller-Rabin Primality Test

3.Miller – Rabin Primality Test

```
Function Miller-Rabin (x)
  x-1 = (2^w)y     //x is the input number for primality test
                   //y is an odd number a 2

select a randomly in the range [2, (x-1)]
Z = a^y mod x
if Z congruent 1 (mod x) then return prime
for i = 1 to w – 1
{
If Z congruent -1 (mod x) then return prime
Z = Z^2 mod x
}
return composite
```

23. What is Discrete Logarithm

Discrete Logarithm are fundamental to a number of public-key algorithms, including Diffie Hellman key exchange and the digital signature algorithm. Consider the equation

y = g^x mod p

given g, x and p, it is a straight forward matter to calculate y. At the worst, we must perform x repeated multiplications, and algorithms exist for achieving greater Efficiency.

24. Define Euler's Totient Function

- **Euler's Totient Function**, often denoted as φ (phi) or Euler's phi function, is a mathematical function that is used ***to count the number of positive integers less*** than or ***equal to a given positive integer n*** **that are coprime (relatively prime) to n**.

- The formula for **Euler's Totient Function φ(n)** for a **positive integer n** is as follows:
- $\varphi(n) = n * (1 - 1/p_1) * (1 - 1/p_2) * ... * (1 - 1/p_r)$
- where n is the **given positive integer, and p_1, p_2, ..., p_r** are its **distinct prime factors**. This formula essentially involves multiplying n by the product of (1 - 1/p) for each prime factor
- p of n.

25. Requirements of Public Key Cryptography

- **The PKC algorithm must fulfill the following conditions:**

1. It is computationally easy for party B to generate the key pair (PU_b and PR_b)
2. It is **computationally easy for a sender A**, knowing the public key and the message to be encrypted, M, to generate the corresponding ciphertext. $C = E(PU_b, M)$
3. It is **computationally easy for the receiver B** to decrypt the resulting ciphertext using private key to recover the original message. $M = D(PR_b, C) = D(PR_b, E(PU_b, M))$
4. It is **computationally infeasible for an attacker**, to determine private key from known public key.
5. It is **computationally infeasible for an attacker**, to recover original message from known public key and cipher text.

26 Different attacks in RSA

Four possible approaches to attacking **the RSA algorithm** are

- **Brute force**: This involves **trying all possible private keys**.
- **Mathematical attacks**: There are several approaches, all equivalent in effort to factoring the product of two primes.
- **Timing attacks:** These depend on the running time of the decryption algorithm.
- **Chosen ciphertext attacks**: This type of attack exploits properties of the RSA algorithm

27. What is Man in the Middle Attack

A man in the middle (MITM) attack is a general term for when a perpetrator positions himself in a conversation between a user and an application—either to eavesdrop or to impersonate one of the parties, making it appear as if a normal exchange of information is underway.

28. What is Timing attack in RSA

It is a ***side channel attack based on measuring the length of time*** it takes ***digitally sign a message.***

Timing Attack countermeasures

Timing attack is a serious threat, there are simple countermeasures that can be used, including the following.

- **Constant exponentiation time:** Ensure that **all exponentiations** take the **same amount of time before returning a result**. This is a **simple fix** but does ***degrade performance***

29.What are the two uses of public key cryptography regarding keydistribution?

The **two uses of public key cryptography** regarding the issues of key distribution.

They are **1. Distribution of public keys**

2. Use of public key encryption to distribute secret keys

30. Using Fermat's theorem, check whether 19 is prime or not? Consider a is 7.

Fermat's Little Theorem states that if "p" is a prime number and "a" is an integer not divisible by "p," then:

a^(p-1) ≡ 1 (mod p)

In your case, you want to check whether 19 is prime using Fermat's Little Theorem with "a" being 7. So, let's calculate:

a^(p-1) ≡ 7^(19-1) ≡ 7^18 (mod 19)

Now, calculate 7^18 modulo 19:

7^1 ≡ 7 (mod 19)
7^2 ≡ 7 * 7 ≡ 49 ≡ 11 (mod 19)
7^4 ≡ 11^2 ≡ 121 ≡ 8 (mod 19)
7^8 ≡ 8^2 ≡ 64 ≡ 7 (mod 19)
7^16 ≡ 7^8 * 7^8 ≡ 7 * 7 ≡ 49 ≡ 11 (mod 19)

Now, we can calculate 7^18:

Now, we can calculate 7^18:
7^18 ≡ 7^16 * 7^2 ≡ 11 * 11 ≡ 121 ≡ 8 (mod 19)
According to Fermat's Little Theorem, if 19 were prime, then 7^18 would be congruent to 1 (mod 19). However, we found that 7^18 is congruent to 8 (mod 19), which means 7^18 is not congruent to 1 (mod 19).
Therefore, **based on Fermat's Little Theorem, 19 is not prime**.

23. Find the value of 7^8 mod 15 Using Euler's theorem.

To find the value of $7^8 \mod 15$ using Euler's Totient Theorem, we first need to calculate Euler's Totient Function $\phi(15)$, which gives us the count of positive integers less than 15 are relatively prime to 15.

Prime factorization of 15:

$15 = 3 \times 5$

Euler's Totient Function for a number n that is a product of distinct primes is given by:

$\phi(n) = (p_1 - 1) \times (p_2 - 1) \times \ldots \times (p_k - 1)$

In this case:

$\phi(15) = (3 - 1) \times (5 - 1) = 2 \times 4 = 8$

Now, we can apply Euler's Totient Theorem, which states that if a and n are coprime (relatively prime), then:

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

In our case, $a = 7$ and $n = 15$, and we've already calculated $\phi(15) = 8$, so:

$7^8 \equiv 1 \mod 15$

Part B Questions

1.User A and B use the Diffie Hellman key exchange technique,a common prime q=11 and a primitive root alpha =7

(i) If user A has private key XA=3.What is A's public key YA? (4)

(ii) If user B has private key XB=6. What is B's public key YB? (4)

(iii) What is the shared secret key? Write the Algorithm (5)

Answer

User A and User B want to perform the Diffie-Hellman key exchange with the given parameters:

Common prime (q) = 11

Primitive root (alpha) = 7

Here's how they can perform the key exchange:

User A selects a private key (a). Let's say **User A chooses a = 3.**

User B selects a private key (b). Let's say **User B chooses b = 4.**

To calculate User A's public key (YA) given that User A's private key (XA) is 3, you can use the Diffie-Hellman formula:

Y_A = (alpha^X_A) mod q

In this case:

Common prime (q) = 11

Primitive root (alpha) = 7

User A's private key (XA) = 3

alpha^XA = 7^3 = 343

Now, calculate (343 mod 11):

343 mod 11 = 3

So, User A's public key (YA) is 3.

(ii)if user B has private key X_B = 6.What is B's public key Y_B?

YB = (alpha^XB) mod q

In this case:

- Common prime (q) = 11
- Primitive root (alpha) = 7
- User B's private key (XB) = 6

YB = (7^6) mod 11

Calculate 7^6 first:

7^6 = 7 * 7 * 7 * 7 * 7 * 7 = 117649

Now, calculate (7^6) mod 11:

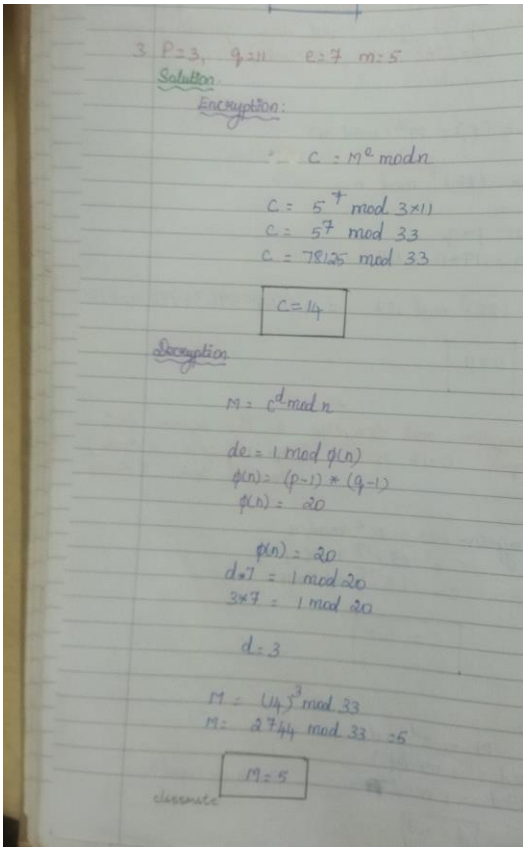
117649 mod 11 = 9

So, User B's public key (YB) is 9.

The shared secret key in the Diffie-Hellman key exchange is calculated by both User A and User B using their own private keys and the other user's public key. Here's the algorithm to calculate the shared secret key:

1. User A and User B agree on common parameters:
   - Common prime (q)
   - Primitive root (alpha)
2. Each user selects a private key:
   - User A selects XA (private key)
   - User B selects XB (private key)
3. Both users calculate their public keys:
   - User A: YA = (alpha^XA) mod q
   - User B: YB = (alpha^XB) mod q
4. User A and User B exchange their public keys with each other.
5. Both users use the received public key and their own private key to calculate the shared secret key:
   - User A calculates K = (YB^XA) mod q
   - User B calculates K = (YA^XB) mod q
6. The shared secret key (K) will be the same for both User A and User B. They can use this key for secure communication.

2.Identify the possible threats for RSA algorithm and list their counter measures. Perform Encryption and decryption using RSA algorithm with p=3 q=11 e=7 and N=5



3. P=3, q=11 e=7 m=5

Solution

Encryption:

$C = M^e \bmod n$

$C = 5^7 \bmod 3\times11$

$C = 5^7 \bmod 33$

$C = 78125 \bmod 33$

$\boxed{C=14}$

Decryption

$M = C^d \bmod n$

$de = 1 \bmod \phi(n)$

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

$\phi(n) = 20$

$\phi(n) = 20$

$d*7 = 1 \bmod 20$

$3*7 = 1 \bmod 20$

$d = 3$

$M = 14^3 \bmod 33$

$M = 2744 \bmod 33 = 5$

$\boxed{M=5}$

RSA (Rivest-Shamir-Adleman) is a widely used public key cryptography algorithm, but like any cryptographic system, it's not immune to threats. Here are some possible threats to RSA and countermeasures to mitigate them:

Brute Force Attack:

Threat: An attacker tries all possible private keys to decrypt ciphertext.

Countermeasure: Choose sufficiently large key sizes (e.g., 2048 bits or more) to make brute force attacks computationally infeasible.

<u>Factorization Attack:</u>

Threat: Attackers try to factor the modulus (N) to compute private keys.

Countermeasure: Use large prime numbers for p and q, and regularly update keys as computational power increases. Employ key lengths that are resistant to current and future factorization methods.

Timing Attacks:

Threat: Attackers analyze the time taken by the decryption process to extract information about the private key.

Countermeasure: Implement constant-time cryptographic operations to eliminate timing variations in decryption.

Chosen Plaintext Attacks:

Threat: Attackers obtain ciphertexts for chosen plaintexts and use them to deduce the private key.

Countermeasure: Apply padding schemes like RSA PKCS#1 v1.5 or OAEP to make ciphertexts indistinguishable from random data.

3. Demonstrate the DH key exchange methodology using following key values : p=11 ,g=2 X_A =9 , 4 X_B =4 .

Answer

- $p = 11$ (the prime modulus)
- $g = 2$ (the base)
- Alice's private key: $X_a = 9$
- Bob's private key: $X_b = 4$

1. Public Key Exchange:
   - Alice calculates her public key Y_a:
     $Y_a = g^{X_a} \mod p = 2^9 \mod 11 = 512 \mod 11 = 4$
   - Bob calculates his public key Y_b:
     $Y_b = g^{X_b} \mod p = 2^4 \mod 11 = 16 \mod 11 = 5$
2. Exchange Public Keys:
   - Alice sends her public key $Y_a = 4$ to Bob.
   - Bob sends his public key $Y_b = 5$ to Alice.

3. Shared Secret Calculation:
   - Alice calculates the shared secret key using Bob's public key:

     $K_{\text{shared}} = Y_b^{X_a} \mod p = 5^9 \mod 11$

     To compute $5^9 \mod 11$, you can use successive squaring:
     - $5^2 \mod 11 = 25 \mod 11 = 3$
     - $5^4 \mod 11 = (5^2 \mod 11)^2 \mod 11 = 3^2 \mod 11 = 9$
     - $5^8 \mod 11 = (5^4 \mod 11)^2 \mod 11 = 9^2 \mod 11 = 4$
     - $5^9 \mod 11 = 5^8 \cdot 5 \mod 11 = 4 \cdot 5 \mod 11 = 20 \mod 11 = 9$
   - Bob calculates the shared secret key using Alice's public key:

     $K_{\text{shared}} = Y_a^{X_b} \mod p = 4^4 \mod 11$

     To compute $4^4 \mod 11$:
     - $4^2 \mod 11 = 16 \mod 11 = 5$
     - $4^4 \mod 11 = (4^2 \mod 11)^2 \mod 11 = 5^2 \mod 11 = 25 \mod 11 = 3$
4. Both Alice and Bob have computed the same shared secret key $K_{\text{shared}} = 9$.

Now, Alice and Bob can use this shared secret key for secure communication, such as encryption and decryption, because only they know the private keys X_a and X_b, and it's computationally difficult for an eavesdropper to calculate the shared secret without knowing at least one of the private keys.

3.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).[NOV 2016]

Or

State Chinese Remainder Theorem and find X for the given set of congruent equations using CRT

X=1(MOD 5)

X=2(MOD 7)

X=3(mod 9)

X=4(mod 11) (13 Marks Nov/Dec 2020]

Answer

Refer the content in the last page of this Notes

4(i).Find the gcd (6432,768)by using Extended Euclidean algorithm

1. Begin by using the Euclidean Algorithm to find the GCD of the two numbers:
   $6432 = 8 \cdot 768 + 288$
2. Now, replace 6432 with 768 and 768 with the remainder (288):
   $768 = 2 \cdot 288 + 192$
3. Continue the process:
   $288 = 1 \cdot 192 + 96$
   $192 = 2 \cdot 96 + 0$
4. When you reach a remainder of 0, the GCD is the last non-zero remainder, which is 96.

So, $\mathrm{GCD}(6432, 768) = 96$.

Now, let's use the Extended Euclidean Algorithm to find the coefficients x and y such that:

$$6432x + 768y = \mathrm{GCD}(6432, 768) = 96$$

We will work our way backward from the last non-zero remainder (96):

We will work our way backward from the last non-zero remainder (96):

1. Starting with the equation $192 = 2 \cdot 96 + 0$, we can express 96 in terms of 192 and 288:
   $96 = 192 - 2 \cdot 288$
2. Next, we use the equation $288 = 1 \cdot 192 + 96$ to express 288 in terms of 192 and 6432:
   $288 = 6432 - 8 \cdot 768$
3. Now, we substitute the expression for 288 into the previous equation:
   $96 = 192 - 2 \cdot (6432 - 8 \cdot 768)$
4. Continue to simplify:
   $96 = 192 - 2 \cdot 6432 + 16 \cdot 768$
5. Rearrange the terms:
   $96 = -2 \cdot 6432 + 16 \cdot 768 + 192$
6. Now, we can see the coefficients x and y:
   - $x = -2$
   - $y = 16$

So, the GCD of 6432 and 768 is 96, and the coefficients for the Bézout's identity are $x = -2$ and $y = 16$.

(ii)Find φ(519)

To do this, you can use the formula for φ(n) when n is a product of prime factors:

If $n = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_k^{a_k}$, where $p_1, p_2, \ldots, p_k$ are distinct prime factors, then

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_k}\right)$$

In the case of 519, you can factor it as follows:

$$519 = 3 \cdot 7 \cdot 31$$

Now, apply the formula:

$$\phi(519) = 519\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{7}\right)\left(1 - \frac{1}{31}\right)$$

Calculate the values inside the parentheses:

$$\phi(519) = 519\left(\frac{2}{3}\right)\left(\frac{6}{7}\right)\left(\frac{30}{31}\right)$$

Now, multiply these fractions:

$$\phi(519) = 519 \cdot \frac{2}{3} \cdot \frac{6}{7} \cdot \frac{30}{31}$$

Simplify:

$\phi(519) = 260 \cdot \frac{6}{7} \cdot \frac{30}{31}$

Now, multiply the numbers together:

$\phi(519) = \frac{260 \cdot 6 \cdot 30}{7 \cdot 31}$

Calculate the numerator and denominator separately:

Numerator: $260 \cdot 6 \cdot 30 = 46800$

Denominator: $7 \cdot 31 = 217$

Now, divide the numerator by the denominator:

$\phi(519) = \frac{46800}{217} \approx 215.60$

Since φ(n) should be an integer, we round it down to the nearest integer:

$\phi(519) \approx 215$

So, φ(519) is approximately 215.

5(i).State Chinese Remainder Theorem and find X for the given set ofcongruent equations using CRT

X=10(mod 2)

X=7(mod 9)

X=3(mod 5) (13 Marks Apr/May 2023]

(ii)Find 103^{27} mod 467

1. Find 103^{27} mod 467

$103^{27} = 103 \times 103^2 \times 103^4 \times 103^8 \times 103^8 \times 103^4$

$103^1 = 103 \bmod 467 = 103$

$103^2 = 10609 \bmod 467 = 335$

$103^4 = 11255088 1 \bmod 467 = 145$

$103^8 = 103^4 \times 103^4 = 145 \times 145 = 21025 = 10$

$103^{27} \bmod 467 = 103 \times 335 \times 145 \times 10 \times 145 \bmod 467$

$= 34505 \times 210250 \bmod 467$

$= 414 \times 100 \bmod 467$

$= 304$

$\boxed{103^{27} \bmod 467 = 304}$

6.State and prove Fermat's theorem.

Definition
Proof
Example problem

3.Explain RSA algorithm,perform encryption and decryption to the system with p=7 and q=11 e=17 and M=8

Definition
Algorithm
Problem

Perform encryption and decryption to the system with $p=7$ $q=11$ $e=17$ $M=8$ [Apr/May 2016, 6 Marks]
Nov/Dec 2016, 8 Marks

Solution:

Encryption $(C) = M^e \bmod n$

$C = (8)^{17} \bmod p*q$

$C = (8)^{17} \bmod 7*11$

$\boxed{C = 57}$

Decryption

$M = C^d \bmod n$

$ed = 1 \bmod \phi(n)$

$17d = 1 \bmod 60$ $\therefore 17*53 = 1 \bmod 60$

$\boxed{d = 53}$

$M = (57)^{53} \bmod 77 = 8$

$\boxed{M = 8}$

7.Users alice and bob use the diffie hellman key exchange technique with a common prime q=83 and a primitive root α=5.
i) if Alice has a private key XA=6, what is Alice's public key YA? (6 marks)
ii) if bob has a private key XB =10 what is bob's public key YB? (6 marks)
iii) What will be shared secret key (8 marks)

Refer Class Notes

8.Explain Diffie-Hellman Key exchange algorithm in detail(Apr/May 2017)
Or
Explain briefly about Diffie-Hellman Key exchange algorithm with its merits and demerits [Apr/May 2019]

- Definiton

- ❖ Algorithm
- ❖ Example Problem
- ❖ Merits and Demerits

9.With a neat sketch explain the Elliptic curve cryptography with an example[Apr/May 2018]

- ❖ Definition
- ❖ Mathematical Equation
- ❖ ECC Diffie Hellman KeyExchange
- ❖ Explanation
- ❖ Decryption
- ❖ Computational effort for CryptAnalysis

10.Why ECC is better than RSA?However,why it is not used widely?.Defind it?
[Speed of RSA is reduced]

- **The solution is Elliptic Curve Cryptography (ECC)**
  - **Smaller key size equal security compared to RSA**
  - **Reduced processing overhead**

11.Find the secret key shared between user A and user B usingDiffie Hellman algorithm for the following q=353,α(primitive root)=3 ,X_A=45 and X_B=50

- ❖ Definition
- ❖ Formula
- ❖ Given Values
- ❖ To be find
- ❖ Refer Classwork Note Book

12.Describe RSA algorithm

Definiton
Algorithm
Explanation
Example Problem

13. Perform encryption and decryption using RSA algorithm for the following with p=7 and q=11 e=7 M-9.[Apr/May 2018]

- ❖ Definiton
- ❖ Algorithm

- ❖ Problem with both encryption and decryption

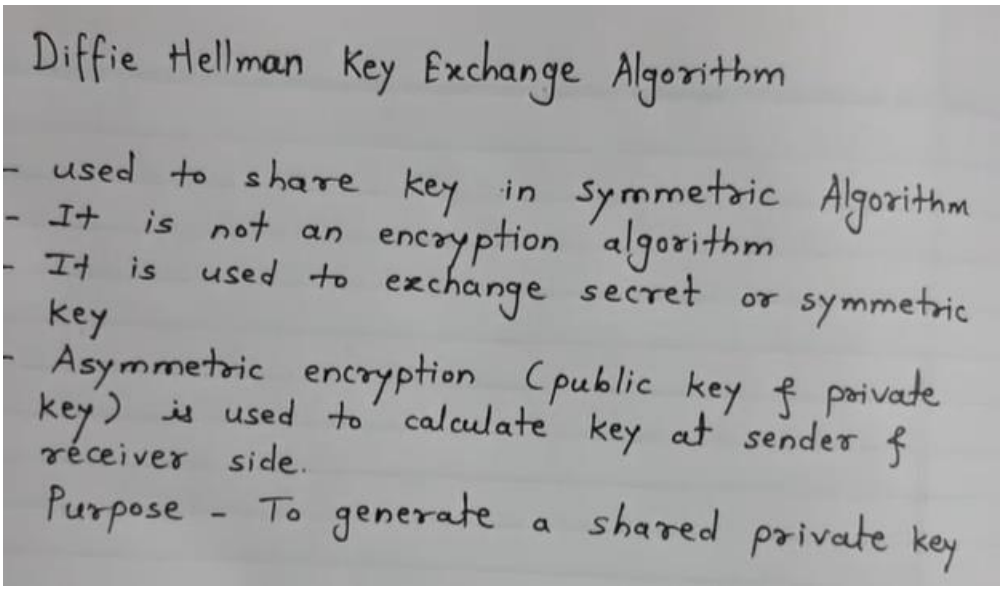
14.Explain Public Key Cryptography and when it is preferred?[Nov/Dec 2019]

- ❖ Definition
- ❖ Diagram Publickey cryptography
- ❖ Characteristics of Public key cryptosystems
- ❖ Components of PublicKey Cryptography

15. Demonstrate the Diffie Hellman key exchange methodology using following key values : 11 p = , 2 g = , XA = 9 , 4 XB = 4[Nov/Dec 2021]

- ❖ Definition
- ❖ Formula
- ❖ Given Values
- ❖ To be find
- ❖ Refer Classwork Note Book

16.Diffie–Hellman key agreement is not limited to negotiating a key shared by only two participants. Any number of users can take part in an agreement by performing iterations of the agreement protocol and exchanging intermediate, Write the steps and formulas to be followed for DH key exchange between Alice, Bob, and Carol.[Nov/Dec 2021]



Steps –

1) Assume prime number q

2) Select α such that

$\alpha \Rightarrow$ primitive root of q

$\alpha < q$

Ex - a is primitive root of p

if $\{a^1 \bmod p,\ a^2 \bmod p \ \ldots\ldots \ a^{p-1} \bmod p\}$

results in $\{1, 2, 3 \ldots\ p-1\}$

3) Assume $X_A \Rightarrow$ private key of user A

$X_A < q$

Calculate $Y_A \Rightarrow$ public key of user A

$Y_A = \alpha^{X_A} \bmod q$ $\quad \{X_A, Y_A\} \Rightarrow$ user A

4) Assume $X_B \Rightarrow$ private key of user B

$X_B < q$

Calculate $Y_B \Rightarrow$ public key of user B

$Y_B = \alpha^{X_B} \bmod q$ $\quad \{X_B, Y_B\} \Rightarrow$ user B

5) Key Generation

User A

$K = (Y_B)^{X_A} \bmod q$

User B

$K = (Y_A)^{X_B} \bmod q$

1) $q = 11$

2) $\alpha = 2$

3) select $X_A < q$, $X_A = 8$

$Y_A = \alpha^{X_A} \bmod q$

$Y_A = 2^8 \bmod 11 = 3$

4) Select $X_B = 4$

$Y_B = \alpha^{X_B} \bmod q$

$Y_B = 2^4 \bmod 11$

$Y_B = 5$

user A = $\{X_A = 8 , Y_A = 3\}$

user B = $\{X_B = 4 \quad Y_B = 5\}$

5) Key Generation

user A (Sender)

$K = (Y_B)^{X_A} \bmod q$

$K = 5^8 \bmod 11$

$K = 4$

user B (Receiver)

$K = (Y_A)^{X_B} \bmod q$

$K = 3^4 \bmod 11$

$K = 4$

17.(i) In a public-key system using RSA, you intercept the ciphertext C = 20 sent to a user whose public key is e = 13, n = 77. What is the plaintext M? (7)

(ii) In an RSA system, the public key of a given user is e = 65, n = 2881, What is the private key of this user?

- ❖ Definiton RSA
- ❖ Algorithm
- ❖ Given Problem
- ❖ What is plaintext
- ❖ What is private key

Part C Question

A Box contains gold coins. If the coins are equally divided among three friends, two coins are left over, If the coins are equally divided among five friends, three coins are left over If the coins are equally divided among seven friends, two coins are left over. If the box holds smallest number of coins that meets these conditions, how many coins are there? (Hint : Use Chinese Remainder Theorem).

Refer Class Notes

Question No 2

(b) (i) Alice chooses 173 and 149 as two prime numbers and 3 as public key in RSA. Check whether the chosen prime numbers are valid or not? (5)

(ii) Prove that Euler's Totient value of any prime number (p) is $p-1$ and the Euler's Totient value of the non-prime number (n) is $(p-1)\times(q-1)$ where $p\times q$ are prime factor of n. (5)

(iii) Mr. Ram chooses RSA for encryption, and he chooses 3 and 7 are two prime numbers. He encrypt the given message (message given in English alphabets) by mapping A = 1, B = 2, C = 3.., Z = 26. Find atleast two problems in his implementation. (5)

Question

Alice chooses 173 and 149 as two prime numbers and 3 as public key in RSA. Check whether the chosen prime numbers are valid or not? (5)

1. We choose e = 3

2. We select primes p=173 and q=149 and check

   - gcd(e, p-1) = gcd(3, 172) = 1 ⇒ OK
   - gcd(e, q-1) = gcd(3, 148) = 1 ⇒ OK.

3. Thus we have $n = pq = 173 \times 149 = 25777$, and
   $\phi = (p-1)(q-1) = 172 \times 148 = 25456$.

4. We compute $d = e^{-1} \bmod \phi = 3^{-1} \bmod 25456 = 16971$.

   - Note that $ed = 3 \times 16971 = 50913 = 2 \times 25456 + 1$
   - That is, $ed \equiv 1 \bmod 25456 \equiv 1 \bmod \phi$

5. Hence our public key is (n, e) = (25777, 3) and our private key is (n, d) = (25777, 16971). We keep the values of p, q, d and ϕ secret.

To encrypt the first integer that represents "ATT", we have

$c = m^e \bmod n = 1289^3 \bmod 25777 = 18524.$

Overall, our plaintext `ATTACK AT SEVEN` is represented by the sequence of five integers m_1, m_2, m_3, m_4, m_5:

```
m_i = (1289, 821, 47, 518, 16187)
```

We compute corresponding ciphertext integers $c_i = m_i^e \bmod n$, (which is still possible by using a calculator, honest):

$c_1 = 1289^3 \bmod 25777 = 18524$

$c_2 = 821^3 \bmod 25777 = 7025$

$c_3 = 47^3 \bmod 25777 = 715$

$c_4 = 518^3 \bmod 25777 = 2248$

$c_5 = 16187^3 \bmod 25777 = 24465$

We can send this sequence of integers, c_i, to the person who has the private key.

```
c_i = (18524, 7025, 715, 2248, 24465)
```

You should get the results:

$$m_1 = 18524^{16971} \bmod 25777 = 1289$$
$$m_2 = 7025^{16971} \bmod 25777 = 821$$
$$m_3 = 715^{16971} \bmod 25777 = 47$$
$$m_4 = 2248^{16971} \bmod 25777 = 518$$
$$m_5 = 24465^{16971} \bmod 25777 = 16187$$

To convert these integers back to the block of three letters, do the following. For example, given m = 16187,

```
16187 ÷ 27^2 = 16187 ÷ 729 = 22 rem 149, 22 → 'V'
149   ÷ 27^1 = 149   ÷ 27  = 5 rem 14,    5 → 'E'
14    ÷ 27^0 = 14    ÷ 1   = 14 rem 0,   14 → 'N'
```

Hence the integer m = 16187 represents the string "VEN".
Similarly, m = 47 is encoded as follows:

```
47 ÷ 27^2 = 0 rem 47, 0  → SPACE;
47 ÷ 27^1 = 1 rem 20, 1  → 'A';
20 ÷ 27^0 = 20 rem 0, 20 → 'T'
```

giving the string "_AT".

Question

(ii) Prove that Euler's Totient value of any prime number (p) is $p-1$ and the Euler's Totient value of the non-prime number (n) is $(p-1)\times(q-1)$ where $p\times q$ are prime factor of n. (5)

Answer

- Definition
- Three cases

UNIT IV – MESSAGE AUTHENTICATION AND INTEGRITY

[QUESTION BANK]

PART – A

1.Name the four requirements defined by Kerberos[Nov/Dec 2022]

Requirements for Kerberos

Secure

An **opponent does not find** it to be the weak link.

Reliable

The system should be able to back up another.

Transparent

An user should not be aware of authentication

Scalable

The system supports large number of clients and servers

2.Difference between MAC and Hash Function?[Nov/Dec 2022]

No	Hash Function	MAC
1	A hash algorithm takes a single input like message and produces a "Hash" which helps to verify and check the integrity of the message.	A MAC algorithm takes two inputs one is a message and another is secret key which will produces a MAC, which helps to verify integrity and the authentication of message.
2	Any change to input message produces different hash being generated.	Any changes to in message or the secret key will result in a different MAC being generated.
3	Once the hash is generated which will not give any clue to the attacker about original content of the message.	Without secret key it is not possible for attacker to identifies and validate the correct MAC.
4	Most popular message digest algorithm are MD5 and SHA-1.	Most popular MACs are MAC using DES in CBC mode and HMAC.

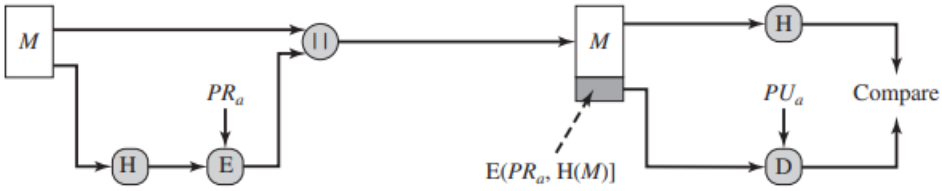
3. What is meant by padding? And, why padding is required?[Nov/Dec 2021]

- Padding in cryptography refers to **the process of adding extra bits or bytes** to data before it is encrypted or processed by a cryptographic algorithm.
- Padding is an essential aspect of many **cryptographic processes, ensuring that data** is processed and encrypted in a secure and consistent manner.

In SSL, the padding added prior to encryption of user data is the minimum amount required so that the total size of the data to be encrypted is a multiple of the cipher's block length.

In TLS, the padding can be any amount that results in a total that is a multiple of the cipher's block length, up to a maximum of 255 bytes.

4. Draw functional diagram of RSA based Digital Signature.[Nov/Dec 2021]



(a) RSA approach

5.How is the security of a MAC function expressed ? (NOV/DEC 2017)

The security of a MAC function expressed in terms of the probability of successful forgery with a given amount of time spent by the forger and a given number of message-MAC pairs created with the same key.

6.Mention the significance of signature function in Digital Signature Standard (DSS) approach. (NOV/DEC 2017)

A digital signature is represented in a computer as a string of binary digits. A digital signature is computed using a set of rules and a set of parameters such that the identity of the signatory and integrity of the data can be verified. An algorithm provides the capability to generate and verify signatures. Signature generation makes use of a private key to generate a digital signature. Signature verification makes use of a public key which corresponds to, but is not the same as, the private key.

7.Write a simple authentication dialogue used in Kerberos. (NOV/DEC 2017)

$$\textbf{(1)}\ \ C \rightarrow AS: \quad ID_C \| P_C \| ID_V$$

$$\textbf{(2)}\ \ AS \rightarrow C: \quad Ticket$$

$$\textbf{(3)}\ \ C \rightarrow V: \quad ID_C \| Ticket$$

$$Ticket = E(K_v, [ID_C \| AD_C \| ID_V])$$

8.List any 2 applications of X.509 Certificates. (NOV/DEC 2017)

- Document signing and Digital signature.
- Web server security with the help of Transport Layer Security (TLS)/Secure Sockets Layer (SSL) certificates.
- Email certificates.
- Code signing.
- Secure Shell Protocol (SSH) keys.
- Digital Identities.

9.How a digital signature differs from authentication protocols? (APRIL/MAY 18)

A (digital) signature is created with a private key, and verified with the corresponding public key of an asymmetric key-pair.

Only the holder of the private key can create this signature, and normally anyone knowing the public key can verify it.

Digital signatures don't prevent the replay attack mentioned previously

Authentication Protocols used **to convince parties of each other's identity** and to ***exchange session keys***.

Mutual Authentication

Protocols enable ***communicating parties to satisfy themselves mutually about each other's identity and to exchange session keys.***

Problem of authenticated key exchange

Problems to Key issues are

- **Confidentiality** – to protect session keys and prevent masqueraded(make believe) and compromised.
- **Timeliness** – to **prevent replay attacks**

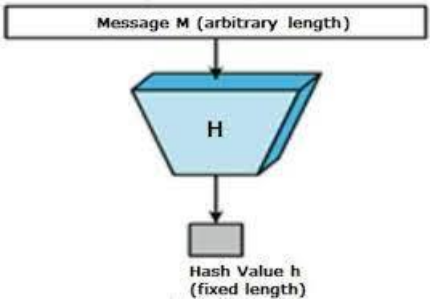
10.What is a hash in cryptography?[Apr/May 2018]

Or

Define the term Message digest[Nov/Dec 2018]

Hashing is **the process of transforming any given value or a string of characters into another value**.

This is usually represented by a **shorter, fixed-length value or key** that represents and makes it easier to find or employ the original string.



11.What is Digital Signature[Nov/Dec 2018]

- A digital signature is an **authentication mechanism** that enables the sender of a message to **attach a code** that **acts as a signature**.
- Typically ***the signature*** is formed by **taking the hash of the message** and encrypting ***the message with the sender's private key.***

The **signature guarantees** the source and integrity of the message

12.Contrast various SHA algorithms[Nov/Dec 2018]

SHA-0: The original version of the 160-bit hash function published in 1993 under the name "SHA". It was withdrawn shortly after publication due to an undisclosed "significant flaw" and replaced by the slightly revised version SHA-1.

SHA-1: A 160-bit hash function which resembles the earlier MD5 algorithm. This was designed by the National Security Agency (NSA) to be part of the Digital Signature Algorithm.

SHA-2: A family of two similar hash functions, with different block sizes, known as SHA256 and SHA-512. SHA-256 uses 32-bit words where SHA-512 uses 64-bit words.

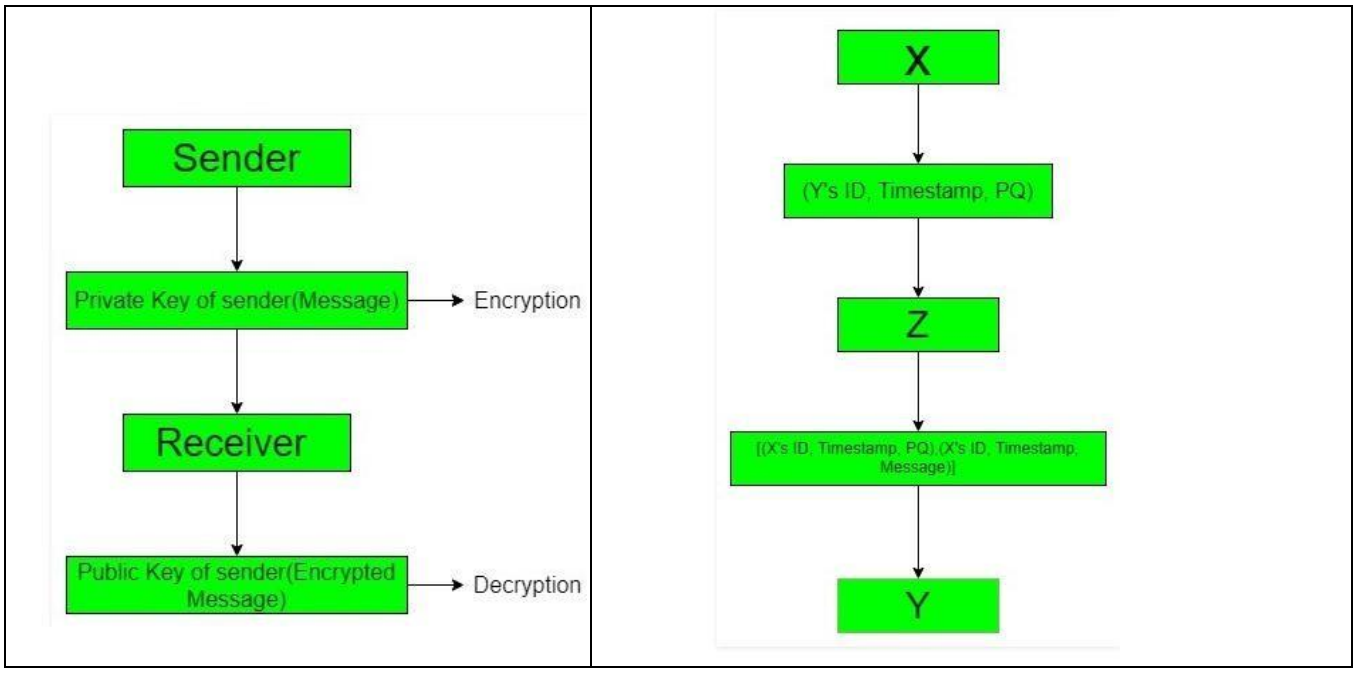
SHA-3: It supports the same hash lengths as SHA-2, and its internal structure differs significantly from the rest of the SHA family.

13.State the requirements of digital signature[Nov/Dec 2019]

- The signature must be a **bit pattern** that ***depends on the message being signed.*** [Somewhat related to Message]
- The signature must use **some information unique to the sender**, to prevent both **forgery and denial.**
- It must be **relatively easy to produce** the digital signature.
- It must be **relatively easy to recognize and verify** the digital signature.[verification must be simpler]
- It must be **computationally infeasible to forge a digital signature**, either by **constructing a new message** for an **existing digital signature** or by constructing a fraudulent digital signature for a given message.
- It must be practical to **retain a copy of the digital signature** in storage.

14.Compare Direct and Arbitrated digital signature. (Understand) [NOV/DEC 19]

Direct Digital Signature	Arbitrated Digital Signature
• The Direct Digital Signature is only include two parties one to send message and other one to receive it. • According to direct digital signature both parties trust each other and knows there public key. • The message are prone to get corrupted and the sender can declines about the message sent by him any time.	• The Arbitrated Digital Signature includes three parties in which one is sender, second is receiver and the third is arbiter who will become the medium for sending and receiving message between them. • The message are less prone to get corrupted because of timestamp being included by default.

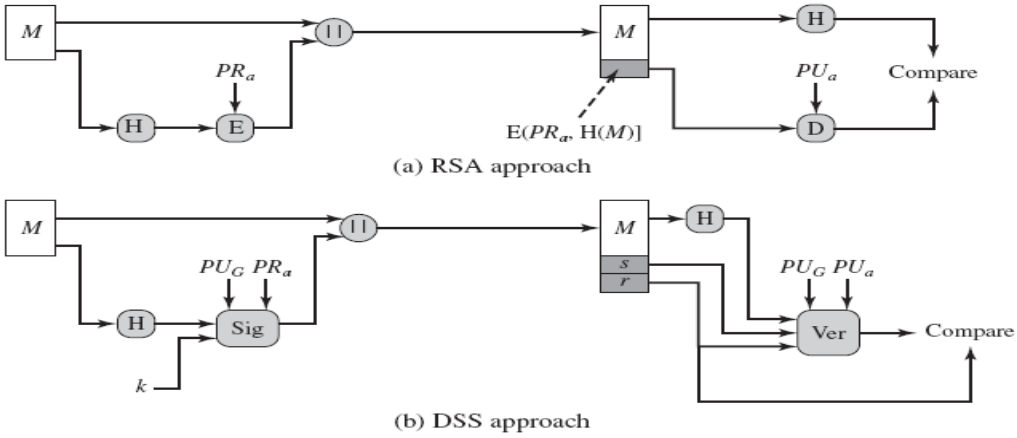


15.What entities constitute a full service in Kerberos environment?

A full service environment consists of a

i) Kerberos server, ii) Number of clients, and iii) Number of application servers

16.Draw functional diagram of RSA and DSS based Digital signature?[Nov /Dec 2021]



17.Define Replay Attack[Nov 2011]

Replay Attacks

A ***valid signed message*** is copied and ***later resent***

Examples of replay attacks

(i)Simple replay :The **opponent** simply ***copies the message and replays*** it later.

(ii)Repetition that can be logged

The **opponent replay** a ***time stamped message*** within ***a valid time window***.

(iii)Repetition that cannot be detected

The attacker would have **suppressed the original message** from the receiver. Only the **replay message alone arrives**.

(iv)Backward replay without modification

This is a ***replay back to the message sender*** itself.This is possible only if ***the sender cannot easily recognize the difference between the message sent and the message received*** based on the content.

18.How is the security of MAC is expressed?[Nov/Dec 2017]

Computation resistance: [Mac value differs if **x ≠xi.]**

Given one or more text-MAC pairs (xi, C_K[$xi_]$), it is computationally infeasible to compute any text-MAC pair (x, C_K(x)) **for any new input x ≠xi**

19. What do you mean by one way property in hash function? (APR/MAY 2011)(NOV/DEC 2012)

The one way property of hash function indicates that it is easy to generate a code given a message, but virtually impossible to generate a message given a code. This property is important if the authentication technique involves the use of a secret value.

- For any given value h, it is computationally infeasible to find x such that H(x) = h – one way property.
- For any given block x, it is computationally infeasible to find y ≠ x with H(y) = H(x) – weak collision resistance.
- It is computationally infeasible to find any pair (x, y) such that H(x) = H(y) – strong collision property

20. What are birthday attacks? (APR/MAY 2014)

If an encrypted 64 bit hash code C is transmitted with the corresponding unencrypted message M , then an opponent would need to find an $M^{'}$ such that H($M^{'}$) = H(M)to substitute another message to substitute another message and fool the receiver. Thus the user has to try about 2^{63} combinations to find one that matches the hash code of the intercepted message. This is called as Birthday attack

PART - B QUESTIONS

1.What is digital signature?Explain the key generation,signingand signature verification algorithm?Bring out the steps followed to create a digital signature[Nov/Dec 2022]

❖ Definition

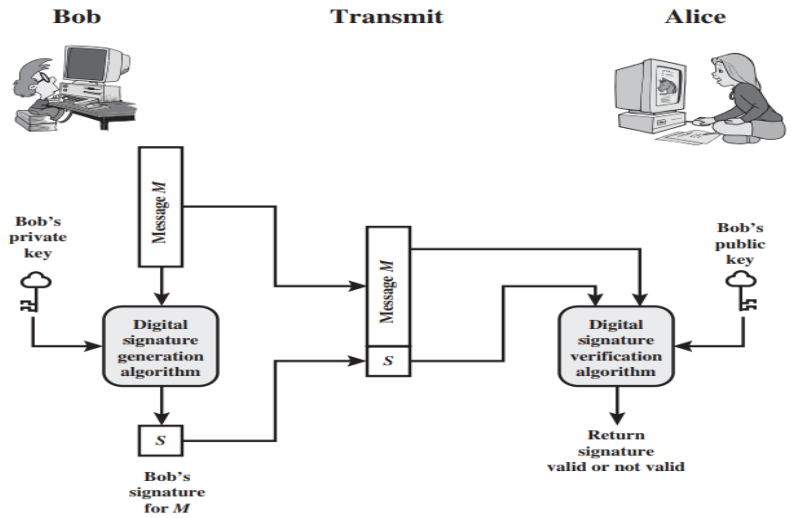


Figure 13.1 Generic Model of Digital Signature Process

Global Public-Key Components

p prime number where $2^{L-1} < p < 2^L$ for $512 \le L \le 1024$ and L a multiple of 64; i.e., bit length of between 512 and 1024 bits in increments of 64 bits

q prime divisor of $(p - 1)$, where $2^{159} < q < 2^{160}$; i.e., bit length of 160 bits

g $= h^{(p-1)/q} \bmod p$, where h is any integer with $1 < h < (p - 1)$ such that $h^{(p-1)/q} \bmod p > 1$

User's Private Key

x random or pseudorandom integer with $0 < x < q$

User's Public Key

$y = g^x \bmod p$

User's Per-Message Secret Number

k = random or pseudorandom integer with $0 < k < q$

Signing

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

$s = [k^{-1} (H(M) + xr)] \bmod q$

Signature = (r, s)

Verifying

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

$u_1 = [H(M')w] \bmod q$

$u_2 = (r')w \bmod q$

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

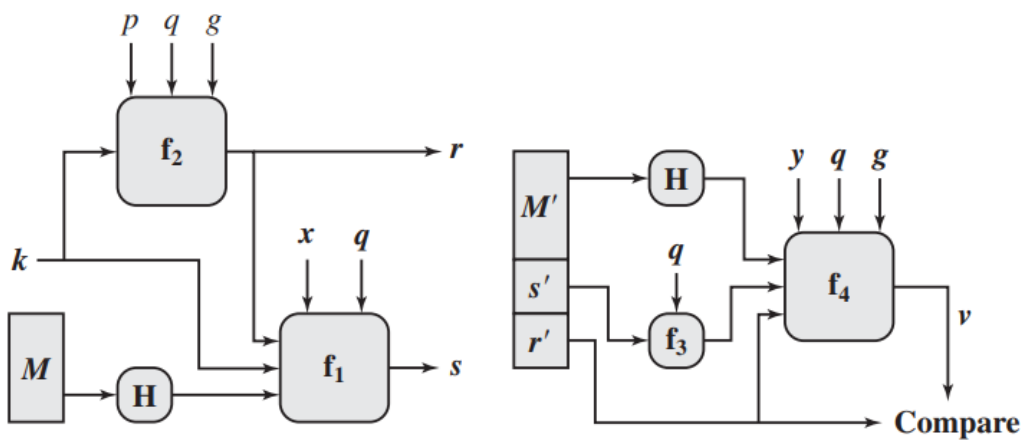
TEST: $v = r'$

M = message to be signed

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

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

Figure 13.4 The Digital Signature Algorithm (DSA)



$s = f_1(H(M), k, x, r, q) = (k^{-1}(H(M) + xr)) \bmod q$

$r = f_2(k, p, q, g) = (g^k \bmod p) \bmod q$

(a) Signing

$w = f_3(s', q) = (s')^{-1} \bmod q$

$v = f_4(y, q, g, H(M'), w, r')$

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

(b) Verifying

Figure 13.5 DSS Signing and Verifying

2. Many websites requires users to register before they can access information or services.Suppose that you register at such as website but when you return later you have forgotten your password,The website then asks you to enter your email and address which you do.Later you receive your original password via email.Discuss several security concerns with this approach to deal with forgotten password.[Nov/Dec 2022]

Answer

Password Forgotten: You, as a user, visit a website where you have previously registered an account, but you've forgotten your password. You click on a "Forgot Password?" or similar link on the login page.

Email and Address Verification: The website prompts you to enter your email address. This step is crucial because the website needs to verify that you are the legitimate owner of the account and not someone trying to gain unauthorized access. Some websites might also ask for additional information, such as your registered address, to further confirm your identity.

Email Confirmation: After you enter your email address and, if required, your address, the website sends an email to the address associated with your account. This email typically contains a link or a code that you can use to reset your password.

Resetting Your Password: You check your email and find the message from the website. You click on the link or use the code provided to access a page where you can reset your password.

Setting a New Password: On the password reset page, you are usually prompted to enter a new password. You choose a new password that meets the website's security requirements.

Password Reset Confirmation: After successfully setting a new password, you receive a confirmation email informing you that your password has been reset.

Logging In: You can now return to the website's login page and use your newly set password to access your account.

This process is designed to be secure and user-friendly. It helps ensure that only the legitimate account owner can reset their password, as access to the associated email account is required. Additionally, it provides a means for users to regain access to their accounts when they forget their passwords, reducing the likelihood of being locked out of their accounts permanently. It's essential to follow password security best practices when setting a new password to keep your account safe.

3. Briefly explain the steps of message digest generation in Whirlpool with a block diagram.[Nov/Dec 2020]

- Whirlpool Hash Structure
- Block Cipher W
- Performance of Whirlpool

4. Explain PKI management model and its operations with the help of a diagram.[Nov/Dec 2020]

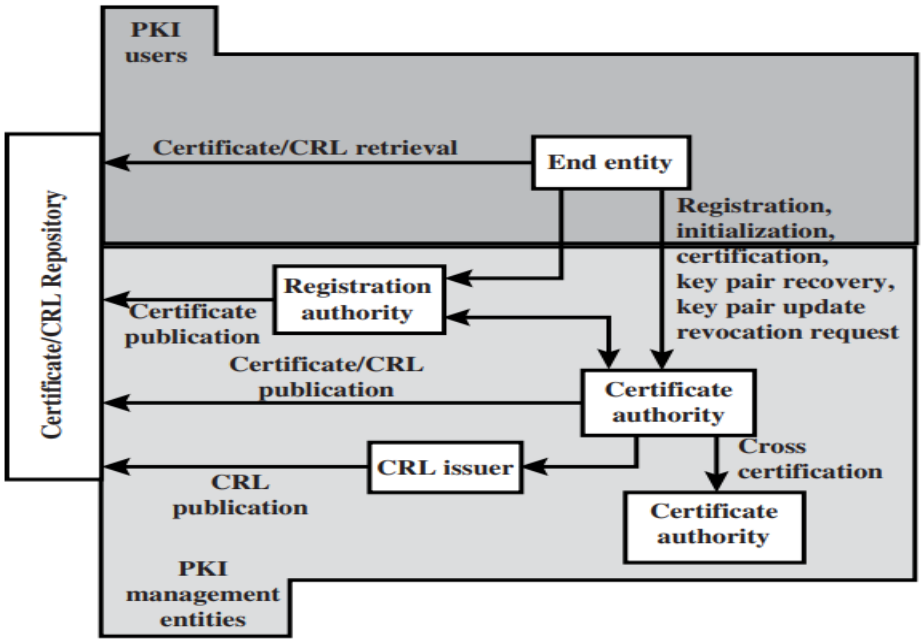


Figure 14.16 PKIX Architectural Model

Explanation about PKI

Question 5

Consider a banking application that is expected to provide cryptographic functionalities. Assume that this application is running on top of another application wherein the end customers can perform a single task of fund transfer. The application requires cryptographic requirements based on the amount of transfer.

Transfer amount	Cryptography functions required
1 – 2000	Message digest
2001 – 5000	Digital signature
5000 and above	Digital signature and encryption

Suggest the security scheme to be adopted in client and server side to accommodate the above requirements and justify your recommendations. **(15)**

Solution

Transfer Amount	Cryptography function required
1-2000	Message digest-To verify the finger print of the transaction.
2001-5000	Digital Signature-To ensure the message integrity and non-repudiation
5000 and above	Digital signature and encryption-To ensure the message integrity and non-repudiation and confidential.

If fund transfer amount upto 2000,we simply reauire a message digest to obtain and verify the fingerprint or integrity of the message.Here we use SSL to avoid attacks.This is the example of cryptography services.

If the transaction amount is in between 2000 to 5000 we require a digital signature to ensure not only message integrity but also non –repudiation.This is an example of authorization services.

At last,if the transaction amount is more than 5000.we must not only sign a message but also encrypt it.This is a combination of authorization services and cryptography services.

6.Discuss Client Server Mutual authentication, with example flow diagram. (NOV/DEC 2016)

Or

What is Kerberos ?Explain how it provides authenticated service.[Apr/May 2019]

Or

List the requirements of Kerberos[Nov 2021]

- Define Kerberos
- Requirements of Kerberos
- A simple authentication dialogue
- Using Authentication Server

- Diagram –Overview of Kerberos
- Using Ticket Granting Server
- Summary of Kerberos Message Exchange

7.Explain SHA512 in detail [Nov/Dec 2016]

Write steps involved in the generation of Message digest [Nov 2021]

Or

With a neat diagram.explain the steps involved SHA algorithm for encrypting a message with maximum length less than 2^{128} bits and produces as output a 512-bit message digest. [Nov/Dec 2017]

Definition

Diagram -Message Digest Generation Using SHA-512

Processing Steps

Step 1 Append padding bits.

Step 2 Append length

Step 3 Initialize hash buffer

Step 4 Process message in 1024-bit (128-word) blocks

- Diagram SHA-512 Processing of a Single 1024 Bit Block
- Diagram Elementary SHA-512 Operation (single round)
- Diagram Creation of 80-word Input Sequence for SHA-512 Processing of Single Block

8.How Hash function algorithm is designed? Explain their features and properties [Apr/May 2018]

- Define hash function
- Block diagram of hash function
- Basic uses of Hash function
- Requirements of Hash Function
- Security of Hash function

9.Explain briefly about the certification mechanisms in X.509[Apr/May 2018]

Or

Explain the format of the X.509 certificate.

Or

(ii)Describe the elements of X509 Certificate.

Define X.509

Diagram

Public Key Certificate Use

Summery of X.509 CERTIFICATE

Version		Version of X.509 to which the Certificate conforms
Serial Number		A number that uniquely identifies the Certificate
Signature Algorithm ID		The names of the specific Public Key algorithms that the CA has used to sign the Certificate (Ex.- RSA with SHA-1)
Issuer (CA) X.500 Name		The identity of the CA Server who issued the Certificate
Validity Period		The period of time for which the Certificate is valid with start date and expiration date
Subject X.500 Name		The owner's identity with X.500 Directory format
Subject Public Key Info	Algorithm ID	The Public Key of the owner of the Certificate and the specific Public Key algorithms associated with the Public Key
	Public Key Value	
Issuer Unique ID		Information used to identify the issuer of the Certificate
Subject Unique ID		Information used to identify the Owner of the Certificate
Extension		Additional information like Alternate name, CRL Distribution Point (CDP)
CA Digital Signature		The actual digital signature of the CA

- ❖ Obtaining a User's Certificate
- ❖ Revocation of certificates

10.Explain Elgammal Digital Signature Scheme[Nov/Dec 2018]

ElGamal encryption scheme is designed to enable encryption by a user's public key with decryption by the user's private key. The ElGamal signature scheme involves the use of the private key for encryption and the public key for decryption that for a prime number q, if α is a primitive root of q, then

$$\alpha, \alpha^2, \ldots, \alpha^{q-1}$$

are distinct (mod q). It can be shown that, if α is a primitive root of q, then

1. For any integer m, $\alpha^m \equiv 1 \pmod q$ if and only if $m \equiv 0 \pmod{q-1}$.
2. For any integers, i, j, $\alpha^i \equiv \alpha^j \pmod q$ if and only if $i \equiv j \pmod{q-1}$.

As with ElGamal encryption, the global elements of **ElGamal digital signature** are a prime number q and α, which is a primitive root of q. User A generates a private/public key pair as follows.

1. Generate a random integer X_A, such that $1 < X_A < q - 1$.
2. Compute $Y_A = \alpha^{X_A} \bmod q$.
3. A's private key is X_A; A's pubic key is $\{q, \alpha, Y_A\}$.

To sign a message M, user A first computes the hash $m = \mathrm{H}(M)$, such that m is an integer in the range $0 \le m \le q - 1$. A then forms a digital signature as follows.

1. Choose a random integer K such that $1 \le K \le q - 1$ and $\gcd(K, q - 1) = 1$. That is, K is relatively prime to $q - 1$.
2. Compute $S_1 = \alpha^K \bmod q$. Note that this is the same as the computation of C_1 for ElGamal encryption.
3. Compute $K^{-1} \bmod (q - 1)$. That is, compute the inverse of K modulo $q - 1$.
4. Compute $S_2 = K^{-1}(m - X_A S_1) \bmod (q - 1)$.
5. The signature consists of the pair (S_1, S_2).

Any user B can verify the signature as follows.

1. Compute $V_1 = \alpha^m \bmod q$.
2. Compute $V_2 = (Y_A)^{S_1}(S_1)^{S_2} \bmod q$.

The signature is valid if $V_1 = V_2$. Let us demonstrate that this is so. Assume that the equality is true. Then we have

$\alpha^m \bmod q = (Y_A)^{S_1}(S_1)^{S_2} \bmod q$	assume $V_1 = V_2$
$\alpha^m \bmod q = \alpha^{X_A S_1}\alpha^{KS_2} \bmod q$	substituting for Y_A and S_1
$\alpha^{m - X_A S_1} \bmod q = \alpha^{KS_2} \bmod q$	rearranging terms
$m - X_A S_1 \equiv KS_2 \bmod (q - 1)$	property of primitive roots
$m - X_A S_1 \equiv KK^{-1}(m - X_A S_1) \bmod (q - 1)$	substituting for S_2

For example, let us start with the prime field GF(19); that is, $q = 19$. It has primitive roots $\{2, 3, 10, 13, 14, 15\}$, as shown in Table 8.3. We choose $\alpha = 10$.

Alice generates a key pair as follows:

1. Alice chooses $X_A = 16$.
2. Then $Y_A = \alpha^{X_A} \bmod q = \alpha^{16} \bmod 19 = 4$.
3. Alice's private key is 16; Alice's pubic key is $\{q, \alpha, Y_A\} = \{19, 10, 4\}$.

Suppose Alice wants to sign a message with hash value $m = 14$.

1. Alice chooses $K = 5$, which is relatively prime to $q - 1 = 18$.
2. $S_1 = \alpha^K \bmod q = 10^5 \bmod 19 = 3$ (see Table 8.3).

3. $K^{-1} \bmod (q - 1) = 5^{-1} \bmod 18 = 11.$
4. $S_2 = K^{-1}(m - X_A S_1) \bmod (q - 1) = 11(14 - (16)(3)) \bmod 18 = -374 \bmod 18 = 4.$

Bob can verify the signature as follows.

1. $V_1 = \alpha^m \bmod q = 10^{14} \bmod 19 = 16.$
2. $V_2 = (Y_A)^{S_1}(S_1)^{S_2} \bmod q = (4^3)(3^4) \bmod 19 = 5184 \bmod 19 = 16.$

Thus, the signature is valid.

CS8792-CRYPTOGRAPHY AND NETWORK SECURITY

UNIT V SECURITY PRACTICE AND SYSTEM SECURITY 9

Electronic Mail security – PGP, S/MIME – IP security – Web Security - SYSTEM SECURITY: Intruders – Malicious software – viruses – Firewalls.

Question Bank

1.Why Email compatibility function in PGP required?[Nov/Dec 2022]

- Many electronic mail systems only permit the **use of blocks consisting of ASCII texts.**
- To accommodate this restriction, PGP provides the service of **converting the raw 8-bit binary stream to a stream of printable ASCII characters.**
- The scheme used for this purpose is **radix-64 conversion**.**Radix 64 conversion** is used to ***convert binary data into ASCII characters***.
- e.g., consider the 24-bit (3 octets) raw text sequence . we can express this input in block of 6-bits to produce 4 ASCII characters.
- 001000 11 0101 110010 010001
- I L Y R => corresponding ASCII characters

2.Define virus.specify the types of viruses.[Nov/Dec 2022]

- A virus is **a piece of software** that can "infect" other programs by modifying them; **the modification includes a copy of the virus program**, which can then go on to infect other programs.
- A virus can do anything that **other programs do**. The only difference is that it **attaches itself to another program and executes** secretly when the host program is run.

Once a virus is executing, it can perform any function, such as **erasing files and programs.**

Types of virus

A virus classification **by target** includes the following categories:

• **Boot sector infector:** Infects a master boot record or boot record and spreads when a system is booted from the disk containing the virus.

• **File infector**: Infects files that the operating system or shell consider to be executable.

• **Macro virus**: Infects files with macro code that is interpreted by an applica tion.

3. List out the applications of SSL.[Nov/Dec 2020]

(i)Secure Websites (HTTPS): SSL/TLS is most commonly used to secure websites through HTTPS (HTTP Secure

(ii)Email Encryption (SMTP/POP/IMAP): SSL/TLS can be used to secure email communication between email clients and servers. This is particularly important for protecting the confidentiality of email content and login credentials.

(iii)Virtual Private Networks (VPNs): SSL/TLS can be employed in VPNs to create secure and encrypted tunnels for remote access to corporate networks. It ensures that data transmitted between a user's device and the corporate network remains confidential and secure.

(iv)File Transfer (FTPS and SFTP): SSL/TLS is used in secure file transfer protocols like FTPS (FTP Secure) and SFTP (SSH File Transfer Protocol). It encrypts files during transmission, preventing unauthorized access to sensitive data.

Instant Messaging (IM): Some instant messaging services and clients use SSL/TLS to encrypt chat messages and protect user privacy.

4. What do you mean by IP Security policy?[Nov/Dec 2022]

Fundamental to the operation of IPsec is the concept of a security policy applied to each IP packet that transits from a source to a destination

IPsec policy is determined primarily by the interaction of two databases, the security association database (SAD) and the security policy database (SPD).

5. Explain the process of Radix 64 conversion[Nov/Dec 2021]

Radix 64 conversion is used to ***convert binary data into ASCII characters***.

e.g., consider the 24-bit (3 octets) raw text sequence . we can express this input in block of 6-bits to produce 4 ASCII characters.

001000	11 0101	110010	010001	
I	L	Y	R	=> corresponding ASCII characters

6. Write short notes on Spammers and Key loggers.[Nov/Dec 2021,Apr/ May 2023]

Spammer programs Used to send large volumes of unwanted e-mail

Keyloggers Captures keystrokes on a compromised system

7.What are the various types of firewall?[Apr/May 2023]

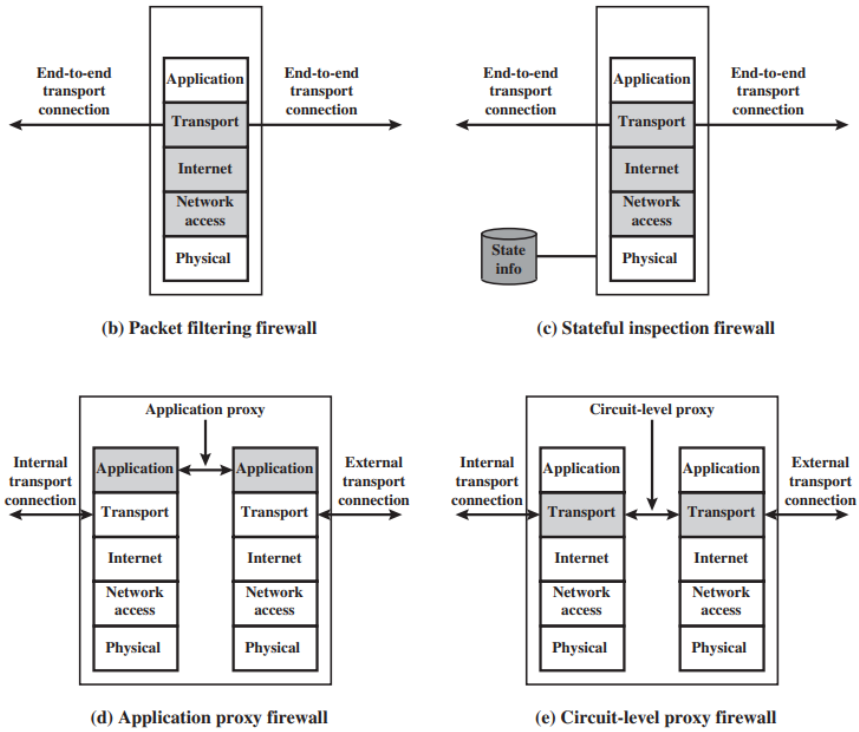


Figure Types of Firewalls

8.List the limitations of SMTP[Nov/Dec 2016]

1. ***SMTP cannot transmit executable files*** or ***other binary objects.***

2. ***SMTP cannot transmit text data that includes national language*** **characters** because these are represented by **8-bit codes** with values of **128 decimal or higher**, and **SMTP is limited to 7-bit ASCII.**

3. **SMTP servers** may **reject mail message** over **a certain size**.

4. **SMTP gateways** that translate ***between ASCII and the character code EBCDIC*** do not use a *consistent set of mappings*, resulting in ***translation problems***.

5. SMTP gateways to ***X.400 electronic mail networks*** cannot handle ***nontextual data*** included in ***X.400 messages***.

6. Some SMTP implementations ***do not adhere completely to the SMTP standards*** defined in **RFC 821**. Common problems include:
   - Deletion, addition, or reordering of carriage return and linefeed
   - Truncating or wrapping lines longer than 76 characters
   - Removal of trailing white space (tab and space characters)
   - Padding of lines in a message to the same length
   - Conversion of tab characters into multiple space characters

9. List out the services provided by PGP.

The ***actual operation of PGP***, as opposed to the management of keys, consists of five services:

(i)authentication, (ii)confidentiality, (iii)compression, and (iv)e-mail compatibility(v)Segmentation [2 Marks]

10.What do you mean by PGP?

- PGP is **an open-source, freely available software package** for e-mail security.
- It provides

(i)**authentication through tthe use of digital signature**,
(ii)**confidentiality** through the use of **symmetric block encryption**,
(iii)compression using the **ZIP algorithm**, and
(iv)**e-mail compatibility using the radix-64 encoding scheme**.

11.Define MIME Header

The five header fields defined in MIME are as follows:

- **MIME-Version**: Must have the parameter **value 1.0**. This field indicates that the message conforms to RFCs 2045 and 2046.
- **Content-Type**: Describes **the data contained in the body** with sufficient detail
- **Content-Transfer-Encoding**: Indicates **the type of transformation** that has been used to represent the body of the message in a way that is acceptable for mail transport.
- **Content-ID:** Used to identify the message.
- **Content-Description**: A text description of the object with the body; this is useful when the object is not readable (e.g., audio data).

12.List of types of MIME

MIME Content Types

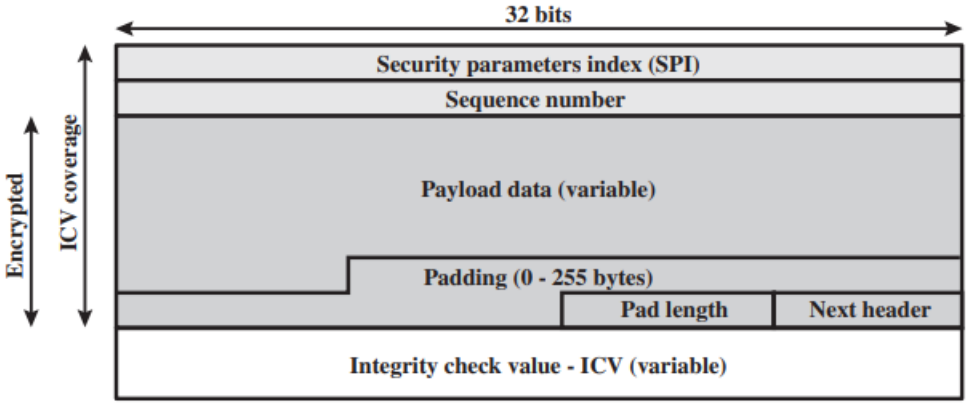
Type	Subtype	Description
Text	Plain	Unformatted text; may be ASCII or ISO 8859.
	Enriched	Provides greater format flexibility.
Multipart	Mixed	The different parts are independent but are to be transmitted together. They should be presented to the receiver in the order that they appear in the mail message.
	Parallel	Differs from Mixed only in that no order is defined for delivering the parts to the receiver.
	Alternative	The different parts are alternative versions of the same information. They are ordered in increasing faithfulness to the original, and the recipient's mail system should display the "best" version to the user.
	Digest	Similar to Mixed, but the default type/subtype of each part is message/rfc822.
Message	rfc822	The body is itself an encapsulated message that conforms to RFC 822.
	Partial	Used to allow fragmentation of large mail items, in a way that is transparent to the recipient.
	External-body	Contains a pointer to an object that exists elsewhere.
Image	jpeg	The image is in JPEG format, JFIF encoding.
	gif	The image is in GIF format.
Video	mpeg	MPEG format.
Audio	Basic	Single-channel 8-bit ISDN mu-law encoding at a sample rate of 8 kHz.
Application	PostScript	Adobe Postscript format.
	octet-stream	General binary data consisting of 8-bit bytes.

13.Specify the benefits of IPSec.

Benefits of IPSec

- **Strong security for all traffic when crossing the perimeter (assuming it is implemented in a firewall or router)**
- **IPSec in a firewall is resistant to bypass**
- **Below the transport layer (TCP, UDP) and transparent to applications**
- **Transparent to the end user**
- **Provides security for individual users – offsite workers, VPN**

14.Draw the ESP packet format



(a) Top-level format of an ESP Packet

15.Differentiate transport and tunnel mode in IPSec

Transport Mode	Tunnel Mode
It provides protection for upper layer protocols	It provides protection to the entire Ip packet
Used end-to-end communication between two host.	It is used when one or both ends of an SA is a security gateway,such as firewall or router that implement IpSec.
Authentication IP payload and selected portions Of IP header and IPV6 extension header	Authenticates entire inner IP packet plus selected portions of outer IP header and outer IPV6 extension headers.

16.List the three classes of Intruders.

Three classes of intruders are as follows:

Masquerader – an ***individual who is not authorized*** to use **the computer** and ***who penetrates a system's access controls*** to exploit **a legitimate user's account**.

Misfeasor – a **legitimate user** who accesses **data, programs, or resources** for which such **access is not authorized**, or who is authorized for such access but **misuse his or her privileges**.

Clandestine user – an individual who ***seizes supervisory control of the system*** and uses this ***control to avoid(escape from) auditing*** and ***access controls or to suppress audit collection.***

17.What is an Intruder

Intruders are the attackers who attempt to breach the security of a network

18.Define Worm

Worm is a program that can **replicate itself and send copies from computer to computer across** network connections.

Upon arrival, the worm may be activated to replicate and propagate again. In addition to propagation, the worm usually performs some unwanted function.

Example

Morris worm ,Email Worms

- Email Worms spread through malicious email as an attachment or a link of a malicious website.
- Instant Messaging Worms: Instant Messaging Worms spread by sending links to the contact list of instant messaging applications such as Messenger, WhatsApp, Skype, etc.
- The Morris worm was designed to spread on UNIX systems and used a number of different techniques for propagation

19.Define Zombie

Zombie A ***program that secretly takes over another Internet-attached computer*** and then uses that computer to **launch attacks** that are difficult to trace to the zombie's creator.

20.Define Malicious software

The software which is used for ***destructive purpose*** .It leads to the destruction process.It is called malware.

The most sophisticated types of threats to computer systems are presented by programs that exploit vulnerabilities in computing systems.

21.What are the effects of malicious software write any two?

Malware impacts your computer in the following ways: **Disrupts operations. Steals sensitive information. Allows unauthorized access to system resources**.

22.Discriminate statistical anomaly detection and rule based detection

Approaches to Intrusion Detection

Statistical Anomaly Detection

- Threshold based Detection
  - Count occurrences of specific event over time
  - Ineffective Detector
- Profile Based
  - Characterize past behaviour of users
  - Detect significant deviations

Rule Based Detection

- Anomaly
  - Observe events on system and apply rules to decide if activity is suspicious or not
- Penetration identification
- Analyse historical audit records to identify usage patterns & auto generate rules for them.
- It does not require prior knowledge of security flaws

23.Define Honeypot

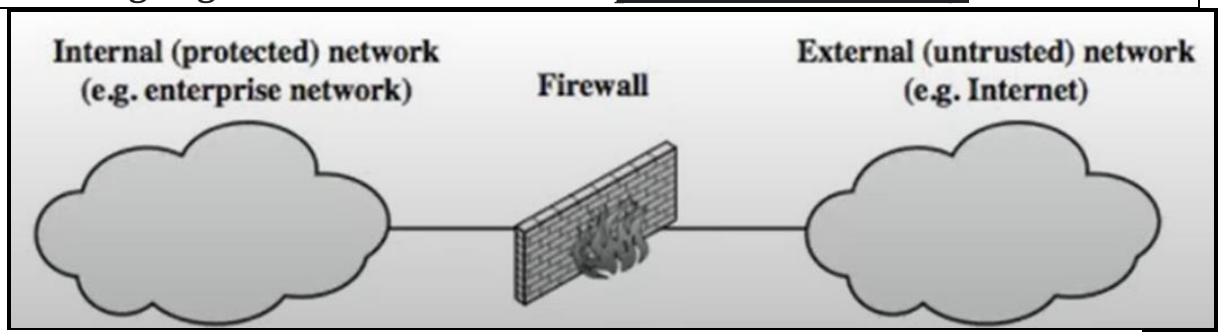
Definition

Honeypots are decoy(tricky) systems that are designed to lure a potential attacker away from critical systems. Honeypots are designed to

- Divert an attacker from accessing critical systems
- **Collect information** about the attacker's activity
- Encourage the attacker to stay on the system long enough for administrators to respond

24.Define the role of firewall

- A Firewall is a network security system that **monitors and filters incoming and outgoing network traffic** based on ***predetermined security rules***.



- A Firewall is a network security device that **monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies**.

25.What are the two functions of a firewall?

- A firewall is a protective measure that safeguards an individual's or company's computer network. It provides two basic security functions, including **packet filtering, which inspects traffic at the packet level, and acting as an application proxy, providing security measures at the application level**.

26.List the Types of Firewall

- 1.Packet Filtering Firewall
- 2. Stateful inspection firewall
- 3. Application proxy firewall
- 4. Circuit-level proxy firewall

27.List the design goals of firewalls

- 1.All traffic **from inside to outside**, and **vice versa**, must pass through the firewall.This is achieved by **physically blocking all access** to the **local network** except via the firewall**.**
- 2. Only **authorized traffic**, as ***defined by the local security policy***, will be allowed **to pass**. Various types of firewalls are used, which implement **various types of security policie**
- 3. The **firewall itself is immune to penetration**.This implies **the use of a hardened system with a secured operating system**.

- **Trusted computer systems** are suitable **for hosting a firewall** and often required in government applications.

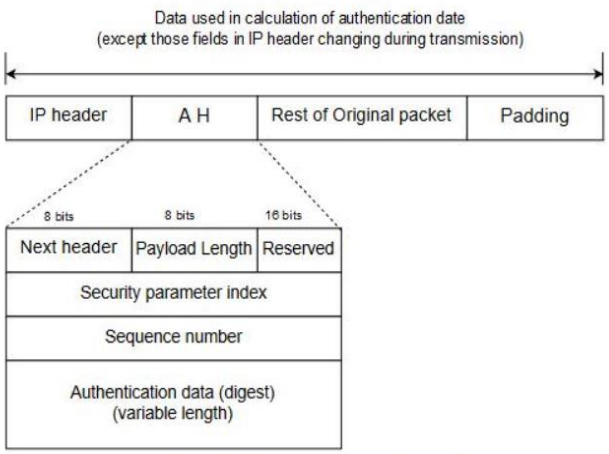
Part B Questions

1.Discuss the seven types of MIME content type.[Nov/Dec 2021]

Table MIME Content Types

Type	Subtype	Description
Text	Plain	Unformatted text; may be ASCII or ISO 8859.
	Enriched	Provides greater format flexibility.
Multipart	Mixed	The different parts are independent but are to be transmitted together. They should be presented to the receiver in the order that they appear in the mail message.
	Parallel	Differs from Mixed only in that no order is defined for delivering the parts to the receiver.
	Alternative	The different parts are alternative versions of the same information. They are ordered in increasing faithfulness to the original, and the recipient's mail system should display the "best" version to the user.
	Digest	Similar to Mixed, but the default type/subtype of each part is message/rfc822.
Message	rfc822	The body is itself an encapsulated message that conforms to RFC 822.
	Partial	Used to allow fragmentation of large mail items, in a way that is transparent to the recipient.
	External-body	Contains a pointer to an object that exists elsewhere.
Image	jpeg	The image is in JPEG format, JFIF encoding.
	gif	The image is in GIF format.
Video	mpeg	MPEG format.
Audio	Basic	Single-channel 8-bit ISDN mu-law encoding at a sample rate of 8 kHz.
Application	PostScript	Adobe Postscript format.
	octet-stream	General binary data consisting of 8-bit bytes.

2.Draw IPSec Authentication Header and write short notes on each element of the Header.[Nov/Dec 2021]



Authentication Header (AH) protocol

- IPSEC defines two protocols
    - a. the Authentication Header (AH)
    - b. Encapsulation Security Payload (ESP)

  to provide authentication and for encryption for the packets at the IP level.

1.Authentication Header (AH) (provide source authentication & data integrity but not privacy)

- AH protocol is designed to authenticate the source host & to ensure the integrity of the payload carried in the IP packet.
- This protocol uses a hash function & a symmetric key to create a message digest; the digest is inserted via the authentication header.
- The AH is then placed on the appropriate location , based on the mode i .e transport or tunnel.

- When an IP datagram carries an authentication header, the original value in the protocol of the IP header is replaced by the value 51.
- The addition of an authentication header follows following steps :
    1. An AH is added to the payload with authentication data field set to 0.
    2. Padding may be added to make the total length ever for a particular hashing algorithm.
    3. Hashing is based on the total packet. However only those fields of the IP header that do not change during transmission are included in the calculation of the message digest i.e authentication data.
    4. The authentication data are inserted in the authentication header.
    5. The IP header is added after changing the value of the protocol filed to 51.

Description of every field of AH protocol

1.Next header : The 8 bit header field defines the type of payload carried by the IP datagrams (such as TCP , UDP, ICMP). The process copies the value of the protocol field in the IP datagram to this field. The value of the protocol field in the new IP datagram is now set to 51 to show that the packet carried an AH.

2.Payload length : It defined the length of the AH in 4 -byte multiples, but it does not include the first 8 bytes.

3.Security Parameter index : The 32 but SPI field plays the role of a virtual circuit identifier & is the same for all packets sent during a connection called Security Association.

4.Sequence Number : A 32 bit sequence number provides ordering information for a sequence of datagrams. It prevents a playback. Sequence number is not repeated even if a packet is retransmitted.

5.Authentication data : This field is the result of applying a hash function to the entire IP datagram except for the fields that are changed during transit.

3. With the help of a neat diagram, explain wired and wireless TLS architecture.[Nov/Dec 2020]

Wireless TLS

WTLS Protocol Architecture

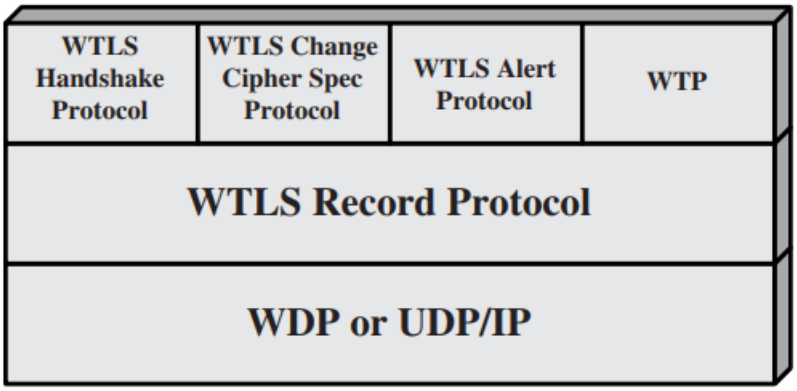


Figure 17.15 WTLS Protocol Stack

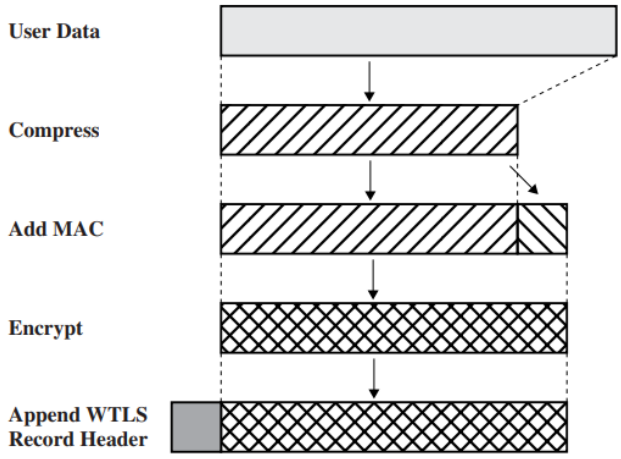


Figure WTLS Record Protocol Operation

Wired TLS

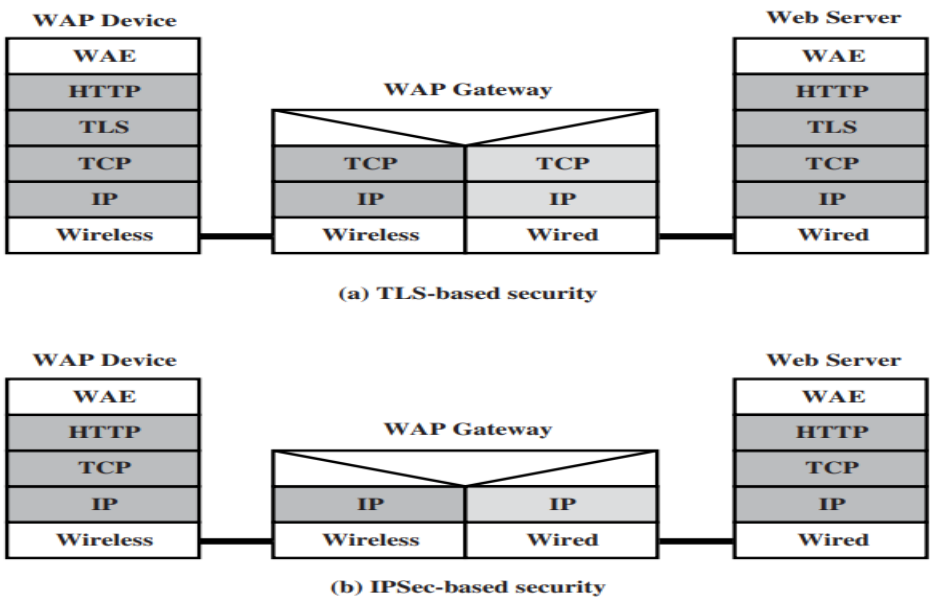


Figure 17.20 WAP2 End-to-End Security Approaches

4. Assume when an attacker tries to modify the database content by inserting an UPDATE statement. Identify this SQL injection attack method and justify. Detail the methods used to prevent SQL injection attack[Nov/Dec 2020]

SQL injection, also known as SQLI, is a common attack vector that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed.
This information may include any number of items, including sensitive company data, user lists or private customer details.

1. Do not rely on client-side input validation.
2. Use a database user with restricted privileges
3. Use prepared statements and query parameterization
4. Scan your code for SQL injection vulnerabilities
6. Don’t rely on blocklisting
7. Perform input validation
8. Be careful with stored procedures

5.Illustrate how PGP encryption is implemented through a suitable diagram.

- Define PGP
- PGP Message Generation

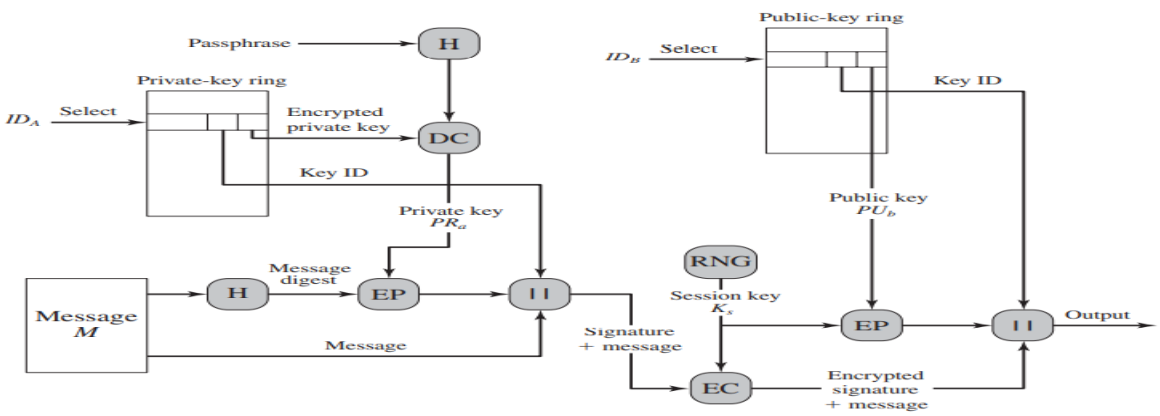


Figure conversion) PGP Message Generation (from User A to User B: no compression or radix-64

6.How does PGP provides confidentiality and authentication service for e-mail and file storage applications?Draw the block diagram and explain its components[Nov/Dec 2020]

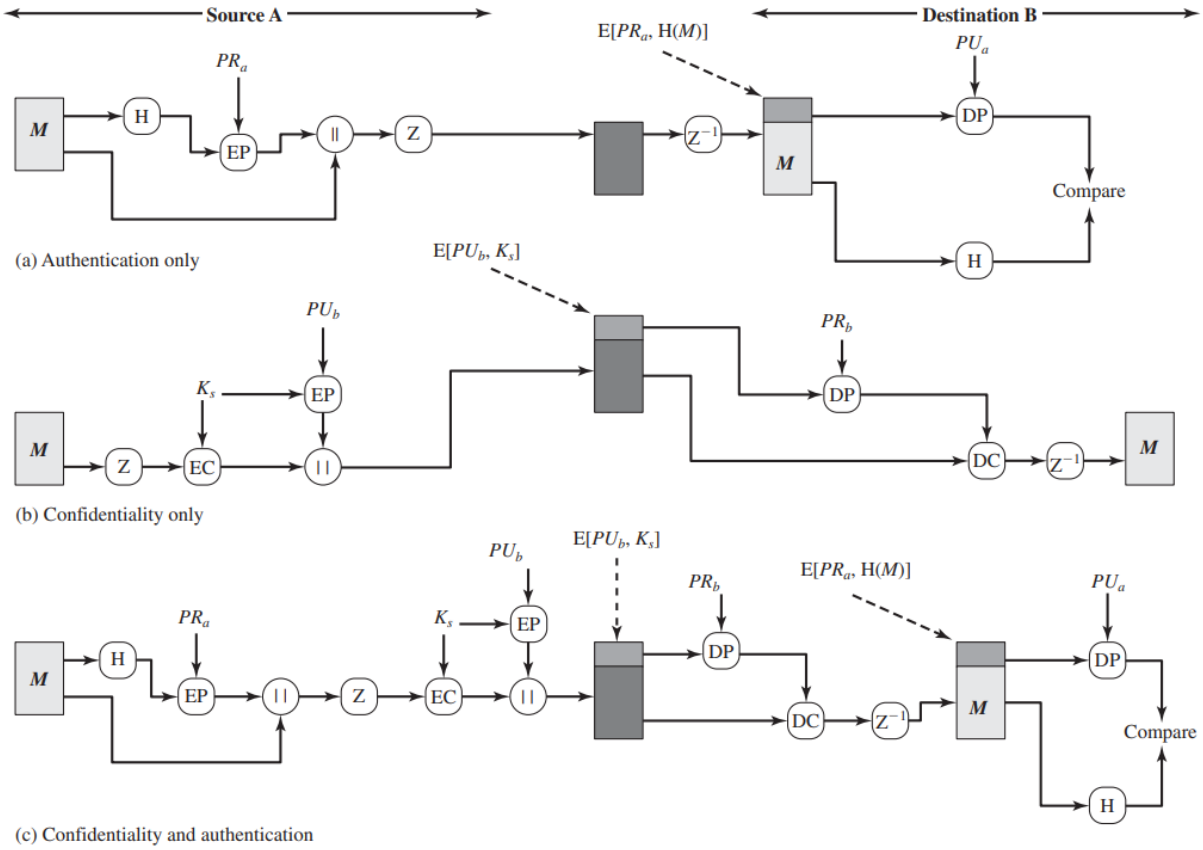


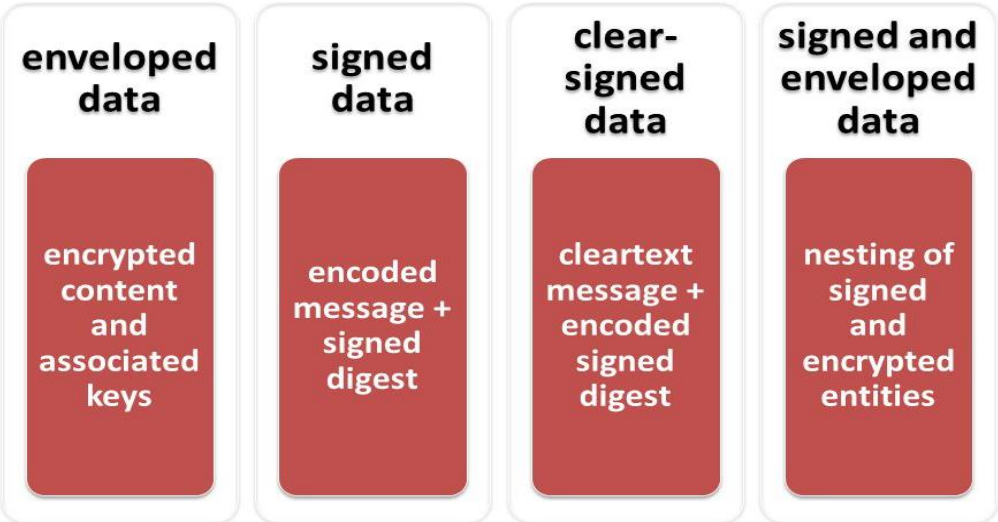
Figure 18.1 PGP Cryptographic Functions

7.Explain about S/MIME in detail

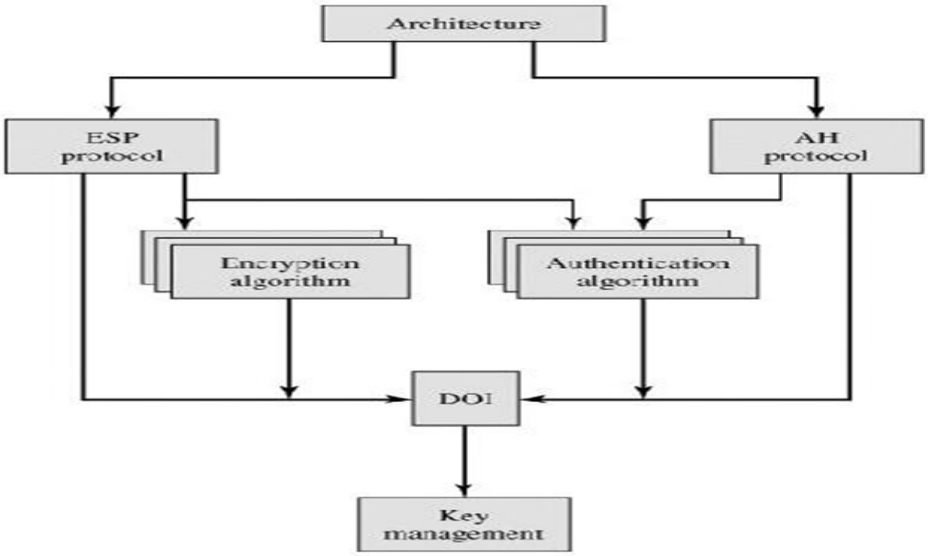
Define

MIME Types

S/MIME Functionality or S/MIME Functions



8.Explain IP Security Architecture in detail

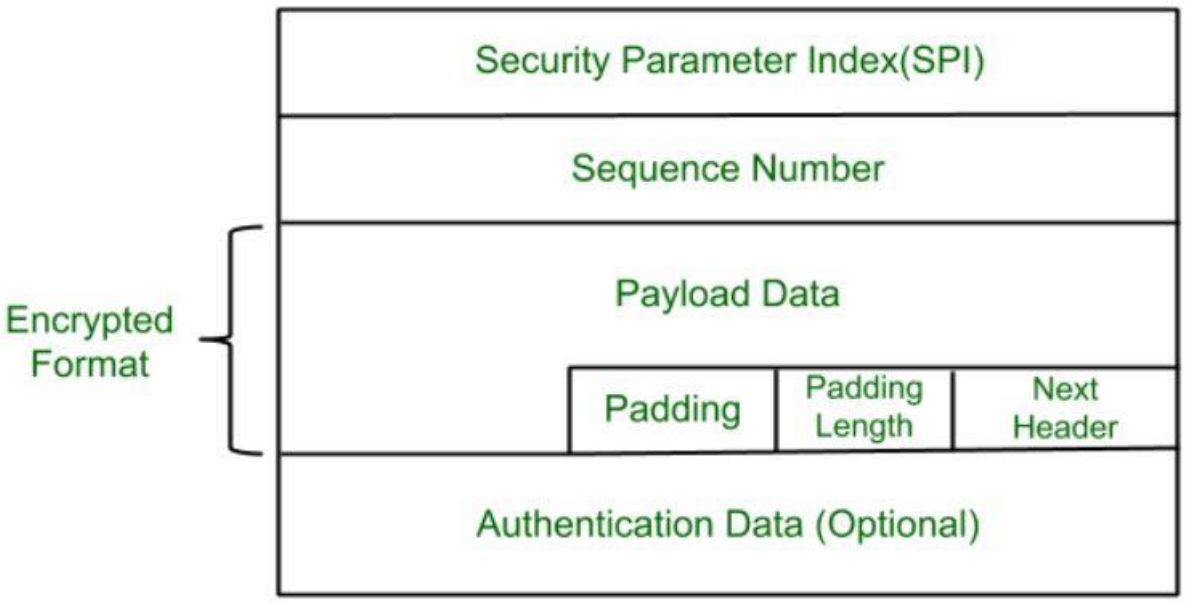


Define IPSecurity

Explain allthe components

9.Explain ENCAPSULATING SECURITY PAYLOAD in detail

ESP Format



- Encryption and Authentication Algorithms
- Padding
- Anti-Replay Service
- Transport and Tunnel Modes

9.How does screened host architecture for firewalls differ from screened subnet firewall architecture?
Which offers more security for information assets on trusted network?
Explain the neat sketch

. Screened subnet firewall configuration is more secure for trustednetwok FIREWALL CONFIGURATIONS:

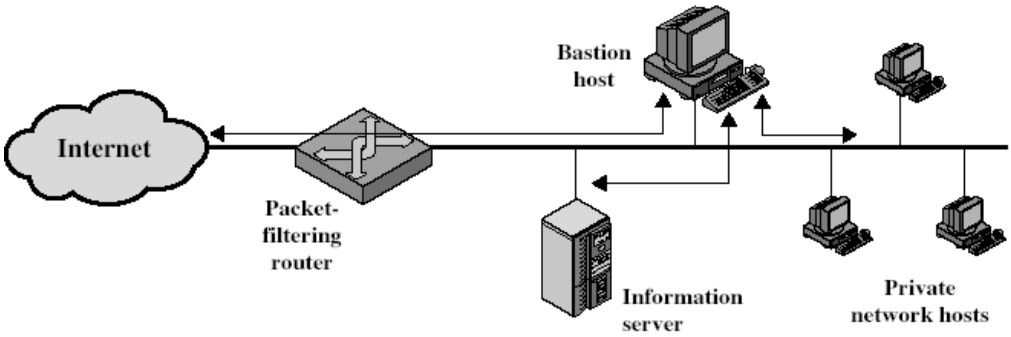


Figure 4.8 **Screened host firewall**

2. Screened host firewall, dual homed basiton configuration

In the previous configuration, if the packet filtering router is compromised, traffic could flow directly through the router between the internet and the other hosts on the private network. This configuration physically prevents such a security break.

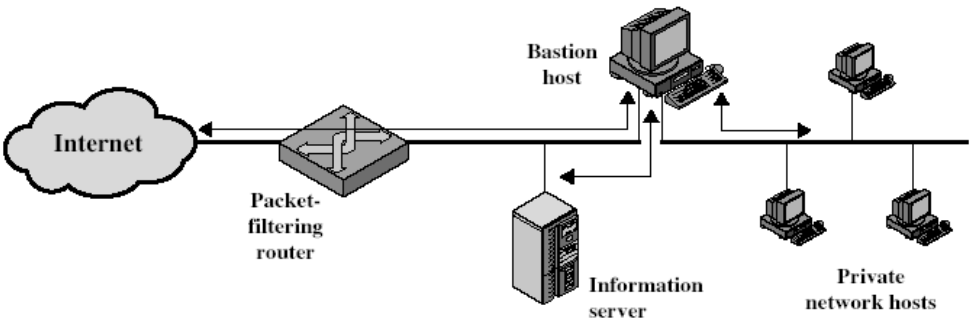


Figure 4.9 Screened host firewall, dual homed basiton configuration

3. Screened subnet firewall configuration

In this configuration, two packet filtering routers are used, one between the basiton host and internet and one between the basiton host and the internal network. This configuration creates an isolated subnetwork, which may consist of simply the basiton host but may also include one or more information servers and modems for dial-in capability.

Typically both the internet and the internal network have access to hosts on the screened subnet, but traffic across the screened subnet is blocked. This configuration offers several advantages:

- There are now three levels of defense to thwart intruders.
- The outside router advertises only the existence of the screened subnet to the internet; therefore the internal network is invisible to the internet.
- Similarly, the inside router advertises only the existence of the screened subnet to the internal network; therefore the systems on the internal network cannot construct direct routes to the internet.

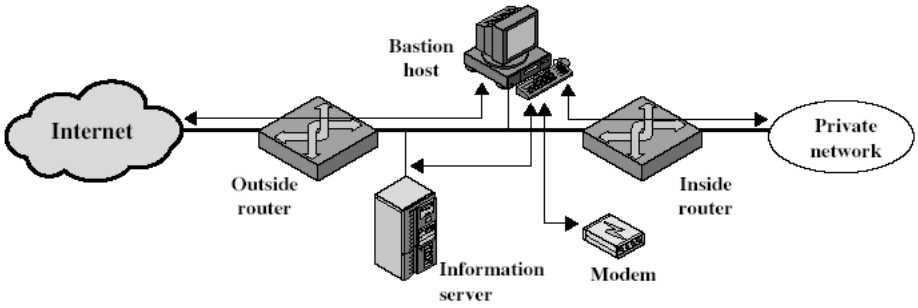


Figure Screened subnet firewall configuration

10.Explain the characteristics and types of firewall?

- Goals of firewall
- General techniques of firewall
- Scope of firewall

Types

- Packet Filtering Firewall
- Statefull Inspection firewall

- Application proxy firewall
- Circuit level proxy firewall

11.Explain WebSecurity in Detail

- Definition
- Web security considerations or How to Secure the Web Site
- 1.Updated Softwares
- 2.Beware of SQL injection
- 3.Cross Site Scripting (XSS)
- 4.Error Message
- 5.Data Validation
- 6.Passwords
- Web Security Threats
- Web Traffic Security Approaches