Name: Sanket Chandrashekhar Harvande : 19

GHARDA FOUNDATION'S
GHARDA INSTITUTE OF TECHNOLOGY GIT

Experiment No. Date :

Assignment No. - 1

1. Explain security services & Mechanisms in detail. Explain the relationship between them.

→ Ans :-

Security Services :-

- X.800 is a service provided by protocol layer of communicating open systems, to ensure the enough security of the system
- RFC 2828 defines security service as a communication service provided by a system to give protection to the system resources.

1. Authentication :-

- It is assurance of parties that they are authentic user in the communication network.
- Authentication helps to identify the claimed identity of an entity, such as username password or any other important information such as encryption or decryption keys stolen during transmission between sender & receiver.

2. Authorization :-

- Authorization service helps for checking whether the entity has the right to perform action requested.
- Authorization means providing authority or permission of accessing the system or privilege of accessing the data.

- Authorization is one of the most important security attacks.

3. Access Control :-

- Access control is the ability to limit & control access to the host systems. It prevents unauthorized use of a resource.
- The service used to prevent unauthorized use of a resource i.e. complete control over who can access to resources, under what conditions access can occur & what are different accessing methodology.

4. Non-Repudiation :-

- Principle of non-repudiation states that if sender sends some information & later on hence denied that he never sends that information, called non-repudiation.

5. Auditing :-

- Auditing services helps to trace which user accessed what? when & which way?
- In general auditing does not provide protection but can be the tool for analysis of problems.

GHARDA FOUNDATION'S
GHARDA INSTITUTE OF TECHNOLOGY GIT

Experiment No. Date :

6. Data Integrity :-

- To assure that message received is as sent with no duplications, insertions or modifications, delays or replays. The destructions of messages have also been recovered.

7. Data Confidentiality :-

- It is a protection of data to be accessed by unauthorized user.

i) Connection confidentiality :- In case of a TCP connection set up between two systems, to protect user data that is transmitted over the connection.

ii) Connectionless confidentiality :- To protect data in a single data block.

iii) Selective-field confidentiality :- To protect selective fields with a user data or a connection or a single data block.

iv) Traffic flow confidentiality :- To protect data that might be derived from observing the data flow.

Security Mechanisms :-

1) Encipherment :- To use mathematical algorithms to transform data into a form that is not easily understandable

2. Digital signature :- The data is appended to, or a cryptographic transformation of a data unit that allows the receiver of the message to prove the source & integrity of data unit against forgery.

3. Access Control :-
Various mechanisms used to enforce access rights to the resources or it is the process of limiting the access to the resources of the Information system. Firewall is the best example of limiting the access control.

4. Data Integrity :-
content should not modify before it reaches to intended person.

5. Authentication Exchange :-
The mechanism used to ensure the identity by information exchange.

6. Traffic Padding :-
To insert bits into gaps in the data stream to frustrate traffic analysis attempt.

7. Routing Control :-
To allow some selected routes in network for routing or can change the route if any attack is detected in the network.

Q.2 List & explain various types of attacks on encrypted message ?

→ Ans :-

The X.800 & RFC2828 classify security attacks into two types :-

Security Attacks

→ (a) Passive attack
→ (b) Active attack.

(a) Passive Attack :-

The information is only monitored during data transmission between two persons & doesn't involve any modification to the contents of original message is called passive attack.

The two types of passive attacks are :-

1. Release of message contents.
2. Traffic Analysis.

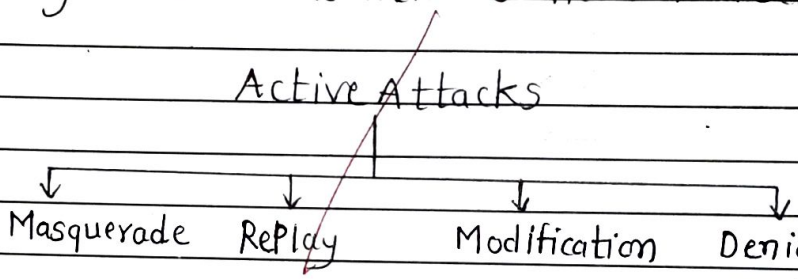
1. Release of message contents :- It is quite simple to understand. When we send a confidential email to our friend, our aim is that only intended person should access this mail.

2. Traffic Analysis :-

The opponent (here it is called third person) is able to capture the contents of the message but not extract the information from the message.

b) Active Attacks :-

- Active attacks involve modification of a data stream or creation of a false stream of messages.
- Attacker aim in such type of attack is to currupt or destroy the data as well as network itself.

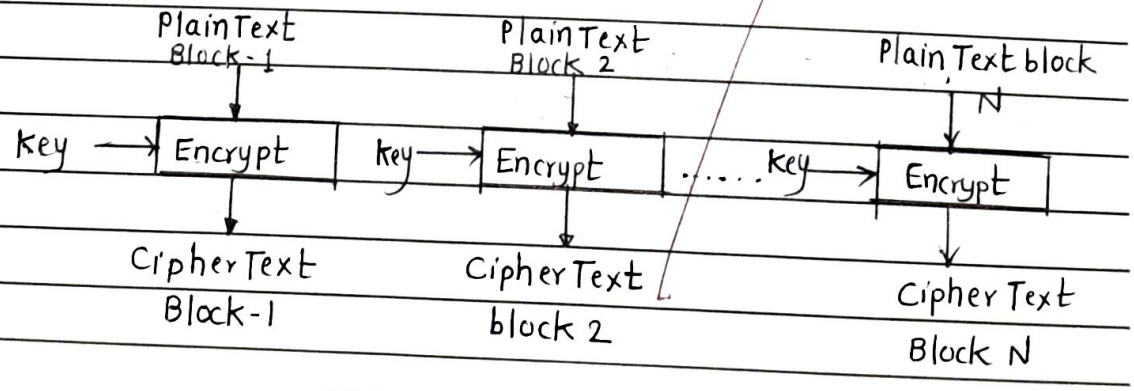


6. Discuss in detail Block Cipher modes of operation.

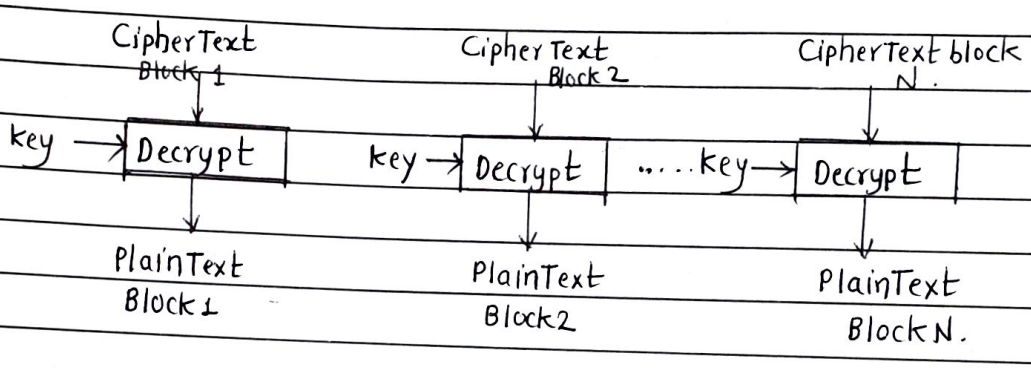
→ Block cipher modes of operation includes :-

(1) Electronic Code Book (ECB) mode
(2) Cipher Block Chaining (CBC) mode
(3) Cipher feedback (CFB) mode
(4) Output Feedback (OFB) mode
(5) Counter (CTR) mode.

1) Electronic Code Book (ECB)

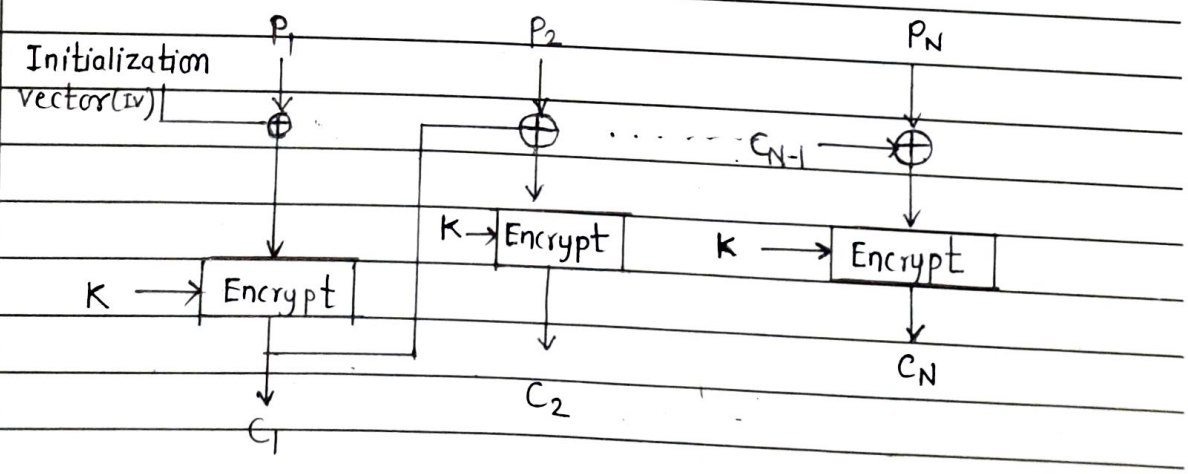


- In ECB mode given the plainText message is divided into blocks of 64 bits each & each 64-bits blocks gets encrypted independently.
- The plainText is encrypted using same key & transfers the encrypted data to receiver.



2. Cipher Block Chaining (CBC) Mode :-

- To overcome the problem of repetition & order independence in ECB even for repeated plaintext the cipher Block chaining (CBC) mode is used.

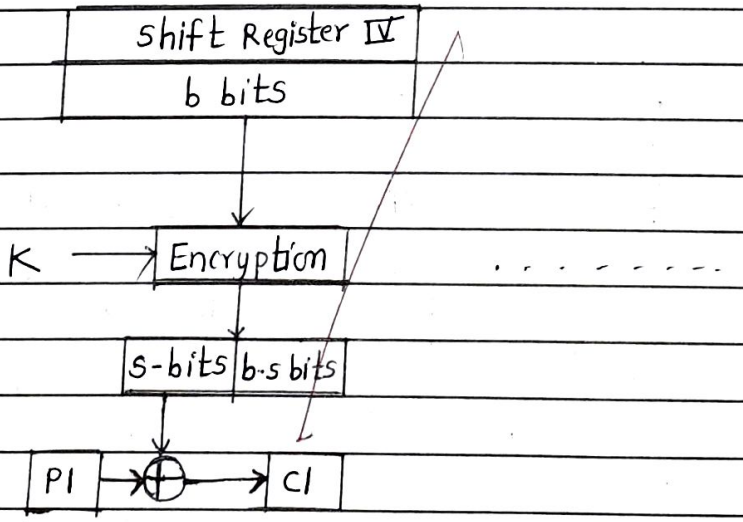


3) Cipher Feedback Mode (CFB) :-

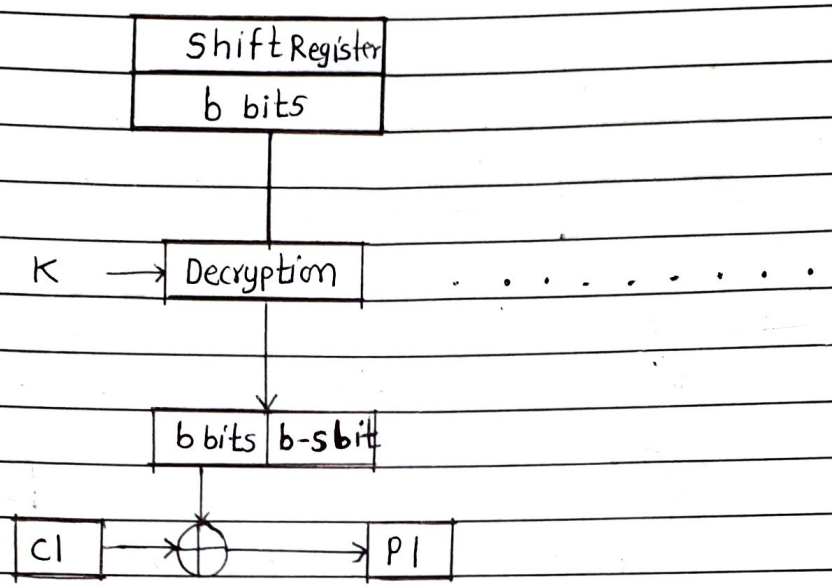
- CFB mode uses block cipher as stream cipher meaning is that data is encrypted in smaller units of block say 8-bits rather than predefined size of 64 bits.
- CFB mode may be used as a stream cipher. In CFB encryption process 64 bits initialization vector is used which is kept in 64 bits of shift register.

4) Output Feedback Mode (OFB) :-

- The output feedback (OFB) mode is similar in structure to that of CFB.
- The output of encryption function that is fed to the shift register in OFB, whereas in CFB the ciphertext unit is fed back to the shift register.



Page No:



5> Counter Mode :

This mode is similar to OFB with the difference is that it uses counters or sequence numbers as input to the algorithm. We put a constant value of counter which will be of same size that of a plaintext block.

- In counter mode, the counter is encrypted & then XORed with the plaintext to ciphertext.
- There is no chaining process is done.
- During the decryption process same counter is used which was encrypted earlier & later XORed with ciphertext to get the original plaintext

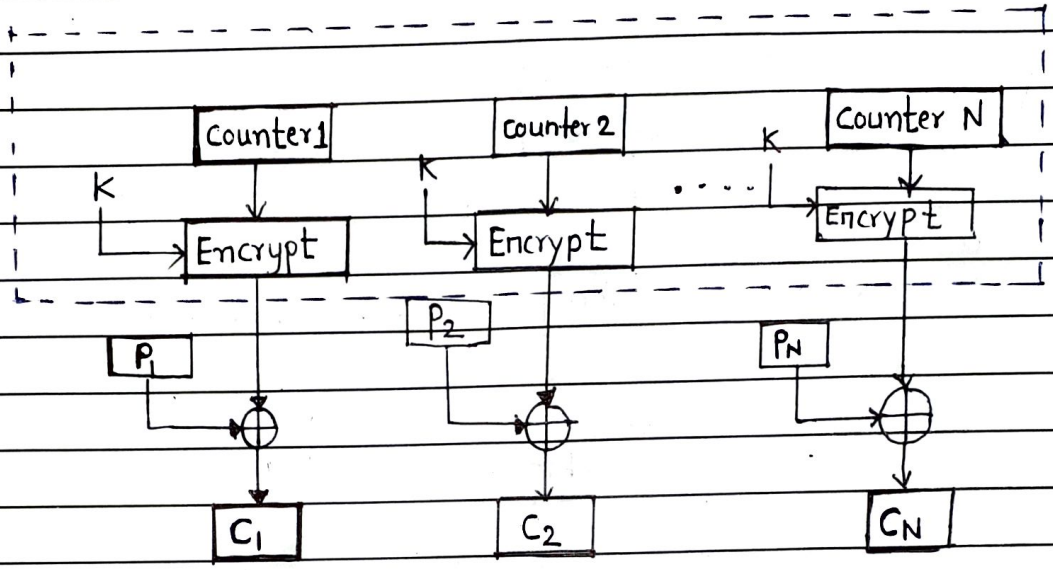


Fig : Counter Encryption Process

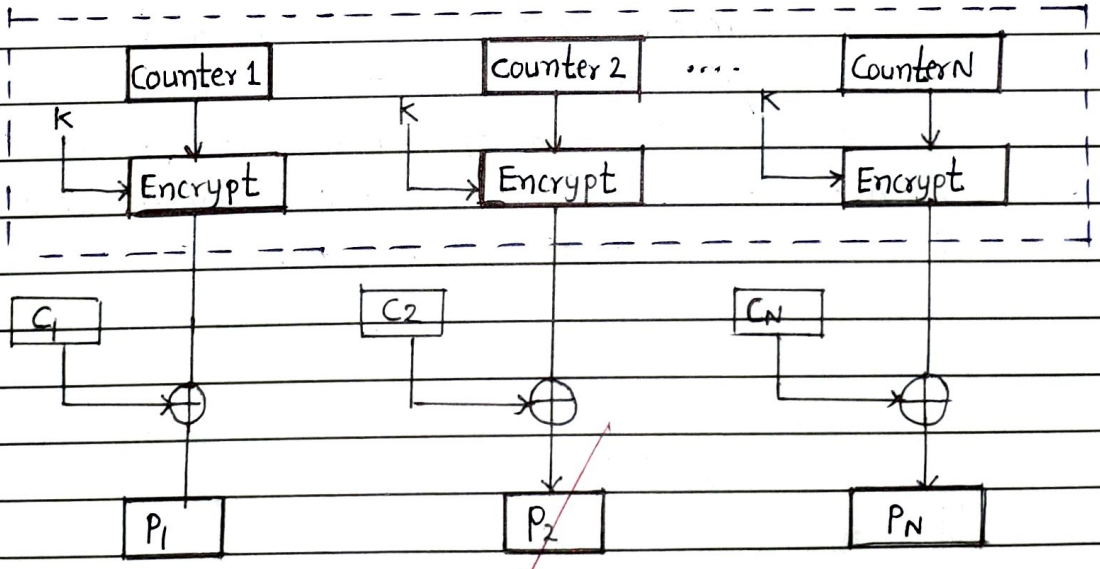


Fig :- Counter (CTR) Decryption Process

Page No:

Q.7 Compare & Contrast - Block Cipher & Stream Cipher

	Stream Cipher	Block Cipher
1.	Keys & algorithms are applied to each binary digit in a data stream, one bit at a time, rather than encrypting block of data.	Block cipher is main method of encrypting text in which keys & algorithm are applied to block of data rather than individual bits like stream cipher.
2.	Stream cipher is less time consuming.	Block cipher is more time consuming.
3.	Because of one bit encrypting at a time, stream cipher is faster than block cipher.	As block of data is encrypting at a time block cipher is slower than stream cipher.
4.	Stream cipher doesn't used in chaining modes of operation.	Block used in chaining modes of operation.
5.	Hardware implementation is easy using stream cipher.	Software implementation is easy using block cipher.

	Confusion	Diffusion
1.	Confusion obscures the relationship between the plaintext & ciphertext.	Diffusion spreads the plaintext statistics through the cipher text.
2.	A one-time pad relies entirely on confusion while a simple substitution cipher is another example of a confusion-only cryptosystem.	A double transposition is the classic example of a diffusion-only cryptosystem.
3.	Confusion alone is, apparently 'enough' since the one-time pad is provably secure.	Diffusion alone is perhaps, not enough at least
4.	The codebook aspects of such systems provide confusion analogous to though on a much grander scale a simple substitution.	Well-designed block ciphers spread any local statistics throughout the block, thus employing the principle of diffusion.

Page No:

Q.8 Describe triple DES with double DES keys. Is man in the middle attack possible on triple DES ?

→

Triple DES : performs the same operation as double DES only difference is that triple DES uses three keys K1, K2, K3 while encrypting plaintext.

- First it performs encryption on plaintext which is encrypted using K1 obtains first ciphertext again this cipher-text is encrypted by using another key called K2 which obtains the second ciphertext which is again encrypted using K3 & converted into final ciphertext, **Cp**.

- Mathematically Double DES is represented as,

$Pt \Rightarrow EK1(Pt) \Rightarrow TEMP = EK1(Pt) \Rightarrow EK2(E(K1(P))) \Rightarrow EK3(Ek2(EK1(Pt))) \Rightarrow$

$Cp = EK3(EK2(EK1(Pt)))$

where,

Pt = Plaintext

EK1(Pt) = Encrypted plaintext with key K1.

TEMP = EK1(Pt) = Temporary Variable to store results.

EK2(E(K1(P))) = Encrypted Results of first ciphertext using K2

EK3(Ek2(EK1(Pt))) = Encrypted results of second step using K2.

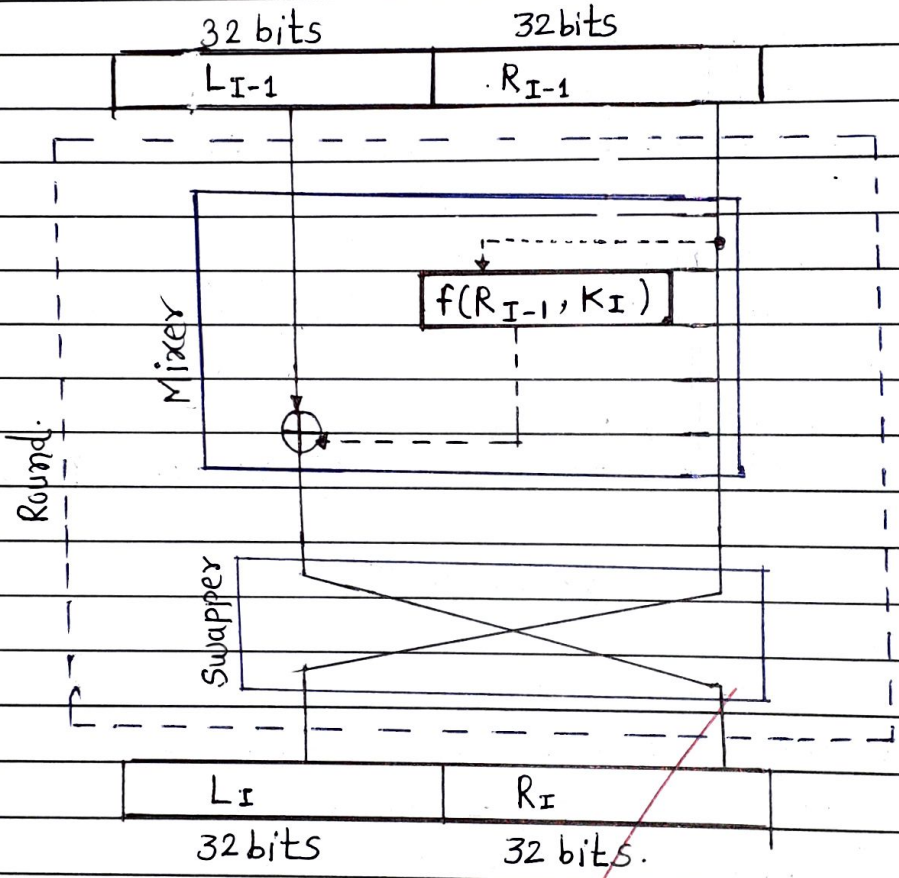
Cp = EK3(EK2(EK1(Pt))) = final Cipher text using K1, K2 & K3.

- Decryption of Triple DES is reverse Encryption.
- To decrypt the Cipher text Cp & obtain the plain text Pt, we need to perform following operation.

$Pt = DK3(DK2(DK1(Cp)))$

Q.9 Explain the structure of DES w.r.t.

i) Fiestal structure & its significance :-



1) DES uses fiestal structure & 16 fiestal rounds. Every round takes 32-bits (L_{I-1}) & Right 32-bit (R_{I-1}) from previous round (from initial permutation box for the very first time).

2) Each round uses two cipher elements : Mixer & swapper

3) The swapper is invertible, the mixer is invertible because of XOR operation.

ii) Significance of Extra swap between left & right half blocks :-

- The input of block to each round is divided into two halves that can be denoted as L & R for the left half & the right half.
- In each round the right half of the block R goes through unchanged. But the left half, L goes through an operation that depends on Round the encrypt the key.
- The permutation step at the end of each round swap the modified L & unmodified R & R for the next round be the output of L of the current round.

iii) Expansion :-

since right-input (RI-1) is 32-bit & round key is a 48 bit, we first need to expansion of right input (RI-1) to 48 bit Logic of permutation is graphically depicted.

iv) Significance of S-box :-

The 32-bit output of S-boxes then subjected to the straight permutation to get 32-bit output with rule shown in following.

16	15	24	21	29	12	28	17
01	07	30	26	05	18	31	10
02	13	20	14	32	27	03	09
19	08	23	06	22	11	04	25

v) DES function :-

DES function is the heart of DES. The DES function applies a 48-bit key to the rightmost 32 bit (RI-1) to produce a 32 bit output. This function consists of four sections

- Expansion p-box
- A straight p-box
- A whitener (XOR)
- A group of S-boxes

Q.10 Compare AES & DES. Which one is bit oriented & which is byte oriented.?

	AES	DES
(1)	AES stands for Advanced Encryption standard.	2) DES stands for Data Encryption standard.
(2)	Key length can be 128 bits, 192 bits & 256 bits.	The length is 56 bits in DES.
(3)	The structure is based on a substitution permutation network.	The structure is based on a fiestal network.
(4)	AES can Encrypt 128 bits of plaintext	DES can encrypt 64 bits of plaintext.

- AES is Byte-Oriented & DES is bit-Oriented.

Q.11 What is meant by Diffie-Hellman key exchange algorithm Explain with example.

→ 1) In public key ecryption schemes are secure only if authenticity of the public key is assured.
2) Diffie-Hellman key exchange is a simple public key algorithm.
3) The protocol enables 2 users to establish a secret key using a public key schemes based on discrete algorithm
4) The protocol is secure only if the authenticity of the 2 participants can be established.
5) The key is exchange in the following.

steps :-
Consider,
Private key of the sender = X_A
public key of the sender = Y_A
Private key of the receiver = X_B
Public key of the receiver = Y_B

step 1 : One of the parties choose two numbers 'g' & 'p' & exchange with the other party.
'g' is the primitive root of prime number 'p'.
After this exchange, both the parties know the value of 'a' & 'n'.

step 2 :-

Both the parties already know their own private key.

sender calculates its public key as - $Y_A = g^{x}A \bmod n$

Receiver calculates its public key as

$Y_B = g^{x}B \bmod n$

step 3 :- Both the parties receive public key of each other

Sender Calculates its secret keys as

Secret key $= (Y_B)^{x}$ A mod P

Receiver calculates secret key as

Secret key $= (Y_A)^{x}$ B mod P

User A		User B
Generate a random $X_A < q$	Y_A → ← Y_B	Generate a random $X_a < q$
Calculate $Y_A = a^{XA} \bmod q$		Calculate ; X_B
calculate		$Y_B = a \bmod q$
$K = (Y_B)^{XA} \bmod q$.		calculate
		$K = (Y_B)^{XA} \bmod q$

Example :-

Consider $q = 353$, $a = 3$ (3 is primitive root of 353)

A & B discrete private keys

$X_A = 97$ & $X_B = 223$

Each computes its public key

Page No:

A computes $Y_A = 3^{97} \bmod 353 = 40$
B computes $Y_B = 3^{233} \bmod 353 = 248$.

After exchange of public key each can compute the common secrete key

A computes $k = (Y_B)^{X_A} \bmod 353$
$= (248)^{97} \bmod 353$
$= 160$.

B computes k
$= (Y_A)^{X_B} \bmod 353$
$= (40)^{253} \bmod 353$
$= 160$.

Q. 12 Explain RSA Algorithm with two examples?

→ RSA scheme is block cipher in which the plaintext & ciphertext are integers between 0 & n-1 for same n.
2) Typical size of n is 1024 bits i.e. $n < 2$.
3) RSA Algorithm as shown below
a) Key Generation :-
• select p, q ..... p & q both are the prime no $p \neq q$.
• calculate $n = p \times q$
• calculate $\phi(n) = (p-1)(q-1)$
• select ~~image~~ integer ..... $\gcd(\phi(n), e) = 1$ & $1 < e < \phi(n)$
• select d :- $d = e^{-1} \bmod \phi(n)$
• public key, $PU = \{e, n\}$

• private key , PR = {d, n}

b) Encryption :-

• plaintext : m < n < p = " "
• Ciphertext : c

c) Decryption :-

• Ciphertext c
• plaintext : M = $C^d \bmod n$
• Note 1 : (n) → Euler's totient function
• Note 2 : Relationship between c & d is
$ed \pmod{(n)} = 1$
$ed = 1 \bmod (n)$
$d = e^{-1} \bmod (n)$.

e.g. Key Generation :-

1. Select 2 prime No → p = 17 & q = 11
2. Calculate $n = p \times q = 17 \times 11 = 187$
3. Calculate = 16 x 10 = 160 select 'e' such that e is relatively prime to (n) = 160.
4. Determine d such that :
$de = 1 \bmod (n) \Rightarrow d \times 7 = 1 \bmod 160 = 161$
$d = e^{-1} \bmod (n) \Rightarrow [161]/7 = \text{div. (d) } 23$ & remainder (mod) = 1, d = 23.
1. Then the resulting key are public key :

PU = {7, 187}
PR = {23, 187}
let M = 88 for encryptim
$C = 88^7 \mod (187)$
$88 \mod 187 = 88.$
$88^2 \mod 187 = 7744 \mod 187 = 77$
$88^2 \mod 187 = 59969536 \mod 187$
$= 132$

$88^7 \mod 187$
$= (88^4 \mod 187) \times (88^2 \mod 187) \times (88 \mod 187) \mod 187$
$= (132 \times 77 \times 88) \mod 187$
$= 894432 \mod 187.$
$= 11.$

for decryptim
$M = C^d \mod 187$
$= 11^{23} \mod 187$
$= 11^1 \mod 187 = 11$
$= 11^2 \mod 187 = 121$
$= 11^4 \mod 187 = 14641/187$
$= 55$
$= 11^8 \mod 187$
$= 33$
$= (11^8 \mod 187 \times 11^8 \mod 187 \times 11^1 \mod 187) \mod 187.$
$= (33 \times 33 \times 55 \times 81 \times 11) \mod 187.$
$= 79720245 \mod 187.$
$= 88.$

Example 2:-

suppose two prime number are.

$p = 3$ & $q = 11$

$\Rightarrow$

$n = p * q \Rightarrow 3 * 11 = 33$ &

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

$= 2 \times 10$

$= 20$

choose public key e, such that e is co-prime to $\phi(n)$ & $1 < e < \phi(n)$. Coprime means it should be not multiply by factors of $\phi(n)$ & also not divide by $\phi(n)$.

factors of $\phi(n)$ are, $20 = 5 \times 4$

$= 5 \times 2 \times 2$ so

e should not multiply by 5 & 2 & not divide by 20 so primes are 3, 7, 11, 17, 19, ... as 3 & 11 are taken choose e as 7.

Therefore, $e = 7$.

Calculate private key : d

$d = (K * \phi(n) + 1) / e$ for some integer k.

for $K = 1$, 21 is divisible by 7 & the value of d is 3.

$(n = 33$ & $e = 7) \Rightarrow$ public key & $(d = 3, n = 33) \rightarrow$ private key.

If $m = 2$; the encryption of $m = 2$ is :-

$c = 2^7 \bmod 33 = 29$.

The decryption of $c = 29$ is : $M = 29^3 \bmod 33$

$= 2$

Page No:

Q.3 Encrypt "Academic committee will meet today" using play fair cipher with keyword.
"ROYAL ENFIELD"

→

Key = "ROYAL ENFIELD"

Plaintext = "Academic committee will meet today"

5×5 matrix

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

Plaintext Cipher :- AC ad em ic co mx mi
te ew il lm ex et
to da yx

Cipherkey :- OH LI BU NH PN SU SE MD EU DA
RI IU DM PL IL AW

Q. 5 Use Hill Cipher substitution technique Find plain text by decryption cipher text "XVWG" with key matrix $\begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix}$

→ The key matrix consists of size 2×2 where 2 is number of row in the plaintext. Hence we divide the given plaintext in matrix of a size 1×2.

$$C = \begin{bmatrix} X \\ V \end{bmatrix} \begin{bmatrix} W \\ G \end{bmatrix} = \begin{bmatrix} 23 \\ 21 \end{bmatrix} \begin{bmatrix} 22 \\ 06 \end{bmatrix}$$

$$K = \begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix}$$

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

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

$$d = \begin{vmatrix} 3 & 7 \\ 5 & 12 \end{vmatrix} = 36 - 35 = 1$$

$$K = \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

$$= \begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix} = \begin{bmatrix} 12 & -7 \\ -5 & 3 \end{bmatrix}$$

$$= 27 \begin{bmatrix} 12 & -7 \\ -5 & 3 \end{bmatrix} = 27 \begin{bmatrix} 12 & +7+26 \\ -5+26 & 3 \end{bmatrix}$$

$$= 27 \begin{bmatrix} 12 & 19 \\ 21 & 81 \end{bmatrix} \text{ mod } 26.$$

$$K^{-1} = \begin{bmatrix} 324 & 513 \\ 567 & 81 \end{bmatrix} \text{ mod } 26.$$

$$K^{-1} = \begin{bmatrix} 20 & 19 \\ 21 & 3 \end{bmatrix}$$

$$P = \begin{bmatrix} 20 & 19 \\ 21 & 3 \end{bmatrix} \begin{bmatrix} 23 \\ 21 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 859 \\ 549 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 1 \\ 0 \end{bmatrix} - \begin{bmatrix} B \\ A \end{bmatrix}$$

$$P = \begin{bmatrix} 20 & 19 \\ 21 & 3 \end{bmatrix} \begin{bmatrix} 22 \\ 06 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 554 \\ 480 \end{bmatrix} \text{ mod } 26.$$

$$= \begin{bmatrix} 8 \\ 12 \end{bmatrix} = \begin{bmatrix} I \\ M \end{bmatrix}$$

$\therefore$ BAIM

Q.4 Use Hill Cipher to encrypt the text "SHORT" The key to be used is "HILL"

→ Plain text = "SHORT"

Key = "HILL"

$$key = \begin{bmatrix} H & I \\ L & L \end{bmatrix} \begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix}$$

vector

$$\begin{bmatrix} S \\ H \end{bmatrix} = \begin{bmatrix} 18 \\ 7 \end{bmatrix}, \quad \begin{bmatrix} O \\ R \end{bmatrix} = \begin{bmatrix} 14 \\ 17 \end{bmatrix}, \quad \begin{bmatrix} T \\ X \end{bmatrix} = \begin{bmatrix} 19 \\ 23 \end{bmatrix}$$

$\because C = KP \bmod 26$

$$\begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix} \begin{bmatrix} 18 \\ 7 \end{bmatrix} = \begin{bmatrix} 126 + 56 \\ 198 + 77 \end{bmatrix} = \begin{bmatrix} 182 \\ 275 \end{bmatrix} \bmod 26$$

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

2> $$\begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix} \begin{bmatrix} 14 \\ 17 \end{bmatrix}$$

$$= \begin{bmatrix} 98 + 136 \\ 154 + 187 \end{bmatrix} = \begin{bmatrix} 234 \\ 341 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 9 \\ 3 \end{bmatrix} = \begin{bmatrix} I \\ D \end{bmatrix}$$

Page No:

Experiment No. Date :

3) $\begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix} \begin{bmatrix} 19 \\ 23 \end{bmatrix}$

$\begin{bmatrix} 133 + 184 \\ 209 + 253 \end{bmatrix} = \begin{bmatrix} 317 \\ 462 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 5 \\ 20 \end{bmatrix} = \begin{bmatrix} F \\ U \end{bmatrix}$

"SHORT" = "APIDFU