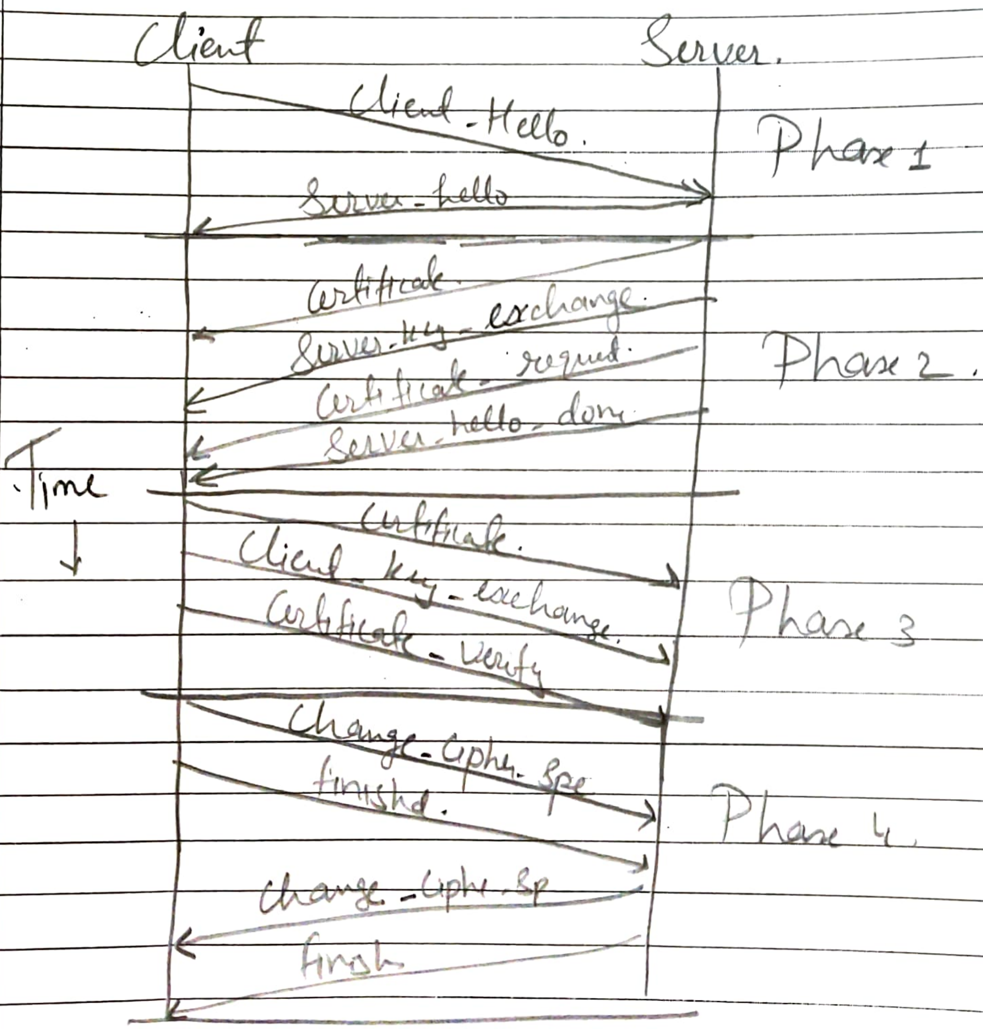
Name of the Subject: E-COMMERCE & E-SECURITY Subject Code: IT-718

Seat No: IT076 Student ID: 18ITUBN116 Branch/Sem: IT-VII

Q2 Attempt the following

a SSL Handshake Protocal.

– Allows Serves & Client To authenticate each other, to negotiate encryption & MAC algorithm & to negotiate Cryptographic key to be used.



Name of the Subject: E-COMMERCE & E-SECURITY Subject Code: IT-718

Seat No: IT076 Student ID: 18ITUBN116 Branch/Sem: IT-VII

- There are multiple steps that takes place in a quick during an SSL handshake

- Client Hello.
  - The Client initiate by Sending a "Hello" message to the Server.

- Server hello
  - In respons to the client, the Server sends a "hello" back, which include SSL Certificate & Selected cipher Suite. & a random String.

- Authentication
  - The Client after receiving the response goes on to verify the identity of the server.

- Paramaster secret
  - After authentication of the Certification & establishing the identity of the Server, the client send a random String of bytes, Only this time, it is encrypted with public key.

- Premaster Secret decryption
  - The Server decryption the premaster secret using private key.

- Creation of Session Key.
  - Both Server & Client generate session key using the client random, server random & Secret.

- Client "finished" message
  - The Client send "finished" message with Session key.

- Server "finished" message.
- Secure Connection established.

· This Conclude the handshake produce & the session Continues.

Q2 b Modular Exponentiation Algorithm

a^b mod n.

```
C=0 ; d=1.
for i=k down to 0
    do C=2×c
       d=(d×d)mod n
          if bi=1   // True.
             then  C=C+1
                   d=(d×a) mod n.
return d.
```

given $a = 88$ $b = 7$ $n = 187$

Compute 88^7 mod 187

Compute b = 7 = 1 1 1

i	2	1	0
b_i	1	1	1
c	1	3	7
d	88	44	$\boxed{11}$

So, the value of d = 11.

if $b_i = 0$
then perfor $(d \times d) \bmod n$.

if $b_i = 1$
then perfor $d = d \times d \bmod n$
$d = (d \times a) \bmod n$.

$$\boxed{88^7 \bmod 187 = 11}$$

$\boxed{Q2}$ $\boxed{C}$ Diffie-Hellman.

$q = 19$ $a = 7$
$X_A = 8$ $X_B = 10$

① A's Key generation Y_A

$Y_A = 7^8 \bmod 19$ $\therefore Y_A = a^{X_A} \bmod q$.
$= 11$.

② B's key generation Y_B

$Y_B = a^{X_B} \bmod q$.
$= 7^{10} \bmod 19$
$= 7$

③ Shared Secret key of both A & B

$K_{AB} = Y_B^{X_A} \bmod q$

$K_{AB} = Y_A^{X_B} \bmod q$.

Name of the Subject: ECES Subject Code: IT-718

Seat No: IT076 Student ID: 18ITUBN116 Branch/Sem: IT-VII

For A

$K_{AB} = 7^8 \bmod 19$
$= 11$

For B

$K_{AB} = 11^{10} \bmod 19$
$= 11$

So, Shared key are $\boxed{11}$

Using Modular Exp. Solving Calculatio.

① 7^8 mod 19.
Compute. 8 = 1000

i	3	2	1	0
bi	1	0	0	0
c	1	2	4	8
d.	7	11	7	$\boxed{11}$

② 11^{10} mod 19.
Compute 10 = 1010

i	3	2	1	0
bi	1	0	1	0
c	1	2	5	10
d	11	7	7	$\boxed{11}$

Name of the Subject: ECES Subject Code: IT-718

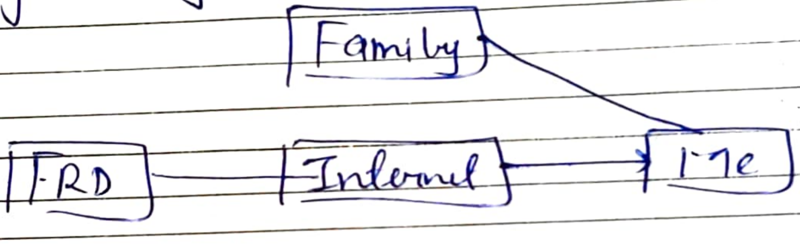
Seat No: IT076 Student ID: 18ITUBN116 Branch/Sem: IT-VII

Q1 e.

Active Attacks

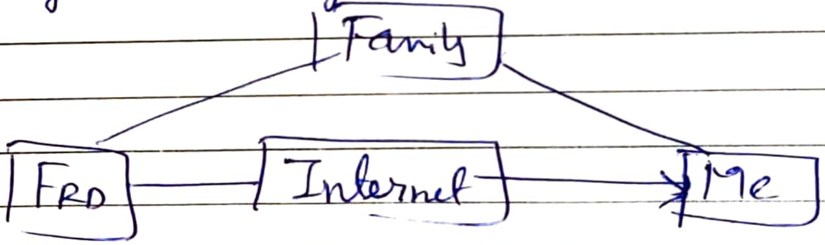
1. Masquerade

– Take place when one enity pretends to be the different enity. Attack involves one of the form of active attack



2. Modification of message.

– Some portion of message is altred or that message is delayed.



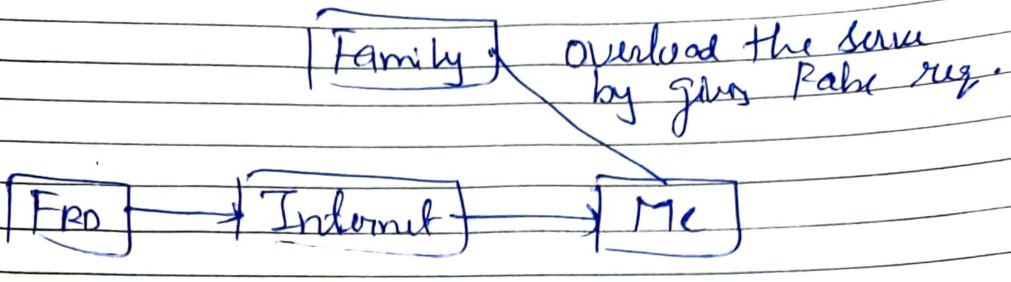
3. Repudiation.

– Done by either sender or Receiver. The sender or receiver can deny later that has send or receive message.

4. Replay.

– Passive capture of a message & its subsequent transmission to produce effect.

Date: 22/11/2021 Signature of Student:



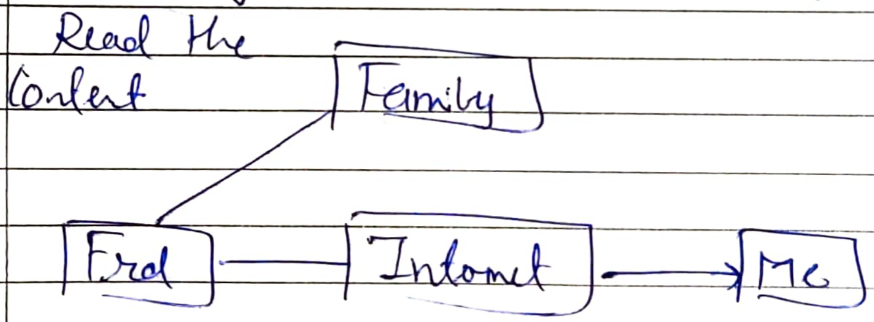
5. Denial of Servis

- It prevent normal use of communication faulits. This attack may have a specific Target.

Passive Attack.

1 The release of message Content

- Telephonic Conversation, an electrone mail message or transferred file may contain information.



2. Traffic analysis

- The opponent could determn the location of Comm. & identity of communication host. & could observe the freq. & length of message being exchanged.

Q1 C

Block Cipher Modes of Operatio.

- Block Cipher is an encryption algorithm that takes a fixed size of input say b bits & produces a ciphertext of b bits again.

- For further different application. there are serval modes of operatio

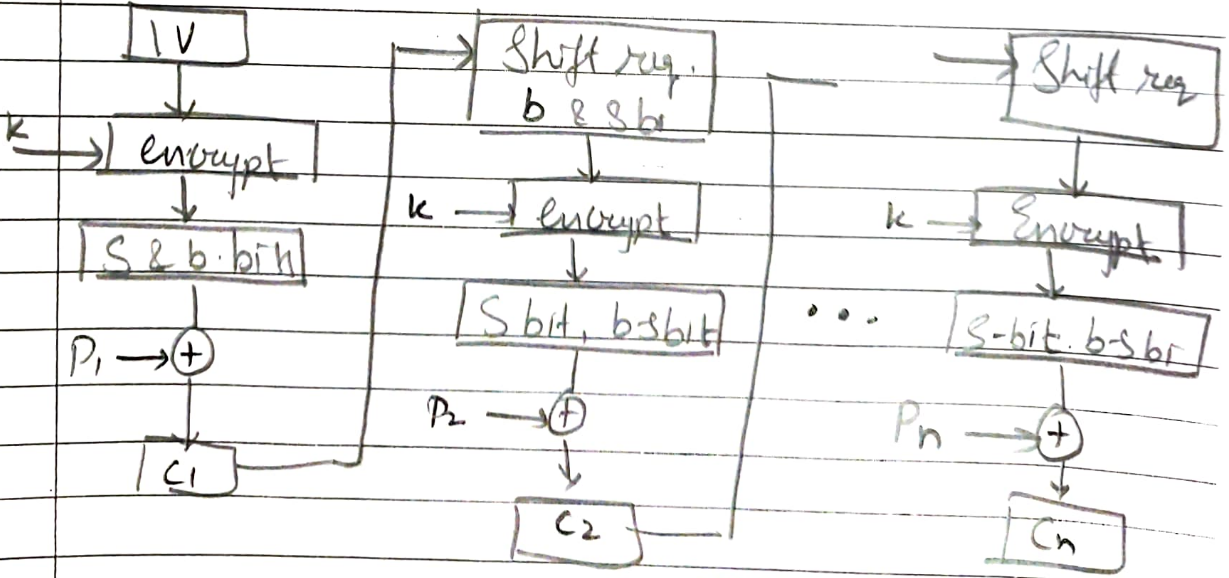
① ECB ② CBC ③ CFB ④ OFB

① CFB – Cipher Feedback Mode.

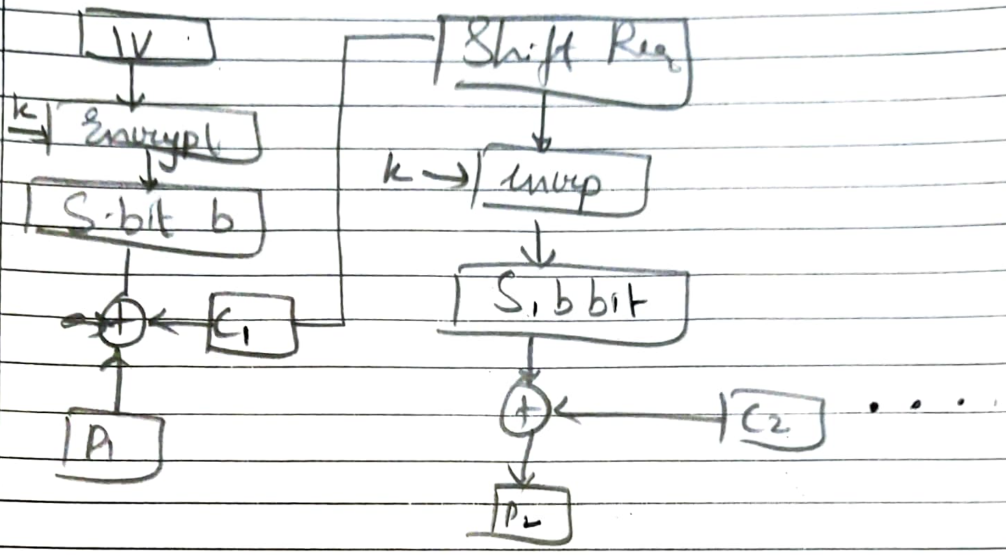
- The Cipher is given as Feedback to the block of encryption with some new specificatio.

- An Initial Vector IV is used for 1st encryption & output bits divides as b-s bits.

Encryption.



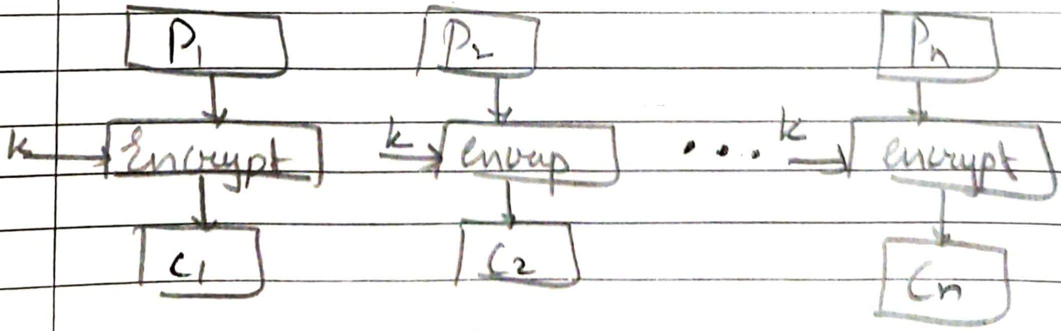
Decryption.



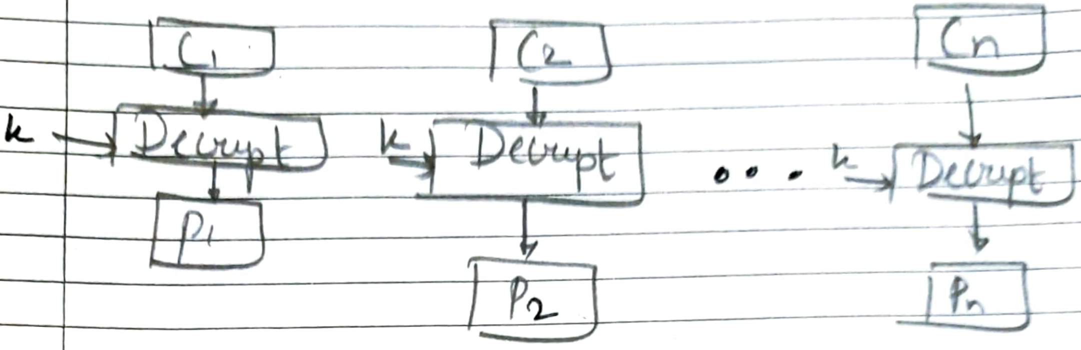
② Electrone Code Block (ECB).

- It is easy because of direct encryption of each block of input plainText & output S is in form of block of encryption Ciphertext.

Encryption.



Decryption.



Q1 d

Attacks on RSA

① Plain Text Attack
② Chosen Cipher Attack
③ Factorization Attack.

① Plain Text Attack

– It is classified into 3 catagories.

(i) Short Message Attack

– The assumption is that the attacker know some block of plain Text message.

– If he/she knows they it could be well try to encrypt the block of plain Text.

(ii) Cycling Attack

– An attacker assums that the ciphertext is formed using some permutation operations.

(iii) Unconcealed Message Attack

– It is found that some encrypted cipher text is the same as the plain text.

② Choosean Cipher Text

– The attacker can find out the plain Text from cipher text using extendded euclidean algorithm.

③ Factorization Attack

– The attacker impersonates the key owners & with the help of stolen data, they decrypt data.

– This attack occurs on RSA library which generates RSA key.

– Attackers can have the private key of n no. of Security token, etc.