Assignment-I

1) What is Cryptography? What are the terms & terminologies in Cryptograph. Explain the types of attacks.

A) Cryptography:

Cryptography is the practice & study of experience for securing communication & data from third parties or adversaries. It involves converting plain text into an unreadable format using encryption analysis, ensuring that only authorized parties can access the original information through decryption.

Terms & Terminologies in Cryptography:

1. Plain Text: The original, readable message or data before encryption.
2. Cipher Text: The encrypted, unreadable version of plain Text.
3. Encryption: The process of converting ~~Cipher~~ cipher text into ~~Plain~~ Text using a key Plain
4. Decryption: The Process of converting Cipher text into Plain Text using a key
5. Key: A piece of information used in ecryption & decryption algorithms to lock or unlock the data.
6. Symmetric key Cryptography:- uses the same key for both encryption & decryption

7. Asymmetric key Cryptography: Uses a Pair of keys Public key & Private key.

8. Hash function: A one way function that Converts data into a fixed size hash value, used for data integrity.

9. Digital signature: An encrypted hash value used to verify the authenticity of a message or document

10. Certificate Authority: An entity that Passes digital Certificates to validate ownership of Public keys.

Types of attacks in Cryptography:

1. Cipher Text - only Attack – The attackers only has access to the Cipher text & attempt to deduce the plaintext or key.
2. Known plaintext Attack :- The attacker has access to both plaintexts & its cipher text & tries to find the key.
3. chosen - Plaintext Attack: The attacker can encrypt chosen Plaintexts to gather information about the key.
4. Chosen - cipher Text: The attacker can decrypt Chosen cipher texts to gain information about the key.
5. Brute force Attack: Trying all Possible Keys untill the Correct one is found.

6. Man in the middle Attack: An attacker intercepts Communication b/w 2 Parties to steal or alternate information.

7. Side Channel Attack: Exploits physical characteristics of the encryption device

2. Explain RC4 & RC5 algorithm.

RC4 -Algorithm:

RC4 is a Stream Cipher and Variable length Key algorithm. This algorithm encrypts one byte at a time. A key input is a pseudorandom bit generator that produces a stream 8-bit number that is unpredictable without knowledge of the input key. The output of the generator is called key-stream, and is Combined one byte at a time with the plaintext stream Cipher Using X-OR operation.

Key generation Algorithm:

A Variable-length key from 1 to 256 bytes is used to initialize a 256-byte state vector S. with elements S[0] to S[255]. for encryption and decryption, a byte K is generated from S by selecting one of the 255 entries in a Systematic fashion, then the entries in S are permuted again.

Pseudo Random Generation Algorithm:

Once the vector S is initialized, the input key will not be used. In this step, for each S[i] algorithm swap it with another byte in S according to a scheme dictated by the current

Configuration of S. After reaching S[255] the process continues, starting from S[0] again.

Intialization of S:

```
i, j = 0
while(true) {
    i = (i + 1) mod 256;
    j = (j + S[i]) mod 256;
    swap(S[i], S[j]);
    t = (S[i] + S[j]) mod 256;
    K = S[t];
}
```

Features of the RC4 Encryption Algorithm:

1. Symmetric key algorithm: RC4 is a symmetric key encryption algorithm, which means that the same key is used for encryption and decryption.
2. Stream Cipher algorithm: RC4 is a stream cipher algorithm, which means that it encrypts and decrypts data one byte at a time. It generates a key stream of pseudorandam bits that are XORed with the plaintext to produce the ciphertext.
3. Variable key size: RC4 supports variable key sizes, from 40 bits to 2048 bits, making it flexible for different security requirements.
4. Fast and efficient: RC4 is a fast and efficient encryption algorithm that is suitable for low-power devices and applications that require high-speed data transmission.

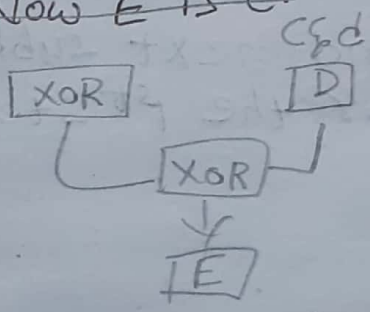
RC5 Encryption Algorithm:

RC5 is a symmetric key block encryption algorithm designed by Ron Rivest in 1994. It is notable for being simple, fast and consumes less memory.

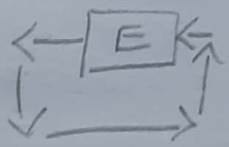
Details of Round:

step-I: The 1st step of each round C&D xored together to form the block called E.

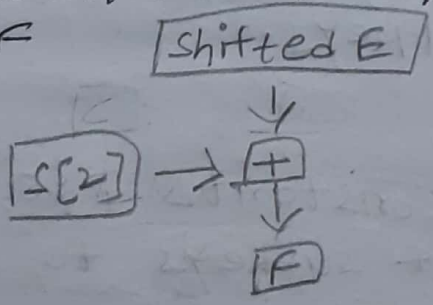
step-II: Now E is C.



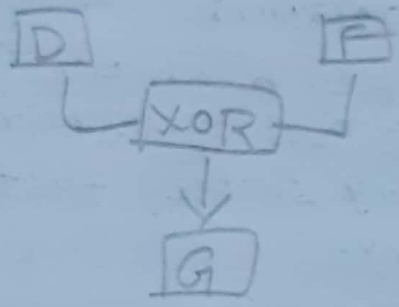
Step-II: Now E is circular left shifted by D positions



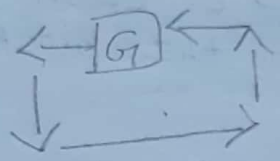
Step-III: In this step E is added to the next subkey which is S[2] for the 1st round and S[i] for any round where i starts with 1. The o/p of the process is Block F



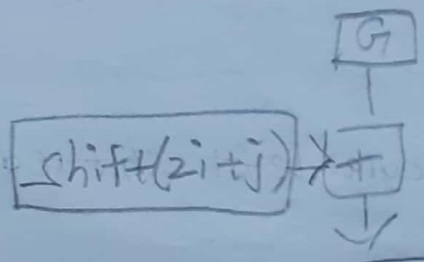
Step-IV: In this step similar to step-I here d and f are xored to produce G Block



step V: In this step similar to step-II G is shifted by F positions



step VI: Add G and next subkey which is s[3] for the 1st step s[2i+1]



step VII: In this step which to see all the rounds completed or not.

Subkey Creation:

step 1: subkeys are generated

step 2: subkeys which are generated in step 1 are mixed with the corresponding subportions of the original keys.

Subkey generation:

In this step 2 constants P&Q are used the array of subkeys to be generated is called as S.

3a. Explain AES Algorithm?

AES (Advanced encryption standards:
It is developed by the National Institute of standards and Technology in 2001. It is widely used today as it is much stronger than DES. AES is a highly trused encryption algorithm.

The main features of AES are
1. Symmetric & Parllel structure
2. Adapoted through modren processes like Paytm
3. suited to smart cars.

1 byte = Group of 8 bits
1 word = 4 bytes - i.e 32 bits
block size - 128

AES 4 types of Transformation functions:

1. Substitution Bytes:
In this step each byte is substituted by another byte. It is performed using a lookup table also called the S-box. The result of this step is 16 byte (4x4 matrix like before.

2. shift rows: The shifting is done to left rotate row of the plain text block i.e state matrix. by k bytes row '0' is rotated to '0' bytes row 1 is rotated to 1byte row 2 is rotated to 2bytes and row3 is rotated to 3 bytes. The shifted row transmission helps in diffusion of data.

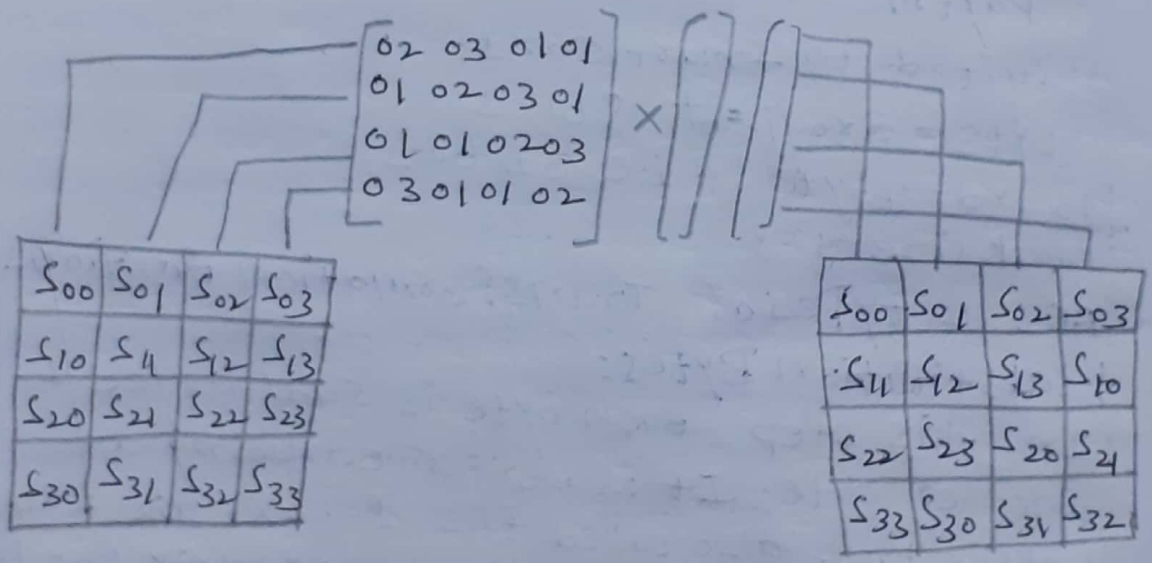
Original Array

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,0}$	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$
$S_{2,0}$	$S_{2,1}$	$S_{2,2}$	$S_{2,3}$
$S_{3,0}$	$S_{3,1}$	$S_{3,2}$	$S_{3,3}$

Modified Array

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,1}$	$S_{1,2}$	$S_{1,3}$	$S_{1,0}$
$S_{2,2}$	$S_{2,3}$	$S_{2,0}$	$S_{2,1}$
$S_{3,3}$	$S_{3,0}$	$S_{3,1}$	$S_{3,2}$

Mix Columns: Matrix Multiplication is used each column of the state array is multiplied with the constant matrix i.e 4 bytes or 4*1 matrix. The output is 4*1 matrix the o/p is 4*1 matrix of 4 bytes and stored in a o/p or state Matrix.



Add round key: It is also procedures one column at a time in this xor the state with the resultant o/p of previous step is xored with corresponding key block. After Performing these each round with 4 bytes using the round key. The resultant encrypted data is given block as o/p.

3b Explain RSA algorithm?

Rivest-Shamir-Adleman

- The RSA algorithm is the most popular and proves assymetric key cryptographic algorithm.
- The RSA algorithm is based on the mathematical fact that is entity to find and multiply large prime numbers together, but it is extremely difficult to factor their product.
- The private and public key in RSA are based on stery large prime numbers.
- The algorithm itself is quite simple. However the real challenge in the case of RSA, is the selection and generation of the public and private keys.
- The whole process of how the public and private keys are generated and using them how we can perform encryption and decryption in RSA is shown below.

1. Choose two large prime Numbers P and Q
2. Calculate $N = P \times Q$
3. Select the public key E such that it is not a factor of $(P-1)$ and $(Q-1)$
4. Select the private key D such that the following equation is true

$$(D \times E) \bmod (P-1) \times (Q-1) = 1$$

5. For encryption, calculate the cipher text CT from the plain text as follows

$$CT = PT^{E} \bmod N$$

6. Send CT as the cipher text to the reciver
7. For decryption, calculate the plain text PT from the cipher text CT as follows

$$PT = CT^{D} \bmod N$$

4a Explain about modes of operation in Block Cipher.

Block Cipher encrypt data in fixed size block since messages are often longer, modes of operation are used to securly process larger plain text. The common modes are

1. Eelectronic Codebook:

Each block is encrypted independently using the same key. It is easier of the direct encryption of each block of input plaintext and output is in the form of block of encrypted ciphertext.

2. Cipher Feedback Mode:

In this mode the cipher is given as feedback to the next block of encryption with some new specifications: first an initial vector IV is used for first encryption and output bits are divided as a set of s and b-s bits. The left-hand side s-bits are selected along with plaintext bits to which an XOR operation is applied. The given result is given as input to a shift register having b-s bits to lhs, s bits to rhs and the process continoues.

3. Output Feedback Mode:

The output feedback mode follows nearly the same process as the cipher feedback mode except that it sends the encrypted output as feedback instead of the actual cipher which is XOR output. In this output feedback mode, all bits of the block are sent instead of sending selected s bits. The output feedback mode of block cipher holds great resistance towards bit transmission errors.

4. Counter Mode:

The Counter Mode or CTR is a simple Counter based block cipher implementation. Every time a Counter initiated value is encrypted and given as input to XOR with plaintext which results in Ciphertext block.

4b. Explain about DES algorithm with neat diagram.

DES is a Symmetric key block cipher developed by IDM and adopted by NIST in 1977. It encrypts data in 64-bit blocks using a 56 bit key producing a 64 bit ciphertext block.

Steps in DES:

1. Initial Permutation (IP):

Rearrange the bits of ~~Permutation~~ of the plain text.

2. 16 Rounds of feistel structure:

Each round Consists of:

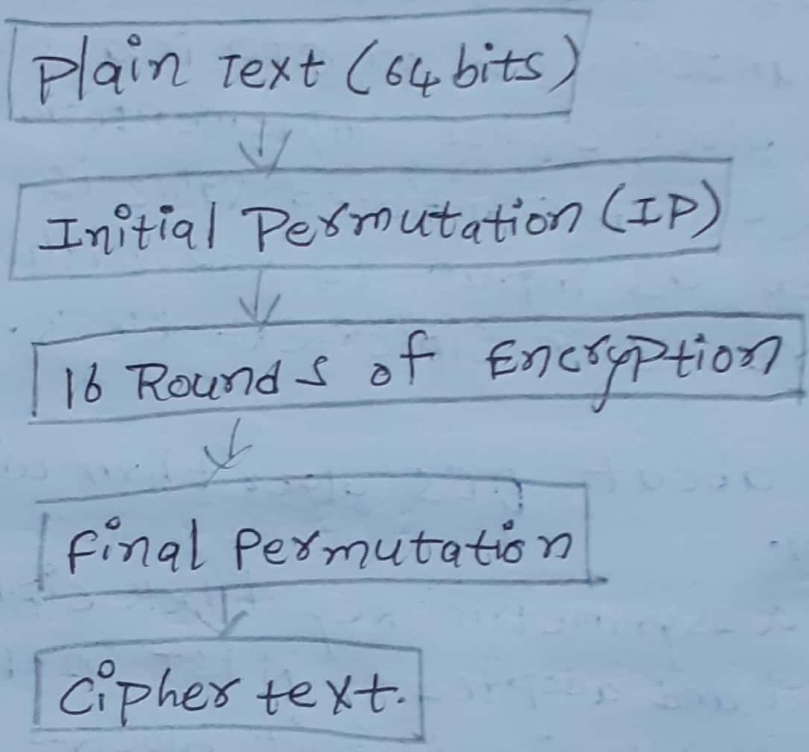
* Splitting data into left (L) & Right (R) halves
* Applying a key dependent function f(R, K)
* Swapping L and R at the end of each round

3. Final permutation:

The inverse of the initial permutation, producing the final ciphertext

Key generation:

* A 56-bit key is divided into two 28-bit halves
* left circular shifts and Compression Permutation Produce 16 subkeys for each round.



strength: simple & easy to implement

weakness: The 56 bit key size is now considered insecure to brute force attack.

5. Explain about Substitution & Transposition techniques in network security:

Substitution Techniques:

* In substitution ciphers, the letters of plaintext are replaced by other letters, numbers or symbols.
* The position of characters remains unchanged but their identity is altered.

Types of substitution Cipher:

1. Ceaser Cipher:

* Each letter is shifted by a fixed no of positions down the alphabet
* Ex: with a shift of 3, "HELLO" becomes "KHOOR"

2. Monoalphabetic cipher:

Each letter is replaced with another letter from a fixed random permutation of the alphabet.

3. Polyalphabetic Cipher:

Uses multiple ceaser ciphers with a key-word to shift letters by varing amounts

* Makes frequency analysis harder.

4. Play Fair Cipher:

Uses 5*5 matrix of letters to encrypt pairs of plaintext letters.

Ex: "Hello" becomes "IBBMO".

2. Transposition Techniques:

In transpose cipher, the plaintext characters remain the same but their positions are shuffled according to a specific pattern or key.

Types of Transpose Cipher:

1. Rail fence cipher:

The plain text is written diagonally over multiple lines & then read row by row

ex: "Hello" written over 2 rails

```
H   L   O
  E   L
```

Ciphertext: HLOEL

2. Columnar:

The Plain text is written into column of a fixed width & columns are rearranged based on a key.

Ex: PT: Computer science, Keyword: orange

O	R	A	N	G	E
c	o	m	p	u	t
e	r	s	c	i	e
n	c	e	x	x	x

A	E	G	N	O	R
m	t	U	P	C	O
s	e	i	C	e	r
e	x	x	x	n	C

~~CT: mtUPCOseicere xxxnc~~

CT: mseterxuix PCXcenorc

Double Transposition:

Applies transposition twice using two different keys for added security.

Ex: PT: KRISHNA RAJAN keyword: NICK

4	2	1	3
N	I	C	K
K	R	I	S
H	N	A	R
A	J	A	N

N	I	C	K
1	2	3	4
I	R	S	K
A	N	R	H
A	J	N	A

CT: IAARNJSRNKHA