Module-1

Data Security & Privacy

Bishal Chaudhary
1CR23AI019
Sec: 7A

1. (a) Define cryptography and Explain Symmetric Ciphermode?

Ans: Cryptography is the science and art of protecting information by transforming plaintext into ciphertext using an encryption algorithm & a key, so that the information cannot be understood by unauthorized persons. The cipher is converted back into plaintext using a decryption algorithm and a key.

A symmetric encryption scheme has five components:

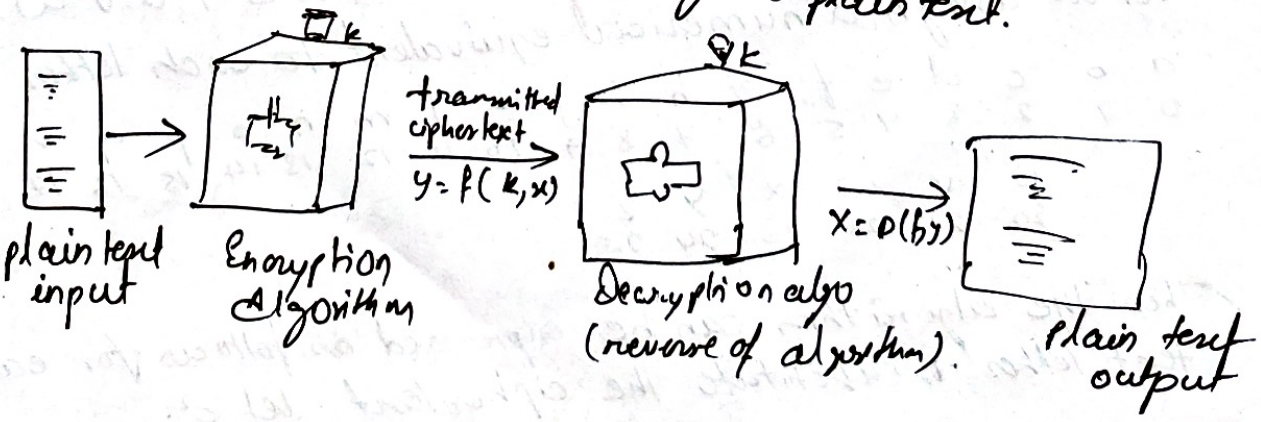
i) Plaintext: This is the original intelligible message or data that is fed into the algorithm as input.

ii) Encryption Algorithm: The encryption algorithm performs various substitutions and transformations on the plain text.

iii) Secret key: The secret key is also input to the encryption algorithm. the key is a value independent of the plaintext output depending on the specific key being used at the time. The exact substution and transformations performed by the algorithm depend on the key.

iv) Ciphertext: This the scrambled message produced as output depends on the plaintext and the secret key. for a given message, two different keys with produce 2 different ciphertexts, the ciphertext is an apparently random stream of data and as standard is unintelligible.

v) Decryption Algorithm: This is essentialy the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plain text.



There are two requirement for secure use of convention encryption:

i) We need a strong encryption algorithm at a minimum use would like the algorithm to be such that an opponent who knows the algorithm and has to one or more ciphertexts would be unable to decipher the ciphertext or figure out the key. This req is usually started in a stronger term. The opponent should be unable to decrypt ciphertext or discover the key even if he or she is in possession of a number of ciphertexts together with the plaintext that produced each ciphertext.

ii) Sender and receiver must have obtained copies after secret key in a secure fashion and must keep the key secure if someone can discover the key and knows the algorithm all communication using the key is readable.

1. (b) Explain Ceaser cipher with example?

Ans: The earlist known and the simplest use of a supstitution cipher was by julius ceasar. The ceasar cipher involves replacing each letter of the alphabet with the letter standing three places first ever down the alphabet. for Eg:

Noun: meet me after the toga party

Cipher: PHHW PH DIWHU WKH WRJD SDUWB

Note the alphabet is wrapped around the so that the letter following z is A we can define the transformation by listing all possibilities, as follows:

plain: 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

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

let us assign a numerical equivalent to each letter:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19

u	v	w	x	y	z
20	21	22	23	24	25

Then the algorithm can be expressed as follows for each plaintext letter P, substitute the ciphertext let C^2:

$$C = E(3, P) = (P + 3) \bmod 26$$

If it is known that a given ciphertext is a caesar cipher, than a brute-force cryptanalysis is easily performed: simply try all the 25 possible keys, the results of applying these strategy to the example ciphertext. In these case, the plaintext leaps occupying the third line.

These important characteristics of this problem enabled us to use a brute-force cryptanalysis.

1. The encryption and decryption algo are known.
2. There are only 25 keys to try.
3. The language of the plaintext is known and easily unrecognizable

1.© Explain Hill cipher & apply it to encrypt plaintext:
pay more money with key.

$$K = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$$

Ans:- The Hill cipher algo takes m succeive plaintext letters and substitutes for them m ciphertext letters the substitution is determined by n linear equations in which each character is assigned a numerical val (a=0, b=1.....z=25) for m=3, the system can be described as

$$C_1 = (k_{11}P_1 + k_{21}P_2 + k_{31}P_3) \bmod 26$$
$$C_2 = (k_{21}P_1 + k_{22}P_2 + k_{23}P_3) \bmod 26$$
$$C_3 = (k_{31}P_1 + k_{23}P_2 + k_{33}P_3) \bmod 26$$

This can be expressed in terms of row vectors and matrices:

$$(C_1\ C_2\ C_3) = (P_1\ P_2\ P_3) \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} \bmod 16$$

The first three letters of the plaintext are represented by the vector (15 0 24) then (15 0 24) (302 306 501) mod 26 = (17 17 11) = RRL continuing in this fashion the ciphertext for the entire plaintext is RRLMWBKASPOH

Decryption require using the inverse of the matrix K are can

compute $\det k = 23$ and therefore $(\det k)^{-1} \bmod 26 = 17$, we can compute the invery as:

$$k^{-1} = \begin{pmatrix} 4 & 9 & 11 \\ 15 & 17 & 6 \\ 24 & 6 & 17 \end{pmatrix}$$

$$= \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} = \begin{pmatrix} 443 & 442 & 442 \\ 856 & 495 & 480 \\ 494 & 52 & 305 \end{pmatrix} \bmod 26 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$C = E(k, P) = Pk \bmod 26$

$P = D(k, C) : Ck^{-1} \bmod 26 = PKk^{-1} = P$

$$\begin{pmatrix} 7 & 2 \\ 17 & 25 \end{pmatrix} = \begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} k \bmod 26$$

The inverse of x can be computed:

$$\begin{pmatrix} 7 & 8 \\ 4 & 4 \end{pmatrix}^{-1} = \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix}$$

$$k = \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix} \begin{pmatrix} 7 & 2 \\ 17 & 25 \end{pmatrix} = \begin{pmatrix} 549 & 600 \\ 398 & 577 \end{pmatrix} \bmod 26 = \begin{pmatrix} 3 & 2 \\ 8 & 5 \end{pmatrix}$$

This result is verified by testing the remaining plain text - ciphertext pair.

2. (A) Explain working of DES algorithm with example

Ans:- Data Encryption standard is a symmetric key block cipher. It takes a 64 bit plaintext and a 64-bit key. of which only 56 bits are used for encryption, the remaining 8 bits maybe parity bits.

DES Encryption process.

The DES encryption process consis of three main phases

i> Initial Permutation (IP): The 64-bit plain text first pares through an initial punctuation (IP), it rearrange the bits of the plaintext and produces the permuted input.

2. Sixteen Rounds: The permuted input is processed through 16 rounds. Each round involves permutation and substitution operations.

The 64-bits input is divided into 2 32bit have

L_0 = left half

R_0 = Right half

for each round: $L_i = R_{i-1}$

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

where K_i is 48 bit subkey generated for that round

generation of subkeys: The 56-bit effective key is first named through a puntuation called puncuted choice (PC.

3. Final puntutation:

After the 16th round, the left and right halves are swapped to form the preoutput.

The preoutput is then pased through the inverse initial puntuation (IP⁻¹)

The result is the 64-bit ciphertext.

E.g: plain text = 0 2 4 6 8 a c e e c a 8 6 4 2 0

key = 0 R 1 5 7 1 C 9 4 7 d 9 e 8 5 9

After applying the DES encryption process:

ciphertext: d a 0 2 c e 3 a 8 9 e c a 3 6

This plaintext → Desry DES Encryption → ciphertext

0 2 4 6 8 a c e e c a 8 6 4 2 0 → DES → d a 0 2 c e 3 a 8 9 e c

Des decryption uses the same algorithm as encryption, but the subkeys, are applied in reverse order

$K_{16}, K_{15}, \ldots\ldots K_2, K_1$

The initial and final permutation are correspondingly reversed. Thus, DES encrypts a 64-bit plaintext using a 56-bit effective key through initial permuted on 16 feistel rounds. Subkey generation, swapping and inverse initial permutation to produce the ciphertext.

2. (R) Explain play fair cipher & apply its rules for the following. E.g: key = MONARCHY plaintext = CRYPTOGRAPHY to get the cipher text.

Ans:- Playfair cipher is the best known multiple-letter encryption cipher is the playfair, which treats di-gram in the plain text as single units and translates there units into a ciphertext diggrams. The playfair algorithm is based on the use of a 5x5 matrix of letters constructed using a keyword. Construction of playfair matrix.

key = MONARCHY

The keyword is written first, removing duplicates letters. the remaining letters of the alphabet are then filled in alphabetic order

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 of playfair cipher

Rule 1: Repeated letters: If two repeated letters occurs in the same pair, they are seperated by a filler letter usually X.

Rule 2: Same row: If the 2 letters are in the same row, each is replaced by the letters immediately to it's right, the row is concidered circular

Rule 3: If the two letters are in the same column, each letter is replaced by the letter immediately.

Rule 4: Rectangle rule: If the two letters are in different row & col each letters is replaced by the letter in the same row but the column occupied by other letter.

plaintext = CRYPTOGRAPHY Divide the letters into pairs: CR | YP | TO | GR | AP | HY

Plaintext Pair	Rule applied	Cipher Pair
CR	Rectangle	DM
YP	"	HC
TO	"	PR
GR	"	KN
AP	"	OS
HY	"	YB

∴ CR → DM YP → HQ TO → PR, GR → KN, AP → VS HY → YB

final ciphertext ⇒ BM14QPRKNVSYD.

3(A) Draw the model of a symmetric Cryptosystem and Explain it.

Ans:- A symmetric cryptosystem is a encryption system in which the same secret key is used for both encryption & decryption. The key must be known only to the sender & receiver.

A symmetric cryptosystem consists of the following components

i) Plaintext: The original message data that is to be transmitted securely.

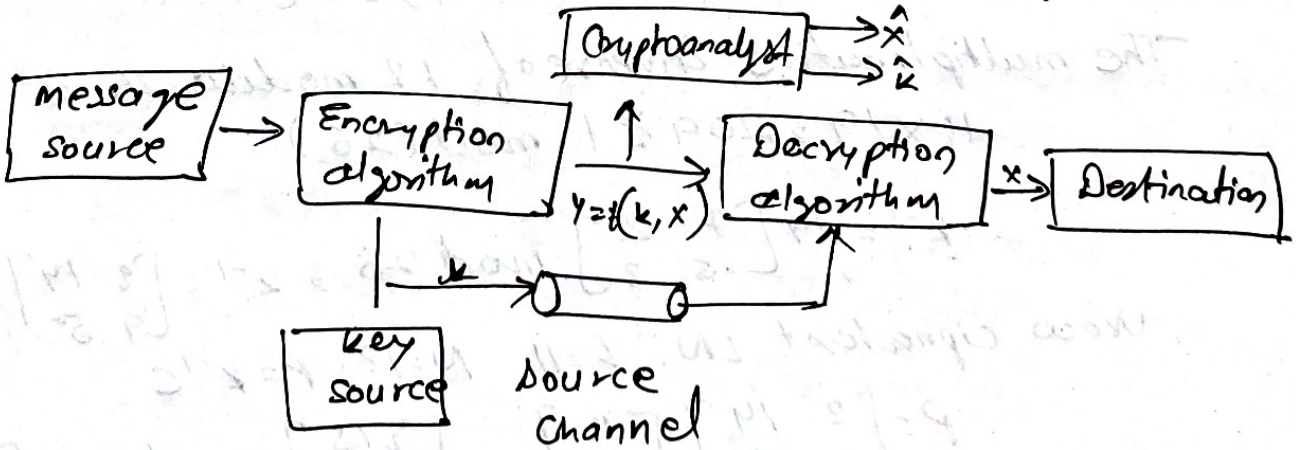
ii) Encryption Algorithm: It converts the plaintext into cipher text, using the secret key.

$$C = E(k, m)$$

iii) Secret key: A common secret key is shared between the sender receiver it must be kept confidential.

iv) Ciphertext: The encrypted and unreadable form the plaintext if it is transmitted through an insecure communition channel.

v) Decryption algorithm: The receiver uses the same secret key to convert ciphertext back into plaintext.



3.(B) Using Hill Cipher to Encipher and decipher the message "Hi" use the $\begin{pmatrix} 08 & 02 \\ 05 & 07 \end{pmatrix}$

Ex:- plaintext = Hi

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

Using the convention A=0, B=1 ... Z=25

1. Encryption : Convert Hi into numbers :

H=7, I=8

plaintext matrix $P = \begin{bmatrix} 7 \\ 8 \end{bmatrix}$

Encryption formula = $C = KP$ $C = \begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 7 \\ 8 \end{bmatrix} = \begin{bmatrix} 37 \\ 91 \end{bmatrix}$

A symmetric cryptosystem consists of the following compo

i) Plaintext : The original message or data that is to transmitted security.

ii) Encryption Algorithm : It converts the plaintext into ciphertext. Taking modulus 26 $C = \begin{bmatrix} 37 \bmod 26 \\ 91 \bmod 26 \end{bmatrix} = \begin{bmatrix} 11 \\ 13 \end{bmatrix}$

11 = L, 13, N

∴ Ciphertext = LN

2. Decryption : The inverse of the key matrix is required :

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

Determinant = $|K| = (3)(7) - 2(5) = 11$

The multiplicative inverse of 11 modulo 26 is 19,

$11 \times 19 = 209 \equiv 1 \pmod{26}$

$\therefore K^{-1} = 19 \begin{bmatrix} 7 & -2 \\ -5 & 3 \end{bmatrix} \bmod 26 = K^{-1} = \begin{bmatrix} 3 & 14 \\ 9 & 5 \end{bmatrix}$

Now ciphertext LN : L=11 N=13 $P = K^{-1}C$

$P = \begin{bmatrix} 3 & 14 \\ 9 & 15 \end{bmatrix} \begin{bmatrix} 11 \\ 13 \end{bmatrix} \quad \begin{bmatrix} 215 \\ 164 \end{bmatrix} \bmod 26 = \begin{bmatrix} 7 \\ 8 \end{bmatrix}$

7 = H 8 = I

Hi $\xrightarrow{\text{Hill cipher}}$ LN, LN $\xrightarrow{\text{Decryption}}$ HI

3. (C) List and Explain the block cipher design principle

Ans:- i) Number of Rounds: The block cipher should have a sufficient number of rounds, more rounds generally provide better security by making cryptoanalysis more difficult.

ii) Design of function f: The round function should provide strong confusion and diffusion so that the relationship between plaintext, ciphertext and key is difficult to determine.

iii) Key size: The cipher should use a large key size to prevent brute-force attacks a large key provides a larger key space and improves security.

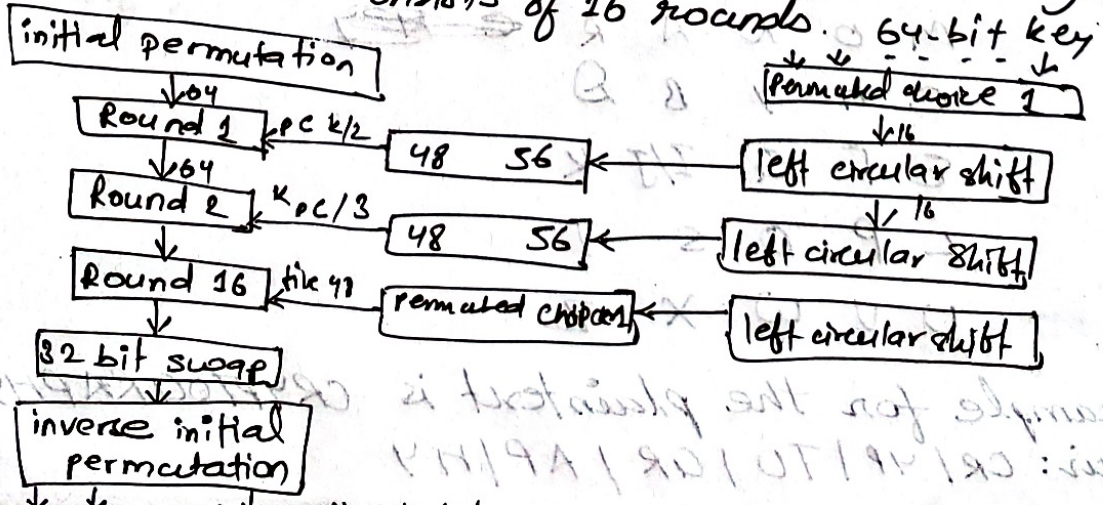
iv) Block size: The block size should be sufficiently large to prevent statistical analysis and reduce patterns in the ciphertext. Common block sizes includes 64 bits & 128 bits.

v) Fast Software Encryption/Decryption: The algorithm should be designed so that encryption & decryption can be performed efficiently in software, allowing practical use.

vi) Ease of Analysis: The design should be easy to analyze & should have no known weakness, its security depend mainly on the key, rather than the secrecy of the algorithm.

4. (A) Explain DES construction in detail with a neat diagram.

Ans:- DES is a symmetric block cipher that encrypts a 64-bit plaintext block using a 64-bit key. of which only 56 bits are effective. DES consists of 16 rounds.



Initial permutation: The 64-bit plaintext is first rearranged using the initial permutation (IP).

Splitting: The permuted block is divided into 32-bit halves Lo = 32 bits Ro = 32 bits

Sixteen Rounds: DES perform 16 feistal rounds. Each rounds uses a different 48-bit subkey.

key generators $L_i = R_{i-1}$ $R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$

final permutation

4(B) Explain playfair cipher and its rules.

Ans:- The playfair cipher is a multi-letter encryption technique that encrypts few plaintext letters at a time. It uses a 5x5 matrix.

constructed using a keyword the letters I and J are treated as one letter.

Rules of playfair Cipher:

i) Repeated letters: If the two letters in a pair are the same insert a filler letter x between them.

ii) Same row: Replace each letters by the letter immediately to its right; the row is circular.

iii) Same column: Replace each letter by the letter immediately below it, the column is circular

iv) Different row and column: Form a rectangle replace each letter with the letter in the same row of the other letter's column.

key = MONARCHY

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

Example for the plaintext is CRYPTOGRAPHY

Pair: CR | YP | TO | GR | AP | HY

9. (c) What is the one-time pad technique? List the advantage and disadvantages.

Ans:- One time pad is a symmetric encryption technique in which a random key is used only once to encrypt a message. The key must be as long as the plaintext msg.

Working:

i) The plaintext is converted into numerical / binary key.

ii) A random key of the same length as the patient is generated.

iii) The plaintext & key are combined using XOR operation.

iv) The result is ciphertext

v) At the receiver, the same key is used with XOR to discover the plaintext.

Advantage:

i) Provides perfect secrecy when the key is truly rando.

ii) Simple encryption & decryption using XOR.

iii) Resistant to brute-force and cryptoanalysis when OTP requirements are satisfied.

Disadvantages:

i) The key must be as long as the message.

ii) Secure key distribution is difficult.

iii) The key must be truly random.

iv) The key must never be reused.