VANDIT
BHALLA
1/19/FET/BCS/126

Assignment 1 - NSM

Date
DELTA Pg No.

Q1 Discuss the concept of Play fair Cipher. What is the output of plaintext "Hello"? If the key used is "Monarchy" to encode it.

Ans **Play Fair Cipher** => (1) Play Fair Cipher is an encryption algorithm or technique to encrypt or encode a message. It is the most popular symmetric encryption technique that falls under the substitution cipher.

(2) It is the same as traditional cipher, the only difference is that it encrypts a digraph (a pair of two letters) instead of a single letter.

Rules of Play Fair Cipher:

1. Create digraphs / digrams (a pair of 2 letters)
2. If repeating letters then add filler letters.
3. If letters are in same column move down, if last then wrap around.
4. If letters are in same row move right, if last then wrap around.
5. If not same row or same column then make a rectangle with the 2 letters as vertices and swap them with the last letter in their row.

Plain Text: HELLO , **Keyword:** MONARCHY

(5x5 matrix)

Digraphs: HE LX LO

(repeating letters so added filler letter)

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

HE	LX	LO
CF	SU	PM

∴ encrypted text ⇒ **CFSUPM**

Q2 Differentiate b/w Stream Cipher and Block Cipher? Explain the encryption and decryption of ECB mode.

Ans

Block Cipher	Stream Cipher
① Block cipher converts the plain text into cipher text by taking plain text's block at a time.	① Stream Cipher converts the plain text into cipher text by taking 1 byte of plain text at a time.
② Block text uses either 64 bits or more than 64 bits.	② Stream Cipher uses 8 bits.
③ The complexity of block cipher is simple.	③ Stream Cipher is more complex
④ Block Cipher uses confusion as well as diffusion.	④ Stream cipher uses only confusion
⑤ The algorithm modes which are used in block cipher are ECB (Electronic Code Book) and CBC (Cipher Block Chaining).	⑤ The algorithm modes which are used in stream cipher are CFB (Cipher Feedback) and OFB (output Feedback)

Date
DELTA Pg No.

Electronic Code Book (ECB) ⇒ ECB is the easiest block cipher mode of functioning. It is easier because of direct encryption of each block of input plaintext and output is in the foorm of blocks of encryted ciphertext. Generally if a message is longer than 'b' bits in size it can be broken down into a bunch of blocks and the procedure is repeated.

Q3 Define Authentication and explain why it is required. Explain with the help of suitable example.

Ans Authentication ⇒ (1) Authentication is the process of verifying the identity of a user or information. User authentication is the process of verifying the identity of a user when that user logs in to a computer system.

(2) Authentication enables organizations to keep their networks secure by permitting only authenticated users or processes to gain access to their protected resources. This may include computer systems, networks, databases, websites and other network based applications or services.

(3) Its main purpose is security. There are different types of authentication systems like :-

Date
DELTA Pg No.

1) Single Factor Authentication
(Username + Password)
2) Two Factor Authentication
(OTP, mail, etc)
3) Multi Factor Authentication
(Biometrics, facial recognition, Signature (voice etc)

Q4 Differentiate b/w Substitution Cipher and Transposition Cipher techniques with example.

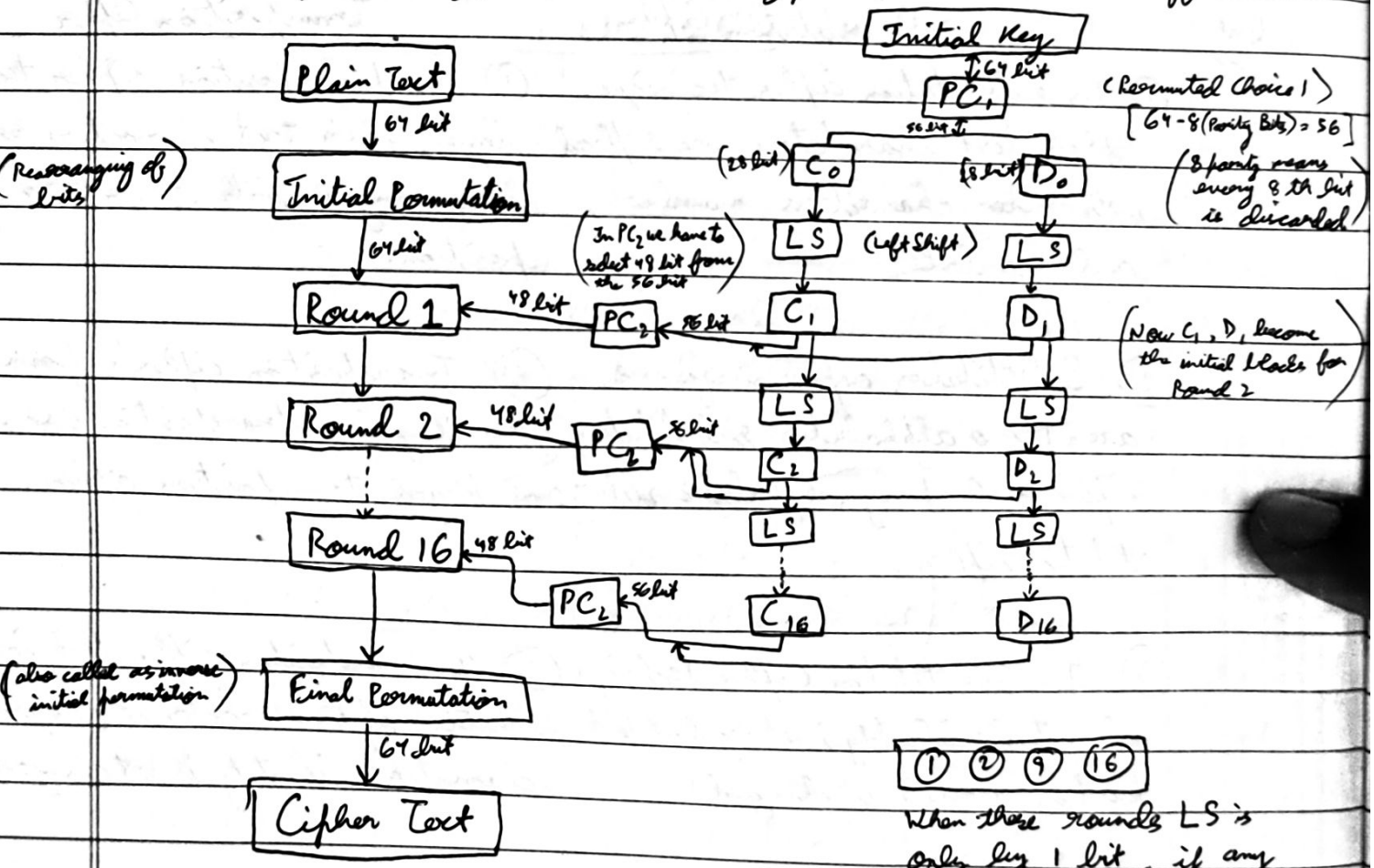
Ans

Substitution Cipher	Transposition Cipher
(1) In substitution cipher technique, plain text characters are replaced with other characters, numbers, and symbols	(1) In transposition cipher technique, plain text characters are rearranged with respect to the position.
(2) Substitution cipher's forms are Mono alphabetic substitution ciphers and poly alphabetic substitution cipher.	(2) Transposition cipher's forms are Key less transposition cipher and Keyed transposition cipher.
(3) In Substitution Cipher technique character's identity is changed while its position remains unchanged.	(3) In Transposition cipher technique the position of the character is changed but character's identity is not changed.
(4) In this the letter with low frequency can detect plain text.	(4) The keys which are nearer to correct key can disclose plain text.
(5) eg Ceasar Cipher.	(5) eg. Rail Fence Ciphers.

Q.5 Explain the different steps involved in the encryption and decryption process of DES ?

Ans (i) Data Encryption Standard (DES) has been found vulnerable to very powerful attacks and therefore, the popularity of DES is on decline.

(ii) DES is a block cipher and encrypts data in blocks of size 64 bits, which means 64 bits of plain text go as the input to the DES, which then produces 64 bits of cipher text. The same algorithm and key are used for encryption and decryption with minor differences.



(1) (2) (9) (16)

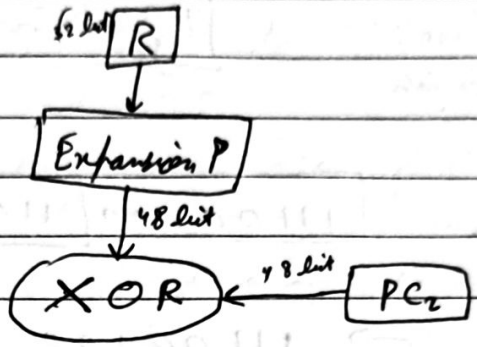
When these rounds LS is only by 1 bit, if any other round then LS is by 2 bit

[LS → LCS (Left Circular Shift)]

Date
DELTA Pg No.

Now we understand what goes on in the Round Functions

(We simply divide the 64 bit plain text in 2 halves randomly)



(In expansion P or function we are adding 16 bits at random to make 32 bits to 48 bits)