	WANDIT BHALLA 1/19/FET/BCS/126 Assignment 1 - NSM DELTA PONO DELTA PONO
	1/19/ PET/ Dent 1 - NS/11
(3)	Discuss the concept of Play fair Ciffren. What is the output of
	Discuss the concept of Play fair Cifhen. What is the output of flaintext "Hello"? If the key used is "Monarchy" to make it
Ang	Clay Fair Cifler = Play Fair Cipher is an encouption algorithm
	on technique to encoupt our encode a
	message. It is the most popular symmetric
	encouption technique Stat that falls under
	the substitution either
-	1) It is the same as toroditional ciffren, the
	only difference is that it encoughts a
	digraph (a pair of two letters) instead
	of a single letter.
	Rules of Play Fair Cipher :  Create digraphs/ digrams (a fair of 2 letters)
-	O Create digraphs/ digrams (a fair of 2 letters)
	D If expesting letters then add filler letters.
	D If seefesting letters them add filler letters.  3 If letters are in same column more down,
	My less from way around.
	My see from way around.
	If letters are in some now more night,
	If letters are in some now more right, if last then weaf around.
	If letters are in some now more right, if last then weaf around.
	If letters are in some now more right, if last then weaf around.
	If letters are in some now more right,  if last then wraf around.  The not same now or same columns then make a rectangle with the 2 letters as vortices and  swaf them with the last letter in their now.
	If letters are in some now more right,  if last then wraf around.  The not same now or same columns then make a rectangle with the 2 letters as vortices and  swaf them with the last letter in their now.
	If letters are in some now more right,  if last then wraf around.  The not same now or same columns then make a rectangle with the 2 letters as vortices and  swaf them with the last letter in their now.
	If letter are in some now more night,  if last the wraf around.  The not same now are same columns than make a rectangle with the letters as vortices and swaf than with the last letter in their now.  Plain Text: MELLO, Keyword: MONARCHY
	If letters are in some now more night,  if last then wraf around.  The not same now or same columns then make a rectangle with the releters as vortices and swaf them with the last letter in their now.  Plain Text: HELLO, Keyword: MONARCHY  (5×5)  Digrafes: HELX LO MONARCHY
	If letters are in some now more sight,  if last then wraf around.  (3) If not some now or some columns then make a rectangle with the r letters as vortices and swaf them with the last letter in their now.  Plain Text: MELLO, Keyword: MONARCHY  (5×5)  Digrafes: HE LX LO MONARCHY  (5×5)  Orefeating letters so alled flow CHY BD
	If letters are in same evour mone right,  if last then waf around.  (3) If not some again our same columna then mole a rectangle with the 2 letters as vortices and swaf them with the last letter in their now.  Plain Text: HELLO, Keyword: MONARCHY  (5×5)  Digrafts: HELX LO MONARCHY  (5×5)  Letter of The K
	If letters are in some now more sight,  if last then wraf around.  (3) If not some now or some columns then make a rectangle with the r letters as vortices and swaf them with the last letter in their now.  Plain Text: MELLO, Keyword: MONARCHY  (5×5)  Digrafes: HE LX LO MONARCHY  (5×5)  Orefeating letters so alled flow CHY BD

DELTA Pg No.

		DELTA Pg No.
	HE LX LO CF SU PM	
	CF SU PM	
255		
	no encounted tout => [	CFSUPM
	4,4,11,24,6,24	
0,2	Differentiate lofu Steream	Cipher and Block Cephen?
11	Explain the encouption	and decryption of ECB mode.
1. 1	the second of the second of the second	
Any	Block Ciphen	Stoream Ciphen
1976	1 Block That down cipher converts	Storesm Cifher commerts the
	the plain text into eigher text	flain text into cipher text ley
- Committee	ly taking plain text's black at a time.	taking I light of flain text at a
	of the first of the All of	
	1 Block text uses either 64	D Stoream Ciphon was 8 bits.
1-4	lite on more than 64 lite.	la de la companya de
10		
The second	(3) The complexity of block	(3) & Stoream Cifhan is more confla
N. 1, N.	3) The complexity of block cipher is simple.	
	March had only a Longly	Co Ctara illa una ante combina
	(9) Block Cipher uses confusion	(4) Stoream cipher uses only confusion
4	as well as diffusion.	
. 32.	(3) The algorithm makes which were	(5) The algorithm mode which are
	used in block either are	used in storom either are CFB
	ECB (Electoronic Code Book) and	(Ciphen Feedback) and OFB
	CBC (Ciphen Block Chaining).	(output faciliace)
	and the training the mind	4-
	9 7	$\mathcal{O}$

Electronic Cade Book (ECB) => ECB is the except black cipher made of functioning. It is easier because of direct encryption of each black of input plaintext and output is in the foorm of blocks of encounted cifhertext. Generally if a necessage is larger than I lik in size it can be broken down into a bunch of blacks and the procedure is expected. Define Authoritiation and explain why it is organized. Explain with the half of suitable expansile. Any Authentication >> 1) Authentication is the forecast of vocitying the identity of a user of our information User authentication is the process of verifying the identity of a uses when that user logs in to a computer system. (V) Authentication enables organizations to beef their networks secure by permitting only attentiated users or forocuses to gain occess to their frotested resousce This way include computer systems, networks databases, websites and other returne basel afflications or services. 3) It's main purpose is security. There are diff-enant types of authentication systems like:

DELTA Pg No

-	DELTA Pg No
1 44	1) Single Factor Authentication
	(Username + Password)
	2) Iwa Factor Authortisation
	(OTP, mail, etc)
2 4	3) Multi Factor Authoritistion
	(Broneteries, facial recognition, Signature
100	(voice etc)
1,211	A Comment of the state of the s
·Q4	Defferentiate bour Substitution Cifhon and Townsposition Cifhon techniques with example.
	Cifhen techniques with example.
N. S. Valley M.	I have a plan and Kennytha with min on fin
Auz	Substitution Cipher Toronsposition Cipher
1 1 m	1 In substitution cipher technique, 1 In transfosition cipher tech-
	plain text characters are replaced nigne, plain text characters are
	with other characters, numbers, secaroranged with respect to the
	and symbols position.
	2) Substitution cipher's forms 2) Transposition cipher's forms
	are Mono alphabetic substitution are key less townsposition cipher
	ciphos and poly alphabetic sub- and Keyed transposition apple.
	stitution ciphon.
	(3) In Substitution Ciphen technique (3) In Transposition ciphen technique the
	character's inantity is changed while its position of the character is changed but
	character's inantity is changed while its position of the character is changed but position genains unchanged. character's identity is not changed.
	Detect plain text. can Disclose plain text.
	Setect plain text. can disclose plain text.
	6 0:10 B. D. D. C. 1900
	3) og Ceason Ciphen. 3) eg., Pail Fonce Ciphen.

Date	J
DELTA Py No.	_
, , , , , , , , , , , , , , , , , , , ,	

0,5	Enflain the different steps involved in the encouptrois and decouption forcess of DES?
	process of DES?
	A STATE OF THE PROPERTY OF THE
Ang	1) Data Encouption Standard (DES) has been found rulnerable to
	(1) Data Encouption Standard (DES) has been found nulnerable to very forwerful attacks and thousand, the popularity of DES is
ralar.	are aller.
	DDES is a block cifher and bothers encoughts data in
	Stocks of size 64 lits, which wears 64 lits of flain
es lies	Level go as the input to the DES, which then foreduces
	64 lick of cifher text. The same algorithm and Ley are
	wed for enoughtion and Decemption with minor Differences,
7	Initial Key
- 10 M	Plain Text [PC, CRevented Choice 1)  [67 lit [64-8 (Roving Bols) = 56]
(Resonande leits	( spirit ( sport reary
· Prits	Initial Comutation (IS) are said (Is) are said
	Solut 49 bit form
37.10	Round 1 PC; Roles C. D. Now C. D. Become the initial blacks for Round 2
	Rand 2
	Round 2 Round 2 PC1
	Round 16 48 lix LS
	DO SELY
N . 4. 4.	
also call initial	permetation   Einal Cornatation
9.4.	(C1) (C) (C) (C)
	Cipher Text When these grounds LS's
. 11.	only by I bit if any
	other ground then LS is 2 lit
	LS -> 1 cs A
	LS -> LCS (Left Circular Shift)

Ý	Date
	DELTA Pg No
	Now we understand what goes on in the Round Functions
( We singly dime	(31 did) [] (2 did R
the Gylid flow to	
only)	Enfansion P
P	1011 1 1011 0 11 1 1 1 1 1 1 1 1 1 1 1
or funtation one one	
16 lug a	
nondon to make	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
32 lite to 48 lites .	
	the second secon
	11000100 (1), 27 202 2
	· (4M) ~ 0000011 1 170000 ~ (4M)