Theory Assignment 01

On

Cryptography & Network Security (CSE 3035)

Submitted by

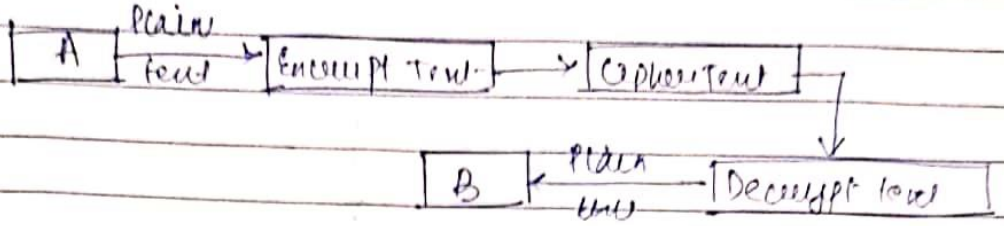
Name	**: JAHNAVI KEDIA**
Reg. No.	**: 1841012226**
Semester	**: 6th**
Branch	**: CSE**
Section	**: E**
Session	**: 2020-2021**
Admission Batch	**: 2018**

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
FACULTY OF ENGINEERING & TECHNOLOGY (ITER)
SIKSHA 'O' ANUSANDHAN DEEMED TO BE UNIVERSITY
BHUBANESWAR, ODISHA – 751030

(1) Define the following terms:

(I) Cryptography (II) Cryptanalysis (III) Steganography (IV) network security
(V) computer security

(i) Cryptography : The art of protecting info by transforming it into an unreadable format is called cryptography.



(ii) Cryptanalysis : It is the process of studying cryptographic systems to look for weakness or ~~lot~~ leak of information.

(iii) Steganography : It means we are hiding the existence of data.

(iv) Network security : It is any activity designed to protect the security and integrity of ~~over~~ network and data. It includes both hardware and software technologies.

(v) Computer security : It is the protection of computer systems and information from harm, theft and unauthorized users.

(2) Formulate ceaser cipher for the cipher Text: PHHW PH DIWHU WKH WRJD SDUWB to identify the plain text with the default key K=3 and also give atleast three important characteristics of this problem that is enabled to bruteforce cryptanalysis.

2. From cipher to plaintext, we will go for decryption.

$P = D(k, C) = (C - K) \bmod 26.$

D(P) = (15-3) mod 26 = 12 = m.
D(H) = (7-3) mod 26 = 4 = e
D(H) = e.
D(W) = (22-3) mod 26 = t.
D(P) = (15-3) mod 26 = M.
D(H) = e.
D(D) = (3-3) mod 26 = a.
D(I) = (18-3) mod 26 = f.
D(W) = t
D(H) = e
D(U) = (20-3) mod 26 = u.
D(W) = t
D(K) = (10-3) mod 26 = h.
D(H) = e
D(W) = t
D(R) = (17-3) mod 26 = o.
D(J) = (9-3) mod 26 = g
D(D) = a
D(S) = (18-3) mod 26 = P
D(D) = a
D(V) = u
D(W) = t
D(B) = (1-3) mod 26 = (-2+26) = 24 mod 26 = y

So the plaintext is -

meet me after the toga party.

There important characteristics of the plaintext that is enabled to brute force cryptanalysis 1) Encryption and decryption algorithm are known.

2. There are only 25 keys in key.
3. The language of the plaintext is known and easily recognizable.

(3) Tabulate the substitution and Transposition techniques in detail. Apply two stage transpositions Cipher on the “treat diagrams as single units” using the keyword “sequence”.

3. (1) Substitution Technique: letters of the plaintext are replaced by other characters or numbers or symbol.

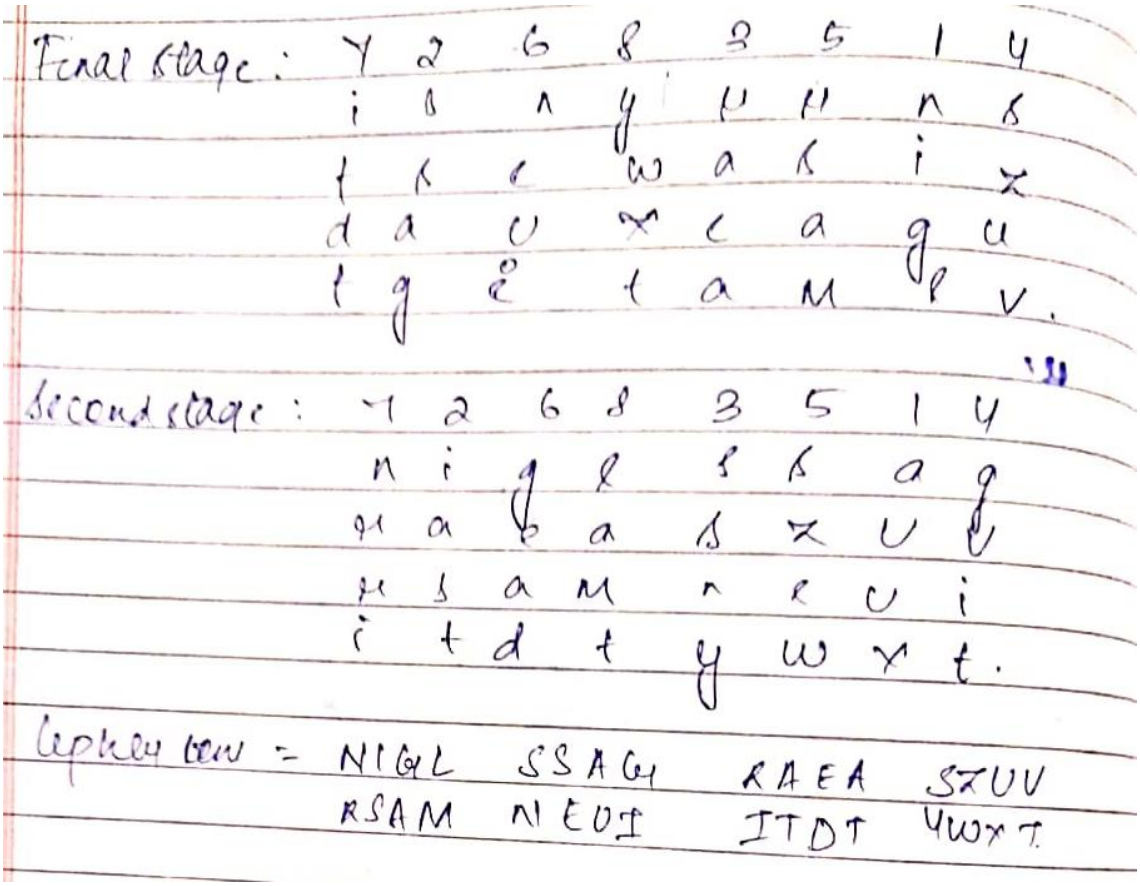
Eg: name → ISTO.

2. Transposition technique: Performing some sort of permutation rearranged according the symbol.

Eg: name $\xrightarrow{4! = 24}$ ANME
NMEA.
....

3. Plain text: treat diagrams as single unit
Keyword: sequence.

s	e	q	u	e	n	c	e
7	2	6	8	3	5	1	4
t	r	e	a	t	d	i	a
g	r	a	m	s	a	s	s
i	n	g	l	e	u	n	i
t	s	o	v	w	x	y	z



(4) What is mono-alphabetic cipher? Examine how it differs from Caesar cipher?

4. Monoalphabetic cipher: A cipher where each symbol is replaced by another symbol, where the replacement doesn't vary is called monoalphabetic cipher.

How it differs from Caesar cipher?

1) If the replacement remains same throughout the message, so the cipher is monoalphabetic as opposed to polyalphabetic cipher

2) In caesar cipher, the total encryption and decryption depends on the key

(5) Solve using playfair cipher. Encrypt the word “Semester Result” with the keyword “Examination”. List the rules used.

5. Plain text : Semester Result.
Keyword : Examination

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

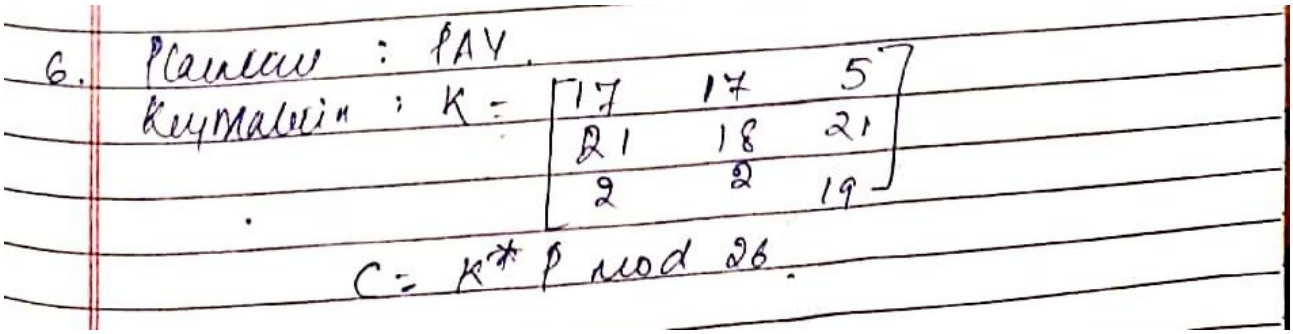
Se = LI
me → IX
st → PC
er → ML
re → LM
sr → LX
lt → PN.

ciphertext = LIIXPCMLLMLXPN.

Rules:
Plaintext is encrypted 2-letters at a time.
1) If a pair is ~~replaced~~ a repeated letter, insert filler like 'X'.
2) If both letters fall in the same row, replace each with letter to the right (wrapping back from start to end)
3) If both letters fall in the same column, replace each with the letter below it. (again wrapping from top to bottom)
4. Otherwise each letter is replaced by the letter in the same row and in the column of the other letter of the pair.

(6) Demonstrate the encryption of the message “PAY” using hill cipher with the following key matrix and show the decryption.

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



$$\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \begin{bmatrix} 5 \\ 80 \\ 24 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 375 \\ 819 \\ 486 \end{bmatrix} \text{mod } 26 = \begin{bmatrix} 11 \\ 13 \\ 18 \end{bmatrix} = \begin{bmatrix} L \\ N \\ S \end{bmatrix}$$

Ciphertext = LNS.

How decryption:

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

Plaintext = $P = K^{-1} C \text{ mod } 26$.

$$adj(K) = \begin{bmatrix} 306 & 25 & 267 \\ 7 & 313 & 8 \\ 6 & 0 & 1 \end{bmatrix} \text{mod } 26$$

$$= \begin{bmatrix} 4 & 9 & 15 \\ 15 & 19 & 6 \\ 24 & 0 & 17 \end{bmatrix}$$

$$\Rightarrow \begin{bmatrix} 4 & 9 & 15 \\ 15 & 19 & 6 \\ 24 & 0 & 17 \end{bmatrix} \begin{bmatrix} 11 \\ 13 \\ 18 \end{bmatrix} \text{mod } 26 = \begin{bmatrix} 15 \\ 0 \\ 24 \end{bmatrix}$$

Plaintext = PAY.

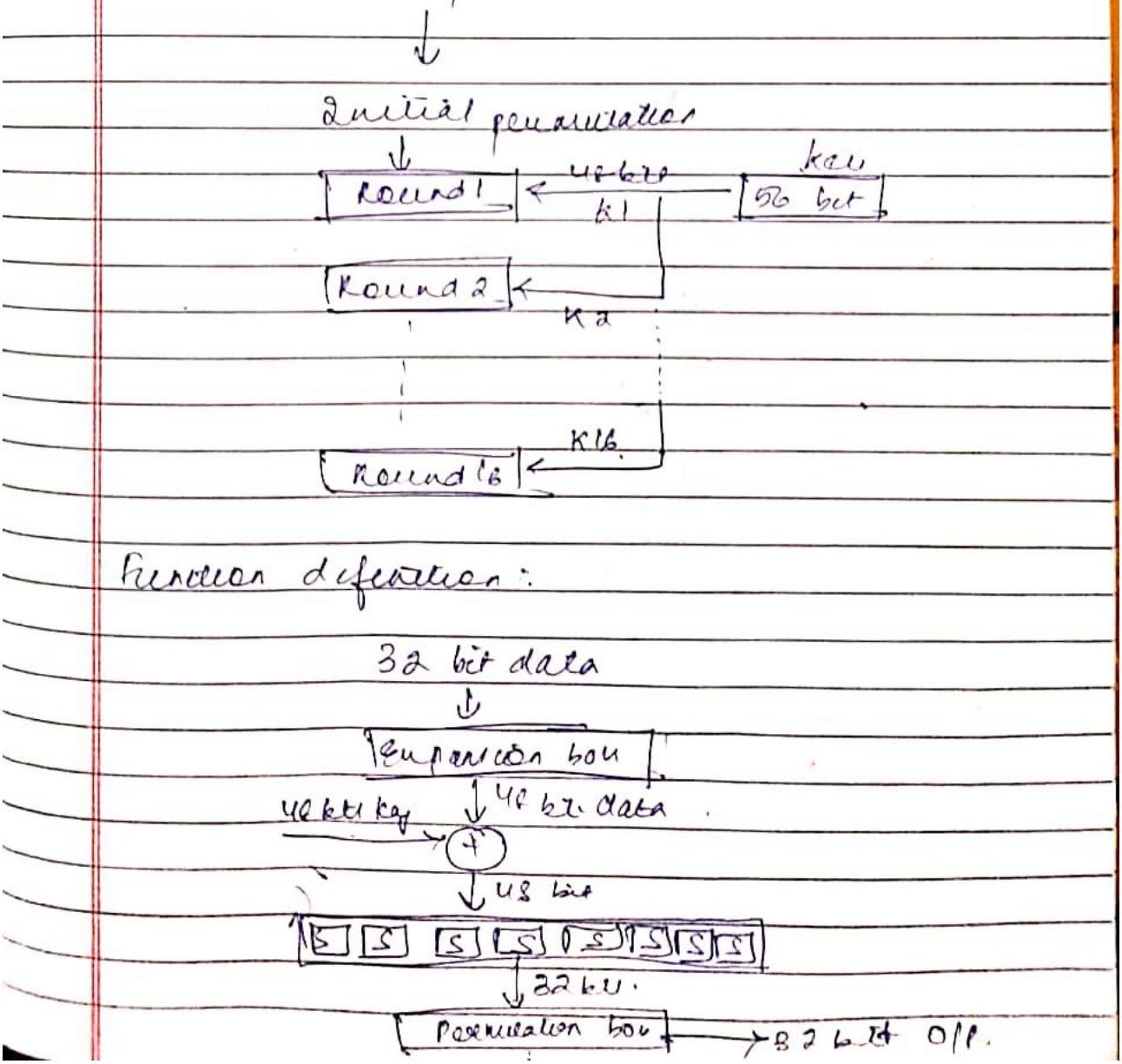
(7) Formulate the single round of DES algorithm and Design the key generation process of DES.

7. DES Algorithm

Step : 1) Initial Permutation
2) 16 Fiestal Rounds.
3) Swapping | left - right swap
4) Final permutation.

Basic Structure

We have 64 bit plaintext.



Function definition :

Expansion box

32 bit data → 48 bit data

Sbox

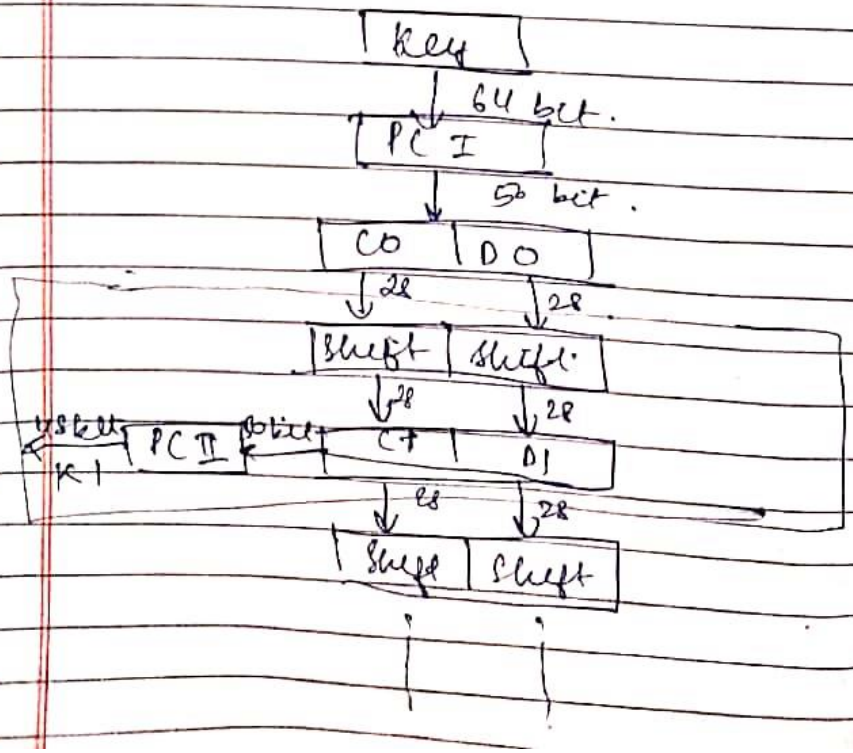
48 bit data → 32 bit data

Definition of DES S-Boxes.

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

How to generate key.

The 64 bit key which goes as I/P to PC-I and we get O/P as 56 bit keys.



(8) The following message was encrypted with a columnar transposition cipher using a full rectangular array and keyword *mathematics*. Decrypt it.

RIUGS IPNCT MSPAL AUNCY SOOCH UEYSA RTE

8. Key = MATHEMATICS

Rearranging key in alphabetic order →

- A A C E H I M M S T.

Number of letters = 33 letters.

Key size = 11.

Matrix dimension : (33/11) × 11.

A	A	C	E	H	I	M	M	S	I	T
1	2	3	4	5	6	7	8	9	10	11
R	G	P	T	R	A	C	O	H	Y	R
I	S	N	M	A	U	Y	O	U	S	T
U	I	C	S	L	N	S	C	E	A	E

Rearranging the matrix key as found MATHEMATICS

M	A	T	H	E	M	A	T	I	C	S
1	C	Y	R	P	T	O	G	R	A	P
H.										
Y	I	S	A	M	O	S	T	U	N	U
S	U	A	L	S	C	I	E	N	C	E

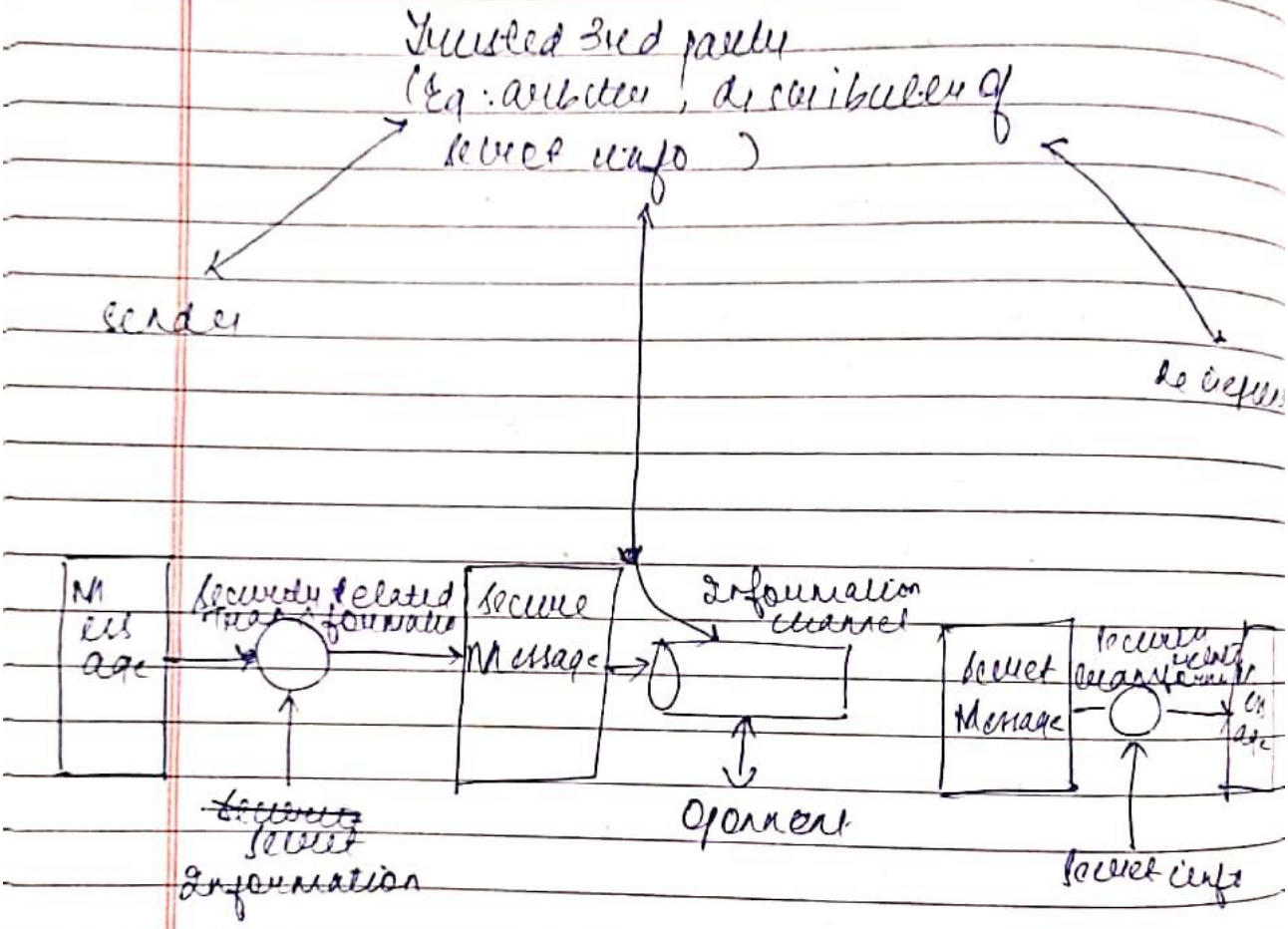
Hence, plaintext or decrypted text =

CRYPTOGRAPHY IS A MOST UNUSUAL SCIENCE.

(9) (i) With a neat block diagram, explain the network security model and the important parameters associated with it.

(ii) Differentiate active and passive security attacks. Categorize these attacks and explain one examples of each.

9(i) Model for network security



1) Transformation: Transformation of the info which has to be sent to the receiver, so that any opponent present at the information channel is unable to read the message. This initiates the encryption of the message.

2) Secret Info: Sharing of the secret info between sender and receiver of which the opponent must not have any clue.

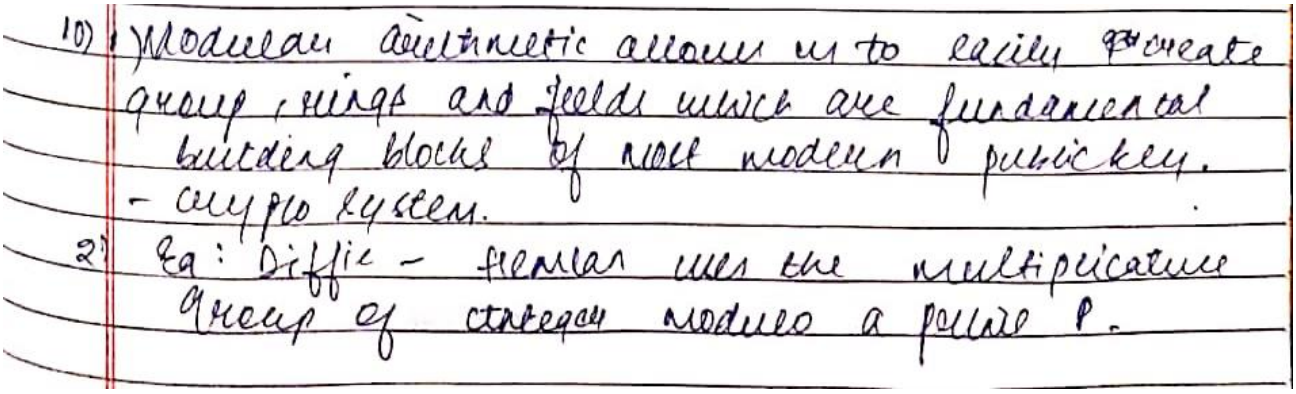
Notarization: There should be a trusted third party which should take the responsibility of distributing the secret info to both the communicating parties and also prevent it from any opponent.

(ii) Security attacks

Security Attacks

Passive Attack	Active Attack
Attempt to learn use of info from the system but doesn't affect the system resources.	~~Attempt~~ Attempt to alter the system resources or affect their operation
→ Release of message content - The attackers can easily be able to understand the details of the message.	→ Masquerade: When one entity pretends to be another entity
→ Traffic Analysis: The attackers will understand the patterns.	→ Replay: Involves passive capture of a message and its subsequent transmission
	→ Modification of message.
	→ Denial of service - It prevents normal use of communication facilities

(10) Explain why Modular arithmetic has been used in cryptography.



(11)What is the difference between :

(I) A block cipher and a stream cipher
(II) Diffusion and Confusion
(III)Differential and Linear cryptanalysis
(IV)Active and Passive attack

11)(i) Block cipher

(i) Plaintext → Ciphertext. By taking plaintext block at a time.
2) Uses both confusion and diffusion.
3) Complexity is simple.
4) Use confusion and diffusion.
5) Reverse encryption is difficult.
6) Eg: DES, CBC

Stream cipher

1) 1 byte plaintext → ciphertext
2) 8 bit.
3) Complexity is more.
4) Uses only confusion.
5) Reverse encryption is easy.
6) Eg: CFB, OFB.

(ii) Diffusion

1) It hides the relationship between ciphertext and plaintext
2) If a single symbol is changed in the plain text then all symbols will change in the ciphertext.

Confusion

1) Hides the relationship between ciphertext and the key
2) If a single key is changed, all bits in the ciphertext will change.

(iii) Differential

1) Differential analysis focuses on statistical analysis of two I/Ps and two O/Ps of cryptographic algorithms.

linear

1) Linear cryptoanalysis focuses on statistical analysis against known round of decrypted ciphertext.

	Differential	Linear
2.	In differential cryptanalysis the changes in the intermediate ciphertexts are obtained between multiple rounds of encryption. The attacks can be combined and thus referred as differential cryptanalysis.	2. The cryptanalysis decrypts each cipher using all possible subkeys for one round of encryption and studies the resulting intermediate cipher text to analyze the random result.
(iv)	Active attack	Passive attack.
1)	The attacker can see the data but can't modify.	1) Attempts to make changes to data on target.
2)	It is a danger of confidentiality.	2) Danger for integrity as well as confidentiality.
3)	System has no impact.	3) System damaged.
4)	System resources are not changed.	4) System resources can be changed.

(12) This problem provides a numerical example of encryption using a one- round version of DES. We start with the same bit pattern for the key *K* and the plaintext, namely:

in hexadecimal notation: 0 1 2 3 4 5 6 7 8 9 A B C D E F

in binary notation: 0000 0001 0010 0011 0100 0101 0110 0111
1000 1001 1010 1011 1100 1101 1110 1111

a. Derive *K*1, the first-round subkey.

b. Derive *L*0, *R*0.

c. Expand *R*0 to get EXP(*R*0).

d. Calculate *A* = EXP(*R*0) XOR *K*1.

e. Group the 48-bit result of (d) into sets of 6 bits and evaluate the corresponding S-box substitutions.

f. Concatenate the results of (e) to get a 32-bit result, *B*.

g. Apply the permutation to get P(*B*).

12) a) In Binary notation: 0000 1011 0000 0010 0110 0111 1001 1011 0100 1001 1010 0101.

in hexadecimal notation: 0 B 0 2 6 - 1 9 B 4 9 A 5.

b) LO, RO are derived by passing the 64-position through initial permutation.

LO = 1100 1100 0000 0000 1100 1100 1111 1111
RO = 1111 0000 1010 1010 1111 0000 1010 1010.

c) Exp (RO) = 011110 100001 010101 010101
011110 100001 010101 010101.

d) A = 011100 010001 011100 110010 111002
010101 111011 100000.

e) 0 (base 10) = 0000 (base 2)
12 (base 10) = 1100 (base 2)
2 (base 10) = 0010 (base 2)
1 (base 10) = 0001 (base 2)
6 (base 10) = 0110 (base 2)
13 (base 10) = 1101 (base 2)
5 (base 10) = 0101 (base 2)
0 (base 10) = 0000 (base 2)

f) B = 0000 1100 0010 0001 0110 1101 0101 0000

g) P(B) = 1001 0010 0001 1000 0010 0000 1001 1100.

(13) Show how to convert the given text “VALLIAMMAI” into cipher text using Rail fence Technique.

13) Plaintext : VALLIAMMAI.
Using depth = 2.

V L I M A
A L A M I.

Ciphertext : VLIMAALAMI.

(14) Which parameters and design choices determines the actual algorithm of a Feistel cipher?

14. Parameters and Algorithm.

1. Block size : Larger block sizes mean greater security but reduced encryption/decryption speed for a given algorithm.

2. Key size : Larger key size means greater security but may decrease encryption/decryption speed.

3) Number of Rounds : A single round offers inadequate security but that multiple round offer increasing security. A typical size is 16 Rounds.

4) Subkey Generation Algorithm : Greater complexity in this algorithm should lead to greater difficulty of cryptanalysis.

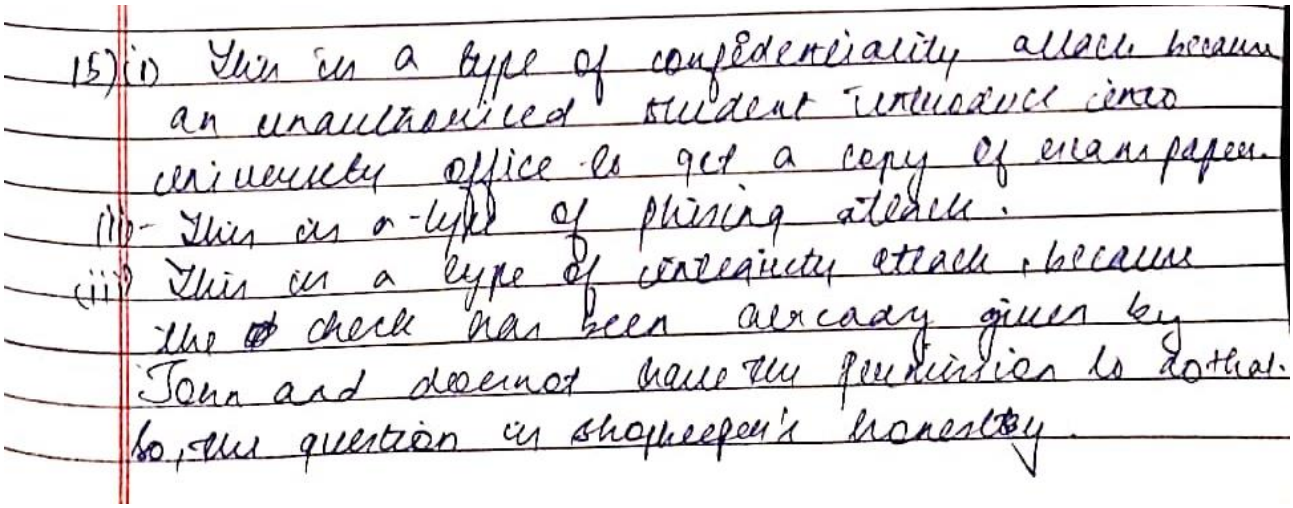
5) Round Function (F) : Greater complexity generally means greater resistance to cryptanalysis.

(15) Define the type of security attack in each of the following cases:

(i) A student breaks into university's office to get a copy of exam paper to be held on the next day.

(ii) A person sends hundreds of e-mails every day to another person using a phony return e-mail address.

(iii) John gives a cheque of $14 to the shopkeeper to buy a book. Later he finds that the cheque was cashed for $140.


15) (i) This is a type of confidentiality attack because an unauthorized student intruded into university office to get a copy of exam paper.

(ii) This is a type of phishing attack.

(iii) This is a type of integrity attack, because the check has been already given by John and doesn't have the permission to do that. So, the question is shopkeeper's honesty.