DAYANANDA SAGAR COLLEGE OF ENGINEERING

(An Autonomous Institute affiliated to VTU, Approved by AICTE & ISO 9001:2008R Certified)
Accredited by National Assessment & Accreditation Council (NAAC) with 'A' grade

DEPARTMENT OF TELECOMMUNICATION ENGINEERING

Accredited by National Board of Accreditation Council (NBA)

SCHEME & SOLUTION: CONTINUOUS INTERNAL ASSESSMENT- 1

Date: 12/10/2020

Course: Cryptography & network security Course Code: 17TE7DECNS

Semester& Section: VII 'A' & 'B' Total no of Pages: 6

Scheme & Solution prepared by: PRUTHVIK RAJ

Signature

Q. No.	Description	Marks Distribution
1. a.	iv) Integrity	10 M
b.	ii) Authorization	
c.	i) ENCRYPTED	
d.	ii) Denial of service	
e.	iii) VIGNERE	
f.	ii) Caesar	
g.	ii) private key	
h.	i) E, T	
i.	i) Steganography	
j.	ii) other symbol	
2.	Public key Encryption — 2 M	

Q. No.	Description	Marks Distribution

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

8M } 10

P.t = IN VE ST ME NT ~~I~~N KN OW LE DGEX

C.t = NT Y~~I~~J BI~~J~~~~Q~~J TE NT GE WN KR AL TY

3) $c = Kp \bmod 26$ P.t = DONT LIE To ~~Yourself~~x

$$\begin{bmatrix} C_1 \\ C_2 \end{bmatrix} = \begin{bmatrix} L & S \\ E & D \end{bmatrix} \begin{bmatrix} P_1 \\ P_2 \end{bmatrix} \bmod 26$$

$$\begin{bmatrix} C_1 \\ C_2 \end{bmatrix} = \begin{bmatrix} 11 & 8 \\ 4 & 3 \end{bmatrix} \begin{bmatrix} 3 \\ 14 \end{bmatrix} \bmod 26 = \begin{bmatrix} 15 \\ 2 \end{bmatrix} = \begin{bmatrix} P \\ C \end{bmatrix}$$

$$\begin{bmatrix} C_1 \\ C_2 \end{bmatrix} = \begin{bmatrix} 11 & 8 \\ 4 & 3 \end{bmatrix} \begin{bmatrix} 13 \\ 19 \end{bmatrix} \bmod 26 = \begin{bmatrix} 9 \\ 5 \end{bmatrix} = \begin{bmatrix} J \\ F \end{bmatrix}$$ — 5M

$$= \begin{bmatrix} 11 & 8 \\ 4 & 3 \end{bmatrix} \begin{bmatrix} 11 \\ 8 \end{bmatrix} \bmod 26 = \begin{bmatrix} 3 \\ 10 \end{bmatrix} = \begin{bmatrix} D \\ U \end{bmatrix}$$

C.t = PC JF DU OV IY CM TS CX FU

Q. No.	Description	Marks Distribution

Decryption :- $P = CK^{-1} \bmod 26$

$$K^{-1} = \frac{\text{adj}|K|}{\det K} =$$

$$\text{adj}|K| = \begin{bmatrix} 3 & -8 \\ -4 & 11 \end{bmatrix}$$

$$\det|K| = 7$$

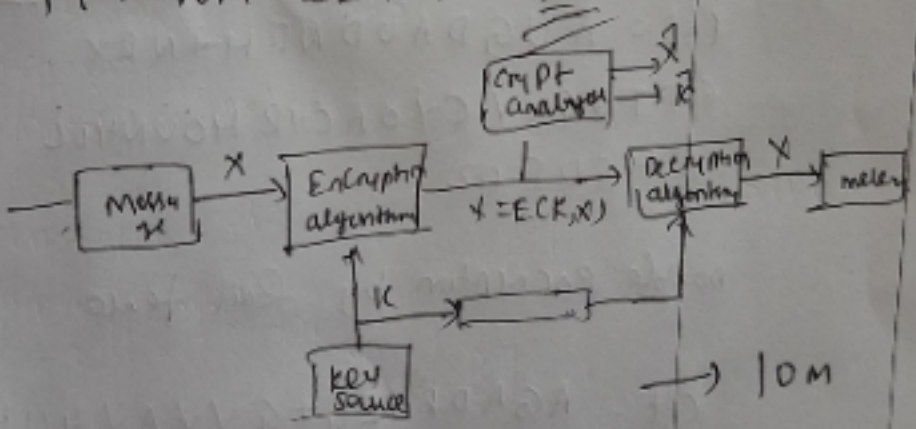
$$K^{-1} = \begin{bmatrix} 3 & 18 \\ 22 & 11 \end{bmatrix}$$

— 5M

$$\begin{pmatrix} P_1 \\ P_2 \end{pmatrix} = \begin{bmatrix} 15 \\ 2 \end{bmatrix} \begin{bmatrix} 3 & 18 \\ 22 & 11 \end{bmatrix} \bmod 26 = \begin{bmatrix} 3 \\ 14 \end{bmatrix} = \begin{bmatrix} D \\ O \end{bmatrix}$$

P.t :- DONT USE TO YourSelf

4)



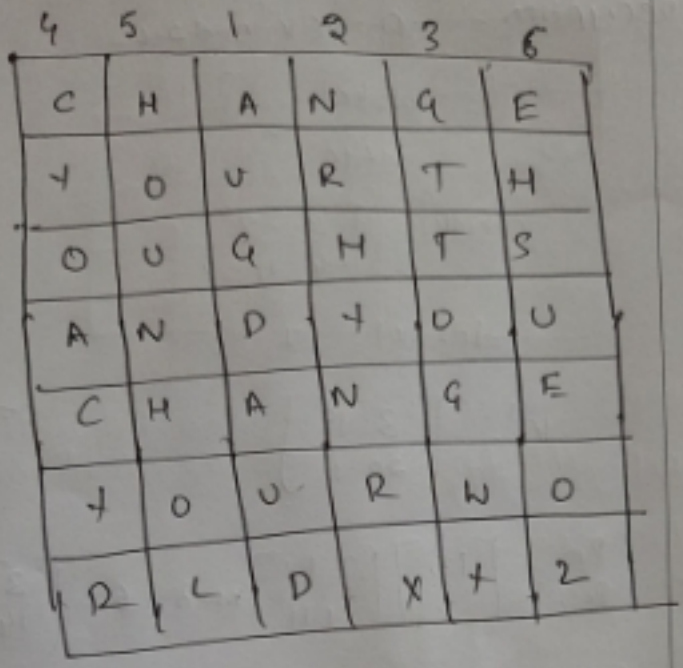
→ 10M

-) Block diagram — 5m
Explanation — 3m
equation — 2m

$Y = E_K(X)$

$X = D_K(Y)$

Q. No.	Description	Marks Distribution
5)		



C.t = ÀUGDAUDNRHÝNRX
GTTOGWÝCÝOACÝRHOÚNHÒL
EHSUEO2

— 4m

Double encryption by Rail fence

C.t = AGADRYRGTGYYAYHUHLHEO
UDUNHNXTOWCOCRONOESEZ

Q. No.	Description	Marks Distribution
6)	p.t = CRYPTOGRAPHY k = 7 Caesar Cipher Encryption: C = (k+p) mod 26 — 1m = (7+2) mod 26 = 9 = J = (7+17) mod 26 = 24 = Y — 4m — 5m ⋮ = (7+24) mod 26 = 5 = F C.t = JYFNAVNYHWOF Decryption: p = (C-k) mod 26 — 1m = (9-7) mod 26 = 2 = C = (24-7) mod 26 = 17 = R — 5m ⋮ = (5-7) mod 26 = 24 = Y p.t = Cryptography	10m

Q. No.	Description	Marks Distribution
7)	Take any of the Example and clearly show one to one mapping Eg: p.t = Hello ↓↓ Key = ABCCD — 6M C.t = HFNNR Strength of monoalphabetic cipher ① Since we get 4×10^{26} possible Combination of key it difficult to break Cipher text by using Brute force attack ② If the Cryptanalyst know the nature of plaintext then He can Exploit the regularities of the language	10M 4M