RAJ KUMAR GOEL INSTITUTE OF TECHNOLOGY & MANAGEMENT, GZB

1st Sessional Examination 2017-18 (Odd Semester)

Roll No.: **Subject Name:** Cryptography and Network Security
Year/Branch: 4th/I.T **Subject Code:** NIT-701
Max Time: 1 Hours 30 Minute **Max Marks:** 50

SECTION-A

Q.1 Attempt all parts carry equal marks. Write answer of each part in short.

(a) Define steganography?
(b) Define brute force attack?
(c) What is the use of S-boxes in DES?
(d) Explain the principle of cryptanalysis?
(e) Differenciate between authentication and authorization.

SECTION-B

Note: Attempt any five questions from this section.

Q.2 What is difference between diffusion and confusion?
Q.3 Differenciate between Symmetric and Asymmetric cryptographic model.
Q.4 Draw block diagram of DES cipher showing size of input/output of every block. How important is swapping step at the end of every round.
Q.5 Write short notes on:
(i) snooping (ii) Masquerading (iii) integrity (iv) denial of service.
Q.6 What can be various applications of one pad ciphers?
Q.7 Distinguish between block cipher and stream cipher.
Q.8 Encrypt the message "meet me at the usual place at ten rather than eight oclock" using the Hill cipher with the key $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$. Show your calculations and the result.
Q.9 Why is it important to study the Feistel Cipher?

SECTION-C

Note: Attempt any two questions from this section.

Q.10 Using playfair matrix:

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

Encrypt this message:"The enemy must be stopped at all costs. Do whatever is necessary. "

Q.11 What do you understand by Network Security Attacks? Describe active and passive security attacks.

Q.12 Brefly describe the Hill Cipher. If a chosen plaintext attack can be mounted, it is easier to solve Hill Cipher. Describe such attack.