AMRITSAR COLLEGE OF ENGINEERING AND TECHNOLOGY, AMRITSAR
(AUTONOMOUS COLLEGE)

Roll No. .....
Total No. of Questions: 06 **Total No. of Pages: 02**

B.Tech. (CSE) – 5th Sem
INFORMATION SECURITY
ACCS-16505

Time: 1: 30 Min **Maximum Marks: 30**

Instruction to Candidates:

1) Section-A contains five questions. All questions are compulsory.
2) Section-B contains three questions. Attempt any two questions.
3) Section-C contains two questions. Attempt any one questions.

Section - A

(5 × 2 = 10)

Q1)

i) Encrypt the text "CHANGE IN PLAN MEET ME AT DAWN" using caesar cipher

ii) In our computing labs, print billing is often tied to the user's login. Sometimes people call to complain about bills for printing they never did only to find out that the bills are, indeed, correct.
What do you infer from this situation? Justify.

iii) Consider the following:
Plaintext: "KEY"
Secret key: "CRYPTOGRAPHY"
Compute the cipher text from given plain text and key using hill cipher method.

iv) In the RSA system, the public key of a given user is e = 31, n = 3599. What is the private key of the user?

v) How can identity theft be prevented?

Section – B

(2 × 5 = 10)

Q2) Client machine C wants to communicate with server S. Explain how it can be achieved through Kerberos protocol?

Q3) With a neat diagram explain how encryption and decryption are done using Blowfish algorithm?

Q4) Consider the following:

Plaintext: “PROTOCOL”

Secret key: “NETWORK”

What is the corresponding cipher text using play fair cipher method?

Section – C

(1 × 10 = 10)

Q5) Alice and Bob wish to share private messages, where each of them of two separate keys generated. What kind of strategy would you suggest to ensure confidentiality, key management and authentication for the conversion between Alice and Bob? Explain the strategy and also highlight the design issues related to the strategy proposed.

Q6) Given two prime numbers p=5 and q=11, and encryption key e=7 derive the decryption key d. Let the message be x=24. Perform the encryption and decryption using R.S.A algorithm.