University Institute of Engineering & Technology
Panjab University, Chandigarh
5th Semester: B.E. Information Technology
Subject: Network Security & Cryptography (IT503)
Minor-1

Max. Time: 1 hour 30 minutes
Max. Marks: 30

Note: Attempt all questions
Attempt paper on A4 sheets and submit scanned pdf in sequence
Same/copied answers shall result in cancelation of answer sheet

1Q.
a) Cipher Text Analysis Vs Brute Force Attack
b) What is discrete logarithm? What is the use of it?
c) How public key certificate is formed? What are its typical contents?
d) What factors are considered while choosing key size in symmetric key cryptography?
e) What is security parameters negotiation?

2*5 = 10

2Q. How a statistical frequency based attack works? Why transposition based ciphers successfully overcome statistical frequency attack? Encrypt following text in quotes "I am an honest UIETian I will neither copy answers from internet nor from answer sheet of any other student If I do so please fail me in this subject" using row transposition cipher. Use integer part of your university roll no as Key. Use 4-rows for performing encryption. Following rules should be followed

- Ignore 0 in the integer part of roll number
- If any single digit integer number is missing in roll number, then use next integer available in roll number for encryption.

e.g. key to be used for roll no. UE183047 is 18347 with 4-rows

2+1+3 =06

3Q. Users A and B use the DiffieHellan Key exchange technique with a common prime q=13 and a primitive root α=2.

i. If user A has public key $Y_A = 6$, what is A's private key X_A?

ii. If user B has public key $Y_B = 3$, what is B's private key X_B? What is the shared secret key agreed with between A and B?

04

4Q. Design a secure communication system having confidentiality, integrity and non-repudiation. Solution should be fast as far as possible and should have lesser bandwidth overheads. Assume and state all terminology being used in communication.

08

5Q. In a public key system using RSA, attacker intercepted the cipher text C=8 sent to a user whose public key e=13, n=33. What is the plaintext M?

02