MANIPAL INSTITUTE OF TECHNOLOGY
MANIPAL
(A constituent unit of MAHE, Manipal)

I SEMESTER M. TECH (Computer Science and Information Security)

END SEMESTER EXAMINATIONS, MARCH, 2021

SUBJECT: ADVANCED CRYPTOGRAPHY (CSE 5171)
REVISED CREDIT SYSTEM

(01-03-2021)

Time: 3 Hours MAX. MARKS: 50

Instructions to Candidates:

- Answer **ALL** the questions.
- Missing data may be suitably assumed.

1A. State and prove Fermat's Little Theorem. Find the following using Fermat's Little Theorem. (i) $3^{31} \bmod 7$ (ii) $2^{35} \bmod 7$ (iii) $128^{129} \bmod 17$. **5M**

1B. Define the Chinese Remainder theorem. Check the condition to find the value of X using Chinese Remainder theorem. Ensure the correctness of X using the congruence equations. **5M**

$x \equiv 3 \bmod 5$

$x \equiv 1 \bmod 7$

$x \equiv 6 \bmod 8$

(ii) Write Miller-Rabin Primality test algorithm.

.

2A. Write Diffie – Hellman Elliptic Curve Cryptography algorithm with illustration by assuming the initial values properly. Prove the correctness of the illustration. Write man in the middle attack algorithm. **5M**

2B. Consider both the classes, equal and unequal co-ordinates to find the points on the elliptic curve Y^2=X^3+2X+2 mod 17, from 2G to 9G, when G= (5,1). Show the calculations for all the points. **5M**

3A. With the help of diagram/diagrams explain the following: **5M**
(i)working of HMAC system.
(ii) applications of hash function using public key approach of cryptography.

3B. What characteristics are needed in secure hash function? Describe steps of MD5 Hash algorithm. Compare the performance of MD5 and SHA-1. **5M**

4A. Write both the diagram and algorithmic representation of Digital Signature Standard. What is the use of global parameters? Compare RSA Digital Signature Scheme with RSA crypto system. **5M**

4B. Using the RSA scheme, let p=809, q=751, and d=23. Calculate the public key e. Then write models and substitute values for the parameter of the models for: (a) sign and verify a message with M1=100. Call the signature S1, (b) sign and verify a message with M2=50. Call the signature S2, and (c) Show that if M=M1*M2=5000, then S=S1*S2. Final calculation is not required. **5M**

5A. With the help of diagrams explain four approaches of fixed password authentication. Give examples for fixed password and One Time Password Authentication. **5M**

5B. (i)What is Key Distribution Center? (ii) Write general diagram of Key Distribution Center. (iii)With the help of diagrams explain flat multiple Key Distribution Center and hierarchical multiple Key Distribution Center. (iv) Explain the Public key generation and Public key exchange issues of public key certificates. **5M**