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

I SEMESTER M. TECH (Computer Science & Information Security)
END SEMESTER EXAMINATION, December 5, 2023
SUBJECT: DESIGN OF SECURE PROTOCOLS (CSE 5119)
REVISED CREDIT SYSTEM

Time: 3 Hours (9.30 AM-12.30 AM) **MAX. MARKS: 50**

Note: Answer ALL the questions.

1A	Explain the purpose of nonce and timestamp in the design of secure protocols.	**2**
1B	Design multi-signature protocol using multiple-key public key cryptography.	**3**
1C	Design Woo-Lam mutual authentication and key exchange protocol using public key cryptography.	**5**
2A	Explain suppress-replay attack.	**2**
2B	Let A, B and S are identities of Alice, Bob and Trusted Server. Let K_{AS} is a symmetric key known only to A and S and let K_{BS} is a symmetric key known only to B and S. Let N_A and N_B are random nonces generated by A and B respectively. Let K_{AB} is random secret session key for A and B generated by S. Consider the following mutual authentication and key exchange protocol between Alice and Bob. $1. A \rightarrow B : A, N_A$ $2. B \rightarrow S : B, \{A, N_A, N_B\}_{K_{BS}}$ $3. S \rightarrow A : \{B, K_{AB}, N_A, N_B\}_{K_{AS}} \{A, K_{AB}\}_{K_{BS}}$ $4. A \rightarrow B : \{A, K_{AB}\}_{K_{BS}} \{N_B\}_{K_{AB}}$ This protocol vulnerable to suppress-replay attack. Modify the above protocol to prevent this attack.	**5**
2C	Discuss 5 important attacks on cryptographic protocols.	**3**
3A	Construct a (3, 5)-threshold secret sharing scheme for the quadratic polynomial $F(x) = (ax^2 + bx + M) \bmod p$, where a = 7, b = 8, M = 11 (secret message) and p = 13 (prime). Select F(2), F(3) and F(5) to reconstruct M.	**4**
3B	Design Bit Commitment protocol using One-Way Hash functions.	**3**
3C	Demonstrate Man-in-the-Middle Attack for Diffie-Hellman Key Exchange protocol for two parties Alice and Bob.	**3**
4A	Design Diffie-Hellman key exchange protocol for three parties Alice, Bob and Candy.	**5**
4B	Explain Message Authentication Code (MAC).	**2**
4C	Let A, B and S are identities of Alice, Bob and Trusted Server. Let N_A and N_B are random nonces generated by A and B respectively. Let MAC is the message authentication code. Consider the following protocol: $1. A \rightarrow B : N_A$ $2. B \rightarrow A : N_B, MAC\{N_A, N_B, B\}$ Modify the above protocol to provide mutual authentication between Alice and Bob.	**3**

5A	Alice, Bob and Candy use the Diffie-Hellman key exchange protocol for three parties with a common prime n = 23 and a primitive root g = 5. Let Y_A =8, Y_B = 10, and Y_C = 12 are public keys of Alice, Bob and Candy respectively. Compute the shared secret key between Alice, Bob and Candy.	**5**
5B	Explain 3 properties of coin flipping protocol.	**3**
5C	Design key and message transmission protocol.	**2**