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

I SEMESTER M.TECH. (COMPUTER SCIENCE AND INFORMATION SECURITY) END SEMESTER EXAMINATIONS, NOV/DEC 2023

SUBJECT: ADVANCED CRYPTOGRAPHY AND CRYPTANALYSIS [CSE 5120]

(07/12/2023)

Time: 3 Hours MAX. MARKS: 50

Instructions to Candidates:

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

1.A Alice and Bob decide to use Elliptic Curve Cryptography Simulating ElGamal to maintain the confidentiality of the communication. Bob selects $E_{67}(2, 3)$ as the elliptic curve over GF(p) and selects $e_1 = (2, 22)$ as a point on the elliptic curve and an integer d = 4. Compute the public key e_2. Bob announces $E_{67}(2, 3)$, e_1 and e_2 and keeps d secret. If Alice wants to send the plaintext P = (24, 26) to Bob and selects r = 2 compute the ciphertext C_1 and C_2. Also verify that upon decryption the plaintext is obtained. Make use of the formulae given below. Show clearly all the steps. **5M**

$e_2 = d \text{ x } e_1$

$C_1 = r \times e_1 \qquad C_2 = P + r \times e_2 \qquad P = C_2 - (d \times C_1)$

1.B Suppose Alice wants to get the message signed by the Notary. She does not want to reveal the contents of the message to the notary. Identify the signature scheme that could be used by the notary to sign the message from Alice, which can be verified by Bob. Use the parameters p=7, q=13, e=5, M=19, b=12. Illustrate the signing and verification process. **3M**

1.C Consider the ciphertext ‘EXXEGOEXSRGI’ that was encrypted using Caesar cipher. Determine the key using brute force method and decipher the ciphertext. **2M**

2.A Consider the symmetric key distribution using asymmetric encryption scenario given in Fig Q 2. A. **5M**

(i) Explain this scenario.
(ii) Illustrate the attack that could be performed on this scenario.
(iii)Propose methods to enhance the security.

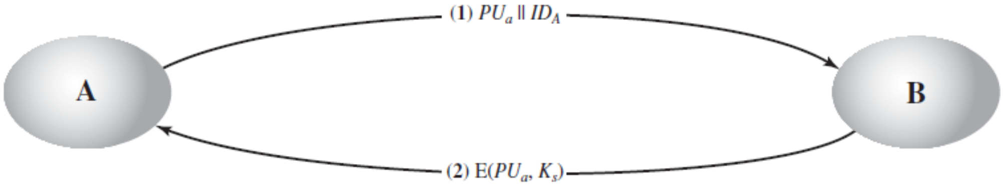

Fig. Q 2.A

2.B The two communicating parties A and B decide to use Diffie Hellman key agreement to share a common session key. They decide to use the following parameters p=11, and g=2. A and B choose the private keys as 9 and 4 respectively, Compute the public key of A and B and the shared symmetric key. **3M**

2.C Analyze the security of CBC-MAC with reference to birthday attacks. **2M**

3.A Illustrate the Personal Identification Verification System Model, with the help of a diagram and explain the same. **5M**

3.B Assume that the RSA cryptosystem is used to secure the session key used for encrypting the communication between two communicating parties. For this, the receiver selects the public modulus N=817. Devise a method of attacking the system, making use of Fermat's differences of squares factorization algorithm. Indicate clearly all the steps. **3M**

3.C Can symmetric key be used to both sign and verify a signature? Justify your answer. **2M**

4.A Consider the S Box Representation given below **5M**

Input	0	1	2	3	4	5	6	7
Output	0	5	3	4	2	7	1	6

(i)Compute the entries at the cells indicated by X, in the Linear Approximation Table given below. Show all the steps needed to arrive at the result.

		Output Sum							
		0	1	2	3	4	5	6	7
Input Sum	0								
	1								
	2			X					
	3								
	4	X					X		
	5								
	6								X
	7								

(ii)Calculate the difference values ΔY for all values of X when ΔX=111 and ΔX=010

4.B Analyze the usage of baby step giant step algorithm to obtain the secret parameter in the Diffie Hellman key agreement protocol if the public parameters are p=11, g=2 and the computed value of public parameter by one of the entities is 5. **3M**

4.C Consider the hierarchical structure of Certificate authorities as shown in Fig. Q 4.C. with root CA and intermediate CA's named CA1, CA2 and CA3. The root CA has a self-signed, self-issued certificate; which is trusted by other CA's. The root CA has signed certificates for CA1, CA2 and CA3. CA1 has signed certificates for User1, User2, and User3; and so on. Illustrate the sequence in which User 1 knowing only the public key of the CA (the root), can obtain a verified copy of User8's public key. **2M**

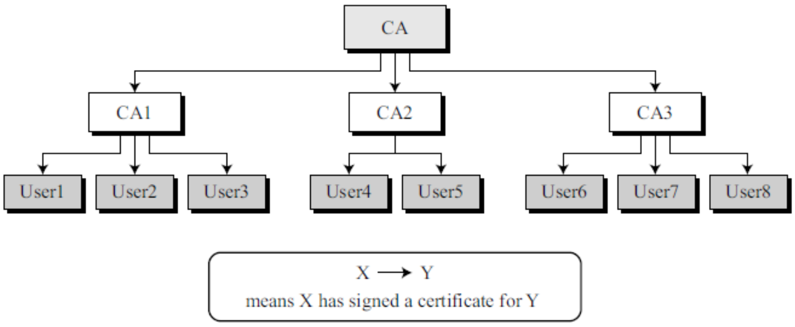

Fig. Q. 4 C

5.A Consider the Known-Message Attack on the RSA digital signature scheme given the following: p = 31, q = 29, and d = 23. Clearly show all the steps in the computation. **5M**

(i)Calculate the public key e.

(ii)Consider the message M1 = 100, compute and verify the signature S1

(iii)Consider the message M2 = 50, compute and verify the signature S2.

(iv)Show that if M = M1 × M2 = 5000, then S = S1 × S2.

5.B Analyse the usage of birthday paradox to attack hash functions. **3M**

5.C Compare parallel and serial hashing schemes. **2M**