Question Paper

Exam Date & Time: 11-Jan-2024 (02:30 PM - 05:30 PM)

MANIPAL ACADEMY OF HIGHER EDUCATION

FIFTH SEMESTER B.TECH (COMPUTER AND COMMUNICATION ENGINEERING) MAKEUP EXAMINATIONS, JANUARY 2024

INFORMATION SECURITY [ICT 3172]

Marks: 50 **Duration: 180 mins.**

Descriptive

Answer all the questions. Section Duration: 180 mins

1A) Given the key K (7,5), decrypt the message 'UPS' using the Affine cipher. Calculate the sum of the letters in the obtained plaintext using the provided mapping [a/A=0, ..., Z/z=25] (e.g., if the plaintext is 'ABC,' the sum would be 0+1+2=3). Now, use this sum as the new plaintext and encrypt it using the ElGamal Algorithm. The ElGamal configuration includes a prime number (p=23), a primitive root (e_1=7), a private key (d=9), and a random number (r=5). Demonstrate the encryption process step by step and provide the final encrypted result. (5)

1B) Compare and contrast the objectives and methods employed in cryptanalysis attacks. Also, analyze how adherence to Kerckhoff 's principle influences the resilience of a cryptographic system against various cryptanalysis techniques. (3)

1C) Differentiate between the following (2)

i. Substitution and Transposition Ciphers

ii. Known plaintext attack and chosen plaintext attacks

2A) Analyze the advantages and limitations of different block cipher modes of operation. Also, discuss the impact of these modes on the overall security and efficiency of block ciphers. (5)

2B) Analyze how the confusion and diffusion properties of the Data Encryption Standard (DES) are achieved via the avalanche effect and completeness. (3)

2C) List the differences between MDC and MAC with respect to their construction and usage. (2)

3A) Define attacks, services and mechanisms with relevant examples. Show the relationship between various security services and security mechanisms. Also identify different attacks with respect to CIA triad. (5)

3B) Evaluate the idea of Merkle-Damgard scheme and why this idea is important for the design of cryptographic function? (3)

3C) In DSS and Schnorr schemes, what happens if attacker can find the value of random number,'r'? Justify your answer. (2)

4A) Alice chooses p=3119, e1=2, d=127 and a number randomly as 307. Alice wants to protect the message 320 during communication. How elgamal digital signature scheme will help for his requirement? Show both sender side and receiver side operations in this case. (5)

4B)	Let K_A be the public key of Alice and K_B be the public key of bob. Using challenge response authentication, how both Alice and Bob authenticate with each other. Illustrate with suitable message exchange.	(3)
4C)	Let Alice be the client who want to securely communicate with Bob using SSL. The cipher suite exchanged between Alice and Bob is SSL_DH_anon_WITH_DES_CBC_SHA. Illustrate with suitable message exchange, how premaster key is established between Alice and Bob.	(2)
5A)	Articulate with suitable example, the significance of X.509. Write the X.509 certificate format and certificate revocation format. Also explain the scenarios where the certificates need to be revoked.	(5)
5B)	Demonstrate the working of signature based intrusion detection system with suitable example.	(3)
5C)	Write the fields of Record Protocol Header (RPH) along with SSL payload, when SSL payload of Record protocol carries the data from Alert protocol	(2)

-----End-----