Indian Institute of Technology Patna
Date: 23 Feb 2025
MIDSEM: CS 457: Big Data Security

DURATION: 2 HOURS. 430-630PM

Full Marks 10

Instruction: All questions are compulsory. No Free hand diagrams allowed. If free hand diagrams are seen, you will be penalized 50% of marks. No doubts would be entertained. Write suitable assumptions, if necessary. Students are allowed to use scientific calculators. Each question from Q1 should start on a fresh page. So if the Q1 takes 1/2 page to finish, begin Q2 from the next page. **If two questions are written on the same page, both will be marked 0.**

Q(1) Describe the CIA triad using Venn Diagram. Explain each of the CIA what it stands for. Which technique can help you preserve CIA. **[Marks 10]**

Q(2) Explain substitution cipher using an example? What are the flaws in it? How can 'n' substitution ciphers help improve it? **[Marks 10]**

Q(3) In a RSA cryptosystem a particular A uses two prime numbers p = 13 and q =17 to generate her public and private keys. If the public key of Ais 35. Then the private key of A is ? Show detailed steps. **[Marks 10]**

Q(4) Using the RSA public key cryptosystem, with a = 1, b = 2, ..., y = 25, z = 26. Using p = 3, q = 11, and d = 9, find e and encrypt "hello". Assume suitable assumption. No doubts to be cleared. **[Marks 10]**

Q(5) Show a schematic diagram explaning Digital signatures. What all features does a digital signature provide? **[Marks 10]**

Q(6) Dr. Meenal, a cybersecurity researcher working with UIDAI (Aadhaar authority), is tasked with encrypting biometric data using a high-security symmetric encryption standard. Which encryption algorithm would best ensure data confidentiality for Aadhaar biometrics? A) Blowfish with 56-bit keys B) AES with 256-bit keys C) Triple DES (3DES) with 112-bit keys D) SHA1 Hashing. Justify your answer. **[Marks 10]**

Q(7) Mohan, a cybersecurity expert at an Indian bank, needs to encrypt customers' transaction data using a symmetric key algorithm to ensure confidentiality. He decides to use AES-256 for encryption. Which of the following best describes the reason Rajiv prefers AES over DES for banking transactions? A) AES has a smaller key size, making it more efficient than DES. B) AES is more resistant to brute-force attacks due to a larger key space. C) AES uses asymmetric key exchange, making it safer than symmetric encryption. D) AES is optimized for hashing and not encryption. Justify your answer. **[Marks 10]**

Q(8) Rahul and Priya are two researchers working on a top-secret project. They need to exchange sensitive information over an insecure channel. They decide to use AES-128 in CBC mode with a random initialization vector (IV) for encryption. However, due to a misunderstanding, Rahul uses a 128-bit key, while Priya uses a 256-bit key. Unbeknownst to them, the 256-bit key used by Priya is actually a concatenation of two 128-bit keys, where the first 128 bits are identical to Rahul's key. What is the most likely outcome when Priya tries to decrypt the ciphertext encrypted by Rahul? A) The decryption will succeed, and Priya will obtain the original plaintext. B) The decryption will fail, and Priya will obtain gibberish. C) The decryption will partially succeed, and Priya will obtain a corrupted version of the plaintext. D) The decryption will succeed, but Priya will obtain plaintext that is different from the original plaintext. Justify your answer. **[Marks 10]**

Q(9) A company is using a symmetric encryption algorithm with a 128-bit key to protect their sensitive data. However, they are concerned about the security of their key management process. Which of the following attacks is most likely to compromise their encryption key? A) Brute-force attack B) Side-channel attack C) Man-in-the-middle attack D) Replay attack. Justify your answer. **[Marks 10]**

Q(10) Why cant hashing be used for encryption? Since its one way and difficult to decrypt, it should be easier to use than cryptography. Justify your answer. **[Marks 10]**