



JK LakshmiPat University, Jaipur
Institute of Engineering and Technology
Introduction to Cryptography (CS1229)
End Semester Examination, B.Tech., VI Semester

Date: May 05, 2025

Duration: 2.5 hours

MM: 30

There are three questions in this paper with sub-parts. You have to attempt all the questions. The simple pocket calculator and Casio FX-82MS version are allowed in the examination.

1. Explain the following: (1x6 - COs 1,2,3)

- (a) What are some of the key challenges associated with Bitcoin? List at least four.
- (b) What is Kerckhoff's principle? What is the importance of this principle?
- (c) There are elements in ring Z_4 and ring Z_6 without a multiplicative inverse. Which elements are these?
- (d) Let m be a message consisting of AES blocks (say $m=100$). Alice encrypts using randomized counter mode and transmits the resulting ciphertext to Bob. Due to a network error, ciphertext block number $m/2$ is corrupted during transmission. All other ciphertext blocks are transmitted and received correctly. Once Bob decrypts the received ciphertext, how many plaintext blocks will be corrupted?
- (e) We want to perform an attack on another LFSR-based stream cipher. In order to process letters, each of the 26 uppercase letters and the numbers 0, 1, 2, 3, 4, 5 are represented by a 5-bit vector. We happen to know the following facts about the system:
The degree of the LFSR is $m = 6$.
Every message starts with the header **WPI**.
We observe now on the channel the following message (the fourth symbol is a zero): **j5a0edj2b**. What is the initialization vector?
- (f) Construct the addition and multiplication tables for ring Z_6 .

2. Short Answer Questions: (3 x 5 - COs 1,2,3,4,5)

- (a) Show the two principal attacks against secret prefix and secret suffix MACs:
 $MAC_k(x) = H(k||x)$ (secret prefix)
 $MAC_k(x) = H(x||k)$ (secret suffix)
where $H(x)$ denotes a cryptographically strong hash function based on the Merkle-Damgard construction.
- (b) Compute the encryption (y) of $x = S, Y, M, M, E, T, R, I, C$ with $p = 29$ and $e = 9$. You can assume a simple mapping of letters to numbers, e.g., $A = 0, B = 1, \dots, Z = 25$. Also, compute the corresponding key d for decryption and show that the decryption of y yields the plaintext x .
- (c) Assume you are a hacker and you got access to the hashed password list. Of-course, you would like to recover the passwords from the list in order to impersonate some of the users. Discuss which of the three attacks below allow this.

Exactly describe the consequences of each of the attacks:

Attack A: You can break the one-way property of h .

Attack B: You can find second preimages for h .

Attack C: You can find collisions for h .

- (d) Compute the RSA signatures for the messages x below with the public key $(n,e) = (2183,97)$ and the private key $(d) = (409)$. Check your results by verifying the signatures.
1. $x = 55$
 2. $x = 584$
- (e) Sometimes error propagation is an issue when choosing a mode of operation in practice. In order to analyze the propagation of errors, let us assume a bit error (i.e., a substitution of a "0" bit by a "1" bit or vice versa) in a ciphertext block y_i . Alice is sending messages to Bob.
1. Assume an error occurs during the transmission in one block of ciphertext, let's say y_i . Which plaintext blocks are affected on Bob's side when using the ECB mode?
 2. Again, assume block y_i contains an error introduced during transmission. Which plaintext blocks are affected on Bob's side when using the CBC mode?
 3. Suppose there is an error in the plaintext x_i on Alice's side. Which plaintext blocks are affected on Bob's side when using the CBC mode?

3. Long Answer Questions:

(4+5 - CO 3, 4)

- (a) Compute the following exponentiations $x^e \bmod m$ applying the square-and-multiply algorithm: $x = 8$, $e = 127$, $m = 151$
After every iteration step, show the exponent of the intermediate result in binary notation.
- (b) What is a digital signature, and how does it ensure authenticity, integrity, and non-repudiation in cryptographic communication? Describe the basic RSA digital signature protocol. Additionally, what are the main types of existential forgeries that can occur in RSA digital signatures, and how can they be prevented?