

(49)



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

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. Answer the following: (1x5 - COs 2,3,4)

- (a) Explain how AES-GCM mode provides both confidentiality and authentication.
- (b) Explain how blockchain and Proof-of-Work ensure security and integrity in Bitcoin transactions.
- (c) Describe the TLS handshake process and explain how session keys are securely established.
- (d) Explain how the Signal Protocol achieves end-to-end encryption and forward secrecy in secure messaging.
- (e) Why must p and q (RSA parameters) be distinct primes? Why is it a bad idea to choose $p = q$?

2. Short Answer Questions: (3x5 - COs 1,2,3,4)

- (a) Suppose you want to enforce password rules such that at least 2^{128} passwords satisfy the rules. Determine the minimum password length required in each of the following cases:
 - (a) Passwords consist of only lowercase letters $a-z$ only.
 - (b) Passwords consist of lowercase and uppercase letters $a-z$ and $A-Z$.
 - (c) Passwords consist of lowercase/uppercase letters and digits 0-9.
 - (d) Passwords consist of lowercase/uppercase letters, digits, and all symbol characters appearing on a standard keyboard (assume there are 33 printable symbols).
- (b) What is so special about defining the One-Time Pad (OTP) using the XOR operation? Suppose we use the bitwise-AND operation (denoted by '&') and define a variant of OTP as follows:

KeyGen:

$$k \leftarrow \{0, 1\}^\ell$$

Enc($k, m \in \{0, 1\}^\ell$):

$$c = k \& m$$

Is this still a good choice for encryption? Justify your answer.

- (c) Explain what is wrong in the following argument:

In Diffie-Hellman Key Agreement (DHKA), Alice sends

$$A = g^a \bmod p$$

and Bob sends

$$B = g^b \bmod p.$$

Their shared key is

$$K = g^{ab} \bmod p.$$

To break the scheme, the eavesdropper can simply compute

$$A \cdot B = (g^a)(g^b) = g^{ab}.$$

Why is this argument incorrect?

- (d) Differentiate between RSA encryption and RSA digital signature. Explain the RSA digital signature process with an example.
- (e) Explain the concept of Message Authentication Code (MAC). How can length extension attacks compromise insecure hash-based MAC constructions? Illustrate with an example.

3. Long Answer Questions:

(5x2 - CO 4, 5)

- (a) Consider an RSA cryptosystem with the following parameters:

$$p = 13, \quad q = 17, \quad e = 5$$

1. Compute the RSA modulus n , Euler's totient function $\phi(n)$, and the private key d .
2. Encrypt the plaintext message

$$M = 11$$

using the RSA public key.

3. Decrypt the obtained ciphertext using the square-and-multiply algorithm. Show all intermediate steps and represent the exponent in binary form.
- (b) Explain how the security of the Diffie-Hellman Key Exchange depends on the hardness of the Discrete Logarithm Problem (DLP). Discuss the role of group size and generator selection in preventing discrete logarithm attacks. Also describe how a man-in-the-middle attack can compromise Diffie-Hellman without solving the DLP, and suggest suitable security mechanisms to prevent such attacks.