Department of Computer Science and Engineering
Central Institute of Technology Kokrajhar

End Semester Examination
M. Tech

Course Title: **Advanced Cryptography and Network Security** Course Code: **PCSE311**
Session: **July-Dec, 2024** Full Marks: **100** Time: **3:00** hrs

---

Figure in the margin indicates full marks. Answer any five questions!

1 Fill in the blanks 2 x 10 = 20

a. In _____ encryption, the same key is used for both encryption and decryption.
b. The Advanced Encryption Standard (AES) operates on a fixed block size of _____ bits.
c. In RSA, the security relies on the difficulty of the _____ problem.
d. _____ is an algorithm used in asymmetric cryptography which uses elliptic curves.
e. The _____ problem is fundamental to the security of many public-key cryptographic systems.
f. Given g, g^a mod p, finding 'a' is known as computing the _____ logarithm.
g. ECC provides equivalent security with smaller key sizes compared to traditional systems like RSA due to the difficulty of solving the _____ problem on elliptic curves.
h. An elliptic curve is defined by the equation y^2 = x^3 + ax + b, where 4a^3 + 27b^2 ≠ _____.
i. _____ is the process where two parties each generate a public/private key pair and exchange their public keys to establish a shared secret key.
j. The _____ attack involves trying every possible key until the correct one is found, which is impractical for well-designed cryptographic systems.

2 5 x 4 = 20

a. Describe the main weakness of the Caesar Cipher.
b. What property makes a cryptographic hash function secure against collisions?
c. Why does RSA require the use of large prime numbers?
d. How do asymmetric and symmetric encryption systems typically work together in secure communication?

3 10 + 10 = 20

a. Compute $GCD(6622, 645)$ and $77^{-1}\ mod\ 411$
b. An integer $x, 0 \leq x < 210$, satisfies the following set of congruences

$$x \equiv 4\ (mod\ 5)$$
$$x \equiv 3\ (mod\ 6)$$
$$x \equiv 2\ (mod\ 7)$$

What is x?

4	a.	What is a Discrete Logarithm? Explain Diffie Hellman Key Exchange algorithm with a diagram.	10 + 10 = 20
	b.	Explain El-Gamal Algorithm for encrypting and decrypting the messages.	
5	a.	Explain RSA Algorithm?	10 + 10 = 20
	b.	For a particular communication a Ciphertext = 5 was intercepted using a modulus n = 77 and public key e = 7. Calculate the plaintext.	
6	a.	Explain Point addition operation on Elliptic Curve over Real Values.	10 + 10 = 20
	b.	Find whether the following Elliptic Curves are self-intersecting or not i. EC (-5, 8) ii. EC (-5, 3) iii. EC (-3, 2) iv. EC (-5, -2)	
7		Write short notes on any four a. Schnorr Algorithm b. Digital Signature c. Hashing Function d. DES e. AES	5 x 4 = 20

xxXxx