2/11

2503N1097

Candidate's Seat No :_____

M.Sc. Sem.-3 Examination

501

AMS

Time : 2-30 Hours] **March-2025** **[Max. Marks : 70**

Instructions: All questions are compulsory. Use of non-programmable scientific calculator is allowed.

Q.1 **(a)** Bob is using the Caesar cipher to encrypt the message: "SECRET KEY IS ABC". What will be the ciphertext? **(07)**

(b) Discuss the types of random number generators (RNGs) in detail. **(07)**

OR

(a) Jimmy has received ciphertext "LORYHFUBSWRJUDSKB". Show how he can use an exhaustive key search to break this shift cipher. i.e. By taking key $K = 1,2,3,\ldots,26.$ $(Hint: K < 5)$ **(07)**

(b) Introduce the stream cipher and show that encryption and decryption are the same function for the stream cipher. **(07)**

Q.2 **(a)** Define Confusion and Diffusion operations and give an overview of DES algorithm. **(07)**

(b) Define and provide an example of extension field $GF(2^m)$ with its operation addition and multiplication. **(07)**

OR

(a) Explain the internal structure of Advance Encryption Standard. **(07)**

(b) Explain the f-function of DES algorithm with proper diagram. **(07)**

Q.3 **(a)** Write down the key generation, encryption and decryption process of RSA algorithm. **(07)**

(b) Define cyclic group and primitive element then find all the primitive elements of z_{11}^*. **(07)**

OR

(a) Discuss the difference between symmetric and asymmetric key cryptography in detail. **(07)**

(b) Using the protocol of Diffie–Hellman Key Exchange find the session key K_{AB} for $p = 17,\ \alpha = 11,\ a = 9,\ b = 14.$ **(07)**

Q.4 **(a)** Give the definition of Elliptic Curve and for given $E: y^2 \equiv x^3 + 2x + 2\ (mod\ 17)$, $P = (5,1), Q = (3,1)$ find $2P$ and $P + Q$. **(07)**

(b) Explain ElGamal Digital Signature Algorithm. **(07)**

OR

(a) Discuss in brief: The digital signature security services. **(07)**

(b) Calculate 26P for binary representation using Double-and-Add algorithm. **(07)**

(P.T.O)

Q.5 Attempt any **SEVEN** out of **TWELVE:** **(14)**

(1) Give definition of Group and Ring.

(2) Define: Affine Cipher.

(3) Discuss in brief: LFSRs.

(4) Draw a diagram of Feistel structure of DES.

(5) Briefly explain Brute-Force Attack.

(6) Give an overview of AES.

(7) Calculate $gcd\ (973, 301)$ using Euclidean Algorithm.

(8) Define Elliptic Curve Diffie–Hellman Key Exchange (ECDH).

(9) Define square-and-multiply algorithm and give an example.

(10) State the Hasse's theorem on bound of $\#E$.

(11) Define Discrete Logarithm Problem.

(12) Give an overview of Hash function.

**** ****