CBCS SCHEME

USN 15EC744

Seventh Semester B.E. Degree Examination, July/August 2022
Cryptography

Time: 3 hrs. Max. Marks: 80

Note: Answer any FIVE full questions, choosing ONE full question from each module.

Module-1

1 a. Explain the concept of Greatest Common Divisor with respect to Euclidean Algorithm with suitable example. **(05 Marks)**

b. Briefly explain the properties of modular arithmetic, write the table of addition modulo 8. **(07 Marks)**

c. Find GCD (2740, 1760). **(04 Marks)**

OR

2 a. Discuss the properties of Groups, Rings and Fields. **(06 Marks)**

b. What are finite fields of the form GF(P) and explain finding the multiplicative inverse in GF(P). **(05 Marks)**

c. Write a note on Finite field of the form $GF(2^n)$. **(05 Marks)**

Module-2

3 a. Explain with a neat sketch the symmetric Cipher model. **(05 Marks)**

b. List out various techniques used in symmetric ciphers. Explain the substitution technique with an example. **(06 Marks)**

c. Encrypt the plain text "SECURITY" using Hill Cipher technique key $= \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$. **(05 Marks)**

OR

4 a. Compare Stream Cipher with Block Cipher. **(04 Marks)**

b. Briefly explain with relevant diagrams the Feistel encryption and decryption. **(06 Marks)**

c. What is DES? Explain in detail the DES encryption algorithm. **(06 Marks)**

Module-3

5 a. List difference between DES and AES. **(03 Marks)**

b. With a neat sketch, explain in detail the steps involved in encryption and decryption process of AES. **(09 Marks)**

c. Write a note on AES key expansion algorithm. **(04 Marks)**

OR

6 a. Explain the importance of Linear congruential generators. Why these generators cannot be used for cryptography. **(04 Marks)**

b. What are linear feed back shift generators? List different types available. **(05 Marks)**

c. Explain with relevant sketches : (i) Geffe Generator (ii) Gollmann cascade. **(07 Marks)**

Module-4

7 a. If 'P' is prime and 'a' is a positive integer not divisible by 'P'. Then, prove $a^{P-1} \equiv 1 (\text{mod } P)$. **(05 Marks)**

b. Write an explanatory note on Chinese Remainder Theorem. **(05 Marks)**

c. Briefly explain the concept of Discrete Logarithm and show how it is useful in cryptography. **(06 Marks)**

OR

8 a. What is Public Key Cryptography. With relevant steps explain the concept of RSA key generation, encryption and decryption. **(05 Marks)**

b. Users A and B use D-H key exchange technique with common prime $Q = 353$ and primitive root $\alpha = 3$. A and B selects their secret keys as $X_A = 97$ and $X_B = 233$ respectively, then compute the public keys Y_A and Y_B also calculate the common secret key 'K'. **(06 Marks)**

c. Write a note on Elleptic curve cryptography. **(05 Marks)**

Module-5

9 a. What are Hash functions, explain in detail SNEFRU? **(05 Marks)**

b. With a suitable diagram, Explain the concept of MD5. **(05 Marks)**

c. Explain with a neat diagram, one SHA operation. **(06 Marks)**

OR

10 a. Explain the steps involved in generation of DSA signature. **(06 Marks)**

b. Give details about security of DSA. **(05 Marks)**

c. Write a note on Discrete Logarithm signature scheme. **(05 Marks)**

* * * * *