CBCS SCHEME

USN | | | | | | | | | | |

17EC744

Seventh Semester B.E. Degree Examination, July/August 2021
Cryptography

Time: 3 hrs. Max. Marks: 100

Note: ***Answer any FIVE full questions.***

1 a. Explain the working of Euclidean algorithm with a neat flow chart. **(15 Marks)**
b. Demonstrate with an example. Write the properties of Congruence's. **(05 Marks)**

2 a. Explain Groups, Rings and Field with axioms. **(15 Marks)**
b. Demonstrate cyclic subgroup with an example. **(05 Marks)**

3 Encrypt the plaintext "MONDAY". Using HILL cipher with the given key. Show the calculation for Encryption and Decryption (Hint : a = 0, b = 1.....z = 25)
Key : $\begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$. Note : Show all the matrix calculation steps. **(20 Marks)**

4 Describe the working Data Encryption Standards (DES) and Feistel Cipher with neat diagram. **(20 Marks)**

5 Explain the AES Encryption process with a neat diagram. **(20 Marks)**

6 a. Explain stream Cipher with neat diagram. Highlight the two advantages and disadvantages over Block cipher. **(10 Marks)**
b. Describe the working of Threshold generator and Geffe Generator with necessary diagrams. **(10 Marks)**

7 a. Derive the proof of Euler's theorem and also determine $\phi(37)$ and $\phi(35)$. **(10 Marks)**
b. Explain what is Chinese Remainder theorem and steps involved. **(10 Marks)**

8 a. Demonstrate the Diffie-Hellman key Exchange with an example. **(10 Marks)**
b. Briefly explain the Elliptic curve cryptography and mention 2 applications. **(10 Marks)**

9 Explain the principle of Message Authentication Code (MAC) with a neat block diagram. Mention the limitations. **(20 Marks)**

10 a. Describe the working of MD4, MD5 hash functions with neat diagram. **(12 Marks)**
b. Write the DSA digital signature algorithm signature. **(08 Marks)**

* * * * *