CBCS SCHEME

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

17TE71

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

Time: 3 hrs. Max. Marks: 100

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

Module-1

1 a. Explain the concept of divisibility and the division algorithm. **(10 Marks)**

b. State and prove Fermat's and Euler's theorem for public-key cryptography. **(10 Marks)**

OR

2 a. Construct the addition, multiplication and inverses table for Arithmetic in $GF(2^3)$. **(06 Marks)**

b. Mention the Modular Arithmetic Operation properties and prove the same. **(08 Marks)**

c. Explain the following terminologies:
(i) Symmetric Algorithms (ii) Asymmetric Algorithms **(06 Marks)**

Module-2

3 a. With a neat diagram, explain DES encryption process. **(10 Marks)**

b. Explain with a neat diagram the detailed structure of AES cipher. **(10 Marks)**

OR

4 a. Explain the Requirements of public-key cryptography. **(06 Marks)**

b. Describe the RSA algorithm with an example. **(08 Marks)**

c. Explain Elliptic curves over Zp. **(06 Marks)**

Module-3

5 a. Explain the concept of N-Hash with a neat diagram. **(10 Marks)**

b. Explain the following one-way hash functions using symmetric block algorithms:
(i) Tandem and Abreast Davies Meyer (ii) MDC-2 and MDC-4 **(10 Marks)**

OR

6 a. With a neat diagram, explain the operation Secure Hash Algorithm (SHA). **(10 Marks)**

b. Explain Discrete Logarithm Signature Schemes. **(10 Marks)**

Module-4

7 a. Give a comparision on Treats on the web. **(06 Marks)**

b. Explain the Record Protocol of Secure Sockets Layer (SSL). **(08 Marks)**

c. Explain the Alert codes supported by Transport Layer Security (TLS). **(06 Marks)**

OR

8 a. Explain the phase 1 (Establish Security Capabilities) of Handshake Protocol. **(10 Marks)**

b. Describe the concept of HTTPs. **(10 Marks)**

Module-5

9 a. Explain Pretty Good Privacy (PGP) for providing cryptographic functions like authentication, confidentiality and both with a neat diagram. **(10 Marks)**

b. What are the two databases of IP Security policy and explain them. **(10 Marks)**

OR

10 a. Illustrate the working of transport and tunnel mode Encapsulating Security Payload (ESP). **(10 Marks)**

b. With a neat diagram, describe Header and Payload Formats of Internet Key Exchange (IKE). **(10 Marks)**

* * * * *