CBCS SCHEME

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

15CS61

Sixth Semester B.E. Degree Examination, Jan./Feb. 2023
Cryptography, Network Security and Cyber Law

Time: 3 hrs. Max. Marks: 80

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

Module-1

1 a. Explain common cyber attacks. **(04 Marks)**

b. Explain Extended Euclidean Algorithm. Using the extended Euclidean algorithm, compute the inverse of 12 modulo 79. **(06 Marks)**

c. Define :

i) Group and Chinese remainder theorem

ii) Let N = 210 and let $n_1 = 5$, $n_2 = 6$, $n_3 = 7$, $x_1 = 3$, $x_2 = 5$, $x_3 = 2$. Compute f^{-1} (3, 5, 2) and x using Chinese remainder theorem. **(06 Marks)**

OR

2 a. Explain the following Ciphers with example

i) Mono-alphabetic ciphers

ii) The Vigenere cipher

iii) A transposition cipher

iv) Hill cipher **(08 Marks)**

b. With a neat diagram, explain the construction of DES (Data Encryption Standard) **(08 Marks)**

Module-2

3 a. Explain key generation, encryption and decryption RSA operations. Using RSA algorithm encrypt and decrypt the message 00111011, assume prime numbers p = 3 and q = 11 and public key e = 3. **(10 Marks)**

b. With a neat diagram, explain the computation of Secure Hash Algorithm (SHA – 1) **(06 Marks)**

OR

4 a. With a neat diagram, explain Diffie- Hellman Key Exchange protocol and man in the middle attack on Diffie-Hellman key exchange. **(08 Marks)**

b. Explain EL Gamal Encryption algorithm. Give an example. **(08 Marks)**

Module-3

5 a. Explain Public Key Infrastructure (PKI) Architectures with a help of neat diagrams. **(05 Marks)**

b. With a neat diagram, explain password based and certificate based on way Authentication. **(06 Marks)**

c. Explain Preliminary version 1 of the Needham-Schroeder protocol. **(05 Marks)**

OR

6 a. Explain IPSec IN ACTION. (10 Marks)
b. Explain SSL hand shake protocol. (06 Marks)

Module-4

7 a. Explain how Authentication is dealt in 802.11. (05 Marks)
b. In detail explain virus and worm features. (05 Marks)
c. Explain worm propagation models. (06 Marks)

OR

8 a. Explain DDOS Attack Prevention/Detection (08 Marks)
b. Explain Various technologies for web services. (08 Marks)

Module-5

9 a. Explain important provisions of the Information Technology (IT) Act. (06 Marks)
b. Explain Digital Signature certificates. (04 Marks)
c. Explain Penalties and Adjudication of IT Act. (06 Marks)

OR

10 a. Explain Regulations of certifying Authorities. (10 Marks)
b. Mention the cyber Regulations Appellate Tribunal. (06 Marks)

* * * * *