CBCS SCHEME

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

15CS61

Sixth Semester B.E. Degree Examination, Dec.2019/Jan.2020
Cryptography, Network Security and Cyber Laws

Time: 3 hrs. Max. Marks: 80

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

Module-1

1 a. What do you mean by cyber attack? List and explain main motives of launching cyber attacks. **(08 Marks)**

b. Using Extended Euclidean algorithm find the inverse of 12 modulo 79. **(08 Marks)**

OR

2 a. Design known plain test attack to obtain the key used in the Vigenere cipher. **(08 Marks)**

b. Consider a Hill cipher m = 3 (block size = 3) with key k shown below:

$$k = \begin{pmatrix} 25 & 3 & 7 \\ 5 & 9 & 21 \\ 11 & 8 & 13 \end{pmatrix}$$

(i) What is the cipher text corresponding to the plaintext = (VOW)?

(ii) What is the plain text corresponding to the ciphertext = (TQX)? **(08 Marks)**

Module-2

3 a. List and explain RSA operations. **(08 Marks)**

b. The modulus in a toy implementation of RSA is 143

(i) What is the smallest value of a valid encryption key and the corresponding decryption key?

(ii) For the computed encryption key and plaintext = 127, what is the corresponding ciphertext? **(08 Marks)**

OR

4 a. In what way are the properties of the cryptographic hash – the one way property and collision resistance relevant to the security provided by the MAC? Explain. **(08 Marks)**

b. Consider the digital signature created using the Signer's private key operation but without the hash function i.e., sign(m) = $E_{A.pr}(m)$

Demonstrate how a forged signature may be created using this definition of a digital signature. **(08 Marks)**

Module-3

5 a. What do you mean key management? Explain the fields of an X.509 certificate. **(06 Marks)**

b. List and explain PKI Architectures. **(06 Marks)**

c. Define Dictionary Attacks. Explain Attack types. **(04 Marks)**

OR

6 a. Design the Needham – Schroeder protocol. **(06 Marks)**

b. Define Kerberos. Explain Kerberos message sequence. **(05 Marks)**

c. Explain SSL Record Layer Protocol. **(05 Marks)**

Module-4

7	a.	Explain how each key in 802.11i was derived and where it is used.	(06 Marks)
	b.	Define Firewall. List and explain main functions of a firewall.	(06 Marks)
	c.	Classify Intrusion Detection Systems based on their functionality.	(04 Marks)

OR

8	a.	What is the role of a Bloom Filter in packet logging?	(04 Marks)
	b.	Define SOAP. Explain SOAP messages in HTTP packets.	(08 Marks)
	c.	Demonstrate WS-Trust relationship between entities involved in international trade.	(04 Marks)

Module-5

9	a.	List and explain IT act aim and objectives.	(04 Marks)
	b.	Explain (i) Secure electronic record (ii) Secure digital signature	(04 Marks)
	c.	List and explain Functions of a controller.	(08 Marks)

OR

10	a.	List and explain offences with reference to computer system.	(06 Marks)
	b.	When network service providers not to be liable under IT Act? Explain.	(04 Marks)
	c.	What are miscellaneous provisions of IT Act? Explain.	(06 Marks)

* * * * *