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)

* * * * *

CBCS SCHEME

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

15CS61

Sixth Semester B.E. Degree Examination, June/July 2019
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. Describe the types of Vulnerabilities to domain of security. (04 Marks)
b. List the guiding principles of security. (04 Marks)
c. Write the extended Euclidean algorithm, with an example. (08 Marks)

OR

2 a. Calculate the value of x using Chinese remainder theorem by given below data :
$N = 210$, $n_1 = 5$, $n_2 = 6$, $n_3 = 7$, $x_1 = 3$, $x_2 = 5$, $x_3 = 2$. (05 Marks)
b. Explain the Vigenere Cipher and the Hill Cipher techniques with illustration. (06 Marks)
c. With neat diagram, explain Fiestel structure. (05 Marks)

Module-2

3 a. Illustrate the RSA algorithm for encryption and decryption. (08 Marks)
b. Briefly explain the practical issues of RSA algorithm. (04 Marks)
c. List the properties of the cryptographic hash. (04 Marks)

OR

4 a. Discuss the case study : SHA – 1. (08 Marks)
b. Explain the Man – In – the Middle attack on Diffie – Hellman key exchange, with neat diagram. (08 Marks)

Module-3

5 a. Explain the different Public Key Infrastructure (PKI) architectures. (08 Marks)
b. Describe the Mutual authentication using a shared secret. (08 Marks)

OR

6 a. Explain the Kerberos message sequence with diagram. (06 Marks)
b. Describe the IP Sec protocols Authentication Header and Encapsulating Security Pay load in transport mode. (05 Marks)
c. Explain Secure Sockets Layer (SSL) hand shake protocol. (05 Marks)

Module-4

7 a. Explain the Authentication and Master Session Key exchange in 802.11i. (05 Marks)
b. List and explain the worm characteristics. (05 Marks)
c. Explain Firewall functionality and Proxy fire wall. (06 Marks)

OR

8 a. Write a note on Intrusion Detection System (IDS). (05 Marks)
b. Explain the types of Intrusion Detection System. (05 Marks)
c. Briefly explain the Technologies for Web Services. (06 Marks)

Module-5

9 a. Explain Digital Signature Certificates. (10 Marks)
b. Describe the duties of Subscribers. (06 Marks)

OR

10 a. List any eight functions of the Controller. (08 Marks)
b. Briefly explain Penalties and Adjudication in IT Act. (08 Marks)

* * * * *

CBCS SCHEME

USN | | | | | | | | | | 15CS61

Sixth Semester B.E. Degree Examination, Dec.2018/Jan.2019
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.

Important Note : 1. On completing your answers, compulsorily draw diagonal cross lines on the remaining blank pages.
2. Any revealing of identification, appeal to evaluator and /or equations written eg, 42+8 = 50, will be treated as malpractice.

Module-1

1 a. Define cyber security? Explain the motives of cyber attack. **(05 Marks)**
b. Use extended Euclidean algorithm to find inverse of 12 modulo 79? **(05 Marks)**
c. Apply Chineese reminder theorem to find square roots of 3 modulo 143 and list all square roots of -3 modulo 143. **(06 Marks)**

OR

2 a. Explain DES construction in detail. **(05 Marks)**
b. Explain confusion and Diffusion with example. **(05 Marks)**
Explain three sounds SPN Network. **(06 Marks)**

Module-2

3 a. Explain RSA operation in detail. **(06 Marks)**
b. Explain Public Key Cryptography Standards (PKCS) **(10 Marks)**
c. Explain Deffie Helman key exchange.

OR

4 a. If the RSA public key is (31, 3599) what is the corresponding private key. **(05 Marks)**
b. Explain Basic properties of hash function. **(05 Marks)**
c. Explain Birthday attack. **(06 Marks)**

Module-3

5 a. Explain identity based encryption. **(05 Marks)**
b. Explain Needham Schroeder protocol version – 1. **(05 Marks)**
c. Explain Kerberos with message sequence. **(06 Marks)**

OR

6 a. Explain password based one way authentication. **(05 Marks)**
b. Explain Needham – Schroeder protocol version – 2. **(05 Marks)**
c. Explain SSL Handshake protocol. **(06 Marks)**

Module-4

7 a. Explain authentication and master session key exchange in 802.11i? **(05 Marks)**
b. Explain worm features. **(05 Marks)**
c. Explain Function of Firewall. **(06 Marks)**

OR

8 a. Explain 802.11i four way handshanke with neat diagram. **(05 Marks)**
b. List and explain practice issues of Firewall. **(05 Marks)**
c. Explain DDOS attack prevention and detection. **(06 Marks)**

Module-5

9 a. Discuss OFFENES defined as per IC Act 2000 (any Four) **(08 Marks)**

b. Explain briefly certifying authority, suspensions, and revocations of digital signature. **(08 Marks)**

OR

10 a. What is information technology act? Discuss scope and objectives. **(08 Marks)**

b. Discuss the provisions of the IT act as regards to the following :

i) Legal Recognition of Electronic records

ii) Authentication of electronic records. **(08 Marks)**

* * * * *