

USN	1
Sixth Semester B.E. Degre	ee Examination, Dec.2019/Jan.2020
BANGA Cryptography, Netwo	rk Security and Cyber Laws

Time: 3 hrs.

OF TEO

Max. Marks: 80

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

Module-1

- What do you mean by cyber attack? List and explain main motives of launching cyber 1 (08 Marks)
  - Using Extended Euclidean algorithm find the inverse of 12 modulo 79.

(08 Marks)

15CS61

- OR Design known plain test attack to obtain the key used in the Vigenere cipher. (08 Marks)
  - 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 List and explain RSA operations.

(08 Marks)

- The modulus in a toy implementation of RSA is 143
  - What is the smallest value of a valid encryption key and the corresponding decryption key?
  - For the computed encryption key and plaintext = 127, what is the corresponding (ii) ciphertext? (08 Marks)

## OR

- 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.
  - 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

- What do you mean key management? Explain the fields of an X.509 certificate. 5 (06 Marks)
  - List and explain PKI Architectures. b. C.

(06 Marks)

Define Dictionary Attacks. Explain Attack types.

(04 Marks)

## OR

Design the Needham – Schroeder protocol. 6 a.

(06 Marks)

Define Kerberos. Explain Kerberos message sequence. b.

(05 Marks)

Explain SSL Record Layer Protocol.

(05 Marks)

	Module-4	
7		Iarks)
		Iarks)
	c. Classify Intrusion Detection Systems based on their functionality. (04 M	Iarks)
8	a. What is the role of a Bloom Filter in packet logging? (04 N	(Lawles)
0		Iarks)
	c. Demonstrate WS-Trust relationship between entities involved in international trade.	(Iarks
		(Iarks
		,
	Module-5	
9		(arks
		(Iarks
	c. List and explain Functions of a controller. (08 N	Iarks)
10	OR	
10	1 J	Iarks)
		Iarks)
	c. What are miscellaneous provisions of IT Act? Explain. (06 N	Iarks)
	****	
	A A CONTRACTOR OF THE CONTRACT	
	2 of 2	
	2 01 2	
	2 of 2	