Reg No.:_____ Name:_____

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

EIGHTH SEMESTER B.TECH DEGREE EXAMINATION, MAY 2019

Course Code: IT402

Course Name: CRYPTOGRAPHY & CYBER SECURITY

Max. Marks: 100 Duration: 3 Hours

PART A

Answer any two full questions, each carries 15 marks.

			Marks
1	a)	Compute gcd (42, 105, 91).	(5)
	b)	Compute 33^{100} (mod 40) (use Euler's theorem).	(3)
	c)	Explain with examples some of the attacks threatening confidentiality and integrity.	(7)
2	a)	Compute gcd(85,289). Using Euclid's extended algorithm compute x and y such that 85x + 289y = gcd(85, 289).	(6)
	b)	Explain about the different types of cryptanalysis attacks. Give examples	(9)
3	a)	Find the value of x for the set of congruence given using Chinese Remainder Theorem. x≡4 mod 5, and x≡ 10 mod 11	(6)
	b)	What is quadratic congruence?	(3)
	c)	What is Confusion and Diffusion? How are they achieved?	(6)

PART B

Answer any two full questions, each carries 15 marks.

4	a)	What is an Affine cipher? Encrypt the message "this is an exercise" using Affine cipher with key (15, 20).	(6)
	b)	Distinguish between stream and block ciphers.	(2)
	c)	Illustrate and explain the key generation process in DES.	(7)
5	a)	Using Hill cipher encrypt the message "Hill" with the key matrix K= $\begin{bmatrix} 11 & 8 \\ 3 & 7 \end{bmatrix}$. Perform decryption on the resultant ciphertext and show that original plaintext is retrieved.	(6)
	b)	With diagram and examples for each transformation, explain the structure of each round of AES.	(9)
6	a)	Explain with examples about keyless and keyed transposition ciphers.	(7)
	b)	Explain in detail about Message authentication code (MAC) and security of a MAC.	(8)

PART C

Answer any two full questions, each carries20 marks.

7 a) Explain the key generation process of RSA cryptosystem. Bob chooses p=17 and q= 11 and selects e=7. Find the value of n, $\phi(n)$ and d. (10)

b) What are the different modes of IPSec? (4)

c) What is an intrusion detection system? Explain about its types and usages. (6)

8 a) Differentiate between a conventional encryption system and a public-key encryption system. (4)

b) Alice and Bob use Diffie-Hellman key exchange technique with a common prime 353 and a primitive root α=3. (6)

i) If Alice has a private key X_A= 97, find her public key Y_A.

ii) If Bob has a private key X_B= 233, find his public key Y_B.

iii) What is the shared secret key between Alice and Bob?

c) Illustrate and explain the IPSec architecture. (10)

9 a) Explain in detail about the man-in-the-middle attack on Diffie-Hellman key exchange protocol. (10)

b) Explain the steps for signing and verifying process in RSA digital signature scheme. (6)

c) Explain about different types of distributed denial of service attacks. (4)

****