P P SAVANI UNIVERSITY

Sixth Semester of B. Tech. Examination

November 2022

SEIT3062 Cryptography & Network Security

26.11.2022, Saturday   Time: 01:00 p.m. To 03:30 p.m.   Maximum Marks: 60

Instructions:

1. The question paper comprises of two sections.
2. Section I and II must be attempted in same answer sheet.
3. Make suitable assumptions and draw neat figures wherever required.
4. Use of scientific calculator is allowed.

SECTION – I

Q - 1	Answer the Following: (MCQ/Short Question/Fill in the Blanks)	[05]	CO	BTL
(i)	To provide authentication through public key cryptosystem sender encrypt with sender's private key. TRUE/FALSE		1	2
(ii)	Which formula is used to calculate cipher text in Hill cipher?		1	1
(iii)	Change one bit of the input, at least 50% of the output should be different, this property is called ___________.		3	1
(iv)	___________ is the assurance that someone cannot deny something. a. Access Control b. Integrity b. Non-Repudiation d. Authentication		1	2
(v)	What is the block size of AES-192?		1	1
Q - 2 (a)	Explain any two security attacks in detail.	[05]	3	2
Q - 2 (b)	Discuss single round of Data Encryption Standard with neat sketches.	[05]	1	3
	OR			

Q - 2 (a)	Use Playfair cipher substitution technique and find out cipher text for the following given key and plaintext.
	Key = INDIAN
	Plaintext= PPSAVANIUNIVERSITY
		[05]	2	5

Q - 2 (b)	Explain one round of AES in detail.	[05]	3	3
Q - 3 (a)	In a public key cryptosystem using RSA, sender wants to send message m which is sent to the user whose public key is e=7 and two distinct primes p=11, q=17. Find the Ciphertext only when message M=9.	[05]	2	5
Q - 3 (b)	Find the Inverse of integer value 31 when mod value is 3480 with Extended Euclid Algorithm.	[05]	1	5
	OR			
Q - 3 (a)	Explain various general categories of schemes for the distribution of public keys.	[05]	1	4
Q - 3 (b)	Discuss X.509 Certificate in detail.	[05]	1	2
Q - 4	Attempt any one.	[05]		
(i)	List out block cipher modes of operations and explain any one in detail.		1	2
(ii)	Write the necessary condition to satisfy Groups, Rings and Fields.		1	1

SECTION – II

Q - 1	Answer the Following: (Short Question/Fill in the Blanks)	[05]		
(i)	Define pre-image resistant property of cryptography hash function.		1	1
(ii)	What is the output size of SHA-1 algorithm?		1	1
(iii)	What is the full form of IKE?		1	1
(iv)	Define Firewall.		1	2
(v)	_______is a type of malicious software that infects a computer and restricts users' access to it until a ransom is paid to unlock it.		3	2
Q - 2 (a)	Explain Elgamal digital signature algorithm in detail.	[05]	3	2
Q - 2 (b)	Explain the use of Cipher Block Chaining for generation of hash function.	[05]	3	3

OR

Q - 2 (a)	Draw structure of MAC based on hash functions and explain its components.	[05]	1	2
Q - 2 (b)	Explain any two scenarios where authentication is required to ensure security of the system.	[05]	2	6
Q - 3 (a)	Enlist the characteristics of Hash function. Explain any two properties with suitable example.	[05]	1	2
Q - 3 (b)	Demonstrate the steps involved in Kerberos version 4.	[05]	3	4

OR

Q - 3 (a)	Write a note on AH and ESP.	[05]	1	1
Q - 3 (b)	Write a note on securities at various layers of TCP/IP.	[05]	3	6
Q - 4	Attempt any one.	[05]		
(i)	Write short note on digital signature algorithm.		1	3
(ii)	Describe hand shake protocol of SSL with suitable example.		2	5

****

CO : Course Outcome Number BTL : Blooms Taxonomy Level

Level of Bloom's Revised Taxonomy in Assessment

1: Remember	2: Understand	3: Apply
4: Analyze	5: Evaluate	6: Create