Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

ME - SEMESTER–I(New course)• EXAMINATION – WINTER- 2015

Subject Code: 2710211 **Date: 04/01/2016**

Subject Name: Information Security

Time:2:30 pm to 5:00 pm **Total Marks: 70**

Instructions:

1. **Attempt all questions.**
2. **Make suitable assumptions wherever necessary.**
3. **Figures to the right indicate full marks.**

Q.1 (a)

1. What is steganography? What is its application? **07**
2. What are the applications of public-key cryptosystems?
3. Define a trapdoor one-way function. What is its use in asymmetric-key cryptography?
4. How can we achieve authentication and confidentiality using public key cryptography?
5. What is a public-key certificate? What are the requirements for the use of a public-key certificate scheme?
6. Digital signature does not provide confidentiality. True/False, Justify
7. What is the application of cryptographic hash function?

(b)

1. What requirements should a digital signature scheme satisfy? **02**
2. What is Kerberos? What problem was Kerberos designed to address? **02**
3. What characteristics are needed in a secure hash function? **03**

Q.2 (a)

1. "Arrival of Asymmetric key cryptography has made Symmetric key cryptography obsolete." State True/False with reason. **02**
2. What is the difference between a message authentication code and a one-way hash function? **02**
3. Define the terms diffusion and confusion? How are they important to make algorithm strong? **03**

(b) Draw the block diagram of AES encryption process and briefly explain its transformation functions. **07**

OR

(b) Draw the block diagram of a single round of DES algorithm and briefly explain its key generation process. **07**

Q.3 (a)

1. What is Euler's Totient function (Ǿ)? Find Ǿ(49). **03**
2. Write the Euclid's algorithm and show the steps of Euclid's algorithm to find gcd(1970,1066). **04**

(b)

1. Is Diffie-Hellman key exchange algorithm vulnerable to man in the middle attack? Justify. **03**
2. Why block cipher modes of operations are required? List out them and state the application of each. **04**

OR

Q.3 (a)

1. Users A and B use the Diffie-Hellman key exchange technique with a common prime q = 71 and a primitive root α= 7. If user A has private key XA = 5, what is A's public key YA? If user B has private key XB = 12, what is B's public key YB? What is the shared secret key? **03**
2. Perform encryption and decryption using the RSA algorithm for p=3, q=11, e=7, M=5. **04**

	(b)	1. What do you mean by avalanche effect? What is the difference between differential and linear cryptanalysis?	**03**
		2. What is the difference between an unconditional secure cipher and a computationally secure cipher? Discuss the possible approaches to attack RSA.	**04**
Q.4	**(a)**	What is digital signature? List the security services provided by digital signature. Write and explain the Digital Signature Algorithm.	**07**
	(b)	1. Explain the process of symmetric key distribution using KDC	**03**
		2. Discus the ways in which public keys can be distributed to two communication parties.	**04**
		OR	
Q.4	**(a)**	What is message Digest? Explain the process of message digest generation used in SHA-512.	**07**
	(b)	1. What is the difference between a session key and a master key? Explain decentralized key distribution.	**03**
		2. Briefly explain how session key is distributed in Kerberos.	**04**
Q.5	**(a)**	List out and explain the elements of X.509 certificate.	**07**
	(b)	1. What is SQL slammer? Why was it so successful?	**03**
		2. Briefly discuss various malware detection methods.	**04**
		OR	
Q.5	**(a)**	1. What do you mean by software insecurity in software? What is the role of disassembler and debugger in software insecurity?	**03**
		2. What is malware? List out their types and discuss metamorphic and polymorphic malware.	**04**
	(b)	1. Explain Buffer overflow, Incomplete Mediation and Race Conditions with respect to software flaws.	**03**
		2. Discuss various miscellaneous software based attacks.	**04**

****