Seat No.: _____ *Enrolment No._____*

GUJARAT TECHNOLOGICAL UNIVERSITY

M. E. Sem. – II[nd] - Examination – June/July- 2011

Subject code: 1722302

Subject Name: Advance Cryptography and Information Security

Date:24/06/2011 **Time: 10:30 am – 01:00 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)**	i.	Do pseudorandom numbers pass the tests of randomness? Which parameters are critical in developing a good linear congruential generator?	**04**
		ii.	Which inspection technique is used TCP and higher layer control data for filtering process? Explain.	**03**
	(b)	I.	For which protocol layer following commands are used? a. ipconfig /renew b. ipconfig /release	**04**
		II.	Write a snort rule that filters all the HTTP traffic that is generated by class C address and destination is class B address.	**03**
Q.2	**(a)**	i.	Using Fermat's theorem, find $3^{201} \bmod 11$.	**04**
		ii.	"A customer keeps on adding items to basket in E-commerce site". This leads to which kind of attack and which mode of intrusion detection can detect this attack?	**03**
	(b)	i.	Briefly describe SubBytes and ShiftRows.	**04**
		ii.	What is traffic padding and what is its purpose?	**03**
			OR	
	(b)	i.	Briefly describe MixColumns and AddRoundKey.	**04**
		ii.	What is the difference between a session key and a master key?	**03**
Q.3	**(a)**	i.	RSA algorithm is vulnerable to which cryptanalytic attack? Why?	**04**
		ii.	Encrypt the message "eight oclock" using the Hill cipher with the key $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$.	**03**
	(b)		How diffusion and confusion is achieved in DES(Data Encryption Standard)? Explain single round of DES algorithm.	**07**
			OR	
Q.3	**(a)**	i.	Explain the authentication technique that involves the use of secret key to generate cryptographic checksum that is appended to the message.	**04**
		ii.	Using the playfair matrix with the key "Lieutenant" encrypt the message "nest in tree".	**03**
	(b)		Write the algorithm for finding multiplicative inverse in GF(p). Find the multiplicative inverse of each nonzero element in Z_5.	**07**

Q.4	**(a)**	What is the difference between direct and arbitrated digital signature? Write the Digital Signature Algorithm.	**07**
	(b)	The Miller-Rabin test can determine if a number is not prime but cannot determine if a number is prime. How can such an algorithm be used to test for primality? Write two properties of prime numbers that is needed for Miller-Rabin algorithm.	**07**

OR

Q.4	**(a)**	What is the difference between weak and strong collision resistance? Explain the general principle used in all hash functions.	**07**
	(b)	Illustrate various ways in which a hash code can be used to provide message authentication.	**07**

Q.5	**(a)**	What is dual homed host? Explain a. Screened Subnet b. Split Screened Subnets.	**07**
	(b)	Why do nonessential services appeal to attackers? How services can be enumerated on Domain Controller?	**07**

OR

Q.5	**(a)**	How can it be verified that a machine is connected to SMTP service? Explain how to spoof e-mail. Is it server level or client level threat? List other threats in that category.	**07**
	(b)	Explain cross site scripting attack and explain the countermeasures for this.	**07**

****