Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

M. E. - SEMESTER – II • EXAMINATION – WINTER • 2013

Subject code: 1722302 Date: 27-12-2013

Subject Name: Advance Cryptography and Information Security

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) Does the following inverse exist? If yes, give the inverse. If no, explain why not. **04**

$102^{-1} \pmod{411}$

(ii) Why should an organization employ firewall to secure their network? Give reasons. **03**

(b) Design known plaintext attacks to obtain the key used in the Hill cipher. **07**

Consider a Hill cipher with m=3 with key $K=\begin{pmatrix} 25 & 3 & 7 \\ 5 & 9 & 21 \\ 11 & 8 & 13 \end{pmatrix}$.

What is the ciphertext corresponding to the plaintext "VOWEL"?

Q.2 **(a)** The modulus in an implementation of RSA is 143. **07**

(i) What is the smallest value of a valid encryption key and the corresponding decryption key?

(ii) For the computed encryption key and plaintext=127, what is the corresponding ciphertext?

(iii) For the computed decryption key and ciphertext=2 what is the corresponding plaintext?

(b) Write about the types of intrusion detection systems. **07**

OR

(b) Explain internal structure of single round of DES algorithm. **07**

Q.3 **(a)** **07**

(i) An integer, n, $0 \le n < 210$, satisfies the following set of congruences : **04**

n mod 5=4

n mod 6=3

n mod 7=2

What is n?

(ii) Consider the set of all integers. Is it field? **03**

(b) Describe SubBytes, ShiftRows, MixColumns, AddRoundKey in AES(Advanced Encryption standard). **07**

OR

Q.3 **(a)** **07**

(i) Write the two properties of prime numbers. **04**

(ii) Write the three desirable properties of hash functions. **03**

(b) Explain the Blum Blum shub generator for generating secure pseudorandom number. Why is it referred to as a cryptographically secure pseudorandom bit generator? **07**

Q.4	**(a)**		**07**
		(i) What types of attacks are addressed by message authentication?	**04**
		(ii) What is the difference between direct and arbitrated digital signature?	**03**
	(b)	Explain phishing attack and open mail relay.	**07**
		OR	
Q.4	**(a)**		**07**
		(i) Give examples of replay attacks.	**04**
		(ii) What is the difference between link and end-to-end encryption?	**03**
Q.4	**(b)**	Differentiate between	**07**
		(i) URLEncoding and HTMLEncoding.	
		(ii) innerText and innerHtml property.	
Q.5	**(a)**	Describe the Domain Controller threats.	**07**
	(b)		**07**
		(i) Explain the rule header in snort rules.	**04**
		(ii) Give example of snort rule that uses content keyword.	**03**
		OR	
Q.5	**(a)**	Explain screened host, screened subnet and split screened subnet.	**07**
	(b)		**07**
		(i) Explain depth keyword in snort rule option.	**04**
		(i) Give an example that shows a SYN-FIN scan detection rule in snort.	**03**

****