Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

M.E –IIst SEMESTER–EXAMINATION – JULY- 2012

Subject code: 1722302 Date: 09/07/2012

Subject Name: Advance Cryptography and Information Security

Time: 10:30 am – 13:00 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) **07**

(i) Which four types of transformations are needed in AES(Advance encryption standard)? **04**

(ii) Determine how many of the following integers pass the Miller Rabin primality test: 109,271. **03**

(b) **07**

(i) How do attackers spoof e-mail? **04**

(ii) Distinguish between packet filtering firewalls and stateful packet filtering. **03**

Q.2 (a) For the group G=<Z_6,*,x>: **07**

a. Is it an abelian group?
b. Show the result of 5x1 and 1⁄5
c. Show that why division by zero in this group is not a problem.

(b) **07**

(i) Are all stream ciphers monoalphabetic? Are all block ciphers polyalphabetic? Explain. **04**

(ii) Compare the permutations in DES and AES. Why expansion and compression permutations are needed in DES, but not in AES? **03**

OR

(b) **07**

(i) The encryption key in a transposition cipher is (3,2,6,1,5,4). Find the decryption key. **04**

(ii) Explain pattern matching. **03**

Q.3 (a) **07**

(i) Find the multiplicative inverse of 38 in Z_{180} using the extended Euclidean algorithm. **04**

(ii) Distinguish between Z and Z_n. Which set can have negative integers? How can an integer in Z be mapped to an integer in Z_n? **03**

(b) What is password attack in domain controller threats? Write the countermeasures for this. **07**

OR

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

(i) Find all solutions to each of the following linear equations. **04**

a. $3x \equiv 4 \pmod 5$

b. $9x \equiv 12 \pmod 7$

(ii) Use a Hill Cipher to encipher the message "world". Use the key $\begin{bmatrix} 03 & 02 \\ 05 & 07 \end{bmatrix}$ **03**

(b) What is diffusion and confusion? Explain Fiestel encryption and decryption. **07**

Q.4 **(a)** Which two criteria are used to validate that a sequence of number is random. Distinguish between Psuedorandom Number generators and cryptographically generated random numbers. Give example. **07**

(b) Explain the following two issues of the complexity of the computation required to use RSA. **07**

a. Encryption/decryption

b. Key generation.

OR

Q.4 **(a)** Prove Fermat's and Euler's theorem. Explain Euler's totient function. **07**

Q.4 **(b)** Write the properties needed for a hash function H to be useful for message authentication. Is hash function resistant against birthday attack? **07**

Q.5 **(a)** **07**

(i) What are some threats associated with a direct digital signature scheme? **04**

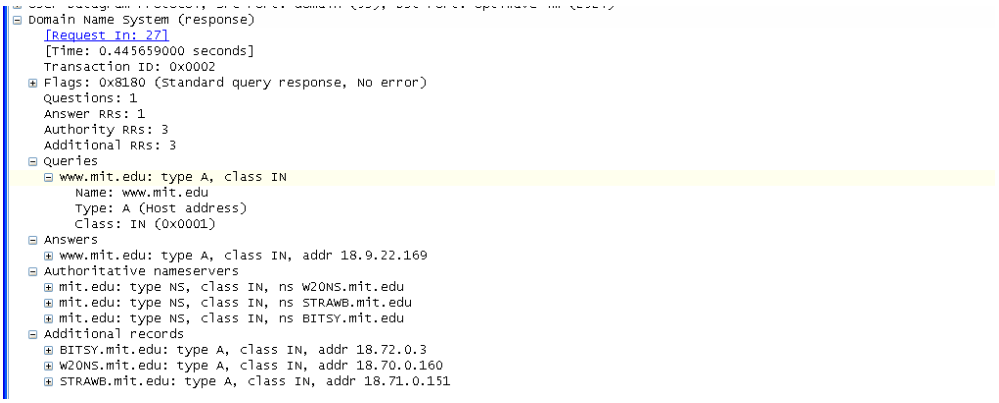
(ii) Write a snort rule that will generate an alert when there is NOP instruction in the content. The limit of content matches for NOP instructions is between bytes 40 and 75 of the data portion of a packet. **03**

(b) Explain how S-box is constructed in AES? Describe MixColumns and AddRoundKey in AES. **07**

OR

Q.5 **(a)** **07**

(i) What is the interpretation of following domain query response in wireshark? **04**



(ii) Write a snort rule that this rule will detect when the SYN and FIN flags are set at the same time. **03**

(b) What are some approaches to produce message authentication? **07**

****