maening
M. Tech.

Date: 08/01/2014

Student Exam No: _____

GANPAT UNIVERSITY
M. Tech. Sem.-I Information Technology
Regular Examination Dec - 2013
3IT105: Cryptography and Network Security

Time: 3 Hours] **[Total Marks: 70**

Instructions:

1. Figures to the right indicate full marks.
2. Each section should be written in a separate answer book.
3. Be precise and to the point in your answer.

SECTION - I

Q.1 (a) Explain active and passive attack with example. (4)

(b) Explain following terms of Mathematics of Cryptography (4)

i. Euler's PHI function

ii. Fermat's little theorem

(c) Show how word W60 is made in SHA-512 Algorithm. (4)

OR

Q.1 (a) Explain the steps of one round in DES in short. (4)

(b) Discuss El-GAMAL Cryptosystem and explain following terms. (4)

i. El-Gamal Key Generation algorithm

ii. Encryption algorithm

iii. Decryption algorithm

(c) Apply majority function on buffers A, B, C and find out the result. (Assume left most hexadecimal digits of these buffers are 0x7, 0xA, 0xE) (4)

Q.2 (a) Explain the process of MD-5 algorithm with diagram. (6)

(b) Given Super increasing table b = [7, 11, 23, 43, 87, 173, 357] and r=41 and modulus n=1001. Encrypt the letter "a" = [1, 1, 0, 0, 0, 0, 1] using knapsack cryptosystem and find the cipher text. (5)

*Use [7 6 5 1 2 3 4] as a permutation table.

OR

Q.2 (a) Define congruent modulo. Also find integer x such that (6)

1. $5x \equiv 4 \pmod 3$
2. $7x \equiv 6 \pmod 5$

(b) Explain structure of each round in SHA-512 with diagram. (5)

Q.3 (a) Define a session key and show how a KDC can create a session key between ALICE and BOB. (6)

(b) Explain RSA Digital Signature scheme and compare it to the RSA Cryptosystems. (6)

SECTION-II

Q.4 (a) Explain One time pad algorithm with example. (3)

(b) In RSA, Find the d and $\phi(n)$, if you know that e=17 and n = 187. (3)

(c) Show how the byte 0E is transformed to AB by sub-byte routine in AES using GF (2^8).required constant matrix for calculation is given below. (6)

Constant Matrix: $\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$ and Constant column matrix: $\begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$

OR

Q.4 (a) Decrypt the following Encrypted message using playfair Cipher Technique. (3)
(Note: put j and i both combine as a single field)
Encrypted Message: tmazinyamtluazinekla
Keyword: india is my country

(b) What is the difference between confusion and diffusion? (3)

(c) Discuss about Key Transformation process of DES step by step. (6)

Q.5 (a) Write Diffie Hellman key exchange algorithm. Explain man-in-the middle Attack on this Diffie Hellman key exchange. (6)

(b) Encrypt the message "Good morning" using the Hill Cipher with the Key $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$. (5)

OR

Q.5 (a) Define about following Security Principles: (5)
i. Confidentiality
ii. Authentication
iii. Integrity
iv. Non-Repudiation
v. Availability

(b) What is public key cryptography? Compare public it with conventional Cryptography. (6)

Q.6 (a) Write a short note on CFB algorithm mode. (6)

(b) Explain following Modular Arithmetic operations: (6)
i. Congruence
ii. Additive inverse
iii. Multiplicative Inverse

END OF PAPER