GANPAT UNIVERSITY
M. TECH. SEM. - I COMPUTER ENGINEERING
REGULAR EXAMINATION DECEMBER - 2014
3CE105: CRYPTOGRAPHY AND NETWORK SECURITY

Time: 3 Hours] [Total Marks: 60

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)** Discuss about following: **(4)**
1) Repudiation 2) Snooping

(b) 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

(c) Find out the multiplicative inverse of 83 in Z_{3230}. **(3)**

OR

Q.1 **(a)** Discuss about CBC and CFB algorithm modes with suitable diagram. **(4)**

(b) Find the inverse of e = 19 for RSA where p = 101 and q = 199 **(4)**

(c) If there are 233 users in the network then how many key pairs is required in symmetric cryptography operation? **(2)**

Q.2 **(a)** Perform mix column transformation of AES on following column matrix. **(6)**
Required constant matrix is given below.

Column matrix: $\begin{matrix} 4D \\ 90 \\ 4A \\ D8 \end{matrix}$ **Constant matrix:** $\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$

(b) Solve the Linear Congruence: $3x+2y \equiv 5 \pmod 7$ **(4)**
$4x+6y \equiv 4 \pmod 7$

OR

Q.2 **(a)** Decrypt the following Cipher Text message using 3x3 Hill Cipher. **(6)**
Cipher Text: edxphy **Key Matrix:** $\begin{bmatrix} 2 & 1 & 1 \\ 1 & 1 & 2 \\ 1 & 0 & -2 \end{bmatrix}$

(b) Discuss about mathematical theory behind the Diffe Hellman key exchange Algo. **(4)**

Q.3 **(a)** Show how the byte **13** is transformed to **7D** by subbyte routine in AES using *GF* (2^8). Required constant matrix for calculation is given below. **(6)**

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

(b) Perform the Primality Test using Fermat's theorem. **(4)**
1) 43 2) 31

SECTION-II

Q.4	(a)	Discuss Vigenere Cipher algorithm and encrypt the message "She is listening" using the 6-character keyword "PASCAL".	(5)
	(b)	Explain about Digital Envelope method with suitable diagram.	(5)

OR

Q.4	(a)	Alice and Bob want to establish a secret key using the diffie-hellman key exchange protocol. Assuming the values as n = 23, g = 5, x = 6, y = 8, Find out the values of A, B and the secret key K1 and K2.	(5)
	(b)	Solve the following Equation using Chinese Remainder Theorem. $X \equiv 3 \bmod 7$ $X \equiv 3 \bmod 13$ $X \equiv 0 \bmod 12$	(5)
Q.5	(a)	Discuss about Message Digest in brief with suitable Diagram.	(4)
	(b)	Discuss about Problem of Key Distribution or Key exchange in symmetric key cryptography.	(4)
	(c)	What is Base-64 bit Encoding Scheme of PGP?	(2)

OR

Q.5	(a)	Discuss about Network Address Translation with Example.	(4)
	(b)	Discuss about Static and Dynamic Packet Filter Firewall.	(4)
	(c)	Solve the ø(360) using Euler's Totient Function.	(2)
Q.6	(a)	Discuss about Rabin Cryptosystem with suitable Example.	(4)
	(b)	Given the super increasing Tuple b= [7, 11, 23, 43, 87,173,357] and modulus n = 1001, encrypt the letter 'g' using knapsack Cryptosystem. Use [7, 6, 5, 1, 2, 3, 4] as the permutation table. (note: ASCII value of 'g' is 1100111)	(6)

END OF PAPER