Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

M. E. - SEMESTER – II • EXAMINATION – WINTER 2012

Subject code: 725104 **Date: 28/12/2012**

Subject Name: PKI and Biometrics

Time: 02.30 pm – 05.00 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)** What is the difference between block cipher and stream cipher? What are the different modes of block cipher operation? Explain any one. **07**

(b) 1. Differentiate: Diffusion and confusion **07**
2. Show the characteristics of Link and End to End encryption

Q.2 **(a)** Compare differential cryptanalysis attack and linear crypt analysis showing the differential propagation through three rounds of DES **07**

(b) Using the play fair matrix **07**

M	F	H	I/J	K
U	N	O	P	Q
Z	V	W	X	Y
E	L	A	R	G
D	S	T	B	C

Encrypt this message: "Must see you over West of North Gujarat. Coming at once"

OR

(b) Differentiate: **07**
SubBytes and SubWord
ShiftRows and RotWord

Q.3 **(a)** Explain various types of attacks on Encrypted messages, along with known information to cryptanalysis **07**

(b) 1. What is repudiation? How can it be prevented in real life? **07**
2. What is Trojan horse? What is principle behind it?

OR

Q.3 **(a)** Consider the Diffie Hellman skim with a common prime q=11 and primitive root $\alpha = 2$ **07**
Show that 2 is indeed a generator
If the user A has public key $Y_A = 9$, what is A's private key
If the user B has public key $Y_B = 3$, what is the secret key k in between A and B

(b) Decrypt the following, which has been encrypted with a Caesar cipher: **07**
YFND LTYN FFUN FLCU RNFF UTYL TBTY LTBZ
WRNF FUTY LTBT FLCU TYLT BNFF U

Q.4	**(a)**	What are the properties a digital signature should have? What is the difference between direct and arbitrated digital signature?	**07**
	(b)	Explain Equivalent Inverse Cipher of AES implementation	**07**
		OR	
Q.4	**(a)**	Explain the key distribution scenario in depth	**07**
Q.4	**(b)**	Explain that how to achieve confidentiality and authentication using secret key distribution?	**07**
Q.5	**(a)**	Explain X.509 in brief	**07**
	(b)	Show impact of Avalanche effect along with suitable example	**07**
		OR	
Q.5	**(a)**	Explain digital signature and how it help's in e-Enabled service security operation with proper example.	**07**
	(b)	Write short note on PGP and DSS	**07**

****