B.Tech. Degree VII Semester Examination, November 2005

IT 705 (C) CRYPTOGRAPHY AND DATA SECURITY

(1999to 2001 Admissions)

Time: 3 Hours Maximum Marks: 100

Answer all questions. All Questions carry equal marks.

I a) Explain how cryptography differ from coding theory.. **10**

b) Suppose that the plaintext "go" corresponds to the cipher text "th", when an Affine Cipher uses the encryption function $x \rightarrow \alpha * x + \beta \pmod{26}$. Find the values of α and β. Assume that the letters of the alphabets are assigned the numbers as follows. **10**

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

OR

II a) Find the encryption of the plaintext "input" and "alter" using the encryption function $x \rightarrow 13 * x + 4 \pmod{26}$. Explain how cryptography differ from coding theory. Assume that the letters of the alphabets are assigned the numbers as follows. **05**

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

b) Discuss the main objectives that arise in information security. **10**

c) Explain what do you mean by absolute security in cryptography? **05**

III a) What do you mean by double encryption is equivalent to single encryption? Is this true in the case of DES? **12**

b) Explain the usage of Linear Feedback Shift Registers in Cryptography. **08**

OR

IV a) Discuss on "DES has begun to show signs of age". **12**

b) Explain the role of finite state machine in cryptography. **08**

V	a)	Demonstrate how an NP-complete problem can be used for public-key cryptography.	08
	b)	Describe in detail, the RSA Algorithm with an example.	12
		OR	
VI	a)	Explain the possible approaches to attacking the RSA algorithm.	08
	b)	Describe in detail, the public key systems based on elliptic curves with an example.	12
VII	a)	Explain different Cryptographic protocols.	08
	b)	Explain the role of Hash function in cryptography. Give any two Hash functions.	12
		OR	
VIII	a)	Describe in detail, message authentication with digital signatures.	10
	b)	Explain how do we achieve message integrity with hash codes.	10
IX	a)	What does Network Security mean?	08
	b)	Explain the general aspects of key management and key distribution.	12
		OR	
X	a)	Discuss in detail key agreement protocols.	10
	b)	What are the ways to employ Network Security?	10

****