00509

M.Sc. (MATHEMATICS WITH APPLICATIONS IN COMPUTER SCIENCE)
M.Sc. (MACS)

Term-End Examination

December, 2010

MMTE-006 : CRYPTOGRAPHY

Time : 2 hours *Maximum Marks : 50*

*Note : Answer **any five** out of **six** questions. Calculators are **not** allowed.*

1. (a) Explain each of the following terms with an example : 6

   (i) Plain text

   (ii) Cipher text

   (iii) Key

   (iv) Encryption algorithm.

   (b) Explain the encryption and decryption processes in the Cipher Feed Back (CFB) mode of operation of block ciphers. What advantage does CFB have when compared to ECB and CBC modes ? 4

2. (a) Explain the Merkle - Damgard strengthening. Assuming a block size of 64 bits and that we use 8 bits to represent a character, what string will you get by applying Merkle - Damgard strengthening to the string "digital signatures" ? 5

(b) Suppose you know that $n = 4307$ is a product of 2 primes and $\phi(n) = 4176$. Factorise 4307 using this information. 3

(c) Encrypt the text "MISSION POSTPONED" using affine cipher with key (3,2). 2

3. (a) Explain how you will construct a LFSR corresponding to a recurrence 5

$$\{x_{n+k} \equiv a_{k-1}x_{n+R-1} + a_{k-2}x_{n+k-2} + \cdots + a_o x_n \pmod 2\}.$$

Construct the LFSR corresponding to the recurrence

$$x_{n+5} \equiv x_{n+4} + x_{n+2} + x_{n+1} + x_n \pmod 2.$$

(b) If $f(x) = x^4 + x^3 + x + 1$ and $g(x) = x^3 + x^2 + x + 1$ are polynomials in 'Q' $[x]$, use the extended Euclidean algorithm to find $p(x)$ and $q(x)$ in 'Q' $[x]$ such that $p(x)f(x) + q(x)g(x) = h(x)$ where $h(x)$ is the gcd of $f(x)$ and $g(x)$. 5

4. (a) A 64 bit key for the DES algorithm is as follows : 6

10011101 10101101
10100001 10011000
11000100 10010111
01011011 10110000

The key permutation table is as follows :

57	49	33	25	17	9	1	58	50	42	34	26	18
10	2	59	43	35	27	19	11	3	60	52	44	36
63	55	47	31	23	15	7	62	54	46	38	30	22
4	6	61	45	37	29	21	13	5	28	20	12	4

The table of key shifts is as follows :

Round	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Shift	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	

Key selection table is as follows :

14	17	11	24	1	5	3	28	15	6	21	10
23	19	12	4	26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40	51	45	33	48
44	49	39	56	34	33	46	42	50	36	29	32

(i) Check whether the key is error free using the parity bits.

(ii) Find the keys for the first two rounds.

(b) Decrypt the following cipher text which was encrypted using the vigenere cipher with the keyword "SECRET". : 4

"KIPUWNHTNZIL" Is the Vigenere cipher a transposition cipher or a substitution cipher ? Justify your answer.

5. (a) Explain the (Fermat) pseudo prime test. Prove that, if a natural number n fails the pseudo prime test for a base b, then it fails the test for at least half of the possible bases $b \in (Z/nZ)^*$. 5

(b) State the Coulomb postulates for pseudo random bit sequences. 3

(c) Define a cryptographic hash function. 2

6. (a) Check whether the number 241 passes the Rabin - Miller test with respect to the base $b = 3$. 4

(b) Let $f(x)$ be the irreducible polynomial $x^4 + x + 1 \in \mathbb{Z}_2[X]$. Find the order of the element $\alpha = x + \varkappa[f(x_1)]$ in the multiplicative group of $\frac{Z_2[X]}{(f(x))}$. 3

(c) Explain the El-Ghamal cryptosystem, clearly stating which information is kept private and which information is made public. 3