00555

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

Term-End Examination

December, 2011

MMTE-006 : CRYPTOGRAPHY

Time : 2 hours *Maximum Marks : 50*

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

1. (a) Describe the various possible attacks on a Cryptosystem briefly. 5

(b) Carry out one round of encryption of the text 1010 0110 1101 using toy block cipher with the key 101111010. The S - boxes are given below : 5

$$S_1 \begin{bmatrix} 101 & 010 & 001 & 110 & 011 & 100 & 111 & 000 \\ 001 & 100 & 110 & 010 & 000 & 111 & 101 & 011 \end{bmatrix}$$

$$S_2 \begin{bmatrix} 100 & 000 & 110 & 101 & 111 & 001 & 011 & 010 \\ 101 & 011 & 000 & 111 & 110 & 010 & 001 & 100 \end{bmatrix}$$

2. (a) Encrypt the text " THE LIGHT HAS GONE OUT OF OUR LIVES", first using columnar transformation of length and followed by the permutation cipher with the key 5

1	2	3	4
3	2	4	1

Is the combined transformation a transposition cipher or a substitution cipher ? Justify your answer.

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

$$\{x_{n+k} \equiv a_{k-1}\, x_{n+R-1} + a_{k-2}\, x_{n+R-2} + .. + a_0 x_n \pmod 2\}$$

Construct the LFSR corresponding to the recurrence.

$$x_{n+5} \equiv x_{n+4} + x_{n+3} + x_{n+1} + x_n \pmod 2$$

3. (a) Find the order of all the elements in Z_{15}. Is the group cyclic ? Justify your answer. 4

(b) Describe the serial test to check whether a given sequence of bits is pseudo random or not. Apply the test to the following sequence. 4

011001010111101110010100

[You may like to use the following values :

$\chi^2_{0.05,1} = 3.84146$ $\chi^2_{0.05,2} = 5.99146$

$\chi^2_{0.05,3} = 7.81473$ $\chi^2_{0.05,4} = 9.48773$]

(c) Check whether x^2+5x+5 is irreducible over F_7. 2

4. (a) Show that, if there are n persons in a room, p(n), the probability that 2 persons have the same birthday is $1-\prod_{i=1}^{n-1}\left(1-\frac{i}{365}\right)$. Derive the approximation $p(n) \approx 1-e^{-n^2/730}$. 4

(b) Construct the addition and multiplication tables for $\frac{F_3[x]}{(x^2+1)}$. 6

5. (a) Apply extended Euclidean algorithm to find a and b such that $253a+391b=d$, where d is the greatest common divisor of 253 and 391. 4

(b) 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 "Digitalsignatures" ? 4

(c) Suppose you know that $n=328021$ is a product of two primes and $\phi(n)=326700$. Factorise n using this information. 2

6. (a) Let $n = 17.19$ and $e = 173$ be the parameters for RSA encryption. If the cipher text is 96, find the plain text. 5

(b) Bob is using 43 as the prime for the El Gamal cryptosystem and 3 as the primitive root. His secret exponent is 2. He receives the pair (27, 39) from Alice where 39 is the message and $27 = 3^3$. Decrypt the message. 2

(c) Explain the Miyaguchi - Preneel method for constructing a hash function from a block cipher. 3