No. of Printed Pages : 3

MMTE-006

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

Term-End Examination

June, 2013

MMTE-006 : CRYPTOGRAPHY

Time : 2 hours *Maximum Marks : 50*

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

1. (a) Check whether polynomial $f(x) = x^3 - 3x^2 + 2x + 1$ is irreducible over the field of rationals Q. Is it irreducible over Z ? Justify your answer. **4**

(b) Explain the construction of the S-box in ABS. Also explain the design considerations behind the construction. **6**

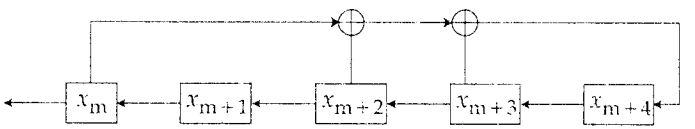
2. (a) Find $5^{17} \bmod 31$ using repeated squaring algorithm. **3**

(b) Describe the OFB and CTR modes of encryption. **4**

(c) Explain the El Gamal crypto system, clearly stating which information is kept private and which information is made public. **3**

3. (a) Construct the multiplicative group of Residues modulo 15 and prove that it is not cyclic. 6

(b) (i) Write down the recurrance for the following LFSR : 4



(ii) Construct the LFSR corresponding to the recurrence

$$x_{m+5} \equiv x_{m+4} + x_{m+2} + x_{m+1} + x_m \pmod 2$$

4. (a) Explain confidentiality and data integrity. Distinguish between them. 4

(b) Check whether the following sequence satisfies the frequency test and serial. 6

1101110110110011110101110100001011000010 01

You may like to use the following values :

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

5. (a) The following lipher text was encrypted using affine cipher. 4

DSXXA

The plain text starts with HA. Decrypt the message.

(b) Suppose you know that $n = 5293$ and $\phi(n) = 5148$. Factorise 'n' using this information. 3

(c) What is the probability of finding a collision in MD5 according to the birthday paradox ? Why MD5 considered as broken now ? 3

6. (a) Decrypt the following cipher text which was encrypted using the Vigenere cipher with the key word "ORDERS" "GLVKVLCDRVIGK". Is the Vigenere cipher a transposition cipher or a substitution cipher ? Justify your answer. 4

(b) Describe the Blum - Blum shut generator for generating pseudo random bits. 2

(c) Explain the following : 4

(i) Diffie Hellman decision problem

(ii) Diffie Hellman computational problem.