No. of Printed Pages : 3

MMTE-006

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

00991

M.Sc. (MACS)

Term-End Examination

June, 2014

MMTE-006 : CRYPTOGRAPHY

Time : 2 hours *Maximum Marks : 50*

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

1. (a) Factorise $x^3 - 9$ into irreducible factors over $\mathbf{F}_{11}[x]$. 5

(b) Explain RC4 pseudo random generation algorithm with pseudo-code. 5

2. (a) Distinguish between the following : 4

(i) MAC and Hash functions.

(ii) Symmetric key cryptosystems and Public key cryptosystems.

(b) Give an example of a PRBG (Pseudo Random Bit Generator). 2

(c) Find 5^{15} (mod 71) using repeated squaring algorithm. 4

3. (a) Find the smallest pseudo prime to the base 7. *4*

(b) Explain the cipher block chaining mode of operation. *3*

(c) Explain the following properties of a Hash function : *3*

(i) One way

(ii) Collision resistance

(iii) Second pre-image resistance

4. (a) Explain the terms Confidentiality, Authentication, Data integrity and Non-repudiation. How can these be achieved ? *5*

(b) Suppose Bob sets up the parameters for ElGamal cryptosystem as follows :

He chooses the prime p = 181 and the primitive root 2. He chooses x = 21 and publishes the values (181, 2, 86). He receives the message (32, 145) from Alice. Decrypt the message. *5*

5. (a) Apply autocorrelation test for d = 3 on the following sequence :

11001001000011111110110100001 at $\alpha = 0{\cdot}05$

You may like to use the following data :

a	0·25	0·05	0·025	0·01
x	0·6745	1·6449	1·9600	2·3263

If X is a random variable having standard normal distribution, then $P(X > x) = a$. *5*

(b) Let $f(x) = x^4 + x^3 + x^2 + 1$ and

$g(x) = x^3 + 1 \in \mathbf{F}_2[x]$.

Find gcd(f, g) using the extended Euclidean algorithm and express the gcd in the form $u(x) f(x) + v(x) g(x)$. *5*

6. (a) Use Fermat factorisation method to factorise 71273. *5*

(b) Use the simple columnar transposition cipher with column width 4 to encrypt the text "ATTACK FROM THE PAVILION END". *2*

(c) Explain the Davies – Meyer method for constructing a block function from a block cipher. *3*