MMTE-006

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

M.Sc. (MACS)

Term-End Examination

00786

June, 2016

MMTE-006 : CRYPTOGRAPHY

Time : 2 hours *Maximum Marks : 50*

Note : *Question no. 1 is **compulsory**. Answer any **four** from questions no. 2 to 6.*

1. Which of the following statements are *true*, and which are *false* ? Justify your answers. *5×2=10*

(a) IP in DES does not contribute to security.

(b) A block cipher in CTR mode of operation can be used as a stream cipher.

(c) An affine cipher is a special case of a simple substitution cipher.

(d) The probability of success in finding the second pre-image of a hash is higher than that of finding a collision for the hash.

(e) Any finite field is isomorphic to $\mathbf{Z}_p$, for some prime p.

2. (a) Generate the first 5 terms of the Blum-Blum-Shub sequence, given p = 19, q = 23 and initial seed = 15. *4*

(b) Is $\mathbf{F}_2[x] / (x^4 + x^2 + 1)$ a field ? Why, or why not ? *2*

(c) Suppose Bano chooses p = 109. Check that 6 is a primitive root modulo 109. Bano chooses the secret value x = 40 and public key (109, 6, 7). Bano receives the pair (96, 45) from Asha. Find the message. *4*

3. (a) (i) Describe the pseudo-random generation algorithm of RC4.

(ii) Starting from state S, such that S[i] = 255-i, run PRGA for 3 steps. *6*

(b) Decrypt the following affine cipher. You are given information that the message starts with the word GOOD *4*

NBBYR BQWXW N.

4. (a) If $f(x) = x^4 + x^3 + x + 1$ and

$g(x) = x^3 + x^2 + x + 1$

are polynomials in $\mathbf{Q}[x]$, use the extended Euclidean algorithm to find p(x) and q(x) in $\mathbf{Q}[x]$ such that $p(x) f(x) + q(x) g(x) = h(x)$, where h(x) is the gcd of f(x) and g(x). *6*

(b) Explain the Birthday Paradox. Calculate the probability of two persons from a group of 5 being born on the same day of the week. *4*

5\. (a) (i) Describe the toy block cipher with a block diagram for 1 round.

(ii) Decrypt the first round toy cipher 010110110111 with the following parameters : *6*

key = 110110111

S-box

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

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

(b) Compute $5^{13} \pmod{43}$ using the repeated squaring algorithm. *4*

6\. (a) Suppose Asha wants to send the message $h(\mathcal{M}) = 25$ to Bano. She wants to sign the message using the RSA signature scheme, with parameters $n = 77$, $e = 13$, $d = 37$.

(i) Find the signature of the message.

(ii) What information should Bano receive to be able to verify the signature ? Further, give the procedure for verifying Asha's signature. *6*

(b) Find the multiplicative inverse of $x^7 + x^3 + 1$ in $\mathbf{F}_2[x] / < x^8 + x^4 + x^3 + x + 1 >$. *4*