No. of Printed Pages : 4

MMTE-006

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

Term-End Examination

00042

December, 2018

MMTE-006 : CRYPTOGRAPHY

Time : 2 hours *Maximum Marks : 50*

Note : *Answer any **four** questions out of questions no. 1 to 5. Question no. **6** is **compulsory**. Calculators are **not** allowed.*

---

1. (a) Using the Extended Euclidean algorithm, find the multiplicative inverse of 139 (mod 141). *4*

(b) Carry out one round of encryption of the text 100110110110 using the toy block cipher with the key 101111011. The S-boxes are given below : *4*

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

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

(c) Define the Euler ϕ-function. Compute $\phi(8)$ and $\phi(45)$. *2*

2. (a) Check whether the following sequence passes the runs test with level of significance $\alpha = 0{\cdot}05$, using the values : *8*

$$\chi^2_{0\cdot05,\,4} = 9{\cdot}48773, \quad \chi^2_{0\cdot05,\,5} = 11{\cdot}0705$$

0000110000001010000100100
1110111011100010001001100
1000100000000110100000110
1111111010010110100001100
1001101000001110110111010
1110111011100011001001100
1010010000

(b) Factorise 4891 using the Fermat factorisation method. *2*

3. (a) Suppose $f : \{0, 1\}^n \to \{0, 1\}^n$ is a pre-image resistant bijective function. Define

$h : \{0, 1\}^{2n} \to \{0, 1\}^n$ as follows :

Given $x \in \{0, 1\}^{2n}$, write $x = x' \parallel x''$,

where $x', x'' \in \{0, 1\}^n$.

Then define $h(x) = f(x' \oplus x'')$. Prove that h is not second pre-image resistant. *3*

(b) Suppose Alia chooses $p = 167$, $q = 83$, $g = 5$, $a = 7$ and makes the values $(p, q, \alpha, \beta) = (167, 83, 25, 126)$ public. What will be the signature for the message $M = 25$ if she chooses $k = 7$? If she sends the message to Babu along with the signature, how will he verify the signature ? *7*

4. (a) Encrypt the plain text 'ICCCRICKETWORLDCUPINAUSTRALIA' cipher using the key 'MACS'. *4*

(b) Suppose Asha wants to use RSA cryptosystem with parameters $p = 19$, $q = 13$, $e = 11$.

(i) Find the decryption key.

(ii) What are the values that Asha makes public ?

(iii) What will the encrypted text for the message 17 ?

(iv) Asha receives the message 2 from Bhola. What is the original message ? *6*

5. (a) Construct a finite field of order 8. Write the multiplication table of the field. *7*

(b) Given the initial sequence 101001, find the linear recurrence that generates the sequence. *3*

6. Which of the following statements are *True* and which are *False* ? Give reasons for your answers. *10*

(a) There is no finite field of order 9.

(b) An S-Box provides the security property of diffusion.

(c) Hash algorithms provide confidentiality and integrity.

(d) The composition of two affine ciphers is again an affine cipher.

(e) The key space of an RSA cryptosystem is finite.