No. of Printed Pages : 3

MMTE-006

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

Term-End Examination

01052 **June, 2017**

MMTE-006 : CRYPTOGRAPHY

Time : 2 hours *Maximum Marks : 50*

Note : *Answer any **four** questions out of Q 1– 5, Q 6 is **compulsory**. Calculators are not allowed.*

1. (a) Using the Extended Algorithm, find the gcd of a = 873 and b = 42. Also find the values of s and t so that gcd = (s × a) + (t × b). *4*

(b) Find multiplication of polynomials $1 + x + x^2 + x^5 + x^7$ and $1 + x^2 + x^7$ modulo $1 + x + x^3 + x^4 + x^8$. All the three polynomials are in $\mathbf{Z}_2[x]$. *3*

(c) Explain four requirements for designing Hash functions. Explain what an HMAC is. *3*

2. (a) Encrypt the plain text

'THECODEISSIMPLEBUTSECURE',

Using Vigenere cipher with keyword "SHORT". *3*

(b) Generate 4 random bits using the RSA pseudorandom generator, for p = 11, q = 13, e = 7, $x_0 = 3$. *3*

(c) Decrypt the cipher text "NIDALNWENJ", when information given is that the cipher is affine and the first two letters of the plain text message is 'IL'. *4*

3. (a) Factor 11021 using the Fermat factorisation method. *2*

(b) Calculate the entry of the S-box of the AES for the input 10110010, by using the transformation $Ax + x_0$, where *8*

$$A = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}, x_0 = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

4. (a) Explain the CBC and CTR modes of a block cipher. Which mode can be used to make a block cipher function as a stream cipher ? Justify your answer. 5

(b) Suppose Asha wants to digitally sign the message $\mu = 15$ using the ElGamal digital signature with parameters $(p, \alpha, \beta) = (17, 3, 5)$, with $a = 5$. If she selects $k = 7$, what is the signature ? 5

5. (a) Use the repeated squaring algorithm to find $5^{17} \pmod{71}$. 3

(b) Solve the discrete logarithm problem $5^x \equiv 8 \pmod{73}$ using the Pohlig-Hellman algorithm. 7

6. Which of the following statements are *True*, and which are *False* ? Justify your answers. 10

(a) $\mathbf{Z}_8$ is a field.

(b) 9 is a Carmichael number.

(c) Discrete logarithm is easy to solve in the group $(\mathbf{Z}_n, +)$, for any $n \in \mathbf{N}$.

(d) Confusion is to spread the influence of individual plain text characters over as much of the cipher text as possible.

(e) The AES algorithm consists of 12 rounds for a key length of 128 bits.