No. of Printed Pages : 3

MMTE-006

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

M.Sc. (MACS)

Term-End Examination

00414

December, 2016

MMTE-006 : CRYPTOGRAPHY

Time : 2 hours *Maximum Marks : 50*

Note : *Question no.* ***6*** *is* ***compulsory****. Answer any* ***four*** *questions from questions no. 1 to 5. Only non-programmable calculators are allowed.*

---

1. (a) Define Euler's Phi function and find $\phi(80)$. *2*

   (b) Find $5^{24} (\text{mod } 8)$ using the repeated squaring algorithm. *4*

   (c) Describe the Merkle-Damgård method and the Davies-Meyer method. Also explain how these methods can be used to construct cryptographic hash functions. *4*

2. (a) Explain the key expansion process in AES-128. *4*

   (b) Encrypt the plain text

   "INDIANEEDSWOMENLIKEYOUTOWINYYY"

   using the permutation cipher with 53124 as the key. *3*

(c) Compute the discrete logarithm and the discrete antilogarithm to the base 3 in $\mathbf{Z}_{17}^{*}$. *3*

3. (a) Explain the key-scheduling algorithm of the RC4 cipher along with its pseudocode. *5*

(b) Use the Miller-Rabin test to check whether 1889 is composite or not. *5*

4. (a) Decrypt the ciphertext $C = 8$, which is obtained by the RSA system with public key $(e, n) = (13, 33)$. *5*

(b) Find the inverse of $(1 + x^2)$ in $R = \mathbf{F}_2[x] / < 1 + x + x^4 >$. Also, is $1 + x + x^4$ invertible in R ? Give reasons for your answer. *5*

5. (a) Find the result of multiplying

$f(x) = 1 + x + x^2 + x^4 + x^6$ with

$g(x) = 1 + x + x^4$

mod $m(x) = 1 + x + x^3 + x^4 + x^8$ in $\mathbf{F}_2[x]$. *4*

(b) Solve the equation $10^x \equiv 52 \pmod{59}$ using the Baby-Step Giant-Step algorithm. *6*

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

(a) The symmetric key cryptosystems have no drawbacks.

(b) There is no field with characteristic 9.

(c) Diffusion is achieved by using an S-box in DES.

(d) 257 is a strong prime.

(e) Given a sequence of bits, the frequency test suffices to check the randomness of the sequence.

———