M.Sc. MATHEMATICS WITH APPLICATIONS IN COMPUTER SCIENCE

00028

Term-End Examination

June, 2010

MMTE-006 : CRYPTOGRAPHY

Time : 2 hours *Maximum Marks : 50*

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

---

1. (a) Use the simple columnar transformation of width five to encrypt the following text : **4**

 'SLINGS AND ARROWS OF OUTRAGEOUS FORTUNE'.

 Is the columnar transformation a transposition cipher or a substitution cipher ? Justify your answer.

 (b) Explain the design criterion behind the DES as published by the IBM. **3**

 (c) Explain the RSA Digital Signature Scheme. **3**

2. (a) Explain the Rabin-Miller pseudo-primality test. **5**

(b) Carry out one round of encryption of the text 110011111001 using the toy block cipher with the key 110111001. The S-boxes are **5**

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

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

3. (a) Describe the Poker test for checking whether a given sequence of bits is pseudo random or not. Apply the test to the following sequence : **5**

110111011011001111010111010000101100001001100101

[You may like to use the following values :

$\chi^2_{0.05,1} = 3.84146$, $\chi^2_{0.05,2} = 5.99146$,

$\chi^2_{0.05,3} = 7.81473$, $\chi^2_{0.05,4} = 9.48773$]

(b) Prove that every carmichael number has at least three prime factors. **3**

(c) Solve the equation $2^x \equiv 9 \pmod{13}$. **2**

4. (a) The following cipher text was encrypted using an affine cipher : 'CRWWZ'. The plain text starts HA. Decrypt the message. 4

(b) Given the initial sequence 101 001 101, find the recurrence that generates it. 4

(c) Describe the Blum-Blum-Shut generator for generating pseudo random bits. 2

5. (a) Encrypt the text 'ATTACK POSTPONED UNTIL TWO AM' using the following permutation cipher : 3

1	2	3	4	5
3	5	1	4	2

(b) Describe the Davies-Meyer method for constructing a compression from a block cipher with a diagram. 3

(c) Construct the finite field $\mathbf{F}_8$ with the addition table. You need not give the multiplication table. 4

6. (a) Compute 7^{98} mod 40 using repeated squaring algorithm. 4

(b) Explain how a byte can be regarded as element of $\mathbf{F}_2[x]/\langle g(x)\rangle$ where $g(x)$ is an irreducible polynomial in $\mathbf{F}_2[x]$. Taking $g(x) = x^8 + x^4 + x^3 + x + 1$ and regarding 11000010 and 11100101 as elements of $\mathbf{F}_2[x]/\langle g(x)\rangle$, multiply them. 6