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

00563

Term-End Examination

June, 2012

MMTE-006 : CRYPTOGRAPHY

Time : 2 hours *Maximum Marks : 50*

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

1. (a) Check that $f(x) = x^2 + x - 1 \in Z_3[x]$ is a primitive polynomial. 5

   (b) For the initial segment of bits 011 001 00 of a sequence of period 15, find the recurrence that generates it. 5

2. (a) Explain the Runs test for random sequences. Apply the test for the following sequence : 5

11101 00011 10110 01001 01101 00010 00000 10101 00110
01001 10001 10011 11101 10111 11110 10110 11010
11100 10011 11001 10001 11000 10100 10010
11010 10011 10100 10110 10011 10100
11011 00010

You may use the following values :

$\chi^2_{0.05,3} = 7.81473, \chi^2_{0.05,4} = 9.48773,$
$\chi^2_{0.05,5} = 11.0705.$

(b) If $f(x) = (x^3 - 2x^2 - 14x - 5)$ and $g(x) = (x^3 - x^2 - 17x - 15)$ are polynomials in $Q(x)$, use the extended Euclidean algorithm to find $Q(x)$ and $R(x)$ in $Q(x)$ such that $Q(x)\, f(x) + R(x)\, q(x) = h(x)$ where $h(x)$ is the gcd of $f(x)$ and $g(x)$. The values at the end of first iteration are given below : 5

$T_1(x) = x^3 - x^2 - 17x - 15,$

$Q_1(x) = 0,\ R_1(x) = 1$

$T_2(x) = -x^2 + 3x + 10,\ Q_2(x) = 1,\ R_2(x) = -1$

3. (a) A 64 bit key for the DES algorithm is as follows : 6

1 0 0 0 0 0 1 1	1 1 0 0 1 0 0 0
1 1 1 0 1 1 0 0	1 0 1 0 1 1 0 1
1 0 0 1 1 1 0 1	1 0 1 0 1 0 0 0
1 1 1 1 0 1 0 0	1 0 0 0 1 0 0 1

The key permutation table is as follows :

57	49	41	33	25	17	9	1	58	50	42	34	26	18
10	2	59	51	43	35	27	19	11	3	60	52	44	36
63	55	47	39	31	23	15	7	62	54	46	38	30	22
14	6	61	53	45	37	29	21	13	5	28	20	12	4

The table of key shifts is as follows :

Round	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Shift	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Key selection table is as follows :

14	17	11	24	1	5	3	28	15	6	21	10
23	19	12	4	26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40	51	45	33	48
44	49	39	56	34	53	46	42	50	36	29	32

(i) Check whether the key is error free using the parity bits. Give reasons for your answer.

(ii) Find the keys for the first two rounds.

(b) Decrypt the following cipher text which was encrypted using the Vigenere cipher with the keyword "ORDERS". **4**

"GLVKVLCDRVIGK".

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

4. (a) Explain the CBC and CFB modes of operation of a block cipher. **4**

(b) Find 17^6 (mod 61) using repeated squaring algorithm. **3**

(c) Find a generator of Z^*_{17}. **3**

5. (a) Which of the following statements are *true* or *false* ? Give reasons. **6**

(i) Hash functions are invertible.

(ii) A stream cipher can be constructed from block cipher.

(iii) Every one way function can be used as hash function.

(b) Explain the (Fermat) Pseudo prime test. Prove that, if a natural number n fails the pseudo prime test for a base b, then it fails the test for at least half of the possible bases bt$(Z/nZ)^*$. **4**

6. (a) Use the congruence $294^2 \equiv 10^2 (\text{mod} 1349)$ to find a non-trivial factorisation of 1349. **4**

(b) For a RSA system $n = 391 = 17.23$, and the encryption exponent is $e = 17$. Find the decryption exponent. You may make use of the following calculation : **3**

$352 = 20.17 + 12, \quad 17 = 12 + 5, \quad 12 = 5.2 + 2,$
$5 = 2.2 + 1.$

(c) A plain text starting with f yields a cipher text starting with PQ when encrypted with affine cipher. Find the key to the affine cipher. **3**