University of Technology
Computer Science Department
Class: fourth year
Branch: information security

Subject: advanced encryption
Examiner: Prof. Abdul Monem Rahma Ph.D.
Time: 3 hours
Date of Exam. : 28/5/2011

Final Exam. / 1st Trail / 2013 -2014

Note: **Answer five questions only**

Q1 A) Discuses the mathematical model of finite **group** and finite **field**

B) For **n** equal **15 , 17** and **19** prove that the finite set Z_n with the two operations

$$A \oplus B = A + B \ (mod n),$$
$$A \odot B = A \ . \ B \ (mod n)$$

is a finite (**group, field**) or not.

Q2 Consider the MixColumns Transformation for Encryption and Decryption mathematical model, based on the field **GF(5)** and by using the key matrix $k = \begin{pmatrix} 4 & 2 \\ 1 & 1 \end{pmatrix}$ and $k^{-1} = \begin{pmatrix} 3 & 4 \\ 2 & 2 \end{pmatrix}$

A) Encrypt the plain text message {2 1 3 2 2 4}.

B) Decrypt the cipher text message { 2 3 4 4 2 2}.

Q3 Compute the **Addison** and **Multiplication** tables of the finite field **GF(2^5)** by choosing the Irreducible polynomial $x^5 + x^4 + x^2 + x + 1$.

Q4 Consider the finite field **GF(2^3)** by choosing irreducible polynomial $x^5 + x^3 + x^2 + x + 1$

A) Compute (1 0 0 1 1)⊕(1 0 0 1 1) and (1 0 0 1 0)⊕(1 0 0 0 0)

B) Compute (0 1 0 1 1)⊙(1 0 1 0 1) and (1 0 0 1 1)⊙(1 0 0 1 1)

C) Compute (1 0 0 0 0) ⊙ ((1 0 1 0 1) ⊕ (1 0 1 0 1))

Q5 Consider the Hill Cipher Encryption System mathematical model, based on the field **GF (2^3)** by choosing irreducible polynomial $x^3 + x + 1$, use the key matrix $K1 = \begin{pmatrix} x^2+1 & 1 & x \\ 1 & x & x^2 \\ x^2 & 1 & x^2 \end{pmatrix}$

to Encrypt the plain text message:

$\{ x^2 + x + 1 \quad x^2 + x \quad x^2 + 1 \quad x^2 \quad x + 1 \quad x \quad 1 \quad 0\}$

Q6 A) Discuss the elliptic curve $E_{23}(1,1)$ basing on the equation $y^2 = x^3+x+1$ and Compute **five** the points { **p1 , p2 , p3 , p4 , p5** } only of its discreet elliptic group.

B) Compute the points **p2 + p4 , p3 + P3**

Good Luke