University of Technology
Department of Applied Sciences
Final Examination 2016/2017

Subject : Mathematical Cryptography **Class : 4th year**
Branch : Mathematics& Comp. Appl. **Time : 3 hours**
Examiner: Prof. Dr. Nadia Al-Saidi **Answer 7 only** **Date :**

Q1/ A- Consider the following ciphertext obtained from the Affine Cipher **VUFE** Suppose we know that **F** is the encryption of **e** and **T** is the encryption of **g.** Recall that $E_K(x) = ax + b$, find a and b, then decrypt the above ciphertext.

B- The Word VPNN is encrypted using the Hill cipher with $K=\begin{pmatrix}3 & 5\\ 7 & 8\end{pmatrix}$. Find the corresponding plaintext. **(10 Mark)**

Q2/ Answer **A or B**

A- Using $x^4 + x + 1$ to generate the elements of $GF(2^4)$, then find the inverse of X^3+X.

B- Solve the following system of congruences:

$7x = 4 \pmod{11}$

$x = 3 \pmod{7}$. **(10 Mark)**

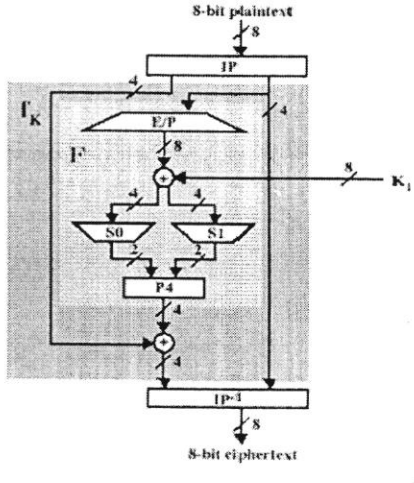
Q3/ Decrypt the code 0100011001111011001110100 , using stream cipher with key generated by $p(x) = x^3 + x^2 + 1$ and initial state 101. **(10 Mark)**

Q4/ Let P=(3,10) and Q(9,7) in $E_{23}(1,1)$. Find P+Q , 2P. **(10 Mark)**

Q5/ Find the output for the simplified DES encryption with one round and the input (1011 1101), IP=2 6 3 1 4 8 5 7, IP^{-1}=4 1 3 5 7 2 8 6, E/P=4 1 2 3 2 3 4 1, P4=2 4 3 1, K=0 1 1 1 0 0 1 1

$$S0=\begin{pmatrix}1&0&3&2\\3&2&1&0\\0&2&1&3\\3&1&3&2\end{pmatrix}\begin{matrix}0\\1\\2\\3\end{matrix} \qquad S1=\begin{pmatrix}0&1&2&3\\2&0&1&3\\3&0&1&0\\2&1&0&3\end{pmatrix}\begin{matrix}0\\1\\2\\3\end{matrix}$$

The S-boxes operate as follows. The 1st and 4th input bits are treated as a 2-bit number that specify a row of the S-box, and the 2nd and 3rd input bits specify a column of the S-box. For ex. 1001=>row3 and column 0 . i.e. in S0 =3 in binary = 11



(10 Mark)

Q6/ Answer A or B

A- In an RSA system, the public key of a given user is $e = 13$, $n = 33$. What is the private key of this user? ? *Decrypt the word ZKR.*

B- How does the man in the middle attack work in Diffie–Hellman? Explain its mechanism through block diagram then write DH algorithm. **(10 Mark)**

University of Technology
Department of Applied Sciences
Final Examination 2016/2017

Subject : Mathematical Cryptography — Class : 4th year
Branch : Mathematics& Comp. Appl. — Time : 3 hours
Examiner: Prof. Dr. Nadia Al-Saidi — **Answer 7 only** — Date : 28/5/2017

Q7/ In the discussion of MixColumns and InvMixColumns, it was stated that $b(x) = a^{-1}(x) \bmod (x^4 + 1)$, where, $a(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\}$ and $b(x) = \{0B\}x^3 + \{0D\}x^2 + \{09\}x + \{0E\}$. Show that this is true. **(10 Mark)**

Q8/ Choose **4** only

1- What is the difference between the symmetric and asymmetric key cryptography?

2- What is the difference between message integrity and message authentication?

3- Design a Digital signature protocol. Explain the differences between digital signatures and public key cryptosystems.

4- The basic principles of encryption are confusion and diffusion. Explain what we mean by these terms and what are the differences between them? Elements of a DES type algorithm include permutations, and combinations of bit sequences using XOR. What are the elements of the DES algorithm that accomplished confusion and the elements that accomplished diffusion?

5- Describe how to perform cryptanalysis on a message encrypted with a Vigenère cipher. **(10 Mark)**

Good Luck