Fundamentals of Cryptography

Homework 1

Sepehr Ebadi **9933243**

Question 1

1. What is the multiplicative inverse of 7 in Z9, Z10, and Z11?

Z9 :
$m = 9 = 3^2$
$a = 7$

$$\phi(m) = m \times \prod_{i=i}^{k} \left\{1 - \frac{1}{\rho_i}\right\} = 9 \times \left(1 - \frac{1}{3}\right) = 6$$

$$a^{-1} = a^{\phi(m)-1} mod\ m = 7^{6-1} mod\ 9 = 4$$

Z10 :
$m = 10 = 2 \times 5$
$a = 7$

$$\phi(m) = m \times \prod_{i=i}^{k} \left\{1 - \frac{1}{\rho_i}\right\} = 10 \times \left(1 - \frac{1}{2}\right) \times (1 - \frac{1}{5}) = 4$$

$$a^{-1} = a^{\phi(m)-1} mod\ m = 7^{4-1} mod\ 10 = 3$$

Z11 :
$m = 11 = 11$
$a = 7$

$$\phi(m) = m \times \prod_{i=i}^{k} \left\{1 - \frac{1}{\rho_i}\right\} = 11 \times \left(1 - \frac{1}{11}\right) = 10$$

$$a^{-1} = a^{\phi(m)-1} mod\ m = 7^{10-1} mod\ 11 = 8$$

2. What is the multiplicative inverse of 9, 10, and 11 in Z7?

9 :
$m = 7 = 7$
$a = 9$

$$\phi(m) = m \times \prod_{i=i}^{k} \left\{1 - \frac{1}{\rho_i}\right\} = 7 \times \left(1 - \frac{1}{7}\right) = 6$$

$a^{-1} = a^{\phi(m)-1} mod\ m = 9^{6-1} mod\ 7 = 4$

10 :
$m = 7 = 7$
$a = 10$

$$\phi(m) = m \times \prod_{i=i}^{k} \left\{1 - \frac{1}{\rho_i}\right\} = 7 \times \left(1 - \frac{1}{7}\right) = 6$$

$a^{-1} = a^{\phi(m)-1} mod\ m = 10^{6-1} mod\ 7 = 5$

11 :
$m = 7 = 7$
$a = 11$

$$\phi(m) = m \times \prod_{i=i}^{k} \left\{1 - \frac{1}{\rho_i}\right\} = 7 \times \left(1 - \frac{1}{7}\right) = 6$$

$a^{-1} = a^{\phi(m)-1} mod\ m = 11^{6-1} mod\ 7 = 2$

Question 2

1. $x = 3^3\ mod\ 13$
   $\equiv 27\ mod\ 13\ \equiv 1\ mod\ 13$

2. $x = 3^{100}\ mod\ 13$
   $\equiv 3^{99} \times 3\ mod\ 13\ \equiv (3^3)^{33} \times 3\ mod\ 13 \equiv 1^{33} \times 3\ mod\ 13\ \equiv 3\ mod\ 13$

3. $x = 6^2\ mod\ 13$
   $\equiv 36\ mod\ 13\ \equiv 10\ mod\ 13$

4. $x = 6^{100}\, mod\ 13$
$\equiv (6^2)^{50}\ mod\ 13 \equiv 10^{50}\, mod\ 13 \equiv (10^2)^{25}\, mod\ 13 \equiv 9^{25}\, mod\ 13$
$\equiv (9^2)^{12} \times 9\, mod\ 13 \equiv (3^3)^4 \times 9\, mod\ 13 \equiv 9\, mod\ 13$

Question 3

In the **affine cipher**, given two pairs of **plaintext-ciphertext**:

$y_1 = a.x_1 + b\ mod\ m$

$y_2 = a.x_2 + b\ mod\ m$

By subtracting the two ciphertexts, we have:

$y_1 - y_2 \equiv a(x_1 - x_2) mod\ m$

$a \equiv (y_1 - y_2) \times (x_1 - x_2)^{-1} mod\ m$

This is how **a** is calculated. Then for **b**, we have:

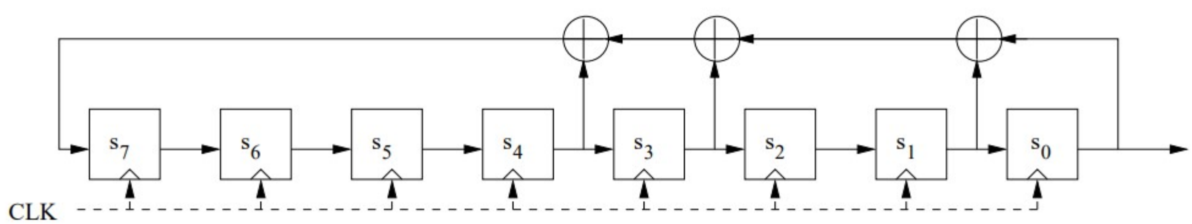
$b \equiv y_1 - a.x_1 mod\ m\ OR\ b \equiv y_2 - a.x_2 mod\ m$

The condition for selecting x_1 and x_2 is that the inverse of $x_1 - x_2$ must exist in mod m:

$$\gcd(x_1 - x_2, m) = 1$$

Question 4

$P(x) = x^8 + x^4 + x^3 + x + 1$



s_7	s_6	s_5	s_4	s_3	s_2	s_1	s_0	output
1	1	1	1	1	1	1	1	$1(s_0)$
0	1	1	1	1	1	1	1	$1(s_1)$
0	0	1	1	1	1	1	1	$1(s_2)$
0	0	0	1	1	1	1	1	$1(s_3)$
0	0	0	0	1	1	1	1	$1(s_4)$
1	0	0	0	0	1	1	1	$1(s_5)$
0	1	0	0	0	0	1	1	$1(s_6)$
0	0	1	0	0	0	0	1	$1(s_7)$
1	0	0	1	0	0	0	0	$0(s_8)$
1	1	0	0	1	0	0	0	$0(s_9)$
1	1	1	0	0	1	0	0	$0(s_{10})$
0	1	1	1	0	0	1	0	$0(s_{11})$
0	0	1	1	1	0	0	1	$1(s_{12})$
1	0	0	1	1	1	0	0	$0(s_{13})$
0	1	0	0	1	1	1	0	$0(s_{14})$
0	0	1	0	0	1	1	1	$1(s_{15})$

the first 16-bit output based on the table : $(1001000011111111)_2 = (90FF)_{16}$

Question 5

1. What is the initialization vector?

   Given that the degree of the LFSR is 3, therfore 3 first bit of key is equal to initial value of LFSR(3 initial bits go out of the LFSR without changing).

   LFSR Initialization Vector = 001

2. Determine the feedback coefficients of the LFSR.

   $s2p2+s1p1+s0p0=s3$

   $s3p2+s2p1+s1p0=s4$

   $s4p2+s3p1+s2p0=s5$

   Now, by substituting the key value (0010111), we find the feedback coefficients:

   $s0=0 , s1=0 , s2=1 \Rightarrow 1p2+0p1+0p0=0\ (s3)$

   $s1=0 , s2=1 , s3=0 \Rightarrow 0p2+1p1+0p0=1\ (s4)$

$s2=1$, $s3=0$, $s4=1 \Rightarrow 1p2+0p1+1p0=1$ $(s5)$

By solving these 3 equations and 3 unknowns, the feedback coefficients are obtained as:

$p0=1$, $p1=1$, $p2=0$

Thus, the LFSR's characteristic polynomial is as follows:

$$P(x) = x^3 + p_2x^2 + p_1x + p_0$$

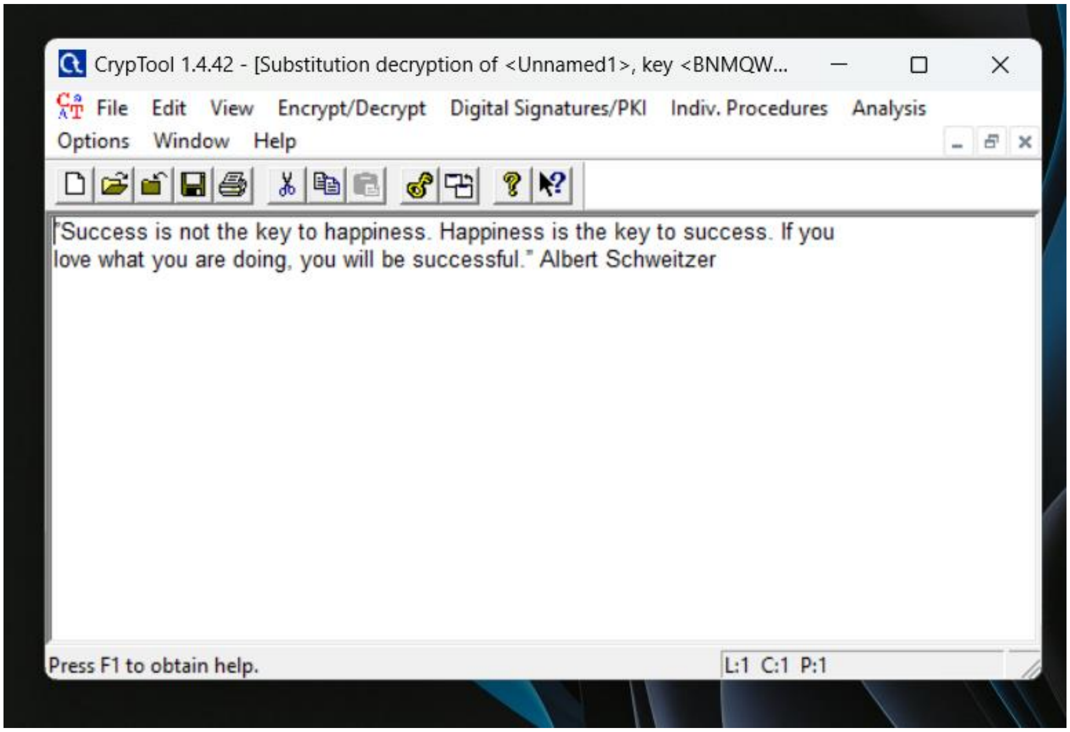
$$P(x) = x^3 + x + 1$$

3. Draw a circuit diagram and verify the output sequence of the LFSR.

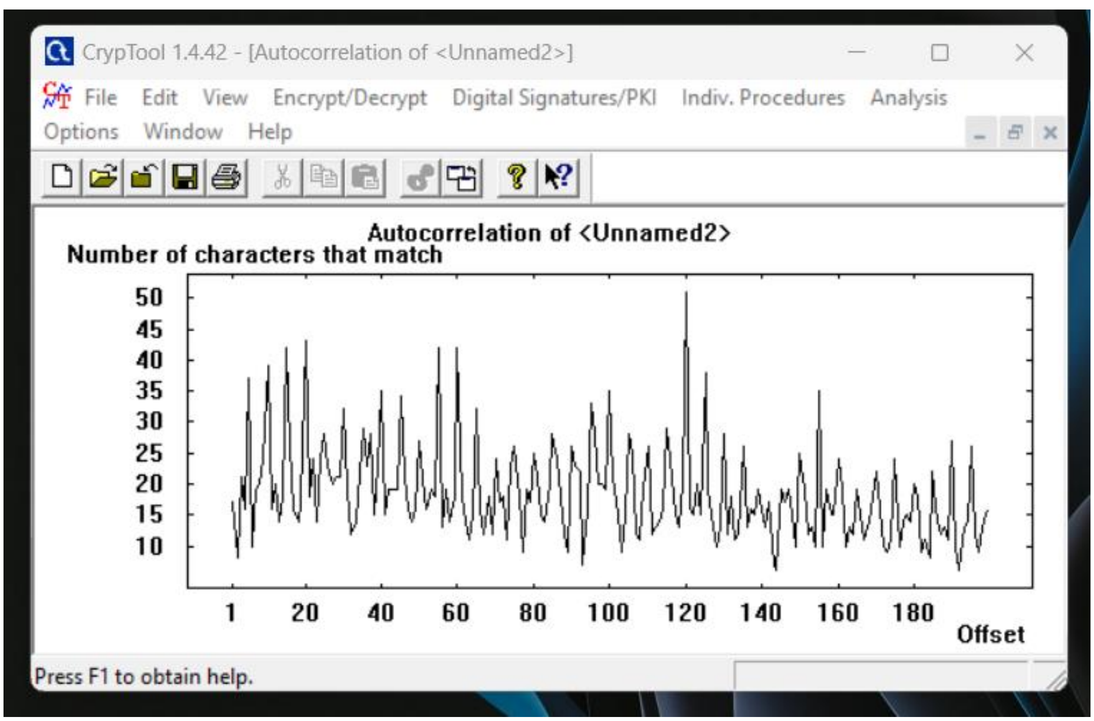
s_2	s_1	s_0	output
1	0	0	$0(s_0)$
0	1	0	$0(s_1)$
1	0	1	$1(s_2)$
1	1	0	$0(s_3)$
1	1	1	$1(s_4)$
0	1	1	$1(s_5)$
0	0	1	$1(s_6)$

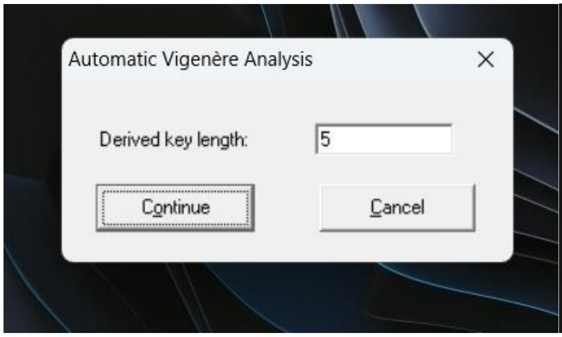
“CrypTool”

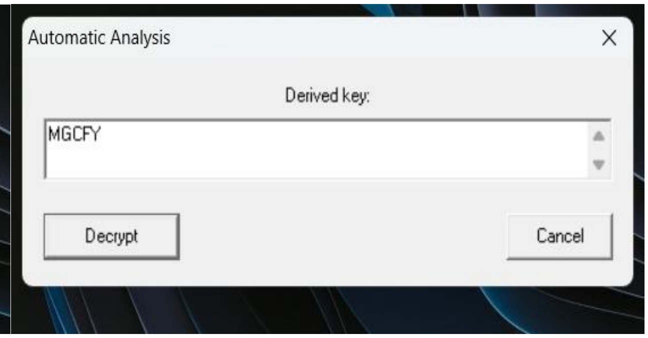
Question 6

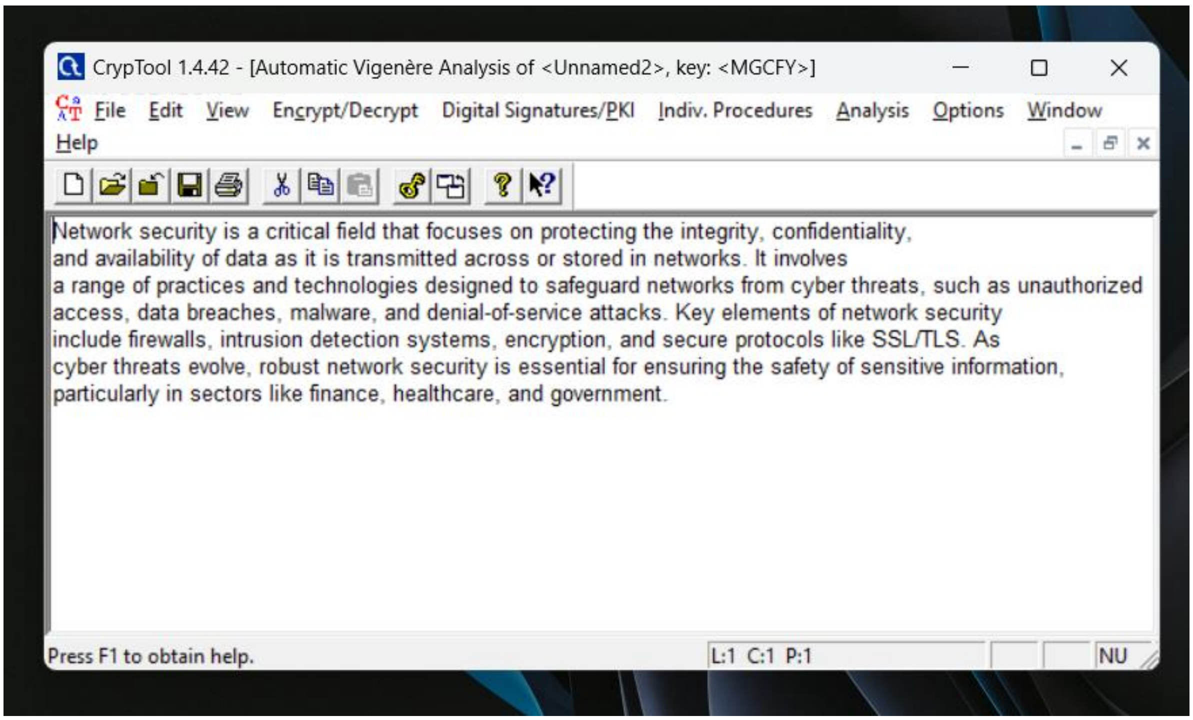


Question 7




Automatic Vigenère Analysis
Derived key length:
5
Continue
Cancel


Automatic Analysis
Derived key:
MGCFY
Decrypt
Cancel


CrypTool 1.4.42 - [Automatic Vigenère Analysis of <Unnamed2>, key: <MGCFY>]
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window
Help
Network security is a critical field that focuses on protecting the integrity, confidentiality,
and availability of data as it is transmitted across or stored in networks. It involves
a range of practices and technologies designed to safeguard networks from cyber threats, such as unauthorized
access, data breaches, malware, and denial-of-service attacks. Key elements of network security
include firewalls, intrusion detection systems, encryption, and secure protocols like SSL/TLS. As
cyber threats evolve, robust network security is essential for ensuring the safety of sensitive information,
particularly in sectors like finance, healthcare, and government.
Press F1 to obtain help.
L:1 C:1 P:1
NU