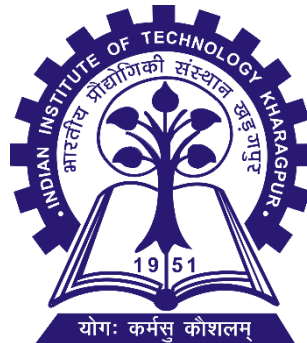


Cryptography and Network Security (CS60065) AUTUMN, 2021-2022

TA: Tapadyoti Banerjee

**Course Instructor: Prof. Dipanwita Roy Chowdhury
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur
West Bengal 721302, India**



**TUTORIAL: 3
DATE: 24th October 2021**

QUESTION : 1 (The Feistel cipher)

Consider a Feistel cipher composed of 16 rounds with block length 128 bits and key length 128 bits. Suppose that, for a given k , the key scheduling algorithm determines values for the first 8 round keys, k_1, k_2, \dots, k_8 , and then sets $k_9 = k_8, k_{10} = k_7, k_{11} = k_6, \dots, k_{16} = k_1$.

Suppose you have a ciphertext c . Explain how, with access to an encryption oracle, you can decrypt c and determine m using just a single oracle query. This shows that such a cipher is vulnerable to a chosen plaintext attack.

QUESTION : 2 (The SubByte Value)

$$(c7c6c5c4c3c2c1c0) = 01100011$$

Calculate the SubByte value of $(53)_{16}$

$$01010011$$
$$x^6 + x^4 + x + 1$$

```
for(i=0to 7)
  do bi = (ai + ai+4 + ai+5 + ai+6 + ai+7 + ci ) mod 2
return (b7b6b5b4b3b2b1b0)
```

Multiplicative inverse

$$x^7 + x^6 + x^3 + x$$

$$11001010$$

$$b_0b_1b_2\dots b_7$$

$$b_0 = (a_0 + a_4 + a_5 + a_6 + a_7 + c_0) \pmod{2} = 0 + 0 + 0 + 1 + 1 + 1 \pmod{2} = 1$$

$$b_1 = a_1 + a_5 + a_6 + a_7 + a_0 + c_1 \pmod{2} = 1 + 0 + 1 + 1 + 0 + 1 \pmod{2} = 0 \pmod{2}$$

$$11101101 \quad \text{ED}$$

QUESTION : 3 (Euclidean Algorithm)

Determine $\gcd(24140, 16762)$ by using Euclidean Algorithm.

34

QUESTION : 4 (Euclidean Algorithm)

Using the extended Euclidean algorithm, find the multiplicative inverse of $24140 \bmod 40902$

0x41010011
x6 +vxcv x4 +x +1

QUESTION : 5 (Field Arithmetic)

For polynomial arithmetic with coefficients in \mathbb{Z}_{10} , perform the calculation:
 $(6x^2 + x + 3) \times (5x^2 + 2)$

QUESTION : 6 (Field Arithmetic)

Develop a generator table for $GF(2^4)$ with $m(x) = x^4 + x + 1$.

Power	Polynomial	Binary	Decimal
$g^0 = 1$	1	0001	1
$g^1 = x$	x	0010	2
$g^2 = x^2$	x^2	0100	4
$g^3 = x^3$	x^3	1000	8
g^4	$x + 1$	0011	3
g^5	$x^2 + x$	0110	6
g^6	$x^3 + x^2$	1100	12
.			
.			
.			
g^{14}	$x^3 + 1$	1001	9
g^{15}			

QUESTION : 7 (Related to AES)

Show that $x^i \bmod (x^4 + 1) = x^{i \bmod 4}$.

$$x^4 \bmod (x^4 + 1) = 1$$

$$x^8 \bmod (x^4 + 1) = 1$$

$$x^{4a} \bmod (x^4 + 1) = 1$$

$$i = 4a + (i \bmod 4)$$

$$x^i \bmod (x^4 + 1) = [x^{4a} * x^{(i \bmod 4)}] \bmod (x^4 + 1)$$

1*

Input 67 89 AB CD

QUESTION : 8 (Related to AES)

$$\text{Output} = \begin{array}{|c|c|c|c|} \hline 2 & 3 & 1 & 1 \\ \hline 1 & 2 & 3 & 1 \\ \hline 1 & 1 & 2 & 3 \\ \hline 3 & 1 & 1 & 2 \\ \hline \end{array} \begin{array}{|c|} \hline 67 \\ \hline 89 \\ \hline AB \\ \hline CD \\ \hline \end{array} = \begin{array}{|c|} \hline 28 \\ \hline 45 \\ \hline EF \\ \hline 0A \\ \hline \end{array}$$

Compute the output of the MixColumns transformation for the following sequence of input bytes "67 89 AB CD". Apply the InvMixColumns transformation to the obtained result to verify your calculations. Change the first byte of the input from '67' to '77', perform the MixColumns transformation again for the new input, and determine how many bits have changed in the output.

$$\text{Input''} = \begin{array}{|c|c|c|c|} \hline E & B & D & 9 \\ \hline 9 & E & B & D \\ \hline D & 9 & E & B \\ \hline B & D & 9 & E \\ \hline \end{array} \begin{array}{|c|} \hline 28 \\ \hline 45 \\ \hline EF \\ \hline 0A \\ \hline \end{array}$$

Input' = 77 89 AB CD