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: 24^{th} 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, k1, k2, ..., k8, and then sets k9 = k8, k10 = k7, k11 = k6, ..., k16 = k1.

0x1010011

x6 + x4 + x +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 $(53)_{16}$

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

01010011
x6 + x4 +x +1

Multiplicative inverse
x7 + x6 + x3 + x

11001010 b0b1b2...b7

b0 = (a0 + a4 + a5 + a6 + a7 c0) (mod 2) = 0 + 0 + 0 + 1 + 1 + 1 (mod 2) = 1

b1 = a1 + a5 + a6 + a7 + a0 + c1 (mod 2) = 1 + 0 + 1 + 1 + 0 + 1 (mod 2) = 0 (mod 2)

11101101 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 mod 40902

0x41010011
x6 +vxcv x4 +x +1

QUESTION : 5 (Field Arithmetic)

For polynomial arithmetic with coefficients in 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
g0 = g15 0x4 10 10011	1	0001	1
g1 x6 + x4 + x +1	g	0010	2
g2	g2	0100	4
g3	g3	1000	8
g4	g+1	0011	3
g5	g2 + g	0110	6
g6	g3 + g2	1100	12
.			
.			
.			
g14	g3 + 1	1001	9
g15			

QUESTION : 7 (Related to AES)

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

x4 mod(x4 + 1) = 1

x8 mod(x4 + 1)= 1

a, x(4a) mod(x4 + 1) = 1

i, i= 4a + (i mod 4)

xi mod (x4 + 1) = [x(4a) * x(i mod 4)] mod (x4 + 1)
1*

Input 67 89 AB CD

QUESTION : 8 (Related to AES)

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

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.

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

Input' = 77 89 AB CD