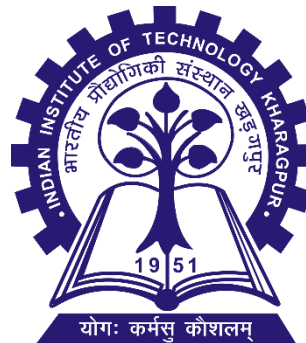


# **Cryptography and Network Security (CS60065)**

**AUTUMN, 2021-2022**

**TA: Tapadyoti Banerjee  
Rijoy Mukherjee**

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



**TUTORIAL: 3  
DATE: 16<sup>th</sup> September 2022**

## 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)

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

### **QUESTION : 3 (Euclidean Algorithm)**

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

## **QUESTION : 4 (Euclidean Algorithm)**

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

## 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  $m(x) = x^4 + x + 1$ .

## QUESTION : 7 (Related to AES)

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



## **QUESTION : 8 (Related to AES)**

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.