**Birzeit University**

**Faculty of Engineering and Technology**

**Department of Electrical and Computer Engineering**

**First Semester – 2023/2024**

**ENCS4320 - Applied Cryptography**

**Homework # 2 - Due Saturday, January 27, 2024**

---

| **Section A** | **Symmetric Key Ciphers (PRFs, PRPs, Block Ciphers), Group Theory, and Number Theory** |
|---|---|

## Question 1 (12 points):

Consider a **Feistel cipher** with ***four rounds***. Then the plaintext is denoted as $\boldsymbol{P} = (\boldsymbol{L_0}, \boldsymbol{R_0})$ and the corresponding ciphertext is $\boldsymbol{C} = (\boldsymbol{L_4}, \boldsymbol{R_4})$. What is the **simplest form** of the ciphertext $\boldsymbol{C}$, in terms of $\boldsymbol{L_0}$, $\boldsymbol{R_0}$, and the subkeys, for each of the following round functions? (You should clearly show steps about how you get the answer)

A) $\boldsymbol{F(R_{i-1}, K_i) = 0}$

B) $\boldsymbol{F(R_{i-1}, K_i) = R_{i-1}}$

C) $\boldsymbol{F(R_{i-1}, K_i) = R_{i-1} \oplus K_i}$

## Question 2 (5 points):

Within a single round, the Data Encryption Standard **(DES)** employs both confusion and diffusion.

A) What is the difference between confusion and diffusion in cryptography?

B) Give one source of confusion within a DES round.

C) Give one source of diffusion within a DES round.

## Question 3 (8 points):

Compute $(345^{28567} \times 23^{567} + 1078) \bmod 29$ given that 29 is a prime.

## Question 4 (9 points):

Using the Extended Euclidean algorithm,

A) Find the *greatest common divisor* of **19** and **999**, that is, **gcd(999, 19)**. Show your work clearly step by step.

B) Express the **gcd(999, 19)** as a *linear combination* of **999** and **19**.

C) Compute the *multiplicative inverse* of **19 mod 999**, which is a number between **0** and **998**.

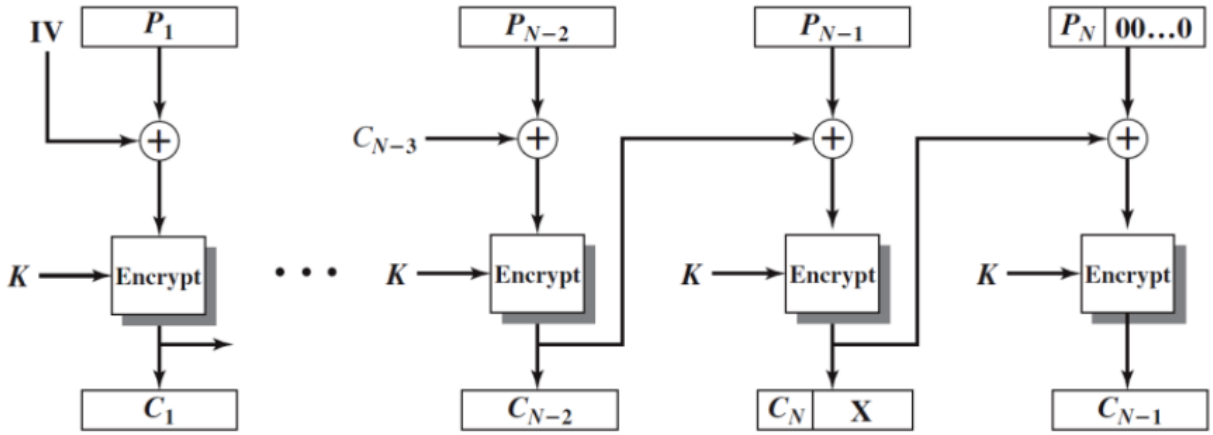
D) Compute the *multiplicative inverse* of **999 mod 19**, which is a number between **0** and **18**.

# Section B — Block Cipher Modes, Integrity, and Authenticated Encryption

## Question 5 (14 points):

Bob wishes to encrypt some plaintext and stores the resulting ciphertext on his hard drive. Specifically, he wants the ciphertext to be the *same length* as the original plaintext. For this purpose, he employed the **ciphertext stealing (CTS)** mode, the implementation of which is shown in the figure below. Initially, the plaintext is divided into independent blocks of length $\boldsymbol{S}$ bits, giving the plaintext blocks $\boldsymbol{P_1}$, $\boldsymbol{P_2}$, …, $\boldsymbol{P_N}$. Assume that the last block of plaintext (i.e., $\boldsymbol{P_N}$) is $\boldsymbol{L}$ bits long, where $\boldsymbol{L < S}$. The encryption sequence is as follows:

1. Encrypt the first $(\boldsymbol{N-2})$ blocks using the traditional cipher block chaining (**CBC**) technique.
2. XOR $\boldsymbol{P_{N-1}}$ with the previous ciphertext block $\boldsymbol{C_{N-2}}$ to create $\boldsymbol{Y_{N-1}}$.
3. Encrypt $\boldsymbol{Y_{N-1}}$ to create $\boldsymbol{E_{N-1}}$.
4. Select the first $\boldsymbol{L}$ bits of $\boldsymbol{E_{N-1}}$ to create $\boldsymbol{C_N}$.
5. Pad $\boldsymbol{P_N}$ with $(\boldsymbol{S-L})$ zeros at the end and exclusive-OR with $\boldsymbol{E_{N-1}}$ to create $\boldsymbol{Y_N}$.
6. Encrypt $\boldsymbol{Y_N}$ to create $\boldsymbol{C_{N-1}}$.




A) Describe how to decrypt the ciphertext $(\boldsymbol{C_1}, \ldots, \boldsymbol{C_{N-1}}, \boldsymbol{C_N})$, that is, show the decryption sequence.

B) If a single bit error occurs in the storage of ciphertext $\boldsymbol{C_i}$, which plaintext blocks, if any, will be correctly restored by the decryption algorithm? Explain your answer.

## Section C — Hash Functions

### Question 6 (6 points):

Suppose that $\boldsymbol{H(m)}$ is a secure hash function that generates a $\mathbf{12}$-bit output.

A) How many collisions would you expect to find if you hash $\mathbf{1024}$ randomly selected messages?

B) What is the expected number of hashes that must be computed to find $\mathbf{25}$ collisions? That is, what is the expected number of hashes that must be computed to find pairs $\boldsymbol{(x_i, y_i)}$, $\boldsymbol{x_i \neq y_i}$, with $\boldsymbol{H(x_i) = H(y_i)}$, for $\boldsymbol{i = 1, 2, \ldots, 25}$?

### Question 7 (6 points):

Consider the following hash function $\boldsymbol{H(m)}$, which receives as an input a message in the form of a sequence of decimal numbers, $\boldsymbol{m = (D_1, D_2, \ldots, D_I)}$.

A) If $\boldsymbol{H(m)}$ is defined as $\left(\sum_{i=1}^{I} \boldsymbol{D_i}\right) \boldsymbol{mod\ n}$, for some predefine large value $\boldsymbol{n}$. Does this hash function satisfy the pre-image resistance (one-way property) requirement? Explain your answer.

B) If $\boldsymbol{H(m)}$ is defined as $\left(\sum_{i=1}^{I} \boldsymbol{D_i^2}\right) \boldsymbol{mod\ n}$, for some predefine large value $\boldsymbol{n}$. Does this hash function satisfy the collision resistance requirement? Explain your answer.

C) Calculate the hash function of part (B) for $\boldsymbol{m} = (\mathbf{189}, \mathbf{632}, \mathbf{900}, \mathbf{722}, \mathbf{349})$ and $\boldsymbol{n} = \mathbf{989}$.

***GOOD LUCK***