POIS ASSIGNMENT 1

TASK 3

USE THE PRF TO OBTAIN A CPA-SECURE ENCRYPTION SCHEME

THEORY

Chosen Plaintext Attacks : CPA-attacker influences messages that the honest party encrypts.

Advantages of CPA-security : Minimal security notion for a modern cryptosystem.
Limitations of CPA-Security :

- Does not model and adversary who attempts to modify messages.
- Can get honest party to (partially) decrypt some messages

Theorem: An encryption scheme Π = (*G*en, *E*nc,*D*ec) that is CPA-Secure for single encryptions is also CPA-secure for multiple encryptions.

Observation: Given a CPA-secure encryption scheme $\Pi = (\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ that supports messages of a single bit ($\mathcal{M} = \{0,1\}$) it is easy to build a CPA-secure scheme $\Pi' = (\mathrm{Gen}', \mathrm{Enc}', \mathrm{Dec}')$ that supports messages m = $m_1, \ldots, m_n \in \{0,1\}^n$ of length n.

$$\mathrm{Enc}'_{\mathrm{k}}(m) = \langle \mathrm{Enc}_{\mathrm{k}}\ (m_1), \ldots, \mathrm{Enc}_{\mathrm{k}}\ (m_n) \rangle$$

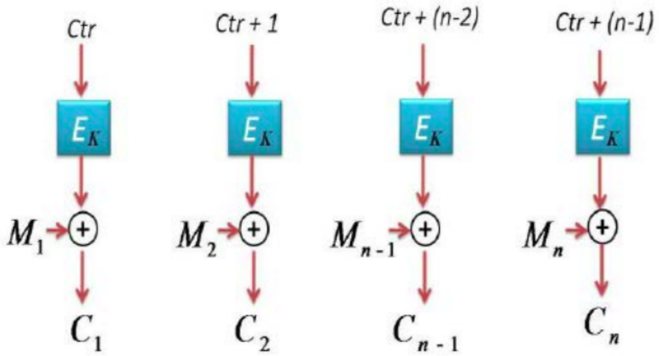
Constructing a CPA-secure encryption from any PRF:

Let $F(\cdot,\cdot)$ be a secure pseudorandom function with output length ℓ, then define a private-key encryption scheme for messages of length *ell* as follows:

1. **Gen:** on input 1^n, choose uniform $k \in \{0,1\}^n$ and output it
2. **Enc:** on input a key $k \in \{0,1\}^n$ and a message $m \in \{0,1\}^\ell$, choose uniform $r \in \{0,1\}^n$ and output the ciphertext:
$$c = [r, m \oplus F_k(r)]$$
3. **Dec:** on input a key $k \in \{0,1\}^n$ and a ciphertext $c = [r, y]$, output the plaintext message
$$m = y \oplus F_k(r)$$

.

COUNTER MODE :
In the randomized counter mode of operation for block ciphers.
We begin by choosing a random IV. Then, we encrypt the message by encrypting each plaintext block i with F(k, IV +i): m[i]⊕F(k, IV +i). Note that randomized counter-mode can be parallelized: each block can be encrypted independent of the previous ones.



- **Input:** $m_1, \ldots, m_n$
- **Output:** c = (ctr, $c_1, c_2, \ldots, c_n$) where ctr is chosen uniformly at random
- **Theorem**: If E_k is PRF then counter mode is CPA-Secure
- **Advantages**: Parallelizable encryption/decryption