GTU

**DEPARTMENT OF COMPUTER ENGINEERING**

**CSE 470 – Autumn 2022**

**PROJECT REPORT**

SÜLEYMAN GÖLBOL 1801042656

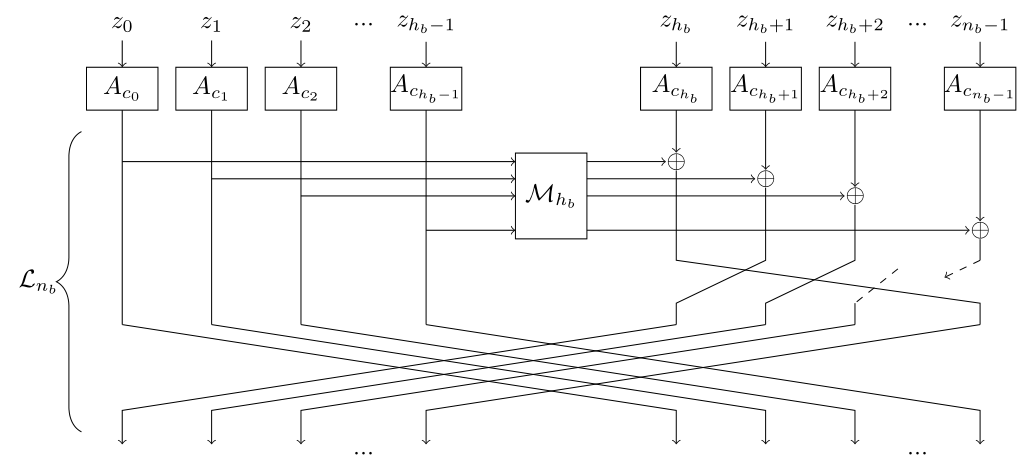
# ALGORITHM DETAILS

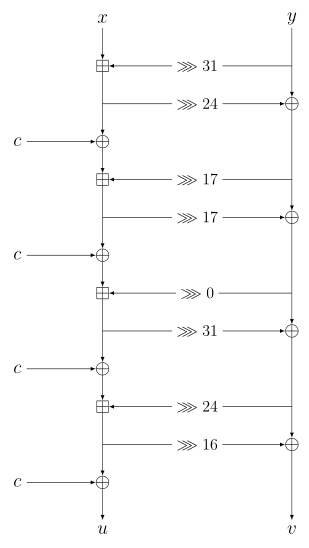
# Lightweight cryptography algorithms are the cryptographic algorithms and protocols that are designed to be efficient in terms of computation and memory usage, making them suitable for use in resource-constrained environments such as embedded devices, IoT devices, and other types of systems with limited processing power or memory. Sparkle and TinyJambu are some of them.

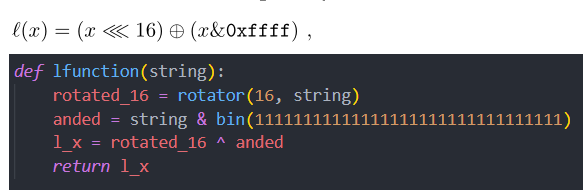
# Block ciphers have mode of operations such as ECB, CBC, OFB and CFB.

# SPARKLE

Sparkle is actually cryptographic permutation set which depends of key features of Esch and Schwaemm and their efficiency are based on small silicon area and requirements.



The picture above shows example of a Sparkle step for Sparkle permutations.  
Second step of sparkle comes with diffusion layer. 



For diffusion layer, I implanted as l(x) like that.

* 1. **TINYJAMBU**

For the complexity of median of an unsorted array, I created a class Q2.

**2) CIRCULAR PLAYER ELIMINATION**

**Part a:**

# As it wanted in the question; for part a,