**UNDERSTANDING THE BLOCK DIAGRAM**

1. **Input Interface**

Function: Accepts incoming data from the IoT sensors or other modules. Purpose: Acts as the entry point for data that needs to be encrypted/decrypted.

1. **Key Management Unit**

Function: Manages cryptographic keys (generation, storage, distribution).

Secure Key Storage: Ensures that keys are safely stored and protected against attacks.

Connection to IoT Host: Shares or syncs with the IoT host for authentication and session key management.

1. **Crypto Engine (Encryption / Decryption)**

Function: Core module for performing encryption and decryption operations.

Input: Data from the Input Interface and cryptographic keys from the Key Management Unit. Encryption Algorithm: Likely uses the PRESENT algorithm

Output: Encrypted or decrypted data to be forwarded for further processing.

1. **Power Control Unit (Clock Gating / Power Gating)**

Function: Optimizes power usage using:

Clock Gating: Turns off the clock signal to idle modules.

Power Gating: Completely shuts down unused sections to save power. Also: Sends back encrypted/decrypted data to other modules if required.

Significance: This block is essential to achieve \*low-power consumption\*, which is critical for IoT devices.

1. **Output Interface**

Function: Sends the processed (encrypted/decrypted) data to the outside world—either to be transmitted or stored.

Purpose: Acts as the final stage in the secure data flow.

1. **IoT Host**

Function: Represents the external microcontroller or processor that the crypto chip supports.

Role: Communicates with the Key Management Unit and handles higher-level operations like network protocols, user interface, etc.