

## WHITE PAPER: RSME ALGORITHM

Project Name: Reactive Stability Mutation Encryption (RSME)

Author: Rangga Soleman

Category: Active Defense Cybersecurity / Lightweight Cryptography

Version: 2.0 (Advanced Hybrid)

### 1. ABSTRACT

RSME is a dynamic encryption system designed for high-security environments. Unlike static algorithms like AES, RSME integrates a "Stability Awareness Sensor" (Delta%) that detects intrusions in real-time and triggers an automatic mutation of the encryption keys, creating a Moving Target Defense (MTD).

### 2. CORE SPECIFICATION

RSME uses a hybrid arithmetic-logic approach to ensure high speed and strong resistance against algebraic attacks.

A. Encryption Formula:

$$C = [(((Data * Y) - P) + Y) XOR S] \text{ MOD } M$$

B. Decryption Formula:

$$Data = [(C + (k * M)) XOR S] - Y + P / Y$$

Key Variables:

Data: Plaintext input.

C: Resulting Ciphertext.

Y, P: Linear Transformation Keys.

S: Secret Salt (Non-linear XOR operator).

M: Dynamic Modulus (Diffusion boundary).

k: Modulo constant for restoration.

### 3. THE "AWARENESS" SENSOR (DELTA%)

The system monitors its internal stability to detect brute-force or side-channel attacks:

$$\Delta = |(Current\_State / Target) - 1| * 100$$

If  $\Delta > 0$ , the system identifies an anomaly and immediately executes a "Key Refresh" from a pool of 1 billion randomized keys stored in an offline Master Seed (Physical Book).

### 4. SECURITY FEATURES

a. Non-Linearity: The use of XOR (Bitwise Logic) breaks the linear mathematical pattern, making it impossible to solve via standard algebra.

b. Reactive Defense: The algorithm "jumps" to a new state (Index Shift) before an attacker can complete a brute-force cycle.

c.Lightweight: Optimized for IoT, Drones, and Satellite communications where CPU resources are limited but high security is mandatory.

d.Air-Gapped Root: The core seed remains offline, making remote "Root Key" theft impossible.

## 5. CONCLUSION

RSME Version 2.0 provides a robust, lightweight, and reactive security layer. By combining mathematical chaos with real-time intrusion detection, it offers a superior defense mechanism for modern digital assets.