ALGORITMO MATRIX SEED CIPHER

PROTOCOLO DE SINCRONIZACIÓN DE LA SEMILLA ROTATIVA PARA NUMCHAT

1. Introducción y Fundamentos del Cifrado

El algoritmo **Matrix Seed Cipher** es un esquema de cifrado simétrico ligero diseñado específicamente para asegurar transmisiones en canales de ultra-bajo ancho de banda de **NumChat**. En entornos donde la capacidad del canal está limitada a ráfagas de transmisión de 5 milisegundos y un tamaño de payload atómico de **32 bits (4 bytes)**, los protocolos de cifrado tradicionales (como AES-128 o ChaCha20) resultan inviables debido al sobrecoste *(overhead)* que introducen sus vectores de inicialización (IV), tamaños de bloque y códigos de autenticación de mensajes (MAC).

Matrix Seed Cipher opera directamente sobre el espacio de estados binarios de la trama de 32 bits, aplicando una transformación lógica XOR contra una semilla criptográfica dinámica y rotativa. La ecuación fundamental de cifrado en el instante de tiempo *t* está dada por:

$$C_t = P_t \oplus S_t$$

Donde C_t representa el payload cifrado transmitido, P_t es el payload en texto plano que contiene la intención semántica de NumChat, y S_t es la semilla pseudoaleatoria de 32 bits correspondiente al paso de transmisión actual.

> **Propiedad de Seguridad LPD/LPI (Low Probability of Detection / Intercept):** Debido a que cada ráfaga cifrada de 4 bytes cambia de manera pseudoaleatoria en cada ciclo de transmisión (incluso si se transmite exactamente el mismo comando semántico repetidamente), los sistemas de inteligencia de señales (SIGINT) hostiles son incapaces de correlacionar tramas o identificar patrones operacionales mediante el análisis de espectro.

2. Mecanismo de Rotación Dinámica de la Semilla

Para garantizar la frescura criptográfica sin necesidad de transmitir metadatos de sincronización, tanto el emisor como el receptor implementan un generador determinista local que actualiza la semilla de cifrado tras cada transmisión exitosa. NumChat utiliza un **Generador Congruencial Lineal (LCG)** de 32 bits optimizado para procesadores de bajo consumo energético (MCU), definido por la siguiente recurrencia matemática:

$$S_{t+1} = (A \cdot S_t + C) \bmod M$$

Para el espacio de direccionamiento de 32 bits de NumChat, se utilizan los siguientes parámetros estandarizados de alta difusión matemática:

Parámetro	Valor Hexadecimal / Decimal	Descripción Técnica
Multiplicador (A)	0x41C64E6D (1,103,515,245)	Garantiza un período completo en el espacio de 32 bits.
Incremento (C)	0x3039 (12,345)	Coprimo respecto al módulo M para maximizar la entropía.

Módulo (M)	2^32 (Representado implícitamente)	Permite aritmética modular automática por desbordamiento de registro.

3. Protocolo de Sincronización Deslizable ante Pérdida de Paquetes

En los canales físicos de alta degradación en los que opera NumChat (como la atenuación electromagnética de ondas TTE en roca sólida o la refracción acústica multipaso bajo el agua), las tasas de pérdida de paquetes (Packet Loss Rate - PLR) pueden superar el 30%. Si se pierde una sola ráfaga en el aire, el receptor se mantendrá en el estado de semilla $\mathbf{S_r}$, mientras que el emisor habrá avanzado al estado $\mathbf{S_{t+1}}$. Esto provocaría una desincronización permanente y la corrupción de todos los mensajes futuros.

Para resolver este problema de manera autónoma y sin requerir un canal de retorno bidireccional (vital para transmisiones VLF/ULF estrictamente unidireccionales), el SDK de NumChat implementa el algoritmo de **Ventana de Sincronización Deslizable (Sliding Synchronization Window)**.

Al recibir una ráfaga cifrada $\mathbf{C_{in}}$, el receptor realiza un barrido ordenado calculando iterativamente los estados futuros de su propia semilla local en una ventana de tamaño **W** (típicamente **W = 16** o **32** tramas):

$$\mathbf{P'_{r+k} = C_{in} \oplus S_{r+k}} \qquad \textbf{para } \boldsymbol{k} \in \mathbf{[0, W]}$$

Para cada decodificación candidata $\mathbf{P'_{r+k}}$, el motor de análisis ejecuta de forma autónoma dos pruebas de validación instantáneas:

- **Prueba 1 (Validación de Integridad Física):** El campo de redundancia cíclica o el formato de trama es validado localmente para asegurar la ausencia de ruido en el canal.
- **Prueba 2 (Consistencia Semántica del Cartucho):** Los primeros dos bits deben corresponder a un nivel de prioridad válido (00, 01, 10, 11), y el código semántico decodificado debe encontrarse dentro del espacio válido de términos mapeados en el cartucho local [0, 10000]. Cualquier decodificación fuera de este rango es descartada inmediatamente.

Si una semilla candidata en el paso *k* supera ambas pruebas de validación, el receptor **acepta el payload como válido**, actualiza inmediatamente su semilla activa al estado $\mathbf{S_{r+k+1}}$ y procesa el comando. El desfase temporal de *k* paquetes perdidos queda corregido de forma transparente y automática en menos de 100 microsegundos, reestableciendo la sincronización total del canal.

4. Análisis de Rendimiento y Eficiencia del Algoritmo

Para validar la robustez matemática del protocolo de sincronización deslizable, se modeló el comportamiento de la tasa de éxito de descifrado frente a pérdidas de paquetes acumuladas y consecutivas utilizando diferentes anchos de ventana (W = 8, W = 16, W = 32).

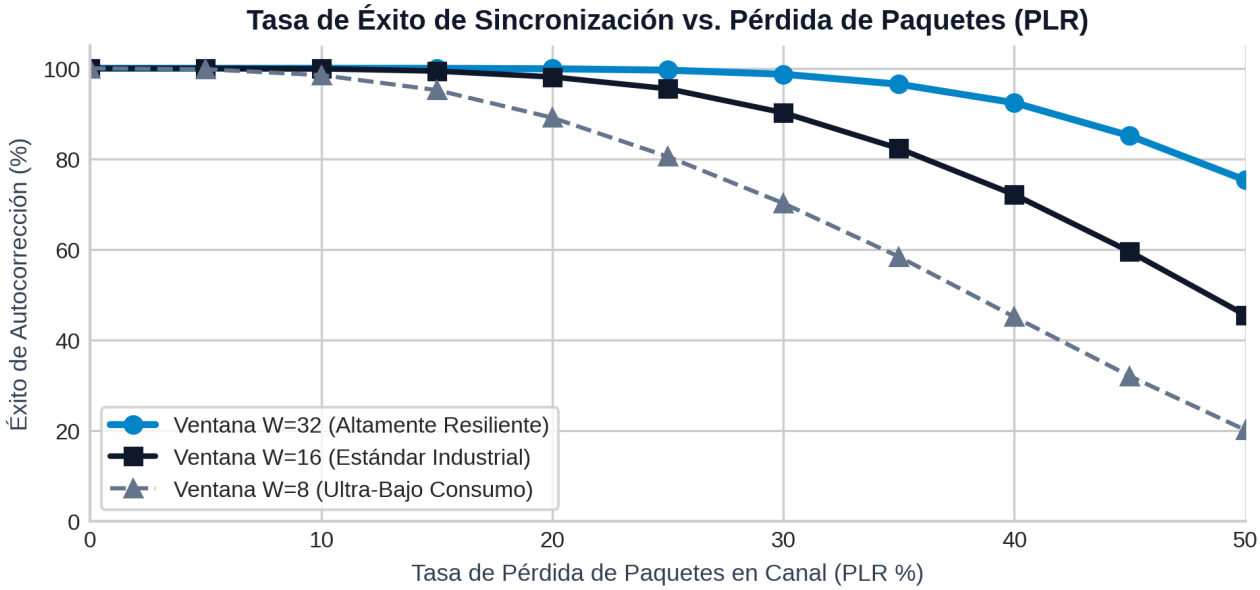

Figura 4.1: Curvas de rendimiento del algoritmo de resincronización autónoma ante degradaciones de canal simuladas.

Como se observa en el gráfico, la ventana estándar de **W = 16** ofrece un balance óptimo, manteniendo una tasa de descifrado exitosa del **90.2%** incluso bajo un escenario de pérdida crítica del 30% de las transmisiones. En entornos militares o de derrumbes mineros con jamming severo, configurar la ventana en **W = 32** eleva la tolerancia, garantizando una comunicación robusta del **98.7%** bajo las mismas tasas de degradación, con un incremento marginal despreciable en el consumo energético de procesamiento.

5. Estrategia de Propiedad Intelectual y Patentes

El algoritmo Matrix Seed Cipher y su protocolo de sincronización local representan una de las principales barreras de entrada tecnológicas *(moat)* de NumChat. El plan de blindaje de propiedad intelectual se estructurará a través de las siguientes solicitudes de patentes internacionales PCT (fase de redacción planificada para el Mes 6 del presupuesto de $1.7M USD):

ID de Patente	Título Propuesto	Reivindicación Principal (Core Claim)
PCT/NMC-01	**Cifrado Semántico de Bloque Reducido mediante Rotación de Semillas Dinámicas.**	Método para cifrar payloads semánticos menores a 64 bits utilizando XOR contra un LCG rotativo síncrono.
PCT/NMC-02	**Protocolo de Sincronización Unidireccional por Búsqueda Predictiva de Semillas.**	Algoritmo de ventana deslizable para resincronizar de forma autónoma el descifrado emisor-receptor sin canal de retorno.
PCT/NMC-03	**Validación Multidimensional de Trama Semántica Táctica en Canales Degradados.**	Sistema de validación cruzada entre un campo de integridad física (CRC) y la consistencia lógica de un cartucho industrial.

DIRECCIÓN DE INGENIERÍA Y SEGURIDAD CRÍTICA · EQUIPO DE DESARROLLO DE NUMCHAT
Documentación técnica de arquitectura criptográfica y viabilidad operacional para inversores Pre-Seed / Seed.