Reporte Didáctico de Ataques - CryptJAD

Este documento explica de forma clara y pedagógica los resultados de un ataque lineal. Cada sección describe qué significan las tablas y cómo deben interpretarse los datos.

1. Información General del Ataque

Esta sección resume los parámetros de la ejecución del ataque. Los datos permiten contextualizar la dificultad del análisis.

Algoritmo: Baby AES
Número de rondas: 4
Pares usados: 1024
Clave real: 0101 0000 0000 0000

2.1 Tabla 1: Distribución Lineal (LAT)

La **Linear Approximation Table (LAT)** muestra cuán fuerte es la correlación entre combinaciones de bits de entrada y salida. En un sistema perfectamente aleatorio, todos los valores deberían estar cercanos a cero. Los valores altos (positivos o negativos) indican un sesgo aprovechable para el ataque.

b0	b1	b2	b3	b4	b5	b6	b7	b8	b9	b10	b11	b12	b13	b14	b15
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	-1/4	-1/4	0	0	1/4	1/4	0	1/2	1/4	-1/4	0	0	1/4	-1/4	1/2
0	-1/4	-1/4	-1/2	1/4	-1/2	0	1/4	0	1/4	-1/4	0	1/4	0	0	-1/4
0	1/2	0	0	1/4	-1/4	-1/4	-1/4	0	0	-1/2	0	-1/4	-1/4	-1/4	1/4
0	-1/4	1/4	0	-1/2	-1/4	-1/4	0	-1/4	1/2	0	-1/4	-1/4	0	0	1/4
0	0	0	-1/2	0	0	1/2	0	-1/4	-1/4	1/4	-1/4	-1/4	-1/4	-1/4	1/4
0	0	0	0	1/4	1/4	1/4	1/4	-1/4	1/4	-1/4	1/4	-1/2	0	1/2	0
0	1/4	1/4	0	-1/4	-1/2	1/2	-1/4	1/4	0	0	1/4	0	1/4	1/4	0
0	1/4	-1/2	-1/4	-1/4	0	-1/4	0	1/4	0	1/4	0	-1/2	1/4	0	-1/4
0	0	1/4	-1/4	-1/4	1/4	0	0	1/4	-1/4	-1/2	-1/2	0	0	1/4	-1/4
0	1/2	-1/4	1/4	0	0	1/4	1/4	-1/4	1/4	0	-1/2	1/4	1/4	0	0
0	1/4	0	-1/4	0	1/4	0	-1/4	1/4	1/2	1/4	0	1/4	-1/2	1/4	0
0	0	1/4	1/4	1/4	-1/4	0	1/2	1/2	0	1/4	-1/4	-1/4	-1/4	0	0
0	1/4	0	-1/4	-1/4	0	-1/4	1/2	0	-1/4	0	1/4	1/4	0	1/4	1/2
0	-1/4	-1/2	1/4	0	-1/4	0	-1/4	0	-1/4	0	-1/4	0	-1/4	1/2	1/4
0	0	-1/4	1/4	-1/2	0	1/4	1/4	0	0	-1/4	1/4	0	-1/2	-1/4	-1/4

3. Candidatos de Subclave

En esta sección se muestran los **candidatos de subclave** que aparecen con mayor frecuencia. La hipótesis del ataque es que el candidato más repetido o con mayor sesgo corresponde a la subclave real del cifrado. Este método no garantiza certeza absoluta, pero reduce significativamente el espacio de búsqueda.

Tabla 1: Top Candidatos

Index	Counter	Key
5	130	0101 0000 0000 0000

Index	Counter	Key
7	-128	0111 0000 0000 0000
119	-120	0111 0000 0000 0111
10	-118	1010 0000 0000 0000
35	-114	0011 0000 0000 0010
38	-110	0110 0000 0000 0010
117	110	0101 0000 0000 0111
134	106	0110 0000 0000 1000
210	104	0010 0000 0000 1101
101	98	0101 0000 0000 0110
106	-98	1010 0000 0000 0110
122	-98	1010 0000 0000 0111
8	94	1000 0000 0000 0000
47	-94	1111 0000 0000 0010
170	94	1010 0000 0000 1010
9	92	1001 0000 0000 0000
209	-92	0001 0000 0000 1101
102	-90	0110 0000 0000 0110
232	-90	1000 0000 0000 1110
234	90	1010 0000 0000 1110

4. Conclusiones y Observaciones

A continuación se presenta una interpretación didáctica de los resultados obtenidos:

El ataque lineal se ejecutó con éxito sobre el algoritmo Baby AES con 4 rondas.
Se usaron 1024 pares de texto plano-cifrado, con un tiempo de ejecución de N/A.
Los resultados muestran que algunas subclaves aparecen repetidamente como candidatas más probables. Esto refleja la existencia de una correlación estadística que puede explotarse para reducir el espacio de búsqueda.