Reporte de Ataque Criptográfico

CryptJAD - Herramienta Educativa

Este documento presenta un análisis detallado de un ataque criptográfico. Incluye la metodología paso a paso, resultados intermedios y conclusiones.

1. Información General del Ataque

Esta sección resume los parámetros y configuración del ataque ejecutado.

Tipo de ataque	Diferencial
Diferencia entrada (∆u■)	[a^2 + a 0] [0 a^3]
Diferencia salida (∆u■)	[a^3 + a 0] [a^3 + a^2 0]
Ratio de propagación	0.01562500
Mejor llave parcial	[a^3 0] [0 a^2 + 1]
Mejor llave (binario)	1000 0000 0000 0101
Apariciones	23

2. Tablas de Distribución

2.1 Tabla de Distribución 1

Esta tabla muestra la distribución de diferencias (DDT). Los valores altos indican diferencias con alta probabilidad de propagación.

Δy=0	Δy=1	Δy=2	Δy=3	Δy=4	Δy=5	Δy=6	Δy=7	Δy=8	Δy=9	Δy=A	Δy=B	Δy=C	Δy=D	Δy=E	Δy=F
16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	2	2	2	2	0	0	0	2	0	0	0	2	4	0	0
0	2	0	4	2	2	2	0	0	2	0	0	0	0	0	2
0	2	4	0	0	2	0	0	2	2	0	2	0	0	2	0
0	0	2	0	4	2	0	0	0	0	2	0	2	0	2	2
0	0	0	2	0	0	0	2	4	2	0	0	2	0	2	2
0	4	0	0	0	2	0	2	0	2	2	0	2	2	0	0
0	2	0	0	0	0	2	0	0	0	0	2	4	2	2	2
0	2	2	0	0	0	2	2	2	0	2	0	0	0	0	4
0	0	2	2	0	0	0	0	0	2	2	4	0	2	0	2
0	0	2	0	2	0	2	2	0	4	0	2	2	0	0	0
0	0	0	0	2	0	2	0	2	2	4	0	0	2	2	0
0	0	0	2	0	4	2	0	2	0	2	2	2	0	0	0
0	0	0	0	2	2	0	4	2	0	0	2	0	2	0	2
0	0	2	2	0	2	4	2	0	0	0	0	0	2	2	0
0	2	0	2	2	0	0	2	0	0	2	2	0	0	4	0

3. Candidatos de Subclave

Los candidatos están ordenados por frecuencia o score. El candidato con mayor valor tiene la mayor probabilidad de ser la subclave correcta.

Tabla 1: Candidatos

Index	Counter	Key
56	23	[a^3 0] [0 a^2 + 1]
53	11	[a^3 0] [0 a^2 + a]
152	11	[a^3 + a 0] [0 a^2 + 1]
52	10	[a^3 0] [0 a + 1]
48	9	[a^3 0] [0 0]
72	8	[a + 1 0] [0 a^2 + 1]
158	6	[a^3 + a 0] [0 a^3 + 1]
248	6	[1 0] [0 a^2 + 1]
62	5	[a^3 0] [0 a^3 + 1]
78	5	[a + 1 0] [0 a^3 + 1]
144	5	[a^3 + a 0] [0 0]
148	5	[a^3 + a 0] [0 a + 1]
149	5	[a^3 + a 0] [0 a^2 + a]
254	5	[1 0] [0 a^3 + 1]
36	4	[a^2 0] [0 a + 1]
104	4	[a^3 + a^2 0] [0 a^2 + 1]
6	3	[0 0] [0 a^3 + a^2]
9	3	[0 0] [0 a^3 + a]
22	3	[a 0] [0 a^3 + a^2]
25	3	[a 0] [0 a^3 + a]

4. Conclusiones y Observaciones

A continuación se presenta una interpretación de los resultados obtenidos:

El ataque Diferencial se ejecutó con éxito sobre el algoritmo N/A.

La probabilidad del trail diferencial es 0.01562500, permitiendo distinguir la clave correcta.

Los resultados muestran candidatos de subclave ordenados por frecuencia. El candidato con mayor aparición tiene la mayor probabilidad de ser correcto.