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.

Algoritmo	Simplified DES (S-DES)
Tipo de ataque	Lineal
Número de rondas	2
Pares usados	5000
Clave real (10 bits)	0011100100
Subkey2 real (8 bits)	11010000
Subkey2 recuperada	11010000
Score	15101
S0 aproximación	α=1111 β=11 LAT=-12
S1 aproximación	α=1101 β=01 LAT=12

2. Tablas de Distribución

2.1 Tabla de Distribución 1

Esta tabla muestra las correlaciones lineales entre bits de entrada y salida. Los valores cercanos a ±1 indican fuertes correlaciones explotables.

β=00	β=01	β=10	β=11
1	-1/8	-1/8	0
0	-5/8	1/8	1/4
0	1/8	1/8	0
0	1/8	-1/8	1/4
0	1/8	1/8	0
0	1/8	3/8	-1/4
0	3/8	3/8	0
0	-1/8	1/8	-1/4
0	1/8	1/8	0
0	-3/8	-1/8	-1/4
0	-1/8	-1/8	0
0	-1/8	1/8	-1/4
0	-1/8	-1/8	0
0	-1/8	-3/8	1/4
0	-3/8	5/8	0
0	1/8	-1/8	-3/4

2.2 Tabla de Distribución 2

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

β=00	β=01	β=10	β=11
1	0	1/8	1/8
0	1/4	-1/8	-3/8
0	1/4	1/8	-1/8
0	0	-5/8	3/8
0	0	1/8	1/8
0	-1/4	-1/8	1/8
0	-1/4	1/8	3/8
0	0	3/8	3/8
0	0	-1/8	-1/8
0	1/4	1/8	-1/8
0	1/4	3/8	1/8
0	0	1/8	1/8

β=00	β=01	β=10	β=11
0	0	-1/8	-1/8
0	3/4	1/8	3/8
0	-1/4	3/8	-3/8
0	0	1/8	1/8

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

k4 (4 bits)	Desviación	Count=0	N
0010	-1914	586	
0011	-1914	586	
0110	-1900	600	
0111	-1900	600	
1110	-1886	614	
1111	-1886	614	
0000	-1877	623	
0001	-1877	623	

Tabla 2: Candidatos

k4 (4 bits)	Desviación	Count=0	N
1000	1935	4435	
1011	1935	4435	
1001	1904	4404	
1010	1904	4404	
0000	1888	4388	
0011	1888	4388	
0001	1868	4368	
0010	1868	4368	

4. Conclusiones y Observaciones

A continuación se presenta una interpretación de los resultados obtenidos:

El ataque Lineal se ejecutó con éxito sobre el algoritmo Simplified DES (S-DES).

El cifrado usa 2 rondas.

Se analizaron 5000 pares de texto plano-cifrado.

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