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: Simplified DES (S-DES)
Número de rondas: 2
Pares usados: 5000
Clave real (10 bits): 0011100100
Subkey2 real (8 bits): 11010000
Subkey2 recuperada: 00101011
Score del mejor candidato: 15101
S0 mejor aproximación: α=1111 β=11 LAT=-12
S1 mejor aproximación: α=1101 β=01 LAT=12

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.

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 2: 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.

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
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

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

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: Top Candidatos

k4 (4 bits)	Desviación	Count=0	N
1000	1935	4435	

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

Tabla 3: Top Candidatos

Subkey2 (8 bits)	Score	Detalles

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 Simplified DES (S-DES) con 2 rondas.
Se usaron 5000 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.