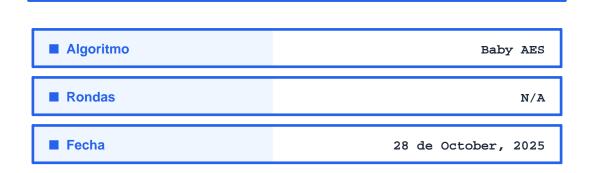
REPORTE DE CRIPTOANÁLISIS

Ataque Diferencial en Baby AES



Documento generado automáticamente por CryptJAD Herramienta Educativa de Criptoanálisis

TRAZA DETALLADA DEL ATAQUE

Este reporte documenta cada fase del criptoanálisis ejecutado. Incluye los cálculos intermedios, decisiones algorítmicas y resultados parciales que conducen a la recuperación de la subclave.

Fase 1: Construcción de la DDT

■ Tabla de distribución de diferencias calculada

■■ DDT calculada

■ Nota: DDT de 16x16 calculada exitosamente

28/10/2025 Página 2 de 7

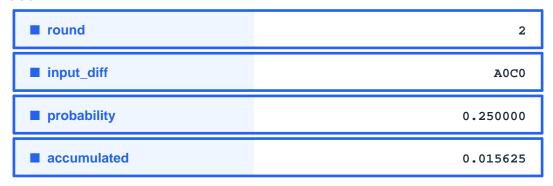
Fase 2: Trail Diferencial

■ Trail de 2 rondas construido

Paso 1

■ round	1
■ input_diff	E000
■ probability	0.062500
■ accumulated	0.062500

Paso 2



Paso 3

■ final_difference	A0C0
■ total_probability	0.015625

28/10/2025 Página 3 de 7

Fase 3: Candidatos Generados

■ 256 candidatos de subclave

Paso 1

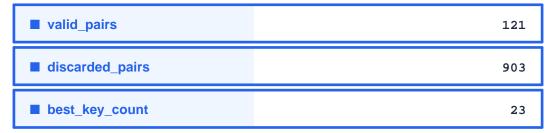
■ total_candidates 256

28/10/2025 Página 4 de 7

Fase 4: Análisis Estadístico

■ Mejor candidato aparece 23 veces

Paso 1



28/10/2025 Página 5 de 7

TABLAS DE DISTRIBUCIÓN

■ Tabla 1

∆y=0	∆y=1	∆y=2	∆y=3	∆ y=4	∆y=5	∆ y=6	∆ y=7	∆ y=8	∆y=9	∆y=A	∆у=В	∆y=C	∆y=D	∆у=Е	∆y=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

28/10/2025 Página 6 de 7

CANDIDATOS DE SUBCLAVE

Index	Counter	Key
56	23	8005
53	11	8006
152	11	A005
52	10	8003
48	9	8000
72	8	3005
158	6	A009
248	6	1005
62	5	8009
78	5	3009
144	5	A000
148	5	A003
149	5	A006
254	5	1009
36	4	4003
104	4	C005
6	3	000C
9	3	A000
22	3	200C
25	3	200A

28/10/2025 Página 7 de 7