Comenzado el	jueves, 22 de febrero de 2024, 09:20
Estado	Finalizado
Finalizado en	jueves, 29 de febrero de 2024, 19:12
Tiempo empleado	7 días 9 horas
Calificación	**7,50** de 10,00 (**75**%)

Pregunta 1

Parcialmente correcta

Se puntúa 7,50 sobre 10,00

Aplicando AES sobre el texto en claro 0001 0203 0405 0607 0809 0A0B 0C0D 0E0F y con la clave 0101 0101 0101 0101 0101 0101 0101 0101 se obtiene lo siguiente (usando notación [fila 1 | fila 2 | fila 3 | fila 4]):

estado inicial	[01 05 09 0D | 00 04 08 0C | 03 07 0B 0F | 02 06 0A 0E]	✗
estado después de la primera ShiftRows	[7C 6B 01 D7 | F2 30 FE 63 | 2B 76 7B C5 | AB 77 6F 67]	✓
estado después de la primera SubBytes	[7C 6B 01 D7 | 63 F2 30 FE | 7B C5 2B 76 | 77 6F 67 AB]	✓
estado después de la primera AddRoundKey	[01 05 09 0D | 00 04 08 0C | 03 07 0B 0F | 02 06 0A 0E]	✓

Respuesta parcialmente correcta.

Ha seleccionado correctamente 3.
La respuesta correcta es:
estado inicial → [00 04 08 0C | 01 05 09 0D | 02 06 0A 0E | 03 07 0B 0F],

estado después de la primera ShiftRows → [7C 6B 01 D7 | F2 30 FE 63 | 2B 76 7B C5 | AB 77 6F 67],

estado después de la primera SubBytes → [7C 6B 01 D7 | 63 F2 30 FE | 7B C5 2B 76 | 77 6F 67 AB],

estado después de la primera AddRoundKey → [01 05 09 0D | 00 04 08 0C | 03 07 0B 0F | 02 06 0A 0E]