

Comenzado el	jueves, 29 de febrero de 2024, 19:15
Estado	Finalizado
Finalizado en	jueves, 7 de marzo de 2024, 18:14
Tiempo empleado	6 días 22 horas
Calificación	10,00 de 10,00 (100%)

Pregunta 1

Correcta

Se puntúa 2,00 sobre 2,00

Realiza la iteración inicial y la primera iteración del bucle de iteraciones del cifrado estándar en el modo CBC, sobre los siguientes parámetros:

Clave: 04040404 03030303 02020202 00000000

Bloque de Texto Original: 00112233 44556677 8899AABB CCDDEEFF

IV: 00112233 43526170 8E9FACBD C8D9EAFB

¿Cuál es el estado salida de la primera SubBytes? Usa la notación [fila 1 | fila 2 | fila 3 | fila 4]

Respuesta: [F2 F2 F2 F2 | F2 F2 F2 F2 | F2 F2 F2 F2 | F2 F2 F2 F2] ✓

La respuesta correcta es: [F2 F2 F2 F2 | F2 F2 F2 F2 | F2 F2 F2 F2 | F2 F2 F2 F2]

Pregunta 2

Correcta

Se puntúa 2,00 sobre 2,00

Realiza la iteración inicial y la primera iteración del bucle de iteraciones del cifrado estándar en el modo CBC sobre los siguientes parámetros:

Clave: 04040404 03030303 02020202 00000000

Bloque de Texto Original: 00112233 44556677 8899AABB CCDDEEFF

IV: 00112233 43526170 8E9FACBD C8D9EAFB

¿Cuál es el estado salida de la primera AddRoundKey? Usa la notación [fila 1 | fila 2 | fila 3 | fila 4]

Respuesta: [04 04 04 04 | 04 04 04 04 | 04 04 04 04 | 04 04 04 04] ✓

La respuesta correcta es: [04 04 04 04 | 04 04 04 04 | 04 04 04 04 | 04 04 04 04]

Pregunta 3

Correcta

Se puntúa 2,00 sobre 2,00

Realiza la iteración inicial y la primera iteración del bucle de iteraciones del cifrado estándar en el modo CBC, sobre los siguientes parámetros:

Clave: 04040404 03030303 02020202 00000000

Bloque de Texto Original: 00112233 44556677 8899AABB CCDDEEFF

IV: 00112233 43526170 8E9FACBD C8D9EAFB

¿Cuál es el estado salida de la primera ShiftRows? Usa la notación [fila 1 | fila 2 | fila 3 | fila 4]

Respuesta: [F2 F2 F2 F2 | F2 F2 F2 F2 | F2 F2 F2 F2 | F2 F2 F2 F2]



La respuesta correcta es: [F2 F2 F2 F2 | F2 F2 F2 F2 | F2 F2 F2 F2 | F2 F2 F2 F2]

Pregunta 4

Correcta

Se puntúa 2,00 sobre 2,00

Realiza la iteración inicial y la primera iteración del bucle de iteraciones del cifrado estándar en el modo CBC, sobre los siguientes parámetros:

Clave: 04040404 03030303 02020202 00000000

Bloque de Texto Original: 00112233 44556677 8899AABB CCDDEEFF

IV: 00112233 43526170 8E9FACBD C8D9EAFB

¿Cuál es el estado salida de la primera MixColumn? Usa la notación [fila 1 | fila 2 | fila 3 | fila 4]

Respuesta: [F2 F2 F2 F2 | F2 F2 F2 F2 | F2 F2 F2 F2 | F2 F2 F2 F2]



La respuesta correcta es: [F2 F2 F2 F2 | F2 F2 F2 F2 | F2 F2 F2 F2 | F2 F2 F2 F2]

Pregunta 5

Correcta

Se puntúa 2,00 sobre 2,00

Realiza la iteración inicial y la primera iteración del bucle de iteraciones del cifrado estándar en el modo CBC sobre los siguientes parámetros:

Clave: 04040404 03030303 02020202 00000000

Bloque de Texto Original: 00112233 44556677 8899AABB CCDDEEFF

IV: 00112233 43526170 8E9FACBD C8D9EAFB

¿Cuál es el estado salida de la segunda AddRoundKey, primera del bucle? Usa la notación [fila 1 | fila 2 | fila 3 | fila 4]

Respuesta: [94 97 95 95 | 95 96 94 94 | 95 96 94 94 | 95 96 94 94]



La respuesta correcta es: [94 97 95 95 | 95 96 94 94 | 95 96 94 94 | 95 96 94 94]