

Comenzado el miércoles, 31 de enero de 2024, 18:39

Estado Finalizado

Finalizado en miércoles, 31 de enero de 2024, 20:13

Tiempo empleado 1 hora 33 minutos

Calificación 10,00 de 10,00 (100%)

Pregunta 1

Correcta

Se puntúa 1,00 sobre 1,00

En el último paso del generador ChaCha20, ¿qué se suma al estado final que resulta de las 20 iteraciones?

Respuesta: el estado original



La respuesta correcta es: El estado inicial

Comentario:

Pregunta 2

Correcta

Se puntúa 1,00 sobre 1,00

¿Apellido del desarrollador de Chacha20?

Respuesta: Bernstein



La respuesta correcta es: Bernstein

Pregunta 3

Correcta

Se puntúa 1,00 sobre 1,00

¿En cuántas palabras se estructura el estado interno en ChaCha20?

Respuesta: 16



La respuesta correcta es: 16

Pregunta 4

Correcta

Se puntúa 1,00 sobre 1,00

¿De cuántos bits es el estado interno en ChaCha20?

Respuesta: 512



La respuesta correcta es: 512

Pregunta 5

Correcta

Se puntúa 1,00 sobre 1,00

¿Desde qué versión de TLS está disponible Chacha20? (Responde solo *.*.)

Respuesta: 1.2



La respuesta correcta es: 1.2

Pregunta 6

Correcta

Se puntúa 1,00 sobre 1,00

En el RFC7539, ¿de cuántos bits es el contador?

Respuesta: 32



La respuesta correcta es: 32

Pregunta 7

Correcta

Se puntúa 1,00 sobre 1,00

Además de Rotar y XOR, ¿cuál es la otra operación en ARX?

Respuesta: adición



La respuesta correcta es: Sumar

Comentario:

Pregunta 8

Correcta

Se puntúa 1,00 sobre 1,00

¿Sobre qué se aplican las iteraciones impares en ChaCha20?

Respuesta: 

La respuesta correcta es: columnas

Pregunta 9

Correcta

Se puntúa 1,00 sobre 1,00

¿Cómo se llama el código de autenticación de mensaje que se suele combinar con ChaCha20?

Respuesta: 

La respuesta correcta es: Poly1305

Pregunta 10

Correcta

Se puntúa 1,00 sobre 1,00

¿De cuántos bits es la clave en ChaCha20?

Respuesta: 

La respuesta correcta es: 256