

Pregunta 1

Finalizado

Puntuación 0,00 sobre 1,25

 Marcar pregunta

¿Cómo representamos los 9 bits en la salida de un elemento en la compresión de LZSS?

Los primeros 5 bits se utilizan para poder escribir el desplazamiento, los 4 bits que quedan son para escribir la longitud. El bit de la posición 0 es el que nos dice si este ya estaba en la ventana o no se le llama la bandera.

Utilizando 2 bytes.

Si es el primer byte en aparecer, los primeros 8 bits van en el primer byte y el último bit será agregado al siguiente byte.

Si en caso no es el primer byte, se utilizarán los primeros N bits, correspondientes a los bits disponibles del byte anterior y los (9-N) restantes serán agregados al siguiente byte

Pregunta 2

Finalizado

Puntúa 1,50 sobre 1,50

 Marcar pregunta

¿Para qué se utiliza la llave del cifrado DES?

Se utiliza para generar las llaves que el usuario no conoce, ya que estas llaves son calculadas y a partir de las llaves calculadas se realiza el proceso de cifrado y descifrado.

Para generar las llaves k para ser usadas en la función f_k

Comentario:

Pregunta 3

Finalizado

Puntuá 1,50 sobre 1,50

 Marcar pregunta

¿Cuál es la diferencia entre el cifrado y el descifrado de SDES?

La diferencia es que en el cifrado se comienza con una permutación inicial se tiene la llave 1, 2 y la de 10 bits. La diferencia es que en el cifrado comienza el proceso del xor con la llave 1 y continua, mientras que para descifrar se invierte el proceso y se aplica la llave 2 en el xor hasta llegar al xor con la llave 1 para al finalizar usar una permutación inversa.


Se invierten las llaves en las funciones de f_k

Comentario:

Pregunta 4

Finalizado

Puntuación 1,50 sobre 1,50

 Marcar pregunta

¿Cuándo utilizamos una firma digital?

Cuando se quiere dar autenticidad de un documento, pero este va en un documento aparte, valida la identidad de quien envió, también la falsificación de documentos.

*más que todo cuando alguien no puede hacer el proceso físicamente se utilizan las firmas digitales.


Cuando queremos demostrar el remitente de un mensaje

Comentario:

Pregunta 5

Finalizado

Puntuación 0,75 sobre 1,25

 Marcar pregunta

¿Cómo se representa la salida un grupo de bytes que ya aparecieron en la ventana corregida?

El bit de la posición 0 es el que nos dice si este ya estaba en la ventana o no, entonces si ya se encuentra cambia a 1 y también se ponen los bits de longitud que depende de cuantas veces se encuentra en la ventana.

Comentario:

No es cuántas veces se encuentra, es cuál es la longitud de los caracteres que están en la ventana

Pregunta 6

Finalizado

Puntúa 1,25 sobre 1,25

 Marcar pregunta

¿Cuál es la propiedad más importante de las claves?

su longitud porque nos dice que tan fuerte es, aunque que también se toma en cuenta su aleatoriedad y periodo de uso.

La longitud

Comentario:

Pregunta 7

Finalizado

Puntuación 0,50 sobre 1,50



Marcar pregunta

¿Qué tipos de cifrado asimétrico existen?

RSA, Diffie-Hellman, firmas digitales

Firma digital

Cifrado con llave pública

Comentario:

Pregunta 8

Finalizado

Puntúa 1,25 sobre 1,25



Marcar pregunta

¿Qué se hace en un cifrado de transposición?

Lo que se hace es la reorganización de caracteres , solo se debe tener en cuenta es que el emisor y el receptor deben tener la llave.


Reorganización de letras o caracteres

Comentario:

Pregunta 9

Finalizado

Puntuá 0,00 sobre 1,50

 Marcar pregunta

¿Quiénes poseen la llave pública?

Receptor

Quien desee comprobar la firma
del emisor

Quien desee cifrar un mensaje al
dueño de la llave privada

Comentario:

¿El receptor de qué?

Pregunta **10**

Finalizado

Puntuá 1,25 sobre 1,25



Marcar pregunta

¿Cuál sería la ventana corregida

Pregunta 11

Finalizado

Puntúa 1,50 sobre 1,50



Marcar pregunta

Explique la función SDES

$$\text{cypherText} = IP^{-1}(f_{k2}(SW(f_{k1}(IP(\text{plainText}))))))$$

tenemos la entrada como plain text, pasa por la función permutación inicial, nos devuelve un byte ese byte pasa por la función con la llave uno, devuelve otro byte y pasa por un swap, luego devuelve otro byte, pasa por la llave 2, devuelve otro byte que pasa por la permutación inversa y ese sería los bytes cifrados.

Comentario:

Pregunta 12

Finalizado

Puntuá 1,25 sobre 1,25



Marcar pregunta

¿Qué se utiliza para la trasposición de un cifrado César?

se utiliza la palabra con la cual se empezara el abecedario, en el abecedario no puede tener letras repetidas de la palabra.


Una clave/llave

Comentario:

Pregunta 13

Finalizado

Puntuá 1,50 sobre 1,50

 Marcar pregunta

¿A qué se refieren las Rondas en SDES?

Se refiere al número de veces que pasará por el algoritmo, eso quiere decir en el número de llaves que se utiliza para hacer el proceso con el xor hasta llegar a la permutación inversa. En esta caso el número de rondas para SDES es de 2.

La cantidad de iteraciones de la función f_k y *SWAP* que se realizarán.

f_k se realizará N veces igual a la cantidad de Rondas que hay en SDES (o DES) y *SWAP* será N-1 veces

Comentario:

Pregunta 14

Finalizado