Parcial 2

Carlos Javier Alonso Caldera

1.- En un sistema de cifrado de flujo, ¿de qué tamaño tiene que ser la secuencia pseudoaleatoria generada para el proceso de cifrado?

El tamaño de la secuencia es del mismo tamaño que el mensaje que se desea cifrar.

2.- ¿En el sistema de Vernam, por qué se utiliza la función XOR para el cifrado? ¿Por qué no otra función como AND u OR?

Porque es una función transformable, usa XOR porque opera como una suma binaria digito a digito, en el caso de usar AND funciona como una multiplicación algebraica y en caso de usar OR es una suma, XOR si realiza la ecuación de suma para binarios.

3.- Describa para qué sirve el proceso KSA en el RC4

Crea una matriz S de 256 elementos con números secuenciales del 0 al 256, crea otra matriz t similar a la matriz S donde escribiremos la clave y esta se repite las veces necesarias hasta que se rellene la matriz t.

Aplicamos KSA en las matrices S y t, este algoritmo se aplicará en todas las posiciones de la matriz S, con una variable iterativa “i” tomará los valores de 0 hasta 255. Con las variables de “i” y de “j”, como resultado de esta operación tendremos nuestra matriz S con las posiciones de los elementos acomodadas en otro orden.

Esta matriz S ayuda al algoritmo PRGA en generar la secuencia de clave que permite cifrar o descifrar el mensaje.

4.- ¿Por qué los cifrados de bloque utilizan tamaños de bloque relativamente pequeños, de 16, 32, 64, 128 bits? ¿Por qué no por ejemplo tamaños de 4096 bits o más?

Porque el cifrar bloques tan grandes como de 4096 bits seria prácticamente cifrar todo el texto junto lo cual sería ineficiente.

5.- ¿Qué representa la cadena RC5-64/32/20?

El 64 representa un bloque de 64 bits, el cual es el bloque a cifrar, 32 es el número de vueltas a realizar y 20 es el tamaño del bloque de la clave.

6.- ¿A qué se refiere que un cifrado sea tipo Feistel?

Es un método de cifrado en bloque desarrollado por Horst Feistel, una gran cantidad de cifrado por bloques lo utilizan, mejor conocido como Data Encryption Standard (DES)

El procedimiento de cifrado utiliza la estructura Feistel que contiene múltiples rondas de manejo del texto en claro, cada redondo que contiene de un "sustitución" Paso monitoreado por un paso de permutación.

7.-En el algoritmo IDEA, ¿en qué es diferente la transformación final a las rondas iniciales?

En un principio realiza 8 rondas donde se aplican operaciones como sumas, multiplicaciones y funciones XOR a los bits, al final de estas 8 rondas se aplica una última ronda en la que aplicaremos funciones de multiplicación y suma con respecto a los datos generados por las 8 iteraciones pasadas.

8.- ¿Cuál es la diferencia entre AES y Rijndael?

AES cuenta con un tamaño fijo de bloque de 128 bits y un tamaño de clave variable entre 128, 192 o 256 bits, a diferencia de Rijndel se puede especificar con tamaños de bloque y clave en cualquier múltiplo de 32 bits, con un mínimo de 128 bits y un máximo de 256 bits.

9.- ¿Por qué las funciones hash criptográficas se enfocan en la integridad y no en la confidencialidad de los datos?

El objetivo principal del hash es que el mensaje no haya sido modificado sin importar si han visto el mensaje.

10.- Describa el proceso a realizar si la entidad A le quiere enviar un documento a la entidad B firmado digitalmente, de forma que cuando la entidad B lo reciba pueda estar seguro que realmente proviene de A

1. Obtenemos el hash del documento de la entidad “A”.
2. Ciframos el hash con la llave privada de la entidad “A”.
3. Concatenamos el hash cifrado con el documento de la entidad “A”.
4. La entidad “B” recibe el documento y el hash cifrado por la entidad “A”.
5. La entidad “B” vuelve a generar el hash del documento enviado por la entidad “A”.
6. La entidad “B” descifra el hash cifrado con la llave pública de la entidad “A”.
7. Comparamos ambos hashes y en caso de ser iguales podremos ver el documento enviado por la entidad “A”.