RC4 y SEAL

Integrantes:

Leon Edward Quezada Reyes
David del Real Sifuentes
Luis Ernesto Herrera Olivas

RC4

¿quien lo creo?

R.-El algoritmo de criptografía RC4 fue diseñado por Ron Rivest de la RSA Security

¿cuando?

R.-en el año 1987

¿cómo funciona?

R.-RC4 es un algoritmo sorprendentemente simple. Este consiste en 2 algoritmos: 1-Key Scheduling Algorithm (KSA) y 2- Pseudo-Random Generation Algorithm (PRGA). Cada uno de estos algoritmos usa 8-by-8 S-box, el cual es solo un array de 256 números en el que ambos son únicos en cuanto a rango y su valor va desde 0 hasta 255. Todos los números de 0 a 255 existen dentro del array, pero están solo mezclados de diferentes maneras, el KSA se encarga de realizar la primera mezcla en el S-Box, basado en el valor de la semilla dada dentro de él, y esta "semilla" puede ser de 256 bits de largo.
Primero, el S-box array es llenado con valores secuenciales desde 0-255. Este array será llamado simplemente S. Entonces, el otro array de 256-bits es llenado con el valor de la "semilla", repitiendo como sea necesario hasta que todo el array es llenado. Este array será llamado K, entonces el array S es mezclado usando el siguiente pseudocódigo.

SEAL

¿quien lo creo?
El algoritmo SEAL fue diseñado por Phil Rogaway y Don Coppersmith
¿cuando?
En el año 1993
¿cómo funciona?
Su funcionamiento se basa en un proceso inicial en el que se calculan los valores para unas tablas a partir de la clave, de forma que el cifrado propiamente dicho puede llevarse a cabo de una manera realmente rápida. Por desgracia, también es un algoritmo sujeto a patentes.

Una característica muy útil de este algoritmo es que no se basa en un sistema lineal de generación, sino que define una familia de funciones pseudoaleatorias, de tal forma que se puede calcular cualquier porción de la secuencia suministrando únicamente un número entero n de 32 bits. La idea es que, dado ese número, junto con la clave k de 160 bits, el algoritmo genera un bloque k(n) de L bits de longitud. De esa forma, cada valor de k da lugar a una secuencia total de L * 232 bits, compuesta por la yuxtaposición de los bloques k(O), k(I), . . . , k(232 - 1).