ALLEGED RC4

Un algoritmo de criptografía simétrica, basado en cifrado de flujo (stream cipher), muy utilizado por su rendimiento y simplicidad. Para efectos de la implementación del Código de Control, la llave se conformará a partir de caracteres de siguiente diccionario:

```
A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z,
a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z,
0, 1, 2, 3, 4, 5, 6, 7, 8, 9, =, #, &, (, ), *, +, -, _, /, \, <, >, @, [, ],
{, }, %, $
```

Implementación (Pseudocódigo)

```
FUNCION CifrarMensajeRC4(CADENA Mensaje, CADENA Key ) : CADENA
        NUMERO State[256], X = 0, Y = 0, Index1 = 0, Index2 = 0 , NMen, I
        CADENA MensajeCifrado = ""
INICIO
        PARA I = 0 HASTA 255 HACER
                State[I] = I
        FIN PARA
        PARA I = 0 HASTA 255 HACER
                Index2 = ( ObtieneASCII(key[Index1]) + State[I] + Index2 ) MODULO 256
                IntercambiaValor( State[I], State[Index2] )
                Index1 = (Index1 + 1) MODULO LargoCadena(Key)
        FIN PARA
        PARA I = 0 HASTA LargoCadena(Mensaje)-1 HACER
                X = (X + 1) MODULO 256
                Y = (State[X] + Y) MODULO 256
                IntercambiaValor( State[X] , State[Y] )
                NMen = ObtieneASCII(Mensaje[I]) XOR State[(State[X] + State[Y]) MODULO 256]
                MensajeCifrado = MensajeCifrado + "-" + RellenaCero(ConvierteAHexadecimal(NMen))
        FIN PARA
        RETORNAR ObtieneSubCadena(MensajeCifrado, 1, LargoCadena(MensajeCifrado) - 1);
FIN FUNCION
```

-> Este Algoritmo opera con valores decimales, es decir tanto la llave, como el mensaje son convertidos a decimal, al final se hace la conversión correspondiente a su equivalente hexadecimal.

-> Definir y llenar un vector con números del 0 a 255

-> **ObtieneASCII:** Obtiene el valor ASCII de un carácter (entre 0 y 255)

-> **IntercambiaValor:** Intercambia el contenido de dos variables

-> **LargoCadena:** Obtiene la cantidad de caracteres que Componen la cadena

-> **RellenaCero:** Completa la expresión con un Cero (0) a la izquierda cuando esta tiene solo un caracter (Ej. “F” pasa a “0F”, “6B” no cambia)

-> **ConvierteAHexadecimal:** Convierte un número decimal a hexadecimal

-> **ObtieneSubCadena:** Obtiene una sub cadena a partir una cadena. Esta función se utiliza para quitar el ‘-’ por delante de MensajeCifrado.

Ejemplo:

1. CadenaCifrada = CifrarMensajeRC4 (“d3Ir6”, “sesamo”) -> Resultado: CadenaCifrada = EB-06-AE-F8-92
2. CadenaCifrada = CifrarMensajeRC4 (“piWCp”, “Aa1-bb2-Cc3-Dd4”) -> Resultado: CadenaCifrada = 37-71-2E-14-A0
3. CadenaCifrada = CifrarMensajeRC4 (“IUKYo”, “XBCPY-GKGX4-PGK44-8B632-X9P33”) -> Resultado: CadenaCifrada = 83-62-FC-B0-F0