RC6

RC6 es un nuevo cifrado en bloque enviado al NIST(Instituto nacional de estándares y tecnología) para su consideración como el nuevo AES(Estándar de cifrado avanzado).

Detalles de RC6

RC6 se designa como RC6 (w, r, b), donde “w” es el tamaño de la palabra en bits, “r” es el número de rondas y “b” denota la longitud de la clave de cifrado en bytes.

Las tres opciones "nominales" para el algoritmo presentado al concurso estadounidense AES son RC6(32, 20, 16), RC6 (32, 20, 24) y RC6 (32, 20, 32). Estas tres versiones tienen un tamaño de bloque de 128 bits, 20 rondas y solo se diferencian en el tamaño de la clave, que es respectivamente de 128, 196 y 256 bits. La clave secreta primero se expande en una matriz de 2r + 4.

Procedimiento de encriptado

Encryption with RC6-$w/r/b$

Input: Plaintext stored in four w-bit input registers A, B, C, D
Number r of rounds
w-bit round keys $S[0, \ldots, 2r + 3]$

Output: Ciphertext stored in A, B, C, D

Procedure:

$B = B + S[0]$
$D = D + S[1]$
for $i = 1$ **to** r **do**
{
$t = (B \times (2B + 1)) \lll \lg w$
$u = (D \times (2D + 1)) \lll \lg w$
$A = ((A \oplus t) \lll u) + S[2i]$
$C = ((C \oplus u) \lll t) + S[2i + 1]$
$(A, B, C, D) = (B, C, D, A)$
}
$A = A + S[2r + 2]$
$C = C + S[2r + 3]$

Procedimiento de descifrado

Decryption with RC6-$w/r/b$

Input: Ciphertext stored in four w-bit input registers A, B, C, D
Number r of rounds
w-bit round keys $S[0, \ldots, 2r + 3]$

Output: Plaintext stored in A, B, C, D

Procedure:

$C = C - S[2r + 3]$
$A = A - S[2r + 2]$
for $i = r$ **downto** 1 **do**
{
$(A, B, C, D) = (D, A, B, C)$
$u = (D \times (2D + 1)) \lll \lg w$
$t = (B \times (2B + 1)) \lll \lg w$
$C = ((C - S[2i + 1]) \ggg t) \oplus u$
$A = ((A - S[2i]) \ggg u) \oplus t$
}
$D = D - S[1]$
$B = B - S[0]$

Diferencias entre RC6 y CR5

RC6 tiene una difusión mucho más rápida que el RC5. Esto también permite que la RC6 se ejecute con menos rondas con mayor seguridad y con mayor rendimiento.