

//encryption subroutine

encrypt(data,key)

{v0,v1} = data //break 32-bit data into 2*16-bit

{k0,k1,k2,k3} = key //break 64-bit key into 4*16-bit

sum = 0

delta = 0x9e37 // $(\sqrt{5}-1) \times 2^{15}$

for i:(0:15)

sum = sum+delta

v0 = v0 + (((v1<<4) + k0) XOR (v1 + sum) XOR ((v1>>5) + k1))

v1 = v1 + (((v0<<4) + k2) XOR (v0 + sum) XOR ((v0>>5) + k3))

data = {v0,v1} //combine 2*16-bit into 32-bit

//decryption subroutine

decrypt(data,key)

{v0,v1} = data //break 32-bit data into 2*16-bit

{k0,k1,k2,k3} = key //break 64-bit key into 4*16-bit

sum = 0xE370

delta = 0x9e37 // $(\sqrt{5}-1) \times 2^{15}$

for i:(0:15)

v1 = v1 - (((v0<<4) + k2) XOR (v0 + sum) XOR ((v0>>5) + k3))

v0 = v0 - (((v1<<4) + k0) XOR (v1 + sum) XOR ((v1>>5) + k1))

sum = sum - delta;

data = {v0,v1} //combine 2*16-bit into 32-bit