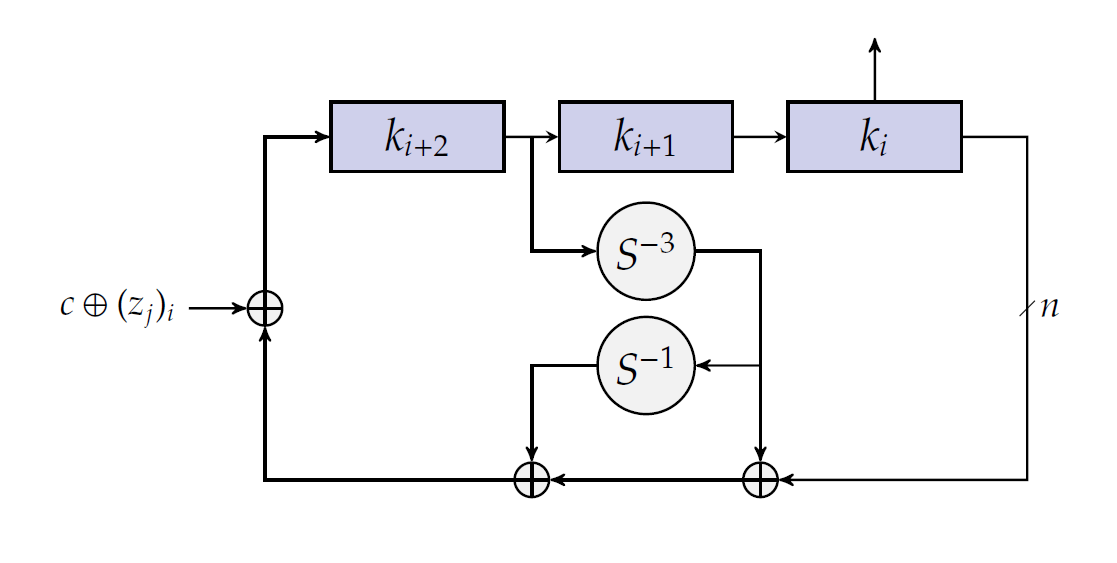
Manualisasi

1. Parameter SIMON 48/72

* wordSize = n = 24 (ukuran kata)
* keyWords = m = 3 (jumlah kata kunci)
* rounds = T = 36 (jumlah iterasi)
* c = 0xFFFFFC (konstanta dengan bilangan 2n-4)
* zj = z0= 11111010001001010110000111001101111101000100101011000011100110 (konstanta z index ke 0 untuk SIMON 48/72)

1. Key Expansion



1. Anggap key yang diinisialisasi adalah “1211100a0908020100” (dengan ukuran wordSize \* keyWords)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 1 | 1 | 1 | 0 | 0 | a | 0 | 9 | 0 | 8 | 0 | 2 | 0 | 1 | 0 | 0 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 1 | 1 | 1 | 0 |  | 0 | a | 0 | 9 | 0 | 8 |  | 0 | 2 | 0 | 1 | 0 | 0 |
|  |  | K1 | |  |  |  |  |  | K2 | |  |  |  |  |  | K3 | |  |  |

Representasi biner :

K1 = 0 0 0 1 0 0 1 0 0 0 0 1 0 0 0 1 0 0 0 1 0 0 0 0

K2 = 0 0 0 0 1 0 1 0 0 0 0 0 1 0 0 1 0 0 0 0 1 0 0 0

K3 = 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0

1. Untuk k[keyWords-1]…..k[0]

k[2] = K1

k[1] = K2

k[0] = K3

1. Untuk i = keyWords…..rounds-1

Misalkan saat ini i = 3

1. tmp = S−3 k[i-1]

tmp = S−3 k[2]

S−3 k[2], merupakan aplikasi dari fungsi Sαx, di mana α merupakan jumlah pergeseran sirkular ke kiri, apabila α bernilai negatif maka pergeseran dilakukan ke arah kanan

k[2] = 0 0 0 1 0 0 1 0 0 0 0 1 0 0 0 1 0 0 0 1 0 0 0 0

S−3 k[2] = 0 0 0 0 0 0 1 0 0 1 0 0 0 0 1 0 0 0 1 0 0 0 1 0

tmp = S−3 k[2]

= 0 0 0 0 0 0 1 0 0 1 0 0 0 0 1 0 0 0 1 0 0 0 1 0

1. if (keyWords = 4) tmp = tmp ⊕ k[i-3]

karena keyWords = 3, maka langkah ini dilewati

1. tmp = tmp ⊕ S−1tmp

tmp = 0 0 0 0 0 0 1 0 0 1 0 0 0 0 1 0 0 0 1 0 0 0 1 0

S−1tmp = 0 0 0 0 0 0 0 1 0 0 1 0 0 0 0 1 0 0 0 1 0 0 0 1

tmp = tmp ⊕ S−1tmp

= 0 0 0 0 0 0 1 0 0 1 0 0 0 0 1 0 0 0 1 0 0 0 1 0 ⊕ 0 0 0 0 0 0 0 1 0 0 1 0 0 0 0 1 0 0 0 1 0 0 0 1

= 0 0 0 0 0 0 1 1 0 1 1 0 0 0 1 1 0 0 1 1 0 0 1 1

1. k[i] = ~k[i-m] ⊕ tmp ⊕ zj[(i- keyWords) mod 62] ⊕ c

k[3] = ~k[0] ⊕ tmp ⊕ zj[0 mod 62] ⊕ c

= 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 ⊕ 0 0 0 0 0 0 1 1 0 1 1 0 0 0 1 1 0 0 1 1 0 0 1 1 ⊕

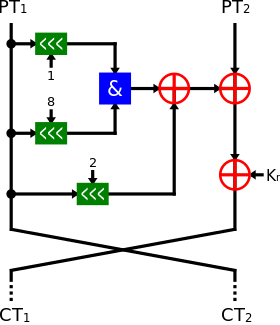
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 ⊕ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0

= 1 1 1 1 1 1 1 0 1 0 0 1 1 1 0 1 1 1 0 0 1 1 1 0

1. ulangi dari langkah a hingga i = rounds-1
2. Enkripsi SIMON 48/72

Enkripsi pada SIMON menggunakan fungsi berikut : Rk(x, y) = (y ⊕ f(x) ⊕ k, x)

Di mana f(x) = (Sx & S8x) ⊕ S2x, dan k adalah kunci yg dihasilkan dari key expansion untuk setiap round



Pada kasus ini yang menjadi plaintext adalah nilai RGB per pixel dari gambar, karena menggunakan metode SIMON dengan ukuran kata 24 bit maka PT1 dan PT2 diambil dari nilai RGB dua pixel yg berurutan yang masing-masing berukuran 24 bit. Misalkan nilai RGB pixel(0,0) = (14,35,55) dan pixel (0,1) = (125,254,0), maka:

PT1 = 0 0 0 0 1 1 1 0 0 0 1 0 0 0 1 1 0 0 1 1 0 1 1 1

PT2 = 0 1 1 1 1 1 0 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0

Lakukan langkah berikut untuk i = 0…..rounds-1

misalkan saat ini i = 0, maka

x = PT1 = 0 0 0 0 1 1 1 0 0 0 1 0 0 0 1 1 0 0 1 1 0 1 1 1

y = PT2 = 0 1 1 1 1 1 0 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0

1. tmp = x

x = 0 0 0 0 1 1 1 0 0 0 1 0 0 0 1 1 0 0 1 1 0 1 1 1

tmp = 0 0 0 0 1 1 1 0 0 0 1 0 0 0 1 1 0 0 1 1 0 1 1 1

1. x = y ⊕ (Sx & S8x) ⊕ S2x ⊕ k[i]

y = 0 1 1 1 1 1 0 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0

Sx = 0 0 0 1 1 1 0 0 0 1 0 0 0 1 1 0 0 1 1 0 1 1 1 0

S8x = 0 0 1 0 0 0 1 1 0 0 1 1 0 1 1 1 0 0 0 0 1 1 1 0

S2x = 0 0 1 1 1 0 0 0 1 0 0 0 1 1 0 0 1 1 0 1 1 1 0 0

k[0] = 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0

x = y ⊕ (Sx & S8x) ⊕ S2x ⊕ k[0]

= 0 1 1 1 1 1 0 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 ⊕ (0 0 0 1 1 1 0 0 0 1 0 0 0 1 1 0 0 1 1 0 1 1 1 0 &

0 0 1 0 0 0 1 1 0 0 1 1 0 1 1 1 0 0 0 0 1 1 1 0) ⊕ 0 0 1 1 1 0 0 0 1 0 0 0 1 1 0 0 1 1 0 1 1 1 0 0 ⊕

0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0

= 0 1 0 0 0 1 1 1 0 1 1 1 0 1 0 1 1 1 0 1 0 0 1 0

1. y = tmp

y = 0 0 0 0 1 1 1 0 0 0 1 0 0 0 1 1 0 0 1 1 0 1 1 1

1. nilai x dan y yang didapat adalah

x = 0 1 0 0 0 1 1 1 0 1 1 1 0 1 0 1 1 1 0 1 0 0 1 0, y = 0 0 0 0 1 1 1 0 0 0 1 0 0 0 1 1 0 0 1 1 0 1 1 1

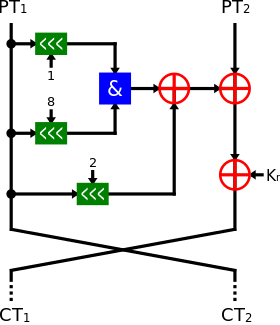
jika diubah menjadi nilai RGB, x = (71,117,210) , y = (14,35,55)

1. ulangi dari langkah a hingga i = rounds-1
2. Dekripsi SIMON 48/72

Dekripsi pada SIMON menggunakan fungsi berikut : Rk-1(x, y) = (y, x ⊕ f(y) ⊕ k)

Di mana f(y) = (Sy & S8y) ⊕ S2y, dan k adalah kunci yg dihasilkan dari key expansion untuk setiap round

Pada kasus ini yang menjadi ciphertext adalah nilai RGB per pixel dari gambar yang telah terenkripsi



PT1

PT2

CT1

CT2

Lakukan langkah berikut untuk i = rounds-1…..0

misalkan saat ini i = 0, maka

x = CT1 = 0 1 0 0 0 1 1 1 0 1 1 1 0 1 0 1 1 1 0 1 0 0 1 0

y = CT2 = 0 0 0 0 1 1 1 0 0 0 1 0 0 0 1 1 0 0 1 1 0 1 1 1

1. tmp = y

y = 0 0 0 0 1 1 1 0 0 0 1 0 0 0 1 1 0 0 1 1 0 1 1 1

tmp = 0 0 0 0 1 1 1 0 0 0 1 0 0 0 1 1 0 0 1 1 0 1 1 1

1. y = x ⊕ (Sy & S8y) ⊕ S2y ⊕ k[i]

x = 0 1 0 0 0 1 1 1 0 1 1 1 0 1 0 1 1 1 0 1 0 0 1 0

Sy = 0 0 0 1 1 1 0 0 0 1 0 0 0 1 1 0 0 1 1 0 1 1 1 0

S8y = 0 0 1 0 0 0 1 1 0 0 1 1 0 1 1 1 0 0 0 0 1 1 1 0

S2y = 0 0 1 1 1 0 0 0 1 0 0 0 1 1 0 0 1 1 0 1 1 1 0 0

k[0] = 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0

y = x ⊕ (Sy & S8y) ⊕ S2y ⊕ k[0]

= 0 1 0 0 0 1 1 1 0 1 1 1 0 1 0 1 1 1 0 1 0 0 1 0 ⊕ (0 0 0 1 1 1 0 0 0 1 0 0 0 1 1 0 0 1 1 0 1 1 1 0 &

0 0 1 0 0 0 1 1 0 0 1 1 0 1 1 1 0 0 0 0 1 1 1 0) ⊕ 0 0 1 1 1 0 0 0 1 0 0 0 1 1 0 0 1 1 0 1 1 1 0 0 ⊕

0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0

= 0 1 1 1 1 1 0 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0

1. x = tmp

x = 0 0 0 0 1 1 1 0 0 0 1 0 0 0 1 1 0 0 1 1 0 1 1 1

1. nilai x dan y yang didapat adalah

x = 0 0 0 0 1 1 1 0 0 0 1 0 0 0 1 1 0 0 1 1 0 1 1 1, y = 0 1 1 1 1 1 0 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0

jika diubah menjadi nilai RGB, x = (14,35,55) , y = (125,254,0)

1. ulangi dari langkah a hingga i = 0