RC4

Ron Rivest
1987

```
Algorithm RC4(byte string K)
byte i,j     //all arith involving these mod 256
for i ← 0 to 255 do S[i] ← i

j ← 0

for i ←0 to 255 do

    j ← j + S[i] + K[i mod |K|]

    S[i] ↔ S[j]


i, j ← 0

repeat

    i ← i + 1

    j ← j + S[i]

    S[i] ↔ S[j]

    output S[(S[i] + S[j]) mod 256]
```

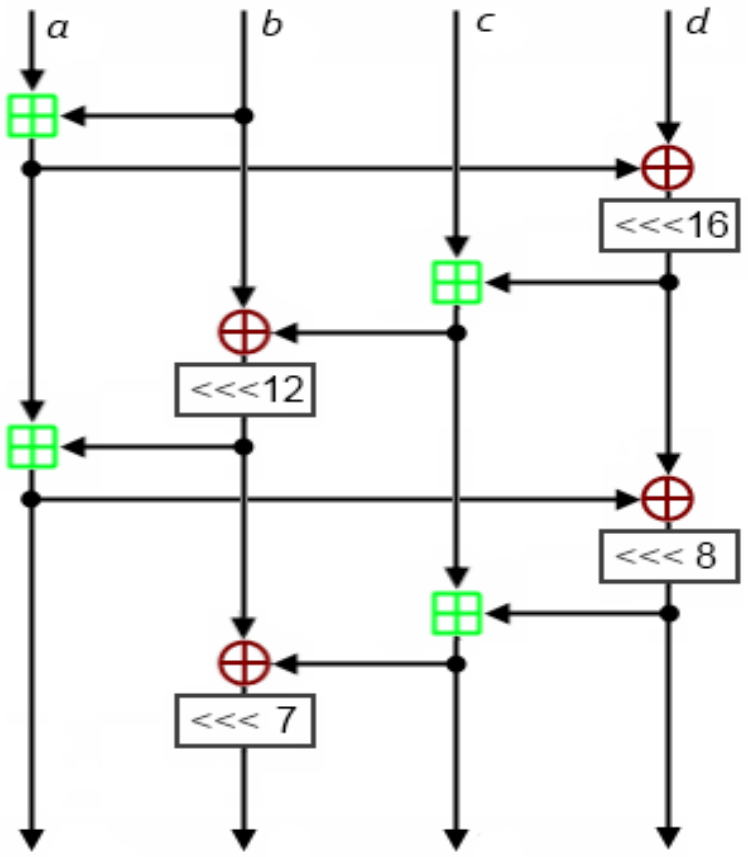
```
Algorithm ChaCha20(key, ctr, non)
                   8     1     3
                4
state ← con | key | ctr | non
s ← state

for i¬1 to 10 do
QR(s[0], s[4],  s[8], s[12])  // col 1
QR(s[1], s[5],  s[9], s[13])  // col 2
QR(s[2], s[6], s[10], s[14])  // col 3
QR(s[3], s[7], s[11], s[15])  // col 4
QR(s[0], s[5], s[10], s[15])  // diag 1
QR(s[1], s[6], s[11], s[12])  // diag 2
QR(s[2], s[7],  s[8], s[13])  // diag 3
QR(s[3], s[4],  s[9], s[14])  // diag 4
od

state += s
return state
```

0	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15

con0	con1	con2	con3
key0	key1	key2	key3
key4	key5	key6	key7
ctr	non0	non1	non2




```
Algorithm QR(a,b,c,d)
a += b; d ^= a; d <<<= 16;
c += d; b ^= c; b <<<= 12;
a += b; d ^= a; d <<<= 8;
c += d; b ^= c; b <<<= 7;
```