Salsa20

created 2005 -- published 2007 -- modified 2008

Created by Daniel J Bernstein

Structure

k is an 32 or 16 byte sequence, v is an 8 byte sequence, l is in {0, 1, ..., 2^70}, m is an l byte sequence.

Salsa20(v)_k XOR m is used to describe an encryption of m with nonce v under key k.

The methodology used to scramble bytes is to conceptualize the sequence as a 4x4 grid where you can rotate rows, columns, and the bits in a word. A round is made up of a "doubleround" which consists of all four rows being rotated and all four columns being rotated. Therefore, every byte will be modified twice.

Uses

With 20 rounds - "for encryption in typical cryptographic applications."

With 8 or 12 rounds - "for users who value speed more than confidence"

Code

An implementation of the salsa20's 20 round block function.

```
#define ROTL(a,b) (((a) << (b)) | ((a) >> (32 - (b))))
#define QR(a, b, c, d)(b ^= ROTL(a + d, 7), c ^=
ROTL(b + a, 9), d ^= ROTL(c + b,13),      a ^= ROTL(d +
c,18))
#define ROUNDS 20
void salsa20_block(uint32_t out[16], uint32_t const
in[16]) {
        int i;
        uint32_t x[16];
        for (i = 0; i < 16; ++i) x[i] = in[i];
        for (i = 0; i < ROUNDS; i += 2) {QR(x[ 0], x[ 4],
x[ 8], x[12]); QR(x[ 5], x[ 9], x[13], x[ 1]); QR(x[10], x[14],
x[ 2], x[ 6]); QR(x[15], x[ 3], x[ 7], x[11]); QR(x[ 0], x[ 1],
x[ 2], x[ 3]); QR(x[ 5], x[ 6], x[ 7], x[ 4]); QR(x[10], x[11],
x[ 8], x[ 9]); QR(x[15], x[12], x[13], x[14]); }
        for (i = 0; i < 16; ++i)
                out[i] = x[i] + in[i];
}
```

Strengths

No attacks are known to exist against Slasa20/20 or Salsa20/12 (the 20 and 12 round version respectively) other than an exhaustive key search. Therefore, it's a very, very strong encryption algorithm when enough rounds are used.

Weaknesses

Some applications may be affected by the short nonce length (a concern addressed in XSalsa20)

It is a very expensive algorithm, and so performant implementations use less rounds and are thus less secure.

https://cr.yp.to/snuffle/spec.pdf
https://www.ecrypt.eu.org/stream/e2-salsa20.html