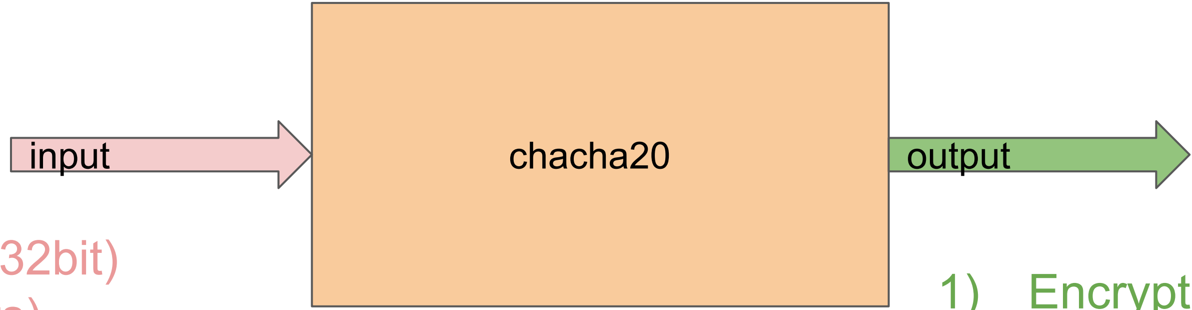
Chacha20

- It is a Cryptographic Algorithm
- Stream cipher(It uses 256 bit key)

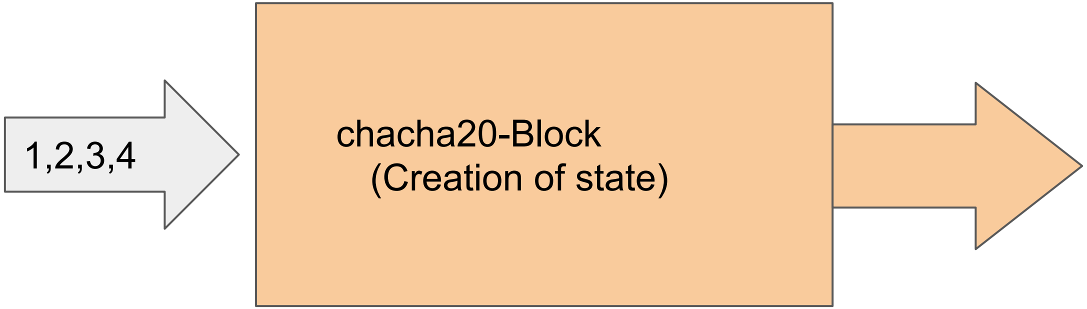
Block Diagram



1) constant(4*32bit)
2) keys(256bits)
3) counter(1*32bit)
4) Nonce(96 bit)
5) Message/Plain text(Arbitrary length)

1) Encrypted message/Cipher text(512 bits)

Block Diagram



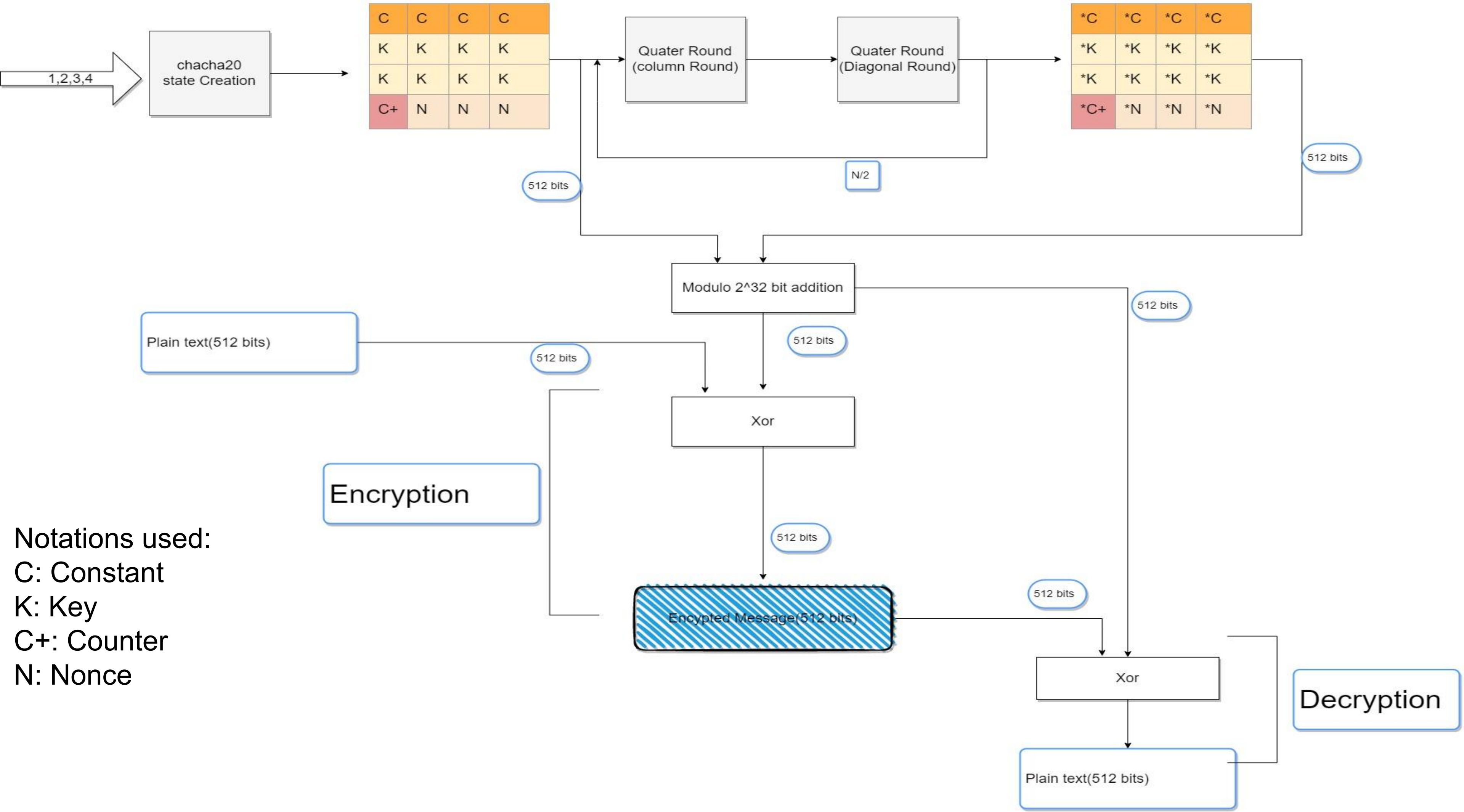
C	C	C	C
K	K	K	K
K	K	K	K
C+	N	N	N

Indexing of state Matrix:

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

- Each Block in the state matrix or vector is 32 bit.

1) There are 4 Constant of 32 bit each.
2) Keys with 256 bits
3) 1 counter with 32 bits,initialized with value zero or one.
4) Nonce(96 bits,occupying 3 blocks in state matrix)



C	C	C	C
K	K	K	K
K	K	K	K
C+	N	N	N

*C	*C	*C	*C
*K	*K	*K	*K
*K	*K	*K	*K
*C+	*N	*N	*N

Notations used:
C: Constant
K: Key
C+: Counter
N: Nonce

Quarter Round operations(Column,Diagonal Round)

A single Quarter round either of Column Round or Diagonal Round Consist of Following Operations:

1. a += b; d ^= a; d <<<= 16;
2. c += d; b ^= c; b <<<= 12;
3. a += b; d ^= a; d <<<= 8;
4. c += d; b ^= c; b <<<= 7;

Quarter Round operations(column Round)

a	C	C	C
b	K	K	K
c	K	K	K
d	N	N	N

(i)

C	a	C	C
K	b	K	K
K	c	K	K
C+	d	N	N

(ii)

C	C	a	C
K	K	b	K
K	K	c	K
C+	N	d	N

(iii)

C	C	C	a
K	K	K	b
K	K	K	c
C+	N	N	d

(iv)

Quarter Round operations(Diagonal Round)

a	C	C	C
K	b	K	K
K	K	c	K
C+	N	N	d

(i)

C	a	C	C
K	K	b	K
K	c	K	c
d	N	N	N

(ii)

C	C	a	C
K	K	K	b
c	K	K	K
C+	d	N	N

(iii)

C	C	C	a
b	K	K	K
K	c	K	K
C+	N	d	N

(iv)

Chacha20:Encryption

- ChaCha20 successively calls the ChaCha20 block function, with the same key and nonce, and with successively increasing block counter parameters. ChaCha20 then serializes the resulting state by writing the numbers in little-endian order, creating a keystream block.

- Concatenating the keystream blocks from the successive blocks forms a keystream.

- The ChaCha20 function then performs an XOR of this keystream with the plaintext.

- Alternatively, each keystream block can be XORed with a plaintext block before proceeding to create the next block, saving some memory.

- There is no requirement for the plaintext to be an integral multiple of 512 bits. If there is extra keystream from the last block, it is discarded.