Ejemplo CHACHA20

Clave introducida
e 99 a3 97 3c 53 eb 1b
e2 42 6b ad 2f 31 2d 24
d9 c2 76 2b 53 5e f4 d7
8e 17 75 a9 45 3a 68 a5

E099A397,3C53EB1B,E2426BAD,2F312D24,D9C2762B,535EF4D7,8E1775A9,453A68A5

E0:99:A3:97 3C:53:EB:1B E2:42:6B:AD 2F:31:2D:24 D9:C2:76:2B:53:5E:F4:D7 8E:17:75:A9 45:3A:68:A5
e0:99:a3:97 3c:53:eb:1b e2:42:6b:ad 2f:31:2d:24 d9:c2:76:2b:53:5e:f4:d7 8e:17:75:a9 45:3a:68:a5

Nonce:
B6 9E DE AC 73 EE
44 5 D3 FA 9A 8E

B6:9E:DE:AC 73:EE:44:50 D3:FA:9A:8E
b6:9e:de:ac 73:ee:44:50 d3:fa:9a:8e
B69EDEAC,73EE4450,D3FA9A8E

El estado inicial
Estado [0] = 61707865 Estado [1] = 3320646e Estado [2] = 79622d32 Estado [3] = 6b206574
Estado [4] = 97a3990e Estado [5] = 1beb533c Estado [6] = ad6b42e2 Estado [7] = 242d312f
Estado [8] = 2b76c2d9 Estado [9] = d7f45e53 Estado [10] = a975178e Estado [11] = a5683a45
Estado [12] = 1 Estado [13] = acde9eb6 Estado [14] = 544ee73 Estado [15] = 8e9afad3

El resultado:
Estado [0] = e3a1f58b Estado [1] = f4c60708 Estado [2] = 26eca951 Estado [3] = c8081b09
Estado [4] = f29f33bf Estado [5] = 19488feb Estado [6] = 28513fab Estado [7] = 3f3e9843
Estado [8] = 9a7df62f Estado [9] = 213d77f Estado [10] = 2e2fc67d Estado [11] = 5e8bd007
Estado [12] = eeddff67 Estado [13] = 300601b3 Estado [14] = a361da5d Estado [15] = 2b7e729d

Modificación;
cccccccc cccccccc cccccccc cccccccc
kkkkkkkk kkkkkkkk kkkkkkkk kkkkkkkk
kkkkkkkk kkkkkkkk kkkkkkkk kkkkkkkk
bbbbbbbb nnnnnnnn nnnnnnnn nnnnnnnn
c=constant k=key b=blockcount n=nonce

Sustituir el contador por un valor aleatorio

```
chacha20_block(key, counter, nonce):
state = constants | key | counter | nonce
working_state = state
for i=1 upto 10
inner_block(working_state)
end
state += working_state
return serialize(state)
end
```