

Specification of Muhammad mahameed's cipher

The cipher is a block cipher with 64-bit key and 64-bit plaintext, and AES like cipher. The cipher computes the cipher text from the plain text in 8 rounds.

given some test vectors:

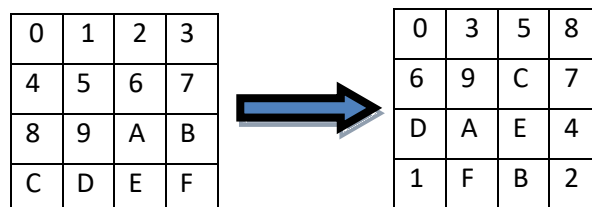
<u>Plaintext</u>	<u>Key</u>	<u>ciphertext</u>
<u>0</u>	<u>0</u>	<u>0x83D2BC89B79D2E25</u>
<u>0x0123456789ABCDEF</u>	<u>0</u>	<u>0x09A184A84569DBF1</u>
<u>0</u>	<u>0x0123456789ABCDEF</u>	<u>0x2F3DA681C94B0B81</u>

Round function:

The round function is very similar to the round function of AES.

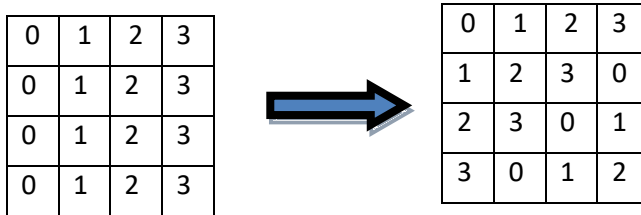
- 1) SubCells (apply SBOX).
- 2) Shift Rows.
- 3) Mix Columns.
- 4) Add Round Key.

- SubCells :
by applying the following substitution box (sbox) to every nibble of the internal state.
SBOX = { 0 3 5 8 6 9 C 7 D A E 4 1 F B 2 }



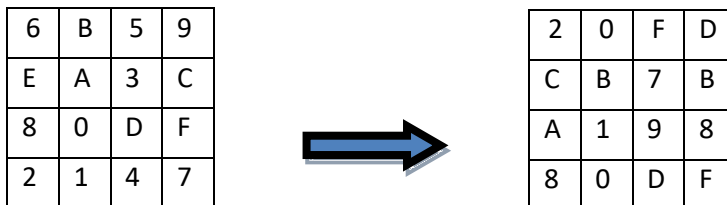
This sbox was taken from : <https://eprint.iacr.org/2011/218.pdf>
Cryptographic Analysis of all 4x4-bit sboxes by Markku-juhani O.Saarinen
one of the "Golden sboxed" (G9)

- Shift Rows:
rotate the nibbles in the rows by 0, 1, 2 and 3 places to the left.



- Mix Columns :
mix the nibbles in every column according to a given matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$



I chose this matrix by trying some matrices while enforcing the algebraic aspects of a good mixcolumns matrices (similar to the AES matrix)

- Add Round Key:
for round i , we calculate round key K_i and use it as follow
word = word \oplus (K_i & 0xffffffff);

Key schedule algorithm :

given a master key K:

$K_0 = K$

$K_i = (K_{i-1} \oplus 3) \lll 16$

Encryption Algorithm :

Input : word , key

- 1) add round key $K(0)$ to word
- 2) FOR i from 1 to 8
 - 2.1) apply sbox to word
 - 2.2) apply shift rows to word
 - 2.3) apply mix columns to word
 - 2.4) add round key $k(i)$ to word
- 3) return word