Specification of MA0X

Iraqi Majd 313138943

June 10 ,2020

Cipher :

The ciphertext is computed in 9 rounds, from 64-bit long key and word.

The state of the cipher is word witch is divided into 16 4-bit nibbles

2.Round function :

My round function is similar to the AES round function.

It consists of 4 phases : add round key, sub cells, shift rows and mix columns.

2.1. Add Roundkey:

XOR the 32 most significant bits of the key state with the cipher state.

2.2. Sub Cells:

It changes the places ogf the nibbles as the following permutation:]

Sbox: [0x0, 0x3, 0x5, 0x8, 0x6, 0xC, 0xB, 0x7, 0xA, 0x4, 0x9, 0xE, 0xF, 0x1, 0x2, 0xD]

This sbox was taken from: *https://eprint.iacr.org/2011/218.pdf*

2.3. Shift rows:

we rotate the nibbles in the rows by 0, 1, 2 and 3 places to the left.

2.4. Mix column :

we mix the nibbles in every column according to a matrix. The matrix that I chose : (I chose this matric because it's inversible matrix)

$$M = \begin{pmatrix} 1\,0\,0\,1 \\ 0\,1\,1\,0 \\ 0\,0\,1\,0 \\ 1\,0\,1\,0 \end{pmatrix}$$

3.Key Schedule algorithm ：

The Key has a 64 - bit state, the i-th keystate is computed as follows ：

k0=key

Ki = (ki-1 ^ 0x3 << 16) | (ki-1 ^ 0x3 >> 48)

Test vector:

Plaintext1：0x0000000000000000

key：0x0123456789ABCDEF

cipher1：0xA9D1517D0000F53

----

plainText2：0x08531277AABCE012

key2：0x0231695487BCAFDE

cipher2：0x13EDA0C586FFD0E1