Lavi Cipher

The Lavi Cipher is very similar to TC02, but with improvements to the sbox, Mix Columns and round key function.

This cipher uses 64-bit key on a 64 bit plaintext and calculates the plaintext in 14 rounds.

The round function is almost the same as TC02 and AES –

1. **Key adding – The current round key is xor'ed with the current text**
2. **Sub Cells – given sbox =**
   [0xc,0x7,0x2,0xe,0x1,0x4,0xb,0xd,0x5,0x8,0x9,0x3,0xa,0xf,0x0,0x6]

3. **Shift Rows - In the shift rows layer we rotate the nibbles in the rows by their index to the left.**
4. **Mix Columns – given by matrix :**
$$\begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix}$$
5. **Key schedule –**
$$k_i = k_{i-1} \oplus 0x3 \oplus (i-1) \ll 16$$
6. **# Of rounds – 14.**

Test Vectors (More in the text file) :

Plaintext	Cipher Text
3FCF6D6713D20A27	5EE37327304F0155
851CB74E44727E64	8878112BDC649681
21D824EE5BF6DE95	7065ECD5A1AD6EBD
04DB5B493D9EA83A	79E344D3D05D2BD8
F9B0CC1770A7C646	CB2A414AA17D0601
34180D06F67EFC88	C50BF37B4040A012
1E11A033250DC4FB	E8404F2AD9F4F9F6
E77520EAD46FFECF	264016EC3FA87188
73630EA10494BAF9	D1A44AB9061C5CCE
ECC223EE1072BF8F	022CA7FCF48CC89F
2CAE6BA3DCDE28BC	59A540D43257662B
CAFC85492CFE436C	AB25ABD2D8EAE7F9
67F44CCEB2BD728C	1B7172BA7ABAB6E9
2F2E00C035217685	C92BD9096DCF17B8
03E8016574FA25DD	6851D185C3FF9118
650032CE994798CA	4F0B8A507B71B416

Design rational:

I've chose to improve TC02 because I've spent a lot of hours trying to attack it, and I fell more comfortable with SPN like encryption.
SBOX:
Even though I looked for a good sbox from known ciphers, I eventually decided to make one of my own:
The sbox was chosen for 2 reasons –

1. **No probability higher then 4/16 in the DDT table**
2. **Many sources on how to build a good sbox stated that given an input to the sbox – any other input with a 1 bit difference should result in at least 2 bit difference in the output.**

This sbox was made by generating s-boxes that matches this 2 criteria.

Mix Columns:
I've tried to find a matrix the results in as much diffusion as possible given that the matrix should be invertible.

Key schedule –
I've tried to look for information on key scheduling, but I lack the knowledge to create a good one on my own, I've used the TC02 scheduler – but added a XOR with the round index –because of Eran's Advice.

Number of rounds –
The mix columns diffusion is a pretty strong one from what I've tried, takes about max 5-6 rounds for total diffusion with most numbers of known key nibbles, I doubled it, added 2 more rounds for the less probable differential attack – which I hope and think that will suffice.

The name –
The name was chosen because of my cat, Lavi.

Note – reference implementation in python file.