ASSIGNMENT REPORT

APPLIED CRYPTOGRAPHY (CS-6530), IIT MADRAS
Designing and Implementing a Block Cipher Similar to AES
(Final Submission)

Faculty

Asst Prof. Chester Rebeiro

Members

Prateek Bhamri (CS17M003)
Vivek Kumar Agrawal (CS17M049)

12. Implement your complete cipher as efficiently as possible. Some implementation options for high speed include (1) using T-tables (refer OpenSSL implementations as studied in class), (2) using bit slicing (refer to this paper: bitslice implementations of AES).

The implementation of the cipher **CLONE** that was submitted earlier was modified through the usage of T-tables for increasing the efficiency. The undermentioned 4 T-tables were used:

```
T0[256] = {
0x00000000, 0x02010103, 0x04020206, 0x06030305,
0x0804040c, 0x0a05050f, 0x0c06060a, 0x0e070709,
0x10080818, 0x1209091b, 0x140a0a1e, 0x160b0b1d,
0x180c0c14, 0x1a0d0d17, 0x1c0e0e12, 0x1e0f0f11,
0x20101030, 0x22111133, 0x24121236, 0x26131335,
0x2814143c, 0x2a15153f, 0x2c16163a, 0x2e171739,
0x30181828, 0x3219192b, 0x341a1a2e, 0x361b1b2d,
0x381c1c24, 0x3a1d1d27, 0x3c1e1e22, 0x3e1f1f21,
0x40202060, 0x42212163, 0x44222266, 0x46232365,
0x4824246c, 0x4a25256f, 0x4c26266a, 0x4e272769,
0x50282878, 0x5229297b, 0x542a2a7e, 0x562b2b7d,
0x582c2c74, 0x5a2d2d77, 0x5c2e2e72, 0x5e2f2f71,
0x60303050, 0x62313153, 0x64323256, 0x66333355,
0x6834345c, 0x6a35355f, 0x6c36365a, 0x6e373759,
0x70383848, 0x7239394b, 0x743a3a4e, 0x763b3b4d,
0x783c3c44, 0x7a3d3d47, 0x7c3e3e42, 0x7e3f3f41,
0x804040c0, 0x824141c3, 0x844242c6, 0x864343c5,
0x884444cc, 0x8a4545cf, 0x8c4646ca, 0x8e4747c9,
0x904848d8, 0x924949db, 0x944a4ade, 0x964b4bdd,
0x984c4cd4, 0x9a4d4dd7, 0x9c4e4ed2, 0x9e4f4fd1,
0xa05050f0, 0xa25151f3, 0xa45252f6, 0xa65353f5,
0xa85454fc, 0xaa5555ff, 0xac5656fa, 0xae5757f9,
0xb05858e8, 0xb25959eb, 0xb45a5aee, 0xb65b5bed,
0xb85c5ce4, 0xba5d5de7, 0xbc5e5ee2, 0xbe5f5fe1,
0xc06060a0, 0xc26161a3, 0xc46262a6, 0xc66363a5,
0xc86464ac, 0xca6565af, 0xcc6666aa, 0xce6767a9,
0xd06868b8, 0xd26969bb, 0xd46a6abe, 0xd66b6bbd,
0xd86c6cb4, 0xda6d6db7, 0xdc6e6eb2, 0xde6f6fb1,
0xe0707090, 0xe2717193, 0xe4727296, 0xe6737395,
0xe874749c, 0xea75759f, 0xec76769a, 0xee777799,
0xf0787888, 0xf279798b, 0xf47a7a8e, 0xf67b7b8d,
0xf87c7c84, 0xfa7d7d87, 0xfc7e7e82, 0xfe7f7f81,
0xcf80804f, 0xcd81814c, 0xcb828249, 0xc983834a,
0xc7848443, 0xc5858540, 0xc3868645, 0xc1878746,
0xdf888857, 0xdd898954, 0xdb8a8a51, 0xd98b8b52,
0xd78c8c5b, 0xd58d8d58, 0xd38e8e5d, 0xd18f8f5e,
0xef90907f, 0xed91917c, 0xeb929279, 0xe993937a,
0xe7949473, 0xe5959570, 0xe3969675, 0xe1979776,
0xff989867, 0xfd999964, 0xfb9a9a61, 0xf99b9b62,
0xf79c9c6b, 0xf59d9d68, 0xf39e9e6d, 0xf19f9f6e,
0x8fa0a02f, 0x8da1a12c, 0x8ba2a229, 0x89a3a32a,
0x87a4a423, 0x85a5a520, 0x83a6a625, 0x81a7a726,
0x9fa8a837, 0x9da9a934, 0x9baaaa31, 0x99abab32,
0x97acac3b, 0x95adad38, 0x93aeae3d, 0x91afaf3e,
```

```
0xafb0b01f, 0xadb1b11c, 0xabb2b219, 0xa9b3b31a,
0xa7b4b413, 0xa5b5b510, 0xa3b6b615, 0xa1b7b716,
0xbfb8b807, 0xbdb9b904, 0xbbbaba01, 0xb9bbbb02,
0xb7bcbc0b, 0xb5bdbd08, 0xb3bebe0d, 0xb1bfbf0e,
0x4fc0c08f, 0x4dc1c18c, 0x4bc2c289, 0x49c3c38a,
0x47c4c483, 0x45c5c580, 0x43c6c685, 0x41c7c786,
0x5fc8c897, 0x5dc9c994, 0x5bcaca91, 0x59cbcb92,
0x57cccc9b, 0x55cdcd98, 0x53cece9d, 0x51cfcf9e,
0x6fd0d0bf, 0x6dd1d1bc, 0x6bd2d2b9, 0x69d3d3ba,
0x67d4d4b3, 0x65d5d5b0, 0x63d6d6b5, 0x61d7d7b6,
0x7fd8d8a7, 0x7dd9d9a4, 0x7bdadaa1, 0x79dbdba2,
0x77dcdcab, 0x75ddda8, 0x73dedead, 0x71dfdfae,
0x0fe0e0ef, 0x0de1e1ec, 0x0be2e2e9, 0x09e3e3ea,
0x07e4e4e3, 0x05e5e5e0, 0x03e6e6e5, 0x01e7e7e6,
0x1fe8e8f7, 0x1de9e9f4, 0x1beaeaf1, 0x19ebebf2,
0x17ececfb, 0x15ededf8, 0x13eeeefd, 0x11efeffe,
0x2ff0f0df, 0x2df1f1dc, 0x2bf2f2d9, 0x29f3f3da,
0x27f4f4d3, 0x25f5f5d0, 0x23f6f6d5, 0x21f7f7d6,
0x3ff8f8c7, 0x3df9f9c4, 0x3bfafac1, 0x39fbfbc2,
0x37fcfccb, 0x35fdfdc8, 0x33fefecd, 0x31ffffce
}

T1[256] = {
0x00000000, 0x03020101, 0x06040202, 0x05060303,
0x0c080404, 0x0f0a0505, 0x0a0c0606, 0x090e0707,
0x18100808, 0x1b120909, 0x1e140a0a, 0x1d160b0b,
0x14180c0c, 0x171a0d0d, 0x121c0e0e, 0x111e0f0f,
0x30201010, 0x33221111, 0x36241212, 0x35261313,
0x3c281414, 0x3f2a1515, 0x3a2c1616, 0x392e1717,
0x28301818, 0x2b321919, 0x2e341a1a, 0x2d361b1b,
0x24381c1c, 0x273a1d1d, 0x223c1e1e, 0x213e1f1f,
0x60402020, 0x63422121, 0x66442222, 0x65462323,
0x6c482424, 0x6f4a2525, 0x6a4c2626, 0x694e2727,
0x78502828, 0x7b522929, 0x7e542a2a, 0x7d562b2b,
0x74582c2c, 0x775a2d2d, 0x725c2e2e, 0x715e2f2f,
0x50603030, 0x53623131, 0x56643232, 0x55663333,
0x5c683434, 0x5f6a3535, 0x5a6c3636, 0x596e3737,
0x48703838, 0x4b723939, 0x4e743a3a, 0x4d763b3b,
0x44783c3c, 0x477a3d3d, 0x427c3e3e, 0x417e3f3f,
0xc0804040, 0xc3824141, 0xc6844242, 0xc5864343,
0xcc884444, 0xcf8a4545, 0xca8c4646, 0xc98e4747,
0xd8904848, 0xdb924949, 0xde944a4a, 0xdd964b4b,
0xd4984c4c, 0xd79a4d4d, 0xd29c4e4e, 0xd19e4f4f,
0xf0a05050, 0xf3a25151, 0xf6a45252, 0xf5a65353,
0xfca85454, 0xffaa5555, 0xfaac5656, 0xf9ae5757,
0xe8b05858, 0xebb25959, 0xeeb45a5a, 0xedb65b5b,
0xe4b85c5c, 0xe7ba5d5d, 0xe2bc5e5e, 0xe1be5f5f,
0xa0c06060, 0xa3c26161, 0xa6c46262, 0xa5c66363,
0xacc86464, 0xafca6565, 0xaacc6666, 0xa9ce6767,
0xb8d06868, 0xbbd26969, 0xbed46a6a, 0xbdd66b6b,
0xb4d86c6c, 0xb7da6d6d, 0xb2dc6e6e, 0xb1de6f6f,
0x90e07070, 0x93e27171, 0x96e47272, 0x95e67373,
0x9ce87474, 0x9fea7575, 0x9aec7676, 0x99ee7777,
0x88f07878, 0x8bf27979, 0x8ef47a7a, 0x8df67b7b,
0x84f87c7c, 0x87fa7d7d, 0x82fc7e7e, 0x81fe7f7f,
0x4fcf8080, 0x4ccd8181, 0x49cb8282, 0x4ac98383,
0x43c78484, 0x40c58585, 0x45c38686, 0x46c18787,
0x57df8888, 0x54dd8989, 0x51db8a8a, 0x52d98b8b,
0x5bd78c8c, 0x58d58d8d, 0x5dd38e8e, 0x5ed18f8f,
0x7fef9090, 0x7ced9191, 0x79eb9292, 0x7ae99393,
```

```
0x73e79494, 0x70e59595, 0x75e39696, 0x76e19797,
0x67ff9898, 0x64fd9999, 0x61fb9a9a, 0x62f99b9b,
0x6bf79c9c, 0x68f59d9d, 0x6df39e9e, 0x6ef19f9f,
0x2f8fa0a0, 0x2c8da1a1, 0x298ba2a2, 0x2a89a3a3,
0x2387a4a4, 0x2085a5a5, 0x2583a6a6, 0x2681a7a7,
0x379fa8a8, 0x349da9a9, 0x319baaaa, 0x3299abab,
0x3b97acac, 0x3895adad, 0x3d93aeae, 0x3e91afaf,
0x1fafb0b0, 0x1cadb1b1, 0x19abb2b2, 0x1aa9b3b3,
0x13a7b4b4, 0x10a5b5b5, 0x15a3b6b6, 0x16a1b7b7,
0x07bfb8b8, 0x04bdb9b9, 0x01bbbaba, 0x02b9bbbb,
0x0bb7bcbc, 0x08b5bdbd, 0x0db3bebe, 0x0eb1bfbf,
0x8f4fc0c0, 0x8c4dc1c1, 0x894bc2c2, 0x8a49c3c3,
0x8347c4c4, 0x8045c5c5, 0x8543c6c6, 0x8641c7c7,
0x975fc8c8, 0x945dc9c9, 0x915bcaca, 0x9259cbcb,
0x9b57cccc, 0x9855cdcd, 0x9d53cece, 0x9e51cfcf,
0xbf6fd0d0, 0xbc6dd1d1, 0xb96bd2d2, 0xba69d3d3,
0xb367d4d4, 0xb065d5d5, 0xb563d6d6, 0xb661d7d7,
0xa77fd8d8, 0xa47dd9d9, 0xa17bdada, 0xa279dbdb,
0xab77dcdc, 0xa875dddd, 0xad73dede, 0xae71dfdf,
0xef0fe0e0, 0xec0de1e1, 0xe90be2e2, 0xea09e3e3,
0xe307e4e4, 0xe005e5e5, 0xe503e6e6, 0xe601e7e7,
0xf71fe8e8, 0xf41de9e9, 0xf11beaea, 0xf219ebeb,
0xfb17ecec, 0xf815eded, 0xfd13eeee, 0xfe11efef,
0xdf2ff0f0, 0xdc2df1f1, 0xd92bf2f2, 0xda29f3f3,
0xd327f4f4, 0xd025f5f5, 0xd523f6f6, 0xd621f7f7,
0xc73ff8f8, 0xc43df9f9, 0xc13bfafa, 0xc239fbfb,
0xcb37fcfc, 0xc835fdfd, 0xcd33fefe, 0xce31ffff
}

T2[256] = {
0x00000000, 0x01030201, 0x02060402, 0x03050603,
0x040c0804, 0x050f0a05, 0x060a0c06, 0x07090e07,
0x08181008, 0x091b1209, 0x0a1e140a, 0x0b1d160b,
0x0c14180c, 0x0d171a0d, 0x0e121c0e, 0x0f111e0f,
0x10302010, 0x11332211, 0x12362412, 0x13352613,
0x143c2814, 0x153f2a15, 0x163a2c16, 0x17392e17,
0x18283018, 0x192b3219, 0x1a2e341a, 0x1b2d361b,
0x1c24381c, 0x1d273a1d, 0x1e223c1e, 0x1f213e1f,
0x20604020, 0x21634221, 0x22664422, 0x23654623,
0x246c4824, 0x256f4a25, 0x266a4c26, 0x27694e27,
0x28785028, 0x297b5229, 0x2a7e542a, 0x2b7d562b,
0x2c74582c, 0x2d775a2d, 0x2e725c2e, 0x2f715e2f,
0x30506030, 0x31536231, 0x32566432, 0x33556633,
0x345c6834, 0x355f6a35, 0x365a6c36, 0x37596e37,
0x38487038, 0x394b7239, 0x3a4e743a, 0x3b4d763b,
0x3c44783c, 0x3d477a3d, 0x3e427c3e, 0x3f417e3f,
0x40c08040, 0x41c38241, 0x42c68442, 0x43c58643,
0x44cc8844, 0x45cf8a45, 0x46ca8c46, 0x47c98e47,
0x48d89048, 0x49db9249, 0x4ade944a, 0x4bdd964b,
0x4cd4984c, 0x4dd79a4d, 0x4ed29c4e, 0x4fd19e4f,
0x50f0a050, 0x51f3a251, 0x52f6a452, 0x53f5a653,
0x54fca854, 0x55ffaa55, 0x56faac56, 0x57f9ae57,
0x58e8b058, 0x59ebb259, 0x5aeeb45a, 0x5bedb65b,
0x5ce4b85c, 0x5de7ba5d, 0x5ee2bc5e, 0x5fe1be5f,
0x60a0c060, 0x61a3c261, 0x62a6c462, 0x63a5c663,
0x64acc864, 0x65afca65, 0x66aacc66, 0x67a9ce67,
0x68b8d068, 0x69bbd269, 0x6abed46a, 0x6bbdd66b,
0x6cb4d86c, 0x6db7da6d, 0x6eb2dc6e, 0x6fb1de6f,
0x7090e070, 0x7193e271, 0x7296e472, 0x7395e673,
0x749ce874, 0x759fea75, 0x769aec76, 0x7799ee77,
```

```
0x7888f078, 0x798bf279, 0x7a8ef47a, 0x7b8df67b,
0x7c84f87c, 0x7d87fa7d, 0x7e82fc7e, 0x7f81fe7f,
0x804fcf80, 0x814ccd81, 0x8249cb82, 0x834ac983,
0x8443c784, 0x8540c585, 0x8645c386, 0x8746c187,
0x8857df88, 0x8954dd89, 0x8a51db8a, 0x8b52d98b,
0x8c5bd78c, 0x8d58d58d, 0x8e5dd38e, 0x8f5ed18f,
0x907fef90, 0x917ced91, 0x9279eb92, 0x937ae993,
0x9473e794, 0x9570e595, 0x9675e396, 0x9776e197,
0x9867ff98, 0x9964fd99, 0x9a61fb9a, 0x9b62f99b,
0x9c6bf79c, 0x9d68f59d, 0x9e6df39e, 0x9f6ef19f,
0xa02f8fa0, 0xa12c8da1, 0xa2298ba2, 0xa32a89a3,
0xa42387a4, 0xa52085a5, 0xa62583a6, 0xa72681a7,
0xa8379fa8, 0xa9349da9, 0xaa319baa, 0xab3299ab,
0xac3b97ac, 0xad3895ad, 0xae3d93ae, 0xaf3e91af,
0xb01fafb0, 0xb11cadb1, 0xb219abb2, 0xb31aa9b3,
0xb413a7b4, 0xb510a5b5, 0xb615a3b6, 0xb716a1b7,
0xb807bfb8, 0xb904bdb9, 0xba01bbba, 0xbb02b9bb,
0xbc0bb7bc, 0xbd08b5bd, 0xbe0db3be, 0xbf0eb1bf,
0xc08f4fc0, 0xc18c4dc1, 0xc2894bc2, 0xc38a49c3,
0xc48347c4, 0xc58045c5, 0xc68543c6, 0xc78641c7,
0xc8975fc8, 0xc9945dc9, 0xca915bca, 0xcb9259cb,
0xcc9b57cc, 0xcd9855cd, 0xce9d53ce, 0xcf9e51cf,
0xd0bf6fd0, 0xd1bc6dd1, 0xd2b96bd2, 0xd3ba69d3,
0xd4b367d4, 0xd5b065d5, 0xd6b563d6, 0xd7b661d7,
0xd8a77fd8, 0xd9a47dd9, 0xdaa17bda, 0xdba279db,
0xdcab77dc, 0xdda875dd, 0xdead73de, 0xdfae71df,
0xe0ef0fe0, 0xe1ec0de1, 0xe2e90be2, 0xe3ea09e3,
0xe4e307e4, 0xe5e005e5, 0xe6e503e6, 0xe7e601e7,
0xe8f71fe8, 0xe9f41de9, 0xeaf11bea, 0xebf219eb,
0xecfb17ec, 0xedf815ed, 0xeefd13ee, 0xeffe11ef,
0xf0df2ff0, 0xf1dc2df1, 0xf2d92bf2, 0xf3da29f3,
0xf4d327f4, 0xf5d025f5, 0xf6d523f6, 0xf7d621f7,
0xf8c73ff8, 0xf9c43df9, 0xfac13bfa, 0xfbc239fb,
0xfccb37fc, 0xfdc835fd, 0xfecd33fe, 0xffce31ff
}

T3[256] = {
0x00000000, 0x01010302, 0x02020604, 0x03030506,
0x04040c08, 0x05050f0a, 0x06060a0c, 0x0707090e,
0x08081810, 0x09091b12, 0x0a0a1e14, 0x0b0b1d16,
0x0c0c1418, 0x0d0d171a, 0x0e0e121c, 0x0f0f111e,
0x10103020, 0x11113322, 0x12123624, 0x13133526,
0x14143c28, 0x15153f2a, 0x16163a2c, 0x1717392e,
0x18182830, 0x19192b32, 0x1a1a2e34, 0x1b1b2d36,
0x1c1c2438, 0x1d1d273a, 0x1e1e223c, 0x1f1f213e,
0x20206040, 0x21216342, 0x22226644, 0x23236546,
0x24246c48, 0x25256f4a, 0x26266a4c, 0x2727694e,
0x28287850, 0x29297b52, 0x2a2a7e54, 0x2b2b7d56,
0x2c2c7458, 0x2d2d775a, 0x2e2e725c, 0x2f2f715e,
0x30305060, 0x31315362, 0x32325664, 0x33335566,
0x34345c68, 0x35355f6a, 0x36365a6c, 0x3737596e,
0x38384870, 0x39394b72, 0x3a3a4e74, 0x3b3b4d76,
0x3c3c4478, 0x3d3d477a, 0x3e3e427c, 0x3f3f417e,
0x4040c080, 0x4141c382, 0x4242c684, 0x4343c586,
0x4444cc88, 0x4545cf8a, 0x4646ca8c, 0x4747c98e,
0x4848d890, 0x4949db92, 0x4a4ade94, 0x4b4bdd96,
0x4c4cd498, 0x4d4dd79a, 0x4e4ed29c, 0x4f4fd19e,
0x5050f0a0, 0x5151f3a2, 0x5252f6a4, 0x5353f5a6,
0x5454fca8, 0x5555ffaa, 0x5656faac, 0x5757f9ae,
0x5858e8b0, 0x5959ebb2, 0x5a5aeeb4, 0x5b5bedb6,
```

```
0x5c5ce4b8, 0x5d5de7ba, 0x5e5ee2bc, 0x5f5fe1be,
0x6060a0c0, 0x6161a3c2, 0x6262a6c4, 0x6363a5c6,
0x6464acc8, 0x6565afca, 0x6666aacc, 0x6767a9ce,
0x6868b8d0, 0x6969bbd2, 0x6a6abed4, 0x6b6bbdd6,
0x6c6cb4d8, 0x6d6db7da, 0x6e6eb2dc, 0x6f6fb1de,
0x707090e0, 0x717193e2, 0x727296e4, 0x737395e6,
0x74749ce8, 0x75759fea, 0x76769aec, 0x777799ee,
0x787888f0, 0x79798bf2, 0x7a7a8ef4, 0x7b7b8df6,
0x7c7c84f8, 0x7d7d87fa, 0x7e7e82fc, 0x7f7f81fe,
0x80804fcf, 0x81814ccd, 0x828249cb, 0x83834ac9,
0x848443c7, 0x858540c5, 0x868645c3, 0x878746c1,
0x888857df, 0x898954dd, 0x8a8a51db, 0x8b8b52d9,
0x8c8c5bd7, 0x8d8d58d5, 0x8e8e5dd3, 0x8f8f5ed1,
0x90907fef, 0x91917ced, 0x929279eb, 0x93937ae9,
0x949473e7, 0x959570e5, 0x969675e3, 0x979776e1,
0x989867ff, 0x999964fd, 0x9a9a61fb, 0x9b9b62f9,
0x9c9c6bf7, 0x9d9d68f5, 0x9e9e6df3, 0x9f9f6ef1,
0xa0a02f8f, 0xa1a12c8d, 0xa2a2298b, 0xa3a32a89,
0xa4a42387, 0xa5a52085, 0xa6a62583, 0xa7a72681,
0xa8a8379f, 0xa9a9349d, 0xaaaa319b, 0xabab3299,
0xacac3b97, 0xadad3895, 0xaeae3d93, 0xafaf3e91,
0xb0b01faf, 0xb1b11cad, 0xb2b219ab, 0xb3b31aa9,
0xb4b413a7, 0xb5b510a5, 0xb6b615a3, 0xb7b716a1,
0xb8b807bf, 0xb9b904bd, 0xbaba01bb, 0xbbbb02b9,
0xbcbc0bb7, 0xbdbd08b5, 0xbebe0db3, 0xbfbf0eb1,
0xc0c08f4f, 0xc1c18c4d, 0xc2c2894b, 0xc3c38a49,
0xc4c48347, 0xc5c58045, 0xc6c68543, 0xc7c78641,
0xc8c8975f, 0xc9c9945d, 0xcaca915b, 0xcbcb9259,
0xcccc9b57, 0xcdcd9855, 0xcece9d53, 0xcfcf9e51,
0xd0d0bf6f, 0xd1d1bc6d, 0xd2d2b96b, 0xd3d3ba69,
0xd4d4b367, 0xd5d5b065, 0xd6d6b563, 0xd7d7b661,
0xd8d8a77f, 0xd9d9a47d, 0xdadaa17b, 0xdbdba279,
0xdcdcab77, 0xddddа875, 0xdedead73, 0xdfdfae71,
0xe0e0ef0f, 0xe1e1ec0d, 0xe2e2e90b, 0xe3e3ea09,
0xe4e4e307, 0xe5e5e005, 0xe6e6e503, 0xe7e7e601,
0xe8e8f71f, 0xe9e9f41d, 0xeaeaf11b, 0xebebf219,
0xececfb17, 0xededf815, 0xeeeefd13, 0xefeffe11,
0xf0f0df2f, 0xf1f1dc2d, 0xf2f2d92b, 0xf3f3da29,
0xf4f4d327, 0xf5f5d025, 0xf6f6d523, 0xf7f7d621,
0xf8f8c73f, 0xf9f9c43d, 0xfafac13b, 0xfbfbc239
}
```

The following code was used for the T-table lookup operation which enhanced the efficiency preventing the time consumed towards the mix-column operation that was performed earlier:

```
void t_mixCol(){
    int i,j;
    unsigned int res[4][4];
    for(i=0;i<4;i++)
              {
             for(j=0;j<4;j++){
                 if(i==0)
             res[i][j] = (T0[state[0][j]]>>24) ^ (T1[state[1][j]]>>24) ^
(T2[state[2][j]]>>24) ^ (T3[state[3][j]]>>24);
                 if(i==1)
             res[i][j] = (T0[state[0][j]]>>16 & 0xff) ^ (T1[state[1][j]]>>16 & 0xff) ^
(T2[state[2][j]]>>16 & 0xff) ^ (T3[state[3][j]]>>16 & 0xff);
```

```
                if(i==2)
            res[i][j] = (T0[state[0][j]]>>8 & 0xff) ^ (T1[state[1][j]]>>8 & 0xff) ^
(T2[state[2][j]]>>8 & 0xff) ^ (T3[state[3][j]]>>8 & 0xff);
                if(i==3)
            res[i][j] = (T0[state[0][j]] & 0xff) ^ (T1[state[1][j]] & 0xff) ^
(T2[state[2][j]] & 0xff) ^ (T3[state[3][j]] & 0xff);

        }
              }

    for(i=0;i<4;i++)
       for(j=0;j<4;j++)
              state[i][j] = res[i][j];
}
```

13. Evaluate your cipher with respect to AES to encrypt the file alice.txt.

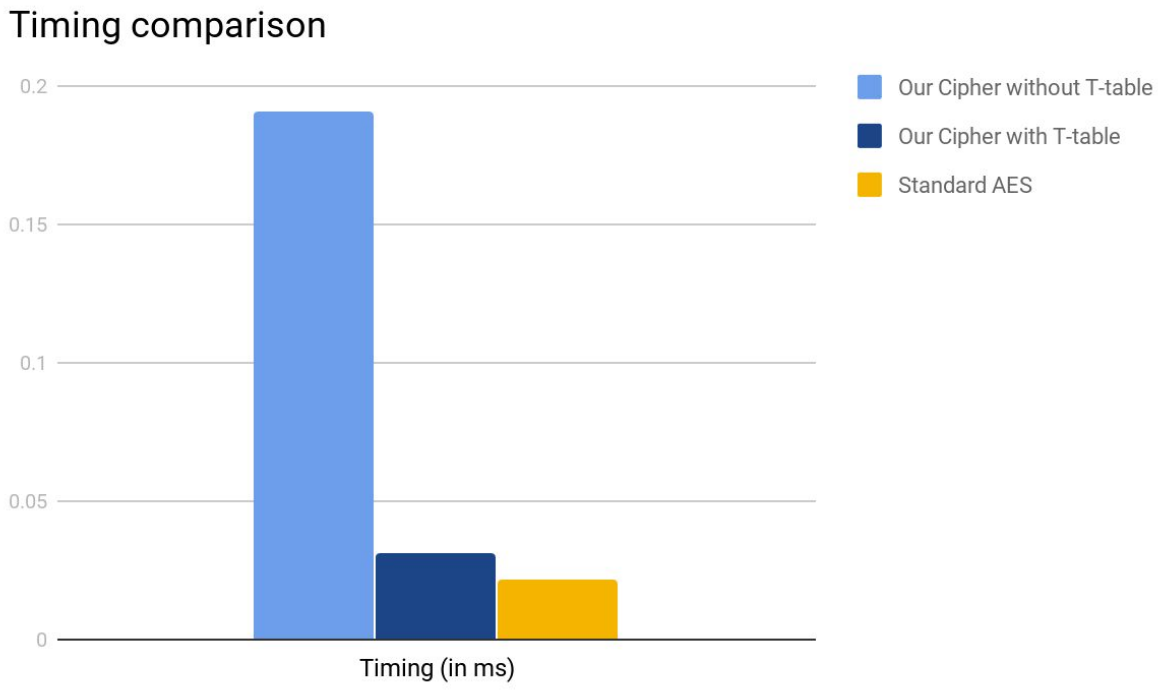
The encryption of the file alice.txt was performed under the given parameters with different implementation:

(a) **TIMING COMPARISON**

The timing of our cipher:

1. Without T-table **0.191 ms**
2. With T-table **0.031 ms**

Standard AES with openSSL was found to take **0.022ms**.



(b) **CPU USAGE COMPARISON**

Standard AES:

```
User time (seconds): 0.00
System time (seconds): 0.00
Percent of CPU this job got: 18%
Elapsed (wall clock) time (h:mm:ss or m:ss): 0:00.02
Average shared text size (kbytes): 0
Average unshared data size (kbytes): 0
Average stack size (kbytes): 0
Average total size (kbytes): 0
Maximum resident set size (kbytes): 1788
Average resident set size (kbytes): 0
Major (requiring I/O) page faults: 0
Minor (reclaiming a frame) page faults: 134
Voluntary context switches: 10
Involuntary context switches: 5
Swaps: 0
File system inputs: 0
File system outputs: 312
Socket messages sent: 0
Socket messages received: 0
Signals delivered: 0
Page size (bytes): 4096
Exit status: 0
```

Our cipher without T-Table

```
User time (seconds): 0.17
System time (seconds): 0.00
Percent of CPU this job got: 92%
Elapsed (wall clock) time (h:mm:ss or m:ss): 0:00.18
Average shared text size (kbytes): 0
Average unshared data size (kbytes): 0
Average stack size (kbytes): 0
Average total size (kbytes): 0
Maximum resident set size (kbytes): 1136
Average resident set size (kbytes): 0
Major (requiring I/O) page faults: 0
Minor (reclaiming a frame) page faults: 102
Voluntary context switches: 9
Involuntary context switches: 19
Swaps: 0
File system inputs: 0
File system outputs: 176
Socket messages sent: 0
Socket messages received: 0
Signals delivered: 0
Page size (bytes): 4096
Exit status: 0
```

Our cipher with T-Table

```
User time (seconds): 0.01
System time (seconds): 0.00
Percent of CPU this job got: 53%
Elapsed (wall clock) time (h:mm:ss or m:ss): 0:00.03
Average shared text size (kbytes): 0
Average unshared data size (kbytes): 0
Average stack size (kbytes): 0
Average total size (kbytes): 0
Maximum resident set size (kbytes): 1308
Average resident set size (kbytes): 0
Major (requiring I/O) page faults: 0
Minor (reclaiming a frame) page faults: 108
Voluntary context switches: 8
Involuntary context switches: 3
Swaps: 0
File system inputs: 0
File system outputs: 176
Socket messages sent: 0
Socket messages received: 0
Signals delivered: 0
Page size (bytes): 4096
Exit status: 0
```

CPU USAGE