CRYPTOGRAPHY #05.1

AES-128 Supplement

Jacek Tchórzewski, jacek.tchorzewski@pk.edu.pl

1. Decryption example from NIST:

```
EQUIVALENT INVERSE CIPHER (DECRYPT):
round[ 0].iinput    69c4e0d86a7b0430d8cdb78070b4c55a
round[ 0].ik_sch    13111d7fe3944a17f307a78b4d2b30c5
round[ 1].istart    7ad5fda789ef4e272bca100b3d9ff59f
round[ 1].is_box    bdb52189f261b63d0b107c9e8b6e776e
round[ 1].is_row    bd6e7c3df2b5779e0b61216e8b10b689
round[ 1].im_col    4773b91ff72f354361cb018ea1e6cf2c
round[ 1].ik_sch    13aa29be9c8faff6f770f58000f7bf03
round[ 2].istart    54d990a16ba09ab596bbf40ea111702f
round[ 2].is_box    fde596f1054737d235febad7f1e3d04e
round[ 2].is_row    fde3bad205e5d0d73547964ef1fe37f1
round[ 2].im_col    2d7e86a339d9393ee6570a1101904e16
round[ 2].ik_sch    1362a4638f2586486bff5a76f7874a83
round[ 3].istart    3e1c22c0b6fcbf768da85067f6170495
round[ 3].is_box    d1c4941f7955f40fb46f6c0ad68730ad
round[ 3].is_row    d1876c0f79c4300ab45594add66ff41f
round[ 3].im_col    39daee38f4f1a82aaf432410c36d45b9
round[ 3].ik_sch    8d82fc749c47222be4dadc3e9c7810f5
round[ 4].istart    b458124c68b68a014b99f82e5f15554c
round[ 4].is_box    c65e395df779cf09ccf9e1c3842fed5d
round[ 4].is_row    c62fe109f75eedc3cc79395d84f9cf5d
round[ 4].im_col    9a39bf1d05b20a3a476a0bf79fe51184
round[ 4].ik_sch    72e3098d11c5de5f789dfe1578a2cccb
round[ 5].istart    e8dab6901477d4653ff7f5e2e747dd4f
round[ 5].is_box    c87a79969b0219bc2526773bb016c992
round[ 5].is_row    c81677bc9b7ac93b25027992b0261996
round[ 5].im_col    18f78d779a93eef4f6742967c47f5ffd
round[ 5].ik_sch    2ec410276326d7d26958204a003f32de
round[ 6].istart    36339d50f9b539269f2c092dc4406d23
round[ 6].is_box    2466756c69d25b236e4240fa8872b332
round[ 6].is_row    247240236966b3fa6ed2753288425b6c
round[ 6].im_col    85cf8bf472d124c10348f545329c0053
round[ 6].ik_sch    a8a2f5044de2c7f50a7ef79869671294
round[ 7].istart    2d6d7ef03f33e334093602dd5bfb12c7
round[ 7].is_box    fab38a1725664d2840246ac957633931
round[ 7].is_row    fa636a2825b339c940668a3157244d17
round[ 7].im_col    fc1fc1f91934c98210fbfb8da340eb21
round[ 7].ik_sch    c7c6e391e54032f1479c306d6319e50c
```

```
round[ 8].istart    3bd92268fc74fb735767cbe0c0590e2d
round[ 8].is_box    49e594f755ca638fda0a59a01f15d7fa
round[ 8].is_row    4915598f55e5d7a0daca94fa1f0a63f7
round[ 8].im_col    076518f0b52ba2fb7a15c8d93be45e00
round[ 8].ik_sch    a0db02992286d160a2dc029c2485d561
round[ 9].istart    a7be1a6997ad739bd8c9ca451f618b61
round[ 9].is_box    895a43e485188fe82d121068cbd8ced8
round[ 9].is_row    89d810e8855ace682d1843d8cb128fe4
round[ 9].im_col    ef053f7c8b3d32fd4d2a64ad3c93071a
round[ 9].ik_sch    8c56dff0825dd3f9805ad3fc8659d7fd
round[10].istart    6353e08c0960e104cd70b751bacad0e7
round[10].is_box    0050a0f04090e03080d02070c01060b0
round[10].is_row    00102030405060708090a0b0c0d0e0f0
round[10].ik_sch    000102030405060708090a0b0c0d0e0f
round[10].ioutput   00112233445566778899aabbccddeeff
```

2. InvMixColumns

State:		After InvMixColumns
0xe9f74eec		0x54d990a1
0x023020f6	→	0x6ba09ab5
0x1bf2ccf2		0x96bbf40e
0x353c21c7		0xa111702f

3. Questions:

   a) Does order of performing SubWords and ShiftRows functions (including inversions) matter?
   b) Can You use fastMul function delivered on previous classes for invMixVars constancances?

      For example, can I write:

      0xbd * 0x0e = 0xbd * 0x02 * 0x02 * 0x02 + 0xbd + 0xbd + 0xbd + 0xbd + 0xbd + 0xbd

      or, maybe, just only maybe, should I write:

      0xbd * 0x0e = 0xbd * 0x08 + 0xbd * 0x04 + 0xbd * 0x02

      How XOR works?

      Replace your fastMul function with functions included in improvedFastMul.java.