08111701班 1120172140 李彦霖

一. 流程图

1. 伪代码说明

- 加密

```
Encode(uint8 in[16], uint8 out[16], uint8 key[16]){
  uint8 state[4,4] = in;
  uint32 w[44] = KeyExpansions(key[16]);

  addRoundKey(state, w[0-3]);

  for (int j = 1; j < 10; ++j) {
    subBytes(state);
    shiftRows(state);
    mixColumns(state);
    addRoundKey(state, w); //w[4-7],w[8-11]...w[37-40]
  }

  subBytes(state);
  shiftRows(state);
  addRoundKey(state, w[41-44]);
  out = state;
}
```

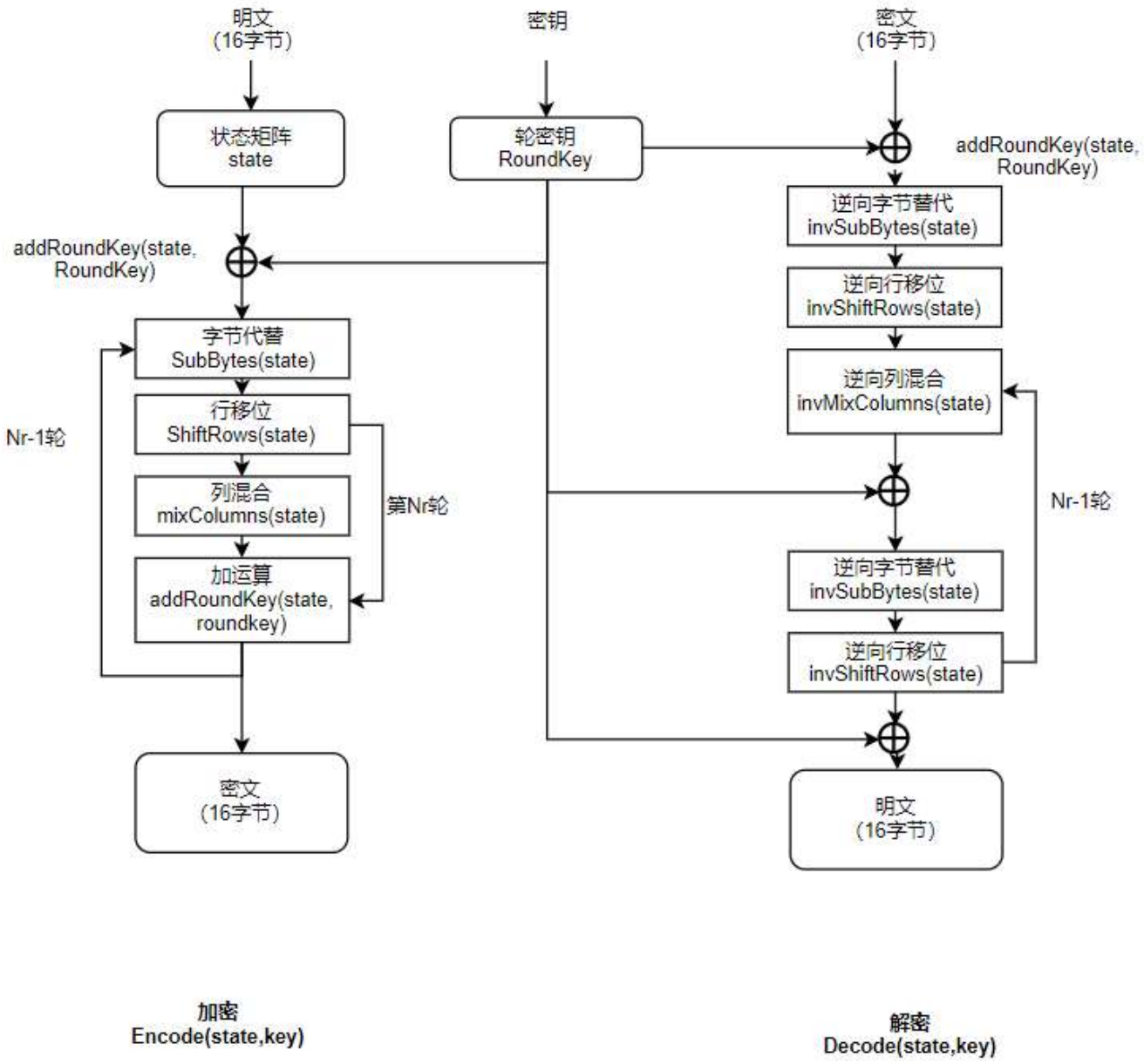
- 解密

```
Decode(uint8 in[16], uint8 out[16], uint8 key[16]){
  uint8 state[4,4] = in;
  uint32 w[44] = KeyExpansions(key[16]);
  //此时使用的秘钥是加密时使用的秘钥的倒序
  addRoundKey(state, w[41-44]);

  for (int j = 1; j < 10; ++j) {
    inverse-subBytes(state);
    inverse-shiftRows(state);
    inverse-mixColumns(state);
    addRoundKey(state, w); //w[37-40], ... w[8-11],w[4-7],...
  }

  inverse-subBytes(state);
  inverse-shiftRows(state);
  addRoundKey(state, w[0-3]);
  out = state;
}
```

2. 流程图



二. 测试用例及结果

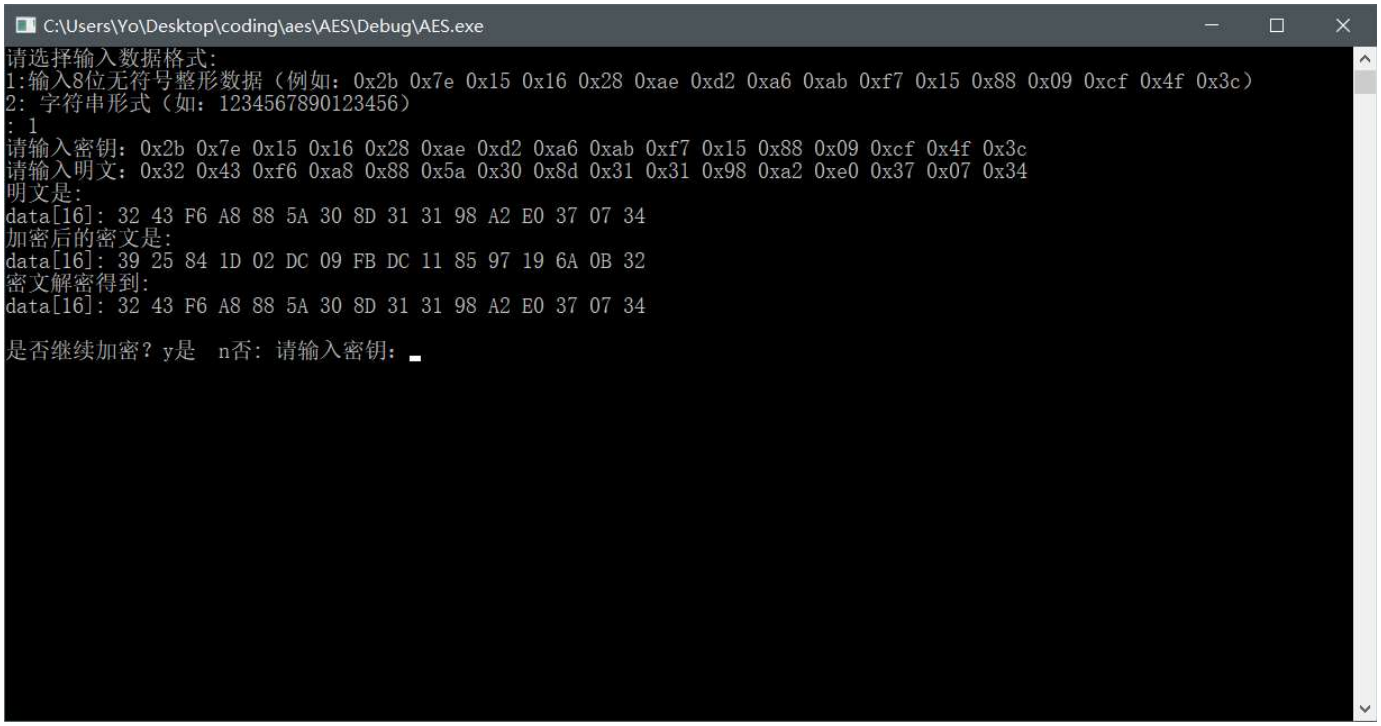
1. 模式1

输入8位无符号整形数据（例如：0x2b 0x7e 0x15 0x16 0x28 0xae 0xd2 0xa6 0xab 0xf7 0x15 0x88 0x09 0xcf 0x4f 0x3c)

- 测试用例

密钥：
0x2b 0x7e 0x15 0x16 0x28 0xae 0xd2 0xa6 0xab 0xf7 0x15 0x88 0x09 0xcf 0x4f 0x3c
明文：
0x32 0x43 0xf6 0xa8 0x88 0x5a 0x30 0x8d 0x31 0x31 0x98 0xa2 0xe0 0x37 0x07 0x34

- 输出



2. 模式2

字符串形式（如：1234567890123456）

- 测试用例

密钥：

1234567890123456

明文：

abcdefghijklmnopqrstuvwxyz123456

- 输出