> 姓名：佘崧林
>
> 学号：1613574

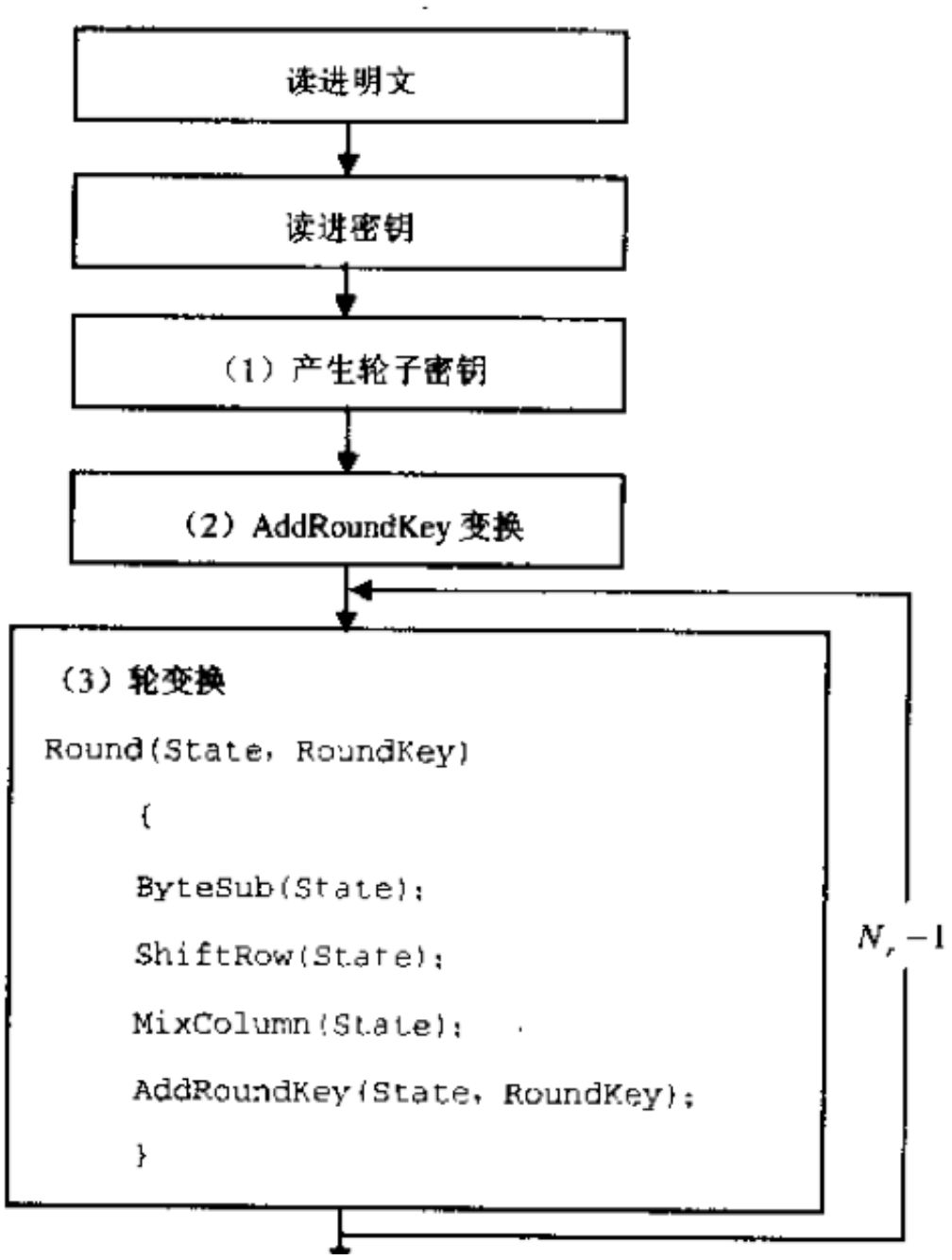
AES

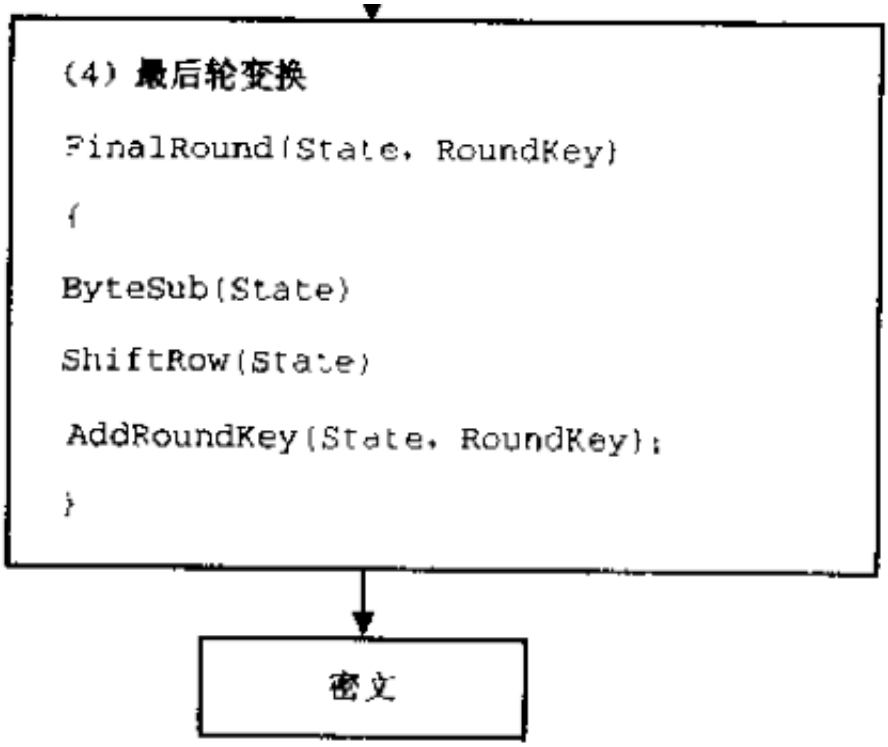
实验目的

通过用 AES 算法对实际的数据进行加密和解密来深刻了解 AES 的运行原理。

实验原理

实验流程图：





实验要求

1. 算法分析：

   对课本中 AES 算法进行深入分析，对其中用到的基本数学算法、字节代 换、行移位变换、列混合变换原理进行详细的分析，并考虑如何进行编程实现。对轮函数、密钥生成等环节要有清晰的了解，并考虑其每一个环节的实现 过程。

2. AES 实现程序的总体设计:

   在第一步的基础上，对整个 AES 加密函数的实现进行总体设计，考虑数据 的存储格式，参数的传递格式，程序实现的总体层次等，画出程序实现的流程 图。

3. 在总体设计完成后，开始具体的编码，在编码过程中，注意要尽量使用 高效的编码方式。

4. 利用 3 中实现的程序，对 AES 的密文进行雪崩效应检验。即固定密 钥，仅改变明文中的一位，统计密文改变的位数;固定明文，仅改变密钥中的 一位，统计密文改变的位数。

实验内容

关键函数

1. 字节替换函数 `ByteSubstitution`：

```
Squre4Marix &Squre4Marix::ByteSubstitution(const uint8_t SBOX[256]) {
    this->ForEach([SBOX](int r, int c, uint8_t *element) {
        *element = SBOX[*element];
    });
    return *this;
}
```

2. 行位移变换函数 `ShiftRows`：

```
Squre4Marix &Squre4Marix::ShiftRows(bool isinv) {
    Squre4Marix temp = *this;
    if (isinv) {
        this->ForEach([temp](int r, int c, uint8_t *element) {
            *element = temp[(r - c + 4) % 4][c];  // NOTICE: -1%4 == -1
        });
    } else {
        this->ForEach([temp](int r, int c, uint8_t *element) {
            *element = temp[(r + c) % 4][c];
        });
    }
    return *this;
}
```

3. 列混淆函数 `MixColumns`：

```
Squre4Marix &Squre4Marix::MixColumns(bool isinv) {
    // learnt from http://cs.ucsb.edu/~koc/cs178/projects/JT/aes.c
    static const auto xtime = [](uint8_t x) -> uint8_t {
        return (x & 0x80u) ? (((x << 1u) ^ 0x1Bu) & 0xFFu) : x << 1u;
    };

    if (isinv) {
        for (auto r : this->data) {
            uint8_t u = xtime(xtime(r[0] ^ r[2])), v = xtime(xtime(r[1] ^
r[3]));
            r[0] ^= u;
            r[1] ^= v;
            r[2] ^= u;
            r[3] ^= v;
        }
    }
    for (auto r : this->data) {
        uint8_t t = r[0] ^r[1] ^r[2] ^r[3], u = r[0];
        r[0] ^= t ^ xtime(r[0] ^ r[1]);
        r[1] ^= t ^ xtime(r[1] ^ r[2]);
        r[2] ^= t ^ xtime(r[2] ^ r[3]);
        r[3] ^= t ^ xtime(r[3] ^ u);
    }
    return *this;
}
```

4. 轮密钥加替换 `AddRoundKey`：

```
void Aes::AddRoundKey(Squre4Marix *state, uint8_t round) {
    assert(round >= 0 && round <= 10);
    state->ForEach([this, round](int r, int c, uint8_t *data) {
        *data ^= (this->roundKey[round][r][c]);
    });
}
```

5. 密钥扩展 `KeyExpansion`：

```
void Aes::KeyExpansion(bitset128 key) {
    roundKey[0] = Squre4Marix(key);

    for (int i = 1; i <= 10; i++) {
        bitset32 rows[4] = {0x00};
        for (int j = 0; j < 4; ++j) {
            rows[0] <<= 8;
            rows[0] |= roundKey[i - 1][0][j] ^ SBOX[roundKey[i - 1][3][(j
+ 1) % 4]];
        }
        rows[0] ^= RCON[i] << 3u * 8;
        for (int j = 1; j < 4; ++j) {
            rows[j] = rows[j - 1] ^ roundKey[i - 1].row(j);
        }
        roundKey[i] = Squre4Marix(rows, true);
    }
}
```

其他实验详细内容，见具体代码。

实验结果

我自己生成了十组实验数据，实验结果如下：

```
$ ./bin/lab3
--------------------------------------------------------------------------------
------------------------------------------------
Initial Key:
11000111100101100111100111001110110111000000010111000010000101001000101111001101
11001100111100000101101101001100000111111110111011
Test Plain :
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000001
Test Cipher:
01110000110010001010110110001011010010101110100000100011011101101001101110010011
00101101111010001110111101001010101000110000110 11
Calc Plain :
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000001
```

```
Calc Cipher:
01110000110010001010110110001011010010101110100000100011011101101001101110010110010110111010001110111101001010100011000011011
################################################################################
################################################
Encrypt avalanche test: (Average 62.7812)
56,63,67,60,54,57,70,62,66,73,61,58,62,69,65,59,60,63,60,62,66,54,67,62,65,57,61,64,63,64,65,59,61,67,61,63,52,56,63,69,65,62,63,66,70,61,64,67,65,66,65,58,53,67,69,69,54,65,67,67,64,67,63,55,
56,63,67,60,54,57,70,62,66,73,61,58,62,69,65,59,60,63,60,62,66,54,67,62,65,57,61,64,63,64,65,59,61,67,61,63,52,56,63,69,65,62,63,66,70,61,64,67,65,66,65,58,53,67,69,69,54,65,67,67,64,67,63,55,
Decrypt avalanche test: (Average 63.5312)
58,72,67,63,70,63,53,65,68,63,59,59,60,66,62,64,68,51,65,65,59,62,70,60,70,66,51,70,61,58,63,69,64,60,60,69,65,55,70,60,62,54,79,63,67,63,61,56,54,69,67,61,59,63,65,65,66,69,62,65,70,61,66,76,
58,72,67,63,70,63,53,65,68,63,59,59,60,66,62,64,68,51,65,65,59,62,70,60,70,66,51,70,61,58,63,69,64,60,60,69,65,55,70,60,62,54,79,63,67,63,61,56,54,69,67,61,59,63,65,65,66,69,62,65,70,61,66,76,
--------------------------------------------------------------------------------
------------------------------------------------
Initial Key:
01100110001101101110011110000100111110110000110011001011101010111010010110000111011100100000101011001111101111001000000100100111
Test Plain :
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000010
Test Cipher:
00100101010000001101100101000010000101010101010011001111101110111111110101110011111011011100111100001001001010101111011111110100 00
Calc Plain :
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000010
Calc Cipher:
00100101010000001101100101000010000101010101010011001111101110111111110101110011111011011100111100001001001010101111011111110100 00
################################################################################
################################################
Encrypt avalanche test: (Average 64.0625)
67,50,64,64,65,74,59,57,78,63,68,58,67,66,56,53,63,72,58,60,70,70,67,55,71,50,70,65,71,67,64,64,55,70,68,56,52,67,62,62,59,74,65,59,63,72,69,55,73,66,59,52,67,70,63,70,62,59,64,70,68,66,73,64,
67,50,64,64,65,74,59,57,78,63,68,58,67,66,56,53,63,72,58,60,70,70,67,55,71,50,70,65,71,67,64,64,55,70,68,56,52,67,62,62,59,74,65,59,63,72,69,55,73,66,59,52,67,70,63,70,62,59,64,70,68,66,73,64,
Decrypt avalanche test: (Average 64.6562)
61,62,70,61,71,57,72,77,59,64,65,61,65,66,64,58,73,62,62,62,72,68,67,68,63,62,63,62,67,55,61,55,57,71,62,59,64,68,67,65,63,71,70,67,61,64,64,71,73,60,67,66,68,63,65,60,75,58,67,59,58,66,73,61,
```

61,62,70,61,71,57,72,77,59,64,65,61,65,66,64,58,73,62,62,62,72,68,67,68,63,62,63,62,67,55,61,55,57,71,62,59,64,68,67,65,63,71,70,67,61,64,64,71,73,60,67,66,68,63,65,60,75,58,67,59,58,66,73,61,

---

Initial Key:
10010101100010011110111010100100011110111001001001011001100010001011010001011100110100000101011011100110101101000010010

Test Plain :
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000100

Test Cipher:
10110011010001100100011010101111011001000010001111110000011000110001011110011001010010000101001000101101000001011001011010111100

Calc Plain :
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000100

Calc Cipher:
10110011010001100100011010101111011001000010001111110000011000110001011110011001010010000101001000101101000001011001011010111100

##

Encrypt avalanche test: (Average 63.2031)
74,66,62,68,64,60,64,59,63,71,62,74,55,56,65,58,64,62,55,66,63,56,59,71,71,67,67,67,69,64,66,66,66,61,69,61,58,64,67,64,75,59,49,69,64,58,60,58,63,59,65,62,63,61,64,67,67,64,66,56,63,57,61,51,
74,66,62,68,64,60,64,59,63,71,62,74,55,56,65,58,64,62,55,66,63,56,59,71,71,67,67,67,69,64,66,66,66,61,69,61,58,64,67,64,75,59,49,69,64,58,60,58,63,59,65,62,63,61,64,67,67,64,66,56,63,57,61,51,

Decrypt avalanche test: (Average 64.5625)
66,51,63,70,62,63,60,66,71,61,60,64,70,61,70,62,56,68,66,58,68,71,69,68,66,58,63,68,67,55,63,66,71,69,65,62,64,74,62,73,56,72,64,67,63,61,58,59,69,64,60,77,68,63,68,61,66,60,57,68,64,64,64,69,
66,51,63,70,62,63,60,66,71,61,60,64,70,61,70,62,56,68,66,58,68,71,69,68,66,58,63,68,67,55,63,66,71,69,65,62,64,74,62,73,56,72,64,67,63,61,58,59,69,64,60,77,68,63,68,61,66,60,57,68,64,64,64,69,

---

Initial Key:
00111101000011010010010001100000111010000110101111110100001101010001000101100111110010101110100110111110001101100001100011001111

Test Plain :
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001000

Test Cipher:
11100101001011110000101000110011111001000101100000000011000101001111111101000001000000010100110101011101100001011001011010110110

```
Calc Plain :
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000001000
Calc Cipher:
11100101001011110000101000110011111001000101100000000110001010011111111010000010
00000001010011010101110110000101100101101011011 00
################################################################################
################################################
Encrypt avalanche test: (Average 64.2656)
64,70,76,60,59,66,63,56,70,61,60,53,63,59,65,64,58,66,50,57,62,71,57,60,69,63,6
4,69,63,69,59,60,54,60,74,58,69,70,63,70,71,66,69,56,66,59,68,69,78,64,66,67,74
,59,73,61,63,61,63,78,63,68,59,68,
64,70,76,60,59,66,63,56,70,61,60,53,63,59,65,64,58,66,50,57,62,71,57,60,69,63,6
4,69,63,69,59,60,54,60,74,58,69,70,63,70,71,66,69,56,66,59,68,69,78,64,66,67,74
,59,73,61,63,61,63,78,63,68,59,68,
Decrypt avalanche test: (Average 63.5938)
63,65,67,61,57,63,67,61,79,67,56,63,53,64,63,65,59,67,62,65,65,53,67,53,67,51,6
4,78,62,65,68,79,57,62,60,58,67,72,75,64,63,62,62,74,52,64,64,60,70,56,66,57,60
,69,56,62,67,54,67,55,68,64,63,81,
63,65,67,61,57,63,67,61,79,67,56,63,53,64,63,65,59,67,62,65,65,53,67,53,67,51,6
4,78,62,65,68,79,57,62,60,58,67,72,75,64,63,62,62,74,52,64,64,60,70,56,66,57,60
,69,56,62,67,54,67,55,68,64,63,81,
--------------------------------------------------------------------------------
------------------------------------------------
Initial Key:
11110011011111111101100011110101010111001000110001000110111011111101001110110010
11111110100111110110110100011111101010010010100
Test Plain :
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000010000
Test Cipher:
11110011001010111101100100100110100010111011111111101100001000000110111101101010
11010011100110111111110000101001111101100110 0101
Calc Plain :
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000010000
Calc Cipher:
11110011001010111101100100100110100010111011111111101100001000000110111101101010
11010011100110111111110000101001111101100110 0101
################################################################################
################################################
Encrypt avalanche test: (Average 63.125)
70,54,70,74,65,64,60,62,69,63,62,66,55,65,63,70,61,57,61,70,54,61,70,60,65,69,5
4,62,54,56,56,74,52,65,66,60,58,58,65,65,68,69,62,70,68,60,66,66,68,59,62,76,64
,60,72,64,57,67,49,60,63,69,61,55,
70,54,70,74,65,64,60,62,69,63,62,66,55,65,63,70,61,57,61,70,54,61,70,60,65,69,5
4,62,54,56,56,74,52,65,66,60,58,58,65,65,68,69,62,70,68,60,66,66,68,59,62,76,64
,60,72,64,57,67,49,60,63,69,61,55,
Decrypt avalanche test: (Average 63.3125)
```

65,53,58,67,71,73,64,63,60,64,65,77,63,64,69,65,53,66,69,59,58,62,70,61,65,70,5
3,60,63,54,61,68,61,60,62,64,60,65,62,59,66,54,59,64,68,65,61,70,61,58,66,60,64
,66,64,54,67,58,62,70,62,65,74,68,
65,53,58,67,71,73,64,63,60,64,65,77,63,64,69,65,53,66,69,59,58,62,70,61,65,70,5
3,60,63,54,61,68,61,60,62,64,60,65,62,59,66,54,59,64,68,65,61,70,61,58,66,60,64
,66,64,54,67,58,62,70,62,65,74,68,

Initial Key:
0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000100000
Test Plain :
0110000101011011110011000110010011101001100110001010000010111001111101111001100
1001001100101011000010011010111111011000100100010
Test Cipher:
0111100011101101010011010100010001100100010101010101000001001100011101000011011
0000111000111011101110101100111100110001101010001
Calc Plain :
0110000101011011110011000110010011101001100110001010000010111001111101111001100
1001001100101011000010011010111111011000100100010
Calc Cipher:
0111100011101101010011010100010001100100010101010101000001001100011101000011011
0000111000111011101110101100111100110001101010001
###
###
Encrypt avalanche test: (Average 63.6719)
66,61,58,65,59,62,65,63,72,66,67,51,67,62,67,58,56,66,71,65,55,60,56,72,69,57,6
4,60,65,68,72,75,64,71,61,65,65,63,61,63,63,65,63,62,62,63,62,58,52,54,70,68,70
,78,67,62,67,64,74,53,55,62,59,69,
66,61,58,65,59,62,65,63,72,66,67,51,67,62,67,58,56,66,71,65,55,60,56,72,69,57,6
4,60,65,68,72,75,64,71,61,65,65,63,61,63,63,65,63,62,62,63,62,58,52,54,70,68,70
,78,67,62,67,64,74,53,55,62,59,69,
Decrypt avalanche test: (Average 63.2656)
72,69,61,53,66,61,67,67,63,67,67,60,66,67,67,74,57,63,70,54,69,60,65,57,63,59,6
0,71,66,64,61,71,62,61,63,67,64,57,48,72,62,65,66,52,62,58,64,66,61,59,59,63,67
,66,59,68,64,65,63,69,57,52,71,60,
72,69,61,53,66,61,67,67,63,67,67,60,66,67,67,74,57,63,70,54,69,60,65,57,63,59,6
0,71,66,64,61,71,62,61,63,67,64,57,48,72,62,65,66,52,62,58,64,66,61,59,59,63,67
,66,59,68,64,65,63,69,57,52,71,60,

Initial Key:
0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000001000000
Test Plain :
0000001110100100001100011100010000000000011101101001011010001001011111100101011
0001110011000111000000000101001110101100000000101

```
Test Cipher:
10101001010011101111001110010111100100001101110001101110110000011000110001010111011110000010011101010011011011011001100010110011 0
Calc Plain :
00000011101001000011000111000100000000000111011010010110100010010111111001010110001110011000111000000000101001110101100000000101
Calc Cipher:
10101001010011101111001110010111100100001101110001101110110000011000110001010111011110000010011101010011011011011001100010110011 0
################################################################################################################################################
Encrypt avalanche test: (Average 62.9375)
67,65,68,62,64,52,68,65,55,56,61,75,65,53,60,67,64,68,70,55,62,64,65,67,56,60,66,64,72,58,60,57,66,68,72,58,59,65,63,61,60,64,76,61,58,53,64,63,63,58,66,59,61,66,68,61,68,61,64,61,60,60,64,66,
67,65,68,62,64,52,68,65,55,56,61,75,65,53,60,67,64,68,70,55,62,64,65,67,56,60,66,64,72,58,60,57,66,68,72,58,59,65,63,61,60,64,76,61,58,53,64,63,63,58,66,59,61,66,68,61,68,61,64,61,60,60,64,66,
Decrypt avalanche test: (Average 63.5156)
72,62,63,66,62,62,66,60,48,68,69,59,61,58,62,70,67,68,58,63,63,61,61,64,68,55,69,60,68,51,68,53,58,63,68,66,67,58,60,47,66,75,64,67,60,74,64,73,68,75,69,57,58,70,55,64,66,69,61,67,58,60,67,66,
72,62,63,66,62,62,66,60,48,68,69,59,61,58,62,70,67,68,58,63,63,61,61,64,68,55,69,60,68,51,68,53,58,63,68,66,67,58,60,47,66,75,64,67,60,74,64,73,68,75,69,57,58,70,55,64,66,69,61,67,58,60,67,66,
--------------------------------------------------------------------------------------------------------------------------------------------
Initial Key:
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000010000000
Test Plain :
11000000010000110111011011100110001000000001011011011000111101001001111101001010100101000101101111001100001001010000011000111 00
Test Cipher:
00101111100101010101110100101110111110011011010011011110011100110010000110000011001000010110000111001001101011100101100100010110 1
Calc Plain :
11000000010000110111011011100110001000000001011011011000111101001001111101001010100101000101101111001100001001010000011000111 00
Calc Cipher:
00101111100101010101110100101110111110011011010011011110011100110010000110000011001000010110000111001001101011100101100100010110 1
################################################################################################################################################
Encrypt avalanche test: (Average 64.0469)
62,62,55,76,66,62,56,56,66,66,64,64,64,61,64,63,64,64,59,63,65,66,59,68,58,71,61,75,61,67,51,66,73,65,54,73,61,55,58,57,72,62,71,71,66,62,66,60,57,57,60,70,68,60,62,70,79,74,71,71,60,60,68,61,
```

```
62,62,55,76,66,62,56,56,66,66,64,64,64,61,64,63,64,64,59,63,65,66,59,68,58,71,6
1,75,61,67,51,66,73,65,54,73,61,55,58,57,72,62,71,71,66,62,66,60,57,57,60,70,68
,60,62,70,79,74,71,71,60,60,68,61,
Decrypt avalanche test: (Average 64.3594)
66,54,73,62,70,55,61,75,73,56,63,64,69,60,75,69,60,61,67,56,68,69,71,67,62,57,6
4,68,63,67,63,57,64,75,72,63,64,62,64,58,68,63,67,64,68,63,70,67,64,64,52,70,58
,57,56,58,66,69,67,63,58,71,63,66,
66,54,73,62,70,55,61,75,73,56,63,64,69,60,75,69,60,61,67,56,68,69,71,67,62,57,6
4,68,63,67,63,57,64,75,72,63,64,62,64,58,68,63,67,64,68,63,70,67,64,64,52,70,58
,57,56,58,66,69,67,63,58,71,63,66,
-------------------------------------------------------------------------------
-------------------------------------------------
Initial Key:
0000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000100000000
Test Plain :
0010101111000011111010000001011111001000001111001001110001110111110000000100001
1100110101000001010101000110011110011010110000000
Test Cipher:
1000001010011100001110001001011101100000100100011100011110110110000100010110110
1010100011111011010110101101011110110100110101100
Calc Plain :
0010101111000011111010000001011111001000001111001001110001110111110000000100001
1100110101000001010101000110011110011010110000000
Calc Cipher:
1000001010011100001110001001011101100000100100011100011110110110000100010110110
1010100011111011010110101101011110110100110101100
###############################################################################
#################################################
Encrypt avalanche test: (Average 62.7969)
74,58,65,79,65,63,56,60,63,62,59,62,63,65,72,50,70,66,62,67,57,63,59,72,68,66,5
6,66,56,55,66,52,63,66,62,64,61,70,61,55,58,51,63,69,68,62,61,60,68,60,56,60,64
,61,53,63,69,64,61,64,65,63,73,64,
74,58,65,79,65,63,56,60,63,62,59,62,63,65,72,50,70,66,62,67,57,63,59,72,68,66,5
6,66,56,55,66,52,63,66,62,64,61,70,61,55,58,51,63,69,68,62,61,60,68,60,56,60,64
,61,53,63,69,64,61,64,65,63,73,64,
Decrypt avalanche test: (Average 63.5312)
64,65,67,55,63,65,62,61,62,66,54,64,70,61,61,53,59,58,62,61,68,66,64,66,65,65,6
8,53,58,61,61,69,64,61,60,61,61,62,62,69,64,66,74,59,71,67,52,66,66,58,67,64,68
,70,70,61,62,56,67,79,56,80,60,66,
64,65,67,55,63,65,62,61,62,66,54,64,70,61,61,53,59,58,62,61,68,66,64,66,65,65,6
8,53,58,61,61,69,64,61,60,61,61,62,62,69,64,66,74,59,71,67,52,66,66,58,67,64,68
,70,70,61,62,56,67,79,56,80,60,66,
-------------------------------------------------------------------------------
-------------------------------------------------
Initial Key:
0000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000001000000000
```

```
Test Plain :
0000000010000011001100111011100110000101010001101010100010101001010011000011010
0100111010110101110101011111111000110000101110001
Test Cipher:
0100100000100100111101110110111000100010100110110101011111110100001011101000111
1101110100110101111010111110100010110111100110011
Calc Plain :
0000000010000011001100111011100110000101010001101010100010101001010011000011010
0100111010110101110101011111111000110000101110001
Calc Cipher:
0100100000100100111101110110111000100010100110110101011111110100001011101000111
1101110100110101111010111110100010110111100110011
################################################################################
################################################
Encrypt avalanche test: (Average 64.125)
63,61,66,65,62,65,66,68,53,56,71,69,65,54,63,62,73,76,63,66,62,60,63,75,54,59,6
1,65,75,72,69,60,57,63,63,67,62,66,72,59,62,61,65,62,53,57,68,66,65,66,60,77,50
,61,72,69,64,72,65,69,57,65,58,69,
63,61,66,65,62,65,66,68,53,56,71,69,65,54,63,62,73,76,63,66,62,60,63,75,54,59,6
1,65,75,72,69,60,57,63,63,67,62,66,72,59,62,61,65,62,53,57,68,66,65,66,60,77,50
,61,72,69,64,72,65,69,57,65,58,69,
Decrypt avalanche test: (Average 63.5)
57,67,55,61,70,59,61,70,70,67,66,61,61,45,67,62,59,65,63,68,61,65,57,60,73,71,5
9,60,72,61,70,56,76,67,66,54,52,66,68,62,64,71,67,61,71,68,60,70,68,60,64,65,64
,61,63,65,66,62,54,66,59,56,52,77,
57,67,55,61,70,59,61,70,70,67,66,61,61,45,67,62,59,65,63,68,61,65,57,60,73,71,5
9,60,72,61,70,56,76,67,66,54,52,66,68,62,64,71,67,61,71,68,60,70,68,60,64,65,64
,61,63,65,66,62,54,66,59,56,52,77,
```