1. 第九轮注入故障

正确密文：

the\_cipher = [0x66, 0xe9, 0x4b, 0xd4,

                      0xef, 0x8a, 0x2c, 0x3b,

                      0x88, 0x4c, 0xfa, 0x59,

                      0xca, 0x34, 0x2b, 0x2e]

错误密文：

faulty\_cipher\_1 = [0xf8, 0xe9, 0x4b, 0xd4,

                      0xef, 0x8a, 0x2c, 0x35,

                      0x88, 0x4c, 0x91, 0x59,

                      0xca, 0x50, 0x2b, 0x2e]

faulty\_cipher\_2 = [0x26, 0xe9, 0x4b, 0xd4,

                      0xef, 0x8a, 0x2c, 0x56,

                      0x88, 0x4c, 0x15, 0x59,

                      0xca, 0xb7, 0x2b, 0x2e]

要求恢复K[0],K[13],K[10],K[7]。

部分正确密钥为：K[0] = 0xb4, K[13] = 0x8f

1. 第八轮注入故障

第一对密文对：

正确密文：

The\_cipher = [0x66, 0xe9, 0x4b, 0xd4,

                      0xef, 0x8a, 0x2c, 0x3b,

                      0x88, 0x4c, 0xfa, 0x59,

                      0xca, 0x34, 0x2b, 0x2e]

错误密文：

faulty\_cipher\_1 = [0xfd, 0x77, 0x6e, 0x56,

                        0x79, 0xbd, 0xe2, 0xf5,

                        0x1d, 0xc6, 0x79, 0x25,

                        0xe3, 0xfd, 0x61, 0xc8]

faulty\_cipher\_2 = [0x6d, 0x6b, 0x8f, 0x2a,

                        0xd4, 0xba, 0x24, 0x3d,

                        0xeb, 0x3b, 0x4b, 0xe2,

                        0x4f, 0xe2, 0x02, 0xcf]

要求恢复第十轮全部十六个字节的密钥：

前四个字节的密钥分别为K[0] = 0xb4,K[1] = 0xef, K[2] = 0x5b, K[3] = 0xcb

第二对密文对：

正确密文：

the\_cipher = [0x69, 0xc4, 0xe0, 0xd8,

                      0x6a, 0x7b, 0x04, 0x30,

                      0xd8, 0xcd, 0xb7, 0x80,

                      0x70, 0xb4, 0xc5, 0x5a]

错误密文：

faulty\_cipher\_1 = [0x0a, 0xfd, 0xd3, 0x71,

                        0xff, 0x34, 0xd1, 0xaf,

                        0x12, 0x96, 0x3c, 0x02,

                        0xb4, 0x06, 0xe8, 0x52]

faulty\_cipher\_2 = [0x52, 0x30, 0x76, 0x7e,

                  0x08, 0xcf, 0x4f, 0x19,

                  0x27, 0x2c, 0xc1, 0x5f,

                  0x87, 0x53, 0x82, 0xd5]

要求恢复第十轮全部十六个字节的密钥：

前四个字节的密钥分别为K[0] = 0x13,K[1] = 0x11, K[2] = 0x1d, K[3] = 0x7f