

实验要求

- 1. 实现SM4算法，速率**不低于300Mbps**，完成助教提供的接口测试；
- 2. 实现SM4-CBC模式，分别测试数据包大小在64B、2KB、10MB下的加解密性能，**提供测试性能截图即可；【注意：每次的IV需要变化】。**
这部分的接口与代码自行编写，提供不同数据包大小的加解密运行界面的完整截图

测试样例

3.3.4 示例

以下为 SM4 算法在 ECB 工作方式下的运算实例，用以验证密码算法实现的正确性。其中，数据采用 16 进制表示。

明 文：01 23 45 67 89 ab cd ef fe dc ba 98 76 54 32 10
加密密钥：01 23 45 67 89 ab cd ef fe dc ba 98 76 54 32 10
轮密钥与每轮输出状态如下：

rk[0] = f12186f9	X[0] = 27fad345
rk[1] = 41662b61	X[1] = a18b4cb2
rk[2] = 5a6ab19a	X[2] = 11c1e22a
rk[3] = 7ba92077	X[3] = cc13e2ee
rk[4] = 367360f4	X[4] = f87c5bd5
rk[5] = 776a0c61	X[5] = 33220757
rk[6] = b6bb89b3	X[6] = 77f4c297
rk[7] = 24763151	X[7] = 7a96f2eb
rk[8] = a520307c	X[8] = 27dac07f
rk[9] = b7584dbd	X[9] = 42dd0f19
rk[10] = c30753ed	X[10] = b8a5da02
rk[11] = 7ee55b57	X[11] = 907127fa
rk[12] = 6988608c	X[12] = 8b952b83
rk[13] = 30d895b7	X[13] = d42b7c59
rk[14] = 44ba14af	X[14] = 2ffc5831

rk[15] = 104495a1	X[15] = f69e6888
rk[16] = d120b428	X[16] = af2432c4
rk[17] = 73b55fa3	X[17] = ed1ec85e
rk[18] = cc874966	X[18] = 55a3ba22
rk[19] = 92244439	X[19] = 124b18aa
rk[20] = e89e641f	X[20] = 6ae7725f
rk[21] = 98ca015a	X[21] = f4cba1f9
rk[22] = c7159060	X[22] = 1dcdfa10
rk[23] = 99e1fd2e	X[23] = 2ff60603
rk[24] = b79bd80c	X[24] = eff24fdc
rk[25] = 1d2115b0	X[25] = 6fe46b75
rk[26] = 0e228aeb	X[26] = 893450ad
rk[27] = f1780c81	X[27] = 7b938f4c
rk[28] = 428d3654	X[28] = 536e4246
rk[29] = 62293496	X[29] = 86b3e94f
rk[30] = 01cf72e5	X[30] = d206965e

```
rk[31] = 9124a012      X[31] = 681edf34
```

最后得到密文: 68 1e df 34 d2 06 96 5e 86 b3 e9 4f 53 6e 42 46

3.4 分组密码的应用技术

我们已经介绍了一些典型的密码算法，但是密码算法的实际应用仍有许多具体的技术问题。这些应用技术不解决，即使采用安全的密码算法也是徒劳的。本节介绍分组密码在实际应用中的一些技术问题。

1977 年 DES 的颁布，对推动密码技术的应用起了重要作用。1981 年美国 NSB 针对 DES 的应用制定了四种基本工作模式：电码本模式 (**ECB**)、密文链接模式 (**CBC**)、密文反馈模式 (**CFB**) 和输出反馈模式 (**OFB**)。2000 年美国在征集 AES 的同时又公开征集 AES 的工作模式^[49]。共征集到 15 个候选工作模式，其中 **X CBC** 模式很有实用价值，**CTR** (Counter Mode Encryption) 模式很有特色。这些新的工作模式将为 AES 的应用作出贡献。下面我们介绍分组密码的这几种工作模式。

提交注意事项

```
1  BUILD_DIR = build
2  INC_DIR = inc
3  SRC_DIR = src
4
5  all:
6      gcc \
7          -Wall -Wextra \
8          -O3 -funroll-loops \
9          -march=native \
10         -I$(INC_DIR) \
11         $(SRC_DIR)/*.c \
12         -o $(BUILD_DIR)/sm4
13
14  clean:
15      rm -f $(BUILD_DIR)/*
```

根据需要可以自行修改 Makefile，但是注意红线框出部分不要修改，确保生成的可执行文件 sm4 在 build 目录下。

学号-姓名		
排序 查看 ...		
名称	修改日期	类型
build	2024/11/25 22:31	文件夹
inc	2024/11/25 22:11	文件夹
src	2024/11/25 22:12	文件夹
Makefile	2024/11/25 22:36	文件

.h文件放到inc文件夹下，.c文件放到src文件夹下。

注意： 为了便于进行验证与测试，将文件夹命名改为自己的第三次实验-学号-姓名，将代码运行结果截图同样放在该文件夹下，将整个文件夹压缩成.zip文件后，进行上传。

提交链接

《密码学基础实验》第三周实验提交 截止时间：2024-12-09 08:50 提交地址：
<https://send2me.cn/bTvllGWI/T2uaSz5j8tvJTg>

请严格按照提交注意事项提交，否则进行扣分处理！！！！