文件加密解密实验说明

2022.11.5

• 实验背景：

密码学是一门研究信息保密的学科。密码学中的对称密码技术，指文件加密和解密使用相同密钥。形式化描述：给定一个密钥 key，加密操作(encrypt)将明文和密钥经过一系列运算转换成密文；解密操作(decrypt)将密文和密钥经过一系列运算转换成明文。解密操作是加密操作的逆操作。

$$\text{ciphertext} = \text{encrypt}_{key}(plaintext)\ ,\qquad \text{plaintext} = \text{decrypt}_{key}(ciphertext)$$

• 实验任务：

编写一个简单加密解密算法，密钥key是一个单字节的无符号整数。

- 对于二进制文件：加密算法，将明文的每个字节x与密钥key进行异或，得到密文字节x',即$x' = x \oplus key$；解密算法，$x = x' \oplus key$
- 对于文本文件：加密算法，将明文的每个字符 ASCII 值x在字符表中向右偏移key个，即$x' = (x + key)\%128$;不可见字符的解密算法，$x = (x' - key + 128)\%128$。这样可确保加密解密后的字符依然在 ASCII 码范围内。

• 程序框架

```
#include <stdio.h>
#include <string.h>

const char *action, *type;  //动作：-e(encrypt)/-d(decrypt);
                            //类型：-t(text)/-b(binary)
const char *input, *output; //输入输出文件名
unsigned char key;          //密钥

void text_encrypt(FILE *fpin, FILE *fpout)
{ /* put your implementation here */ }

void text_decrypt(FILE *fpin, FILE *fpout)
{ /* put your implementation here */}

void binary_encrypt(FILE *fpin, FILE *fpout)
{ /* put your implementation here */ }

void binary_encrypt(FILE *fpin, FILE *fpout)
{ /* put your implementation here */ }
```

```
int main(int argc, char *argv[])
{
    FILE *fpin, *fpout;

    if (argc != 6)
    {
        printf("Error\n");
        exit(-1);
    }

    action = argv[1];
    type = argv[2];
    input = argv[3];
    output = argv[4];
    key = atoi(argv[5]);

    fpin = fopen(input, "rb");
    fpout = fopen(output, "wb+");

    if (strcmp(type, "-t") == 0)
    {
        if (strcmp(action, "-e") == 0)
            text_encrypt(fpin, fpout);
        else if (strcmp(action, "-d") == 0)
            text_decrypt(fpin, fpout);
    }
    else if (strcmp(type, "-b") == 0)
    {
        if (strcmp(action, "-e") == 0)
            binary_encrypt(fpin, fpout);
        else if (strcmp(action, "-d") == 0)
            binary_decrypt(fpin, fpout);
    }

    fclose(fpin);
    fclose(fpout);

    return 0;
}
```

- **相关命令**

  编译：gcc -o cryptography cryptograph.c

运行：

- 文本文件加密：./cryptography -e -t plain.txt cipher.txt 128
- 文本文件解密：./cryptography -d -t cipher.txt plain.txt 128
- 二进制文件加密：./cryptography -e -b plain.bin cipher.bin 128
- 二进制文件解密：./cryptography -d -b cipher.bin plain.bin 128

cryptography 是编译出来的可执行程序名字。命令行参数 argv[1]代表 action(-e 是 encrypt，-d 是 decrypt)，argv[2]代表 type(-b 是 binary，-t 是 text)，argv[3]代表输入文件名，argv[4]代表输出文件名，argv[5]代表密钥。程序中的 argc 为程序接收到的命令行参数个数。