测试点2-1

密码学是什么？其研究工作分为哪两个方向？

密码学是在研究“有敌手存在环境中隐密地传递信息” 这一核心问题中发展起 来的一门科学，包含编码学（加密）和破译学（破解）两个研究方向。

密码学发展经历了那几个阶段？每个阶段的特点是什么？

古代加密方法 古典密码 近代密码 现代密码

古代加密方式：

源于对自然的直接感受， 加密思想简单直观，技巧性强， 安全性依赖方法本身保密性 依赖于实物，不便传输， 仍有一定的安全性

古典密码：

基于替换和置换的思想，能有针对性设计算法， 安全性不仅依赖于算法的保密，数学理论已经被引入了密码设置， 安全性有所提高

近代密码：

密码体制设计的基本原则已经被提出，密码的实现技术从手工迈入了机械电气时代，数学理论开始介入密码分析

现代密码，常见密码算法及应用特点

公开密钥密码体制：加解密密钥不同； 加解密速度慢； 应用： ➢ 可用于认证； 常见算法： RSA，ECC，ElGamal...

Hash算法：任意长输入映射为定长输出； 输入变化，输出发生不可预测 的变化； 输出无法推导出输入。 应用： 完整性校验； 常见算法：SHA-1，MD5，

依据密码体制的定义，给出对凯撒密码体制的明文空间、密文空间、 加密方法、解密方法、密钥空间的描述。

凯撒密码体制：

$$c = f(m,k) = m + kmod26$$
$$m = f^{-1}(c,k) = c - kmod26$$

明文空间:M，所有要加密的明文

密文空间：C，被加密后的密文

加密方法：c=$f(m, k) = m + k\ mod\ 26$

解密方法：m=f^{-1}(c, k) = $c - k \ mod \ 26$

密钥空间：K

对称加密和公钥加密在密钥使用上存在差异，试考虑这样的场景：如 果有一个单位有N名员工，员工间的网络通信需要保密，采用对称加密 需要分配多少个密钥？采用公钥加密需要多少个密钥？

$$N * (N - 1)/2$$

依据凯撒密码体制的工作原理，编制一个可以实现对英文语句进行加 解密转换的C语言程序。（实验一）

```
#include<stdio.h>
#include<string.h>
#include<stdlib.h>
#include<time.h>
#define MAX 101

char ciphertext[MAX];    //密文数组
char plaintext[MAX];     //明文数组
int key;    //密钥

//生成key的函数
int keyGen(){
    srand((int)time(0));    //调用time头文件生成随机数
    return rand()%25+1;     //规定随机数的生成范围 ，凯撒加密算法位移密钥key的区间在(1,25)
}
//加密函数
void Encryption()
{
    printf("please input plaintext: ");
    gets(plaintext);
    printf("ciphertext: ");
    for(int i=0;plaintext[i]!='\0';i++){
        if(plaintext[i]>='A'&&plaintext[i]<='Z'){   //如果当前字符是大写，就和‘A’比较
           ciphertext[i]=(plaintext[i]-'A'+key)%26+'A';
        }
        else if(plaintext[i]>='a'&&plaintext[i]<='z'){  //如果当前字符是小写，就和‘a’比较
            ciphertext[i]=(plaintext[i]-'a'+key)%26+'a';
        }
        else
            ciphertext[i]=plaintext[i]+key;     //非大小写，直接位移
```

```
        printf("%c",ciphertext[i]);      //输出当前字符
    }
    printf("\n");
}

//解密函数
void Decryption()
{
    printf("please input ciphertext: ");
    gets(ciphertext);
    int len=strlen(ciphertext);
    printf("plaintext: ");
    for(int i=0;i<len;i++)
    {
        if(ciphertext[i]>='A'&&ciphertext[i]<='Z'){      //如果当前字符是
大写，就和‘A’比较
           plaintext[i] = ((ciphertext[i]-'A'-key)%26+26)%26 +'A';
        }
        else if(ciphertext[i]>='a'&&ciphertext[i]<='z'){     //如果当前
字符是小写，就和‘a’比较
            plaintext[i]=((ciphertext[i]-'a'-key)%26+26)%26+'a';
        }
        else
            plaintext[i]=ciphertext[i]+key;      //非大小写，直接位移
        printf("%c",plaintext[i]);  //输出当前字符
    }
    printf("\n");
}

int main()
{
    int n,flag=1;
    key=keyGen();   //调用keyGen()函数生成随即加密密钥key
    printf("key: %d\n",key);
    while(flag){         //死循环，只有当用户手动输入才结束
        printf("please choose（1:Encryption，2:Decryption,3:exit）: ");
        scanf("%d",&n);
        getchar();
        switch(n){
        case 1:
            Encryption();   //加密
            break;
        case 2:
            Decryption();   //解密
            break;
        case 3:exit(0);      //退出
        }
    }
}
```

测试点2-2

物理安全包括那些方面？解决物理安全的技术途径有哪些？

方面：设备安全 环境安全 人员安全

解决途径：提供防护措施 提高可靠性 隔绝危险

手机是当前社会环境下重要的个人信息设备，为保护手机的物理安全，谈谈你是如 何做的？

1.防锁防毁报警装置

2.设置手机密码

3.增加手机定位，以便丢失也可以找到

4.锁定装置

某单位对机房环境有严格的安全要求，在机房墙体内设置了金属网，请问该措施的 目的是什么？除了该措施，还有哪些措施可以用于同样的目的？

防电磁泄漏，抑制电磁发射 采用低电磁辐 射的器件和电 路设计方案，干扰电磁发射 采用干扰源， 在电磁辐射中 加入干扰信号

提高系统可靠性的技术手段主要包括哪些？灾备系统往往被称为异地灾备系统，为 什么要强调“异地”？

技术手段：通常可以通过增加冗余（备份）系统的方式来实现

强调异地：隔绝威胁

使用分布式系统的主要目的是什么？在分布式系统中通常将任务进行分解，由统一 的任务调度和负载均衡机制将子任务分配到不同的主机上执行，如果一套分布式系 统包括N台主机，需要至少T台主机正常工作才能保证任务的基本执行，每台主机的 出现故障的概率为p，试问该分布式系统正常工作的概率P是多少？

采取物理隔离

$$C_N^T P^{N-T}(1-P)^T$$

测试点2-3

常见的身份认证方法有哪几种？分别列举出你具体使用过认证方 法实例?

用户所掌握的信息，如口令，

用户所拥有的特定东西，如IC卡、密钥等

用户所具有的个体特征，如笔迹、指纹、虹膜、声纹、步态等

身份认证技术是如何划分的？手机网银支付的认证属于哪一类认 证技术，需要提供哪些认证凭据?

根据认证条件（凭据）的数目 单因子认证、双因子认证、多因子认证

根据认证条件（凭据）的状态 – 静态认证、动态认证

单因子认证，静态认证，提供登录网络银行的支付密码

有人说“刷脸认证”是最安全的认证方式，你认为这种说法是否 正确？为什么？（提示：可以“图像对抗攻击”为关键词进行查 询）

不正确，攻击者可以到去用户的脸部特征或者使用图像对抗攻击中的碰撞攻击，尝试人脸特征的主要提取点模仿人脸指纹，达到盗取使用人脸信息的目的

测试点2-4

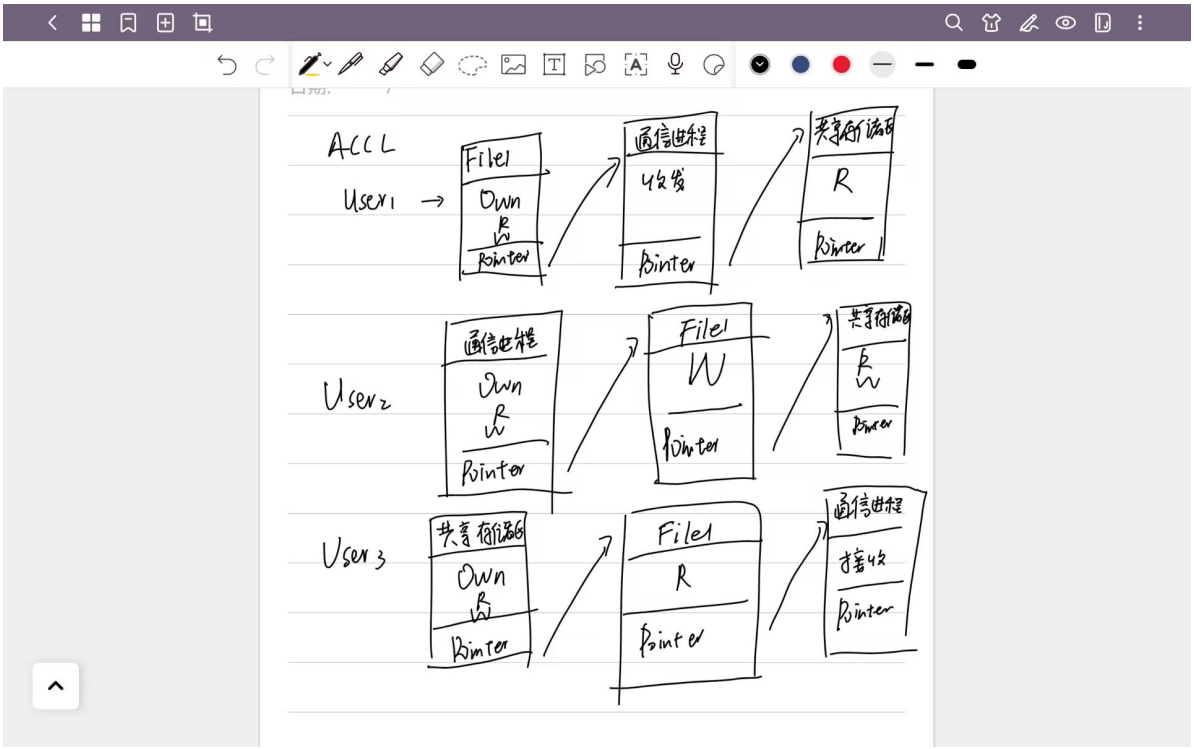
ACL和ACCL各自有什么优缺点？请举例进行说明。

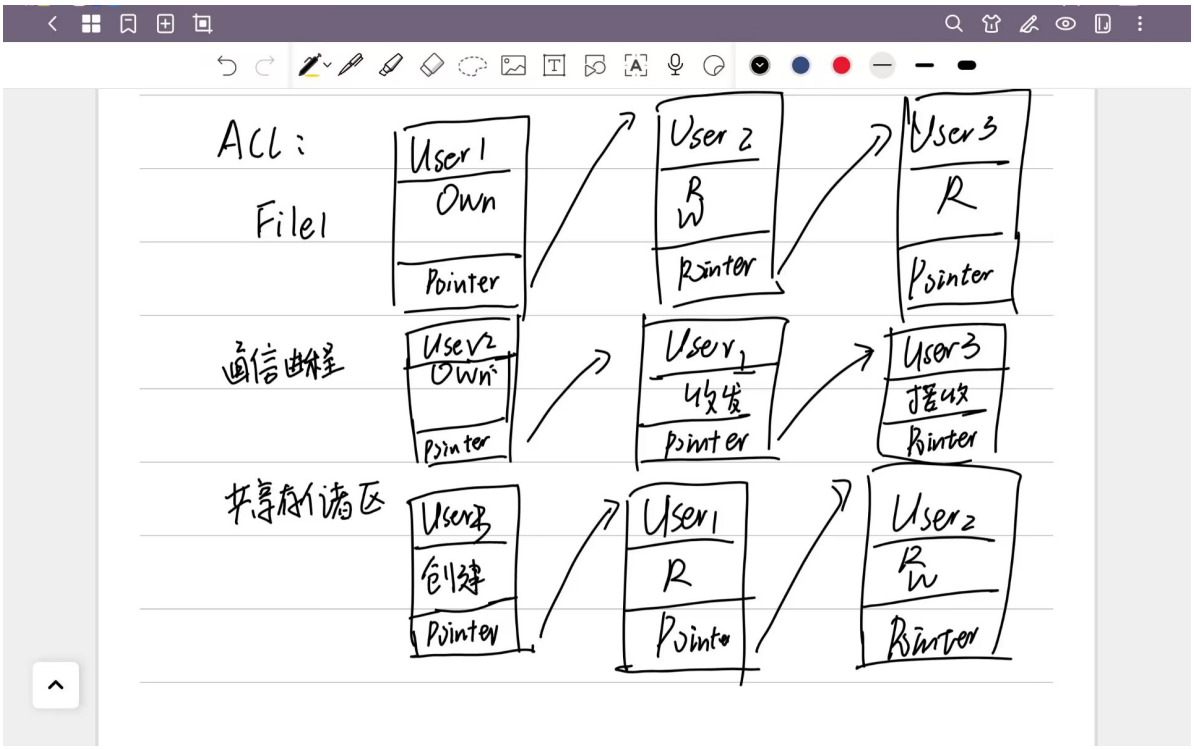
ACL 权限回收容易 权限传递困难 系统需要区分的用户相对较少， 并且这些用户大都比较稳定。

ACCL 权限传递简单 权限回收复杂 适用于分布式系统，用户量大 且不稳定；

举例：ACL：成绩管理系统 ACCL：银行

系统中有三个用户Usr1，Usr2和Usr3， Usr1创建了日志文件 File1，允许Usr2向文件中写入操作记录，允许Usr3打开文件查看 Usr2的操作记录；Usr2创建了一个通信进程，该通信进程允许 Usr1收发消息，但只允许Usr3接收消息；Usr3创建了一个共享存 储区，允许Usr1读存储区内容，Usr2读写存储区内容。根据上述 描述，画出对应的ACL和ACCL。





能否使用ACL或ACCL机制来实现基于角色的访问控制？如果不能，你能否给出实现RBAC的技术思路?

不能，RBAC：每个角色的权限为MngAC={权限1，权限2...}

在Windows操作系统中建立一个文件，并对文件的访问权限进行 管理，判断Windows操作系统采用的访问控制模型，说明自己的 判断理由。

ACL，这个访问控制模型是对文件的访问权限进行管理。