击了携带病毒的链接或程序，在输入登录密码时被黑客窃取密码等，这些都可能给信息系统的安全带来严重的威胁。

个人操作不当所引发的软硬件问题，也会对信息系统的安全产生威胁。例如，系统管理员误删除信息系统中的重要文件，修改影响系统运行的参数，或者没有按照规定要求的方法正确维护信息系统等，频繁开关信息系统的相关设备以及不正确使用这些设备，导致其被毁坏，都会引发信息系统安全问题。

4.1.2 信息系统安全防范

针对上面的信息系统安全风险，往往可以从身份认证、设置防火墙、数据备份、数据加密等方面进行安全防范，以确保信息系统的正常运行。

身份认证

情境4：人脸识别技术在火车站的应用

2016年，北京西站在部分通道启用自助验证验票系统（图4.1.6），旅客持车票和身份证，通过人脸识别系统确认后，可以快速进站候车。

2018年，广州、武汉、深圳等火车站启用了人脸识别验票闸机，实现“刷脸进站”。同时，广州南站还启用了人脸识别系统，通过对人像数据的采集，实现甄别违法犯罪嫌疑人、有效寻找走失人员的功能。



图4.1.6 人脸识别的自助验证验票系统

身份认证是保护信息系统安全的第一道防线，用来防止未授权的用户私自访问系统。身份认证主要有以下三种方式。

第一种是“用户名+密码”的方式。这是最常见的，也是最原始、最不安全的方式，很容易由于用户无意间泄露或者遭受口令猜测、撞库等恶意攻击，导致合法用户的身份被伪造。

第二种是使用用户拥有的唯一信物，如银行卡、信用卡、登录网上银行使用的U盾（图4.1.7）、网络支付时的数字证书等，由合法用户随身携带，随时进行身份验证。



图4.1.7 U盾

扫描全能王
3亿人都在用的扫描App



图4.1.8　面部特征的获取

第三种是利用用户自身具备的、独一无二的特征，如人脸、指纹、声音、虹膜、掌纹等生物特征的方式。

以人脸识别为例，系统先利用人脸识别系统采集用户的面部特征进行数字化，把数字代码组合成特征模板存储在数据库中。当用户登录系统时，人脸识别系统会将获取的面部特征（图4.1.8）与数据库中存储的人脸特征数据进行比对，然后根据比对的结果判断用户的身份是否合法。合法用户可以成功登录系统，不合法的用户会遭到拒绝。其具体流程如图4.1.9所示。

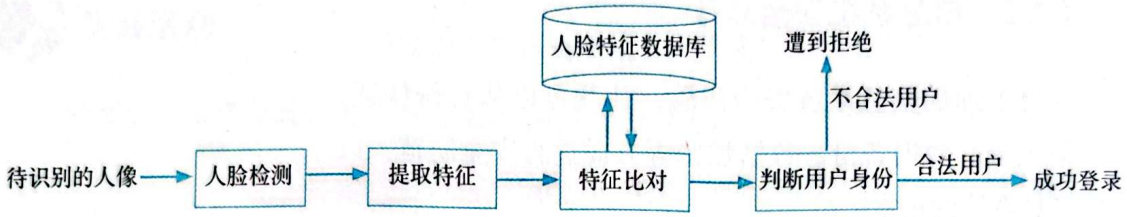


图4.1.9　人脸识别流程

思考活动

人脸识别

目前，一些智能手机具备人脸解锁功能。但是，有双胞胎成功地骗过了识别系统：双胞胎中的一人在手机中录入脸部信息，另一人并未录入脸部信息，结果未录入者成功地解锁了录入者的手机。应该如何改进系统，才能改善这一情况呢？有人说，指纹、虹膜、掌纹等基于纹理特征的识别方式，可以更容易区分双胞胎。查找资料，讨论这种说法是否有相关研究数据的支持。

某大学在学生宿舍安装了人脸识别门禁系统。这个系统具有三种识别模式：第一种是刷校园卡后进行人脸识别；第二种是喊名字后进行人脸识别，机器可以对26种方言进行语言识别；第三种是输入校园卡密码后四位，再比对人脸。这种门禁系统为什么采用多种识别模式？这样做的好处是什么呢？

设置防火墙

防火墙是设置在内部网络和外部网络（如互联网）之间维护安全的系统设施，其简图如图4.1.10所示。

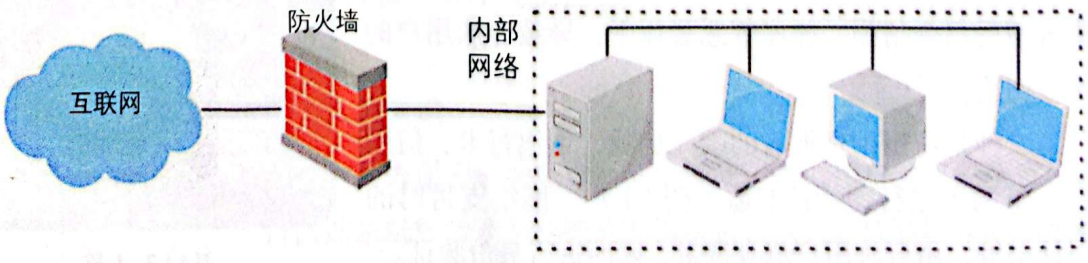


图4.1.10　防火墙

CS 扫描全能王
3亿人都在用的扫描App

防火墙具有以下基本功能：过滤进出网络的数据；管理进出网络的访问行为；封堵某些禁止的业务；记录通过防火墙的信息内容和活动；遇到网络攻击时，及时显示警告信息。

防火墙可以由软件构成，也可以由硬件构成。企业一般以硬件防火墙为主，通过软件防火墙监测。家庭和个人则一般安装软件防火墙。

随着技术的发展，新一代的防火墙集病毒扫描、入侵检测和网络监视功能于一身，可以在网关处对病毒进行初次拦截，并配合病毒库中的上亿条记录，将绝大多数病毒彻底剿灭在内部网络之外，在有效阻挡恶意攻击的同时，大大降低病毒侵袭所带来的各种威胁。

阅读拓展

病毒库

病毒库是一个数据库，记录着计算机病毒的各种“相貌特征”，以便防火墙和杀毒软件能够及时发现、清除病毒，所以有时也把病毒库里的数据称为“病毒特征码”。由于计算机病毒层出不穷，所以病毒库要时常更新，这样才能保护计算机不被最新的病毒侵害。

数据备份

数据是信息系统的核心和关键所在。一旦遭遇自然或者人为的威胁造成数据丢失，会给信息系统带来难以估量的损失。如果提前对系统数据进行备份，可以使系统尽快地恢复工作。

根据实际情况的需要，对信息系统的备份可以分为三种类型：完全备份，针对系统中某一个时间点的数据完整地进行备份；增量备份，首先建立一个基准备份文件，以后每次备份，仅备份相对于上一次备份发生变化的内容；差异备份，首先建立一个完全备份，以后的每次备份均与上一次完全备份的数据内容进行比较，然后备份发生变化的数据内容。

为了避免本地数据的丢失和损毁，确保信息系统在遭受破坏后能迅速恢复原来的正常工作，异地备份是一种有效方法。目前，我国很多地区都成立了数据容灾备份中心，把数字化城市管理、市民卡工程、房产信息管理系统等信息化建设的重要数据库接入数据容灾备份中心，从而实现异地备份（图4.1.11）。

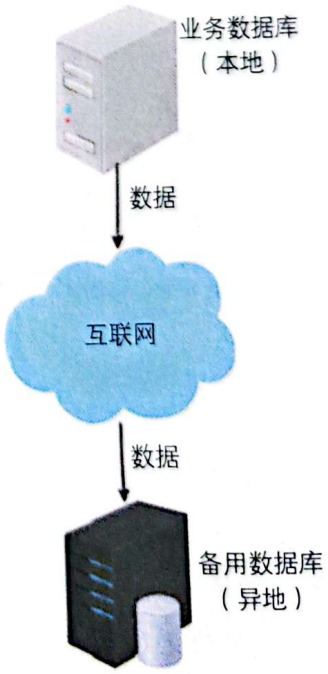


图4.1.11　异地备份

扫描全能王
3亿人都在用的扫描App

数据加密

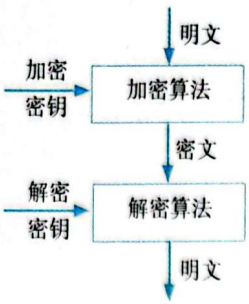


图4.1.12　数据加密和解密

为防止信息系统中的数据被破坏，可以采用数据加密技术，把被保护的信息转换为密文，然后再进行存储或者传输。

数据加密是通过加密算法和加密密钥将明文转变为密文，保护数据在传输过程中不被非法窃取，而解密则是通过解密算法和解密密钥将密文恢复为明文（图4.1.12）。明文是指没有加密的文字或字符串；密文是指经过某个加密算法后，明文转变成另外一些文字。将密文通过与加密算法对应的解密算法进行解密，才能恢复出明文。

数据加密的历史由来已久。例如，凯撒加密是一种较简单且广为人知的加密方法，其明文中的所有字母都在字母表中向后（或向前）按照一个固定数目进行偏移后被替换成密文。在战争时期，为了防止敌对一方破获消息，即便信息技术很不发达，人们还是想到了通过电报传送消息时采用替代密码、换位密码等加密方法，保证情报的安全性。

现在常用的数据加密算法有私钥加密和公钥加密。私钥加密算法用于加密和解密的密钥是相同的，因此也称为对称密钥加密，密钥需要保密管理。公钥加密算法用于加密消息的加密密钥和用于解密消息的解密密钥不同，因此也称为非对称密钥加密。图4.1.13描述了使用公钥加密算法进行加密及解密操作的过程。

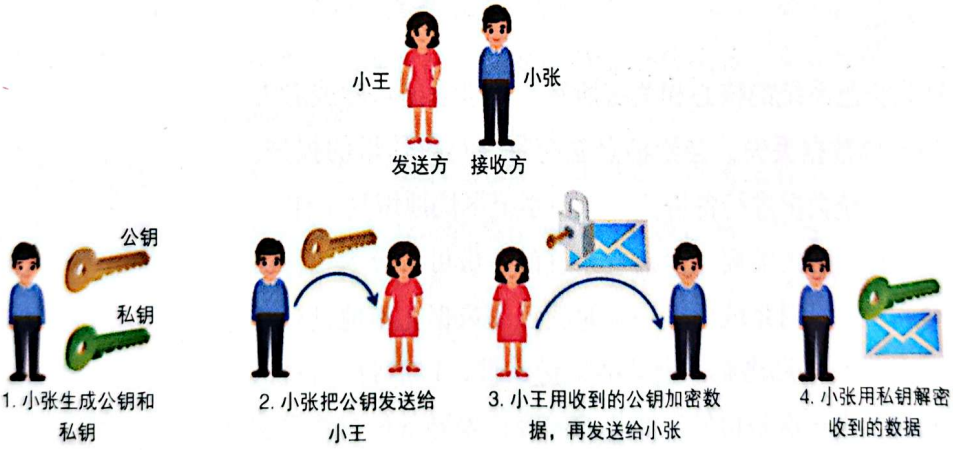


图4.1.13　公钥加密算法的加密和解密过程

RSA算法是1977年由罗恩·李维斯特（Ron Rivest）、阿迪·萨莫尔（Adi Shamir）和伦纳德·阿德曼（Leonard Adleman）联合提出的。

RSA算法是在信息安全领域广泛使用的一种公钥加密算法，其公钥和私钥的生成需要事先给出两个不同的大素数p、q，然后通过一系列数学运算产生出两个相互关联的数对(n, e)和(n, d)，其中$n=p\times q$。RSA算法背后所依赖的安全原理其实很简单：将两个大素数p、q相乘，产生一个更大的数n的过程比较容易，但反过来，先给出数n，再去求p和q就非常难了。

扫描全能王
3亿人都在用的扫描App

实践活动

用 Python 实现 RSA 公钥加密和解密算法

1. 了解利用RSA算法生成公钥、私钥，公钥加密和私钥解密的程序代码。

（1）接收方生成公钥的程序代码。

```
from sympy.crypto.crypto import rsa_public_key
    p,q,e=3,5,7  #p、q是两个不同的素数，d与e模(p-1)(q-1)互逆，即de = 1 (mod
(p-1)(q-1))
    rsa_public_key(p,q,e)
    (15,7)
    rsa_public_key(p,q,30)
    False
#返回RSA公钥对(n,e)，n是两个素数的乘积。若与任何假定相冲突，则返回False
```

（2）接收方生成私钥的程序代码。

```
from sympy.crypto.crypto import rsa_private_key
    p,q,e=3,5,7
    rsa_private_key(p,q,e)
    (15,7)
    rsa_private_key(p,q,30)
    False
#返回RSA私钥对(n,d)，n是两个素数的乘积。若与任何假定相冲突，则返回False
```

（3）发送方使用公钥对明文进行加密的程序代码。

```
from sympy.crypto.crypto import encipher_rsa, rsa_public_key
    p,q,e=3,5,7    #准备公钥，选取p、q两个不同素数
    puk=rsa_public_key(p,q,e)    #生成公钥puk
    msg=12                       #待加密的明文消息
    encipher_rsa(msg,puk)        #使用公钥puk对明文进行加密
```

（4）接收方使用私钥对密文进行解密的程序代码。

```
from sympy.crypto.crypto import decipher_rsa, rsa_private_key
    p,q,e=3,5,7
    prk=rsa_private_key(p,q,e)  #生成私钥prk
    msg=38                      #待解密的密文消息
    decipher_rsa(msg,prk)       #使用私钥prk对密文进行解密
```

2. 启动Python编程软件，利用上述程序代码编写实现RSA公钥加密和解密算法的程序，并调试程序直到实现这一算法。

实践活动

数字签名和数字水印认证技术

为了防止不法分子对信息系统的攻击，目前数字签名、数字水印等认证技术也开始用来对数据进行加密。数字签名就是使用公钥加密等算法，生成别人无法伪造的一段数字串。数字水印是将特定的标记隐藏在数字照片、电子文档等数字产品中，用来保护作者对产品的所有权，防止数字产品被非法复制、传播和篡改。

尝试下载数字签名软件或数字水印软件，加密自己的文档或图片。

扫描全能王
3亿人都在用的扫描App