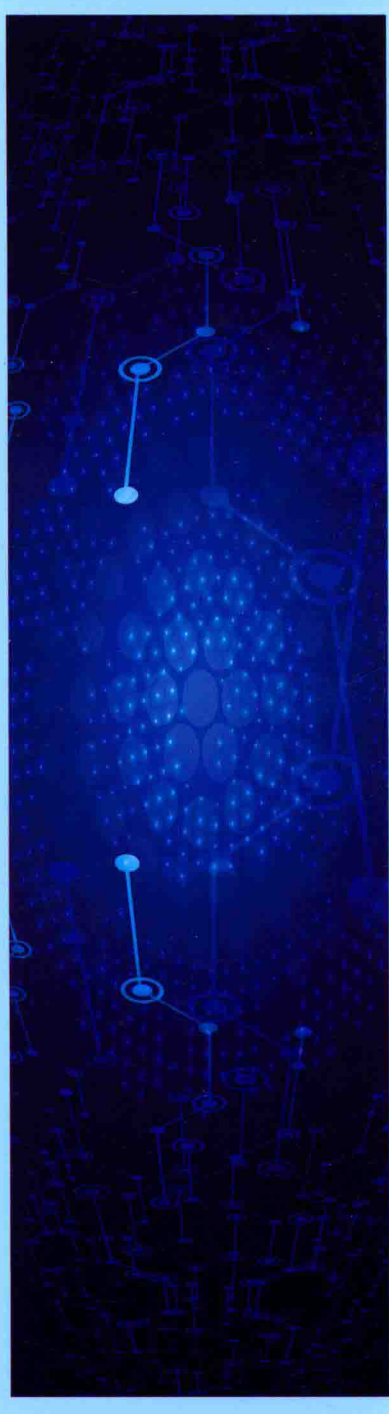
“东北林业大学优秀教材及学术专著
出版与奖励专项资金”资助出版

信息安全技术与应用

（第二版）

XINXI ANQUAN JISHU YU YINGYONG

主　编　张　健　程　媛　邱兆文
副主编　霍　达　陈楠楠



東北林業大學出版社
Northeast Forestry University Press

东北林业大学优秀教材及学术专著
出版与奖励专项资金”资助出版

信息安全技术与应用
（第二版）

主　编　张　健　程　媛　邱兆文
副主编　霍　达　陈楠楠

東北林業大學出版社
Northeast Forestry University Press
·哈尔滨·

图书在版编目（CIP）数据

信息安全技术与应用／张健，程媛，邱兆文主编．—2版．—哈尔滨：东北林业大学出版社，2018.8

（东北林业大学优秀教材系列丛书）

ISBN 978-7-5674-1512-6

Ⅰ.①信… Ⅱ.①张…②程…③邱… Ⅲ.①信息安全-高等学校-教材 Ⅳ.①G203

中国版本图书馆CIP数据核字（2018）第198664号

责任编辑：潘　琦

责任校对：任兴华

封面设计：乔鑫鑫

出版发行：东北林业大学出版社（哈尔滨市香坊区哈平六道街6号　邮编：150040）

印　　装：哈尔滨市石桥印务有限公司

规　　格：185 mm×260 mm　16开

印　　张：9.75

字　　数：231千字

版　　次：2018年8月第2版

印　　次：2018年8月第1次印刷

定　　价：25.00元

前　言

随着通信和计算机技术的快速发展以及经济全球化应用的推动，互联网表现出了极大的使用方便性和信息传递的快捷性，这使得人们对信息网络的依赖程度越来越高。人们在传递信息的同时，信息的安全性自然也成为人们所关心的重要问题。信息安全作为国家的重大战略，其意义不言而喻。信息安全也包括每个人信息的安全。

作者根据多年教学经验和科研经验，在学习和总结国内外相关文献的基础上，完成了本书的撰写工作。本书将从信息安全概述、古典密码技术、密码学的数学基础、分组加密技术、公钥密码技术、序列密码技术、数字签名、密钥管理、操作系统安全技术、计算机病毒与木马、入侵检测技术等方面对信息安全技术与应用进行讲解。本书的特色是使用通俗易懂的语言，对信息安全技术中的基本原理和技术进行准确阐述，并配合适当的例题进行深入研究，包括各种密码体制以及信息安全在日常中的诸多应用安全技术。该书可以作为高等学校计算机、通信工程、信息安全等专业的本科生和硕士生教材；同时也可以供从事相关领域的研究人员及工程技术人员参考使用。

全书共分为11章。霍达编写第1，2章，程媛编写第3，4章，张健编写第5，6，9章并负责全书的统编工作，邱兆文编写第7，8章，陈楠楠编写第10，11章。

在本书出版之际，要特别感谢参考文献中所列的各位作者，是他们的独到见解为本书提供了宝贵的资料及丰富的写作源泉。限于作者的水平和学识，书中难免存在疏漏和错误之处，诚望读者不吝赐教。

最后，谨向每一位关心和支持本书编写工作的各方面人士表示感谢！

作　者

2017年10月

目　录

1 信息安全概述

随着计算机网络的不断发展，全球信息化已成为人类发展的大趋势。但由于计算机网络具有联结形式多样性、终端分布不均匀性和网络开放性、互连性等特征，致使网络易受黑客、怪客、恶意软件和其他攻击，所以网络上信息的安全和保密是至关重要的问题。

1.1 信息安全与网络安全

信息安全是指信息网络的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续、可靠、正常地运行，信息服务不中断。信息安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。

计算机网络最重要的功能是向用户提供信息服务及其所拥有的信息资源，网络安全从其本质上来讲是指网络上信息的安全，可将网络信息分为静态信息和动态信息。静态信息为存储于网络节点上的信息资源；同时我们将传播于网络节点间的信息，称为动态信息。国际标准化组织（ISO）将“计算机安全”定义为“数据处理系统建立和采取的技术和管理的安全保护，保护计算机硬件、软件数据不因偶然和恶意的原因而遭到破坏、更改和泄露”，此概念偏重于对静态信息的保护。此外“计算机安全”亦被定义为“计算机的硬件、软件和数据受到保护，不因偶然和恶意的原因而遭到破坏、更改和泄露，系统连续正常运行”，该定义着重于动态信息的描述。网络安全本质上是信息安全的引申，网络安全是对网络信息保密性、完整性、可用性及真实性的保护。其本质是在信息的安全期内保证信息在网络上流动时或者静态存放时不被非授权用户非法访问，但授权用户可以访问。

网络必须有足够强的安全措施，否则网络将会变得无用，甚至会变为危及国家安全的网络。无论是在局域网还是在广域网中，都存在着自然和人为等诸多因素的脆弱性和潜在威胁。故此，网络的安全措施应是能全方位地应对各种不同的威胁和脆弱性，这样才能确保网络信息的保密性、完整性和可用性。

网络上的信息安全，涉及的领域很广。网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不因为偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续、可靠、正常地运行，网络服务不中断。网络安全包括以下含义：网络运行系统安全；网络上系统信息的安全；网络上信息传播的安全，即信息传播后果的安全；网络上信息内容的安全。

网络安全具有五个要素。

（1）可用性：授权实体有权访问数据。

（2）机密性：信息不暴露给未授权实体或进程。
（3）完整性：保证数据不被未授权修改。
（4）可控性：控制授权范围内的信息流及操作方式。
（5）可审查性：对出现的安全问题提供依据与手段。
网络安全的内容主要包括以下内容：
（1）物理安全；
（2）网络安全；
（3）传输安全；
（4）应用安全；
（5）用户安全。

1.2　网络面临的安全威胁

网络设计之初是为了方便信息的交流与开放，实现网络资源数据的共享，而对于保障信息安全方面的规划则非常有限。伴随着计算机与通信技术的迅速发展，由于各种原因，网络面临着各式各样的安全威胁，诸如灾害（火灾、雷击、地震等）、网络结构的缺陷、一些恶意攻击（窃密、重放、篡改等）以及软件漏洞等。这些威胁导致网络固有的优越性、开放性和互联性变成了信息安全性隐患的便利渠道。确保网络安全的目的是将计算机系统中的服务与资源的任何弱点降到最低限度，即是将计算机系统的脆弱性降低到最低程度。网络安全问题计算机与网络的脆弱性紧密相关，其脆弱性体现在以下几点。

1.2.1　软件的脆弱性

随着软件规模的不断扩大，各种系统软件、应用软件也变得越来越复杂，只要有软件，就有可能存在漏洞，例如从 Windows 98 到 Windows XP、Windows 7、Windows 8 各种版本的操作系统都有存在于操作系统脚本引擎中的安全漏洞，这些漏洞能让黑客利用电子邮件或者恶意网站控制受害者的机器。此外，除了 Windows 操作系统以外，其余的如 Linux、UNIX 等各个版本的操作系统也或多或少地存在一些安全漏洞。虽然设计者不断地发现并公布新的漏洞，但是在修改了已有的漏洞之后又将会出现新的漏洞。软件的漏洞有两类：一类是有意制造的漏洞，另一类是无意制造的漏洞。有意制造的漏洞是指设计者为日后控制系统或窃取信息而故意设计的漏洞，包括各种后门、逻辑炸弹。例如当年风靡电脑界的“江民逻辑炸弹”，该逻辑炸弹在特定条件下对计算机实施破坏，其结果与某些计算机病毒的破坏作用相似，可以造成电脑软硬盘都无法启动。ASP 源码问题是 IIS 服务的设计者留下的一个后门，任何人都可以使用浏览器从网络上方便地调出 ASP 程序的源码，从而收集系统信息，进而对系统进行攻击。无意制造的漏洞是指系统设计者由于疏忽或其他技术原因而留下的漏洞。比如，使用 C 语言的字符串复制函数，因未做合法性检查而导致缓冲区溢出。总之，这些漏洞成为黑客攻击的便利途径，所以我们要及时给系统和应用程序打上最新的补丁，及时更新软件。

1.2.2 协议安全的脆弱性

计算机的运行及网络的互联，都是在各种通信协议的基础上进行的，但是因特网设计的初衷是为了计算机之间交换信息和数据共享，缺乏对安全性的整体构想和设计，协议的开放性、复杂性，以及协议在设计时缺乏认证机制和加密机制，这些使得网络安全存在着先天性的不足。当前计算机系统使用的 FTP、E-MAIL、NFS 以及互联网赖以生存的 TCP/IP 协议等都包含着许多影响网络安全的因素及漏洞。例如，IP 欺骗就是利用了 TCP/IP 网络协议的脆弱性。

1.2.3 数据库管理系统安全的脆弱性

数据库主要应用于客户/服务器（Client/Server，简称 C/S）平台。在服务端，数据库由其上的数据库管理系统（DBMS）进行管理。由于 C/S 结构允许服务器有多个客户端，各个终端对于数据的共享要求非常强烈，这就涉及数据库的安全性与可靠性问题。当前大量的信息都存储在各种各样的数据库中，然而在数据库系统安全方面考虑却很少，有时数据库管理系统的安全与操作系统的安全不配套，这就导致了数据库不安全性因素的存在，对数据库构成的威胁主要有对数据的破坏、泄露和修改等。

1.2.4 人为的因素

人为的无意失误，如操作员安全配置不当造成的安全漏洞，用户安全意识不强，用户口令选择不慎，用户将自己的账号随意转借他人或与别人共享等都会给网络安全带来威胁。

人为的恶意攻击，这是计算机网络所面临的最大威胁，攻击者的攻击和计算机犯罪就属于这一类。此类攻击又可以分为以下两种：一种是主动攻击，它以各种方式有选择地破坏信息的有效性和完整性；另一种是被动攻击，它是在不影响网络正常工作的情况下，进行截获、窃取、破译以获得重要机密信息。这两种攻击均可对计算机网络造成极大的危害，并导致机密数据的泄漏。

主要攻击及威胁手段包括以下方面。

（1）DoS（Denial of Service）。使目标系统或网络无法提供正常服务。DoS，也就是“拒绝服务”的意思。最基本的 DoS 攻击就是利用合理的服务请求来占用过多的服务资源，从而使合法用户无法得到服务。基本过程：首先攻击者向服务器发送众多的带有虚假地址的请求，服务器发送回复信息后等待回传信息，由于地址是伪造的，所以服务器一直等不到回传的消息，分配给这次请求的资源就始终没有被释放。在这种反复发送伪地址请求的情况下，服务器资源最终会被耗尽。

（2）扫描探测。系统弱点探察。

（3）口令攻击。弱口令。

（4）获取权限、提升权限。猜/crack root 口令、缓冲区溢出、利用 NT 注册表、访问和利用高权限控制台、利用启动文件、利用系统或应用 Bugs。

（5）插入恶意代码。病毒、特洛伊木马（BO）、后门、恶意 Applet。

（6）网络破坏。主页篡改、文件删除、毁坏 OS、格式化磁盘。

（7）数据窃取。敏感数据复制、监听敏感数据传输——共享媒介/服务器监听/远程监听 RMON。

（8）伪造、浪费与滥用资源。

（9）篡改审计数据。删除、修改、权限改变、使审计进程失效。

（10）安全基础攻击。防火墙、路由、账号、文件权限修改。

1.3　密码学在网络信息安全中的作用

在现实世界中，安全是一个相当简单的概念。例如，房子门窗上要安装足够坚固的抗变形材料以阻止窃贼的闯入；安装报警器是阻止入侵者破门而入的进一步措施；当有人想从他人的银行账号上骗取钱款时，出纳员会要求其出示相关身份证明也是为了保证存款的安全；签署商业合同时，需要双方在合同上签名以产生法律效力，也是为了保证合同的实施安全。

在数字世界中，安全以类似的方式工作。机密性就像大门上的锁，它可以阻止非法者闯入用户的文件夹读取用户的敏感数据或盗取钱财。数据完整性提供了一种当某些内容被修改时，可以使用户得知的机制，相当于报警器。这些思想是密码技术在保护信息安全方面所起作用的具体体现。

密码是一门古老的技术，但自密码技术诞生直至第二次世界大战结束，对于公众而言，密码技术始终处于一种未知的保密状态，常与军事、机要、间谍等工作联系在一起，让人在感到神秘之余，又有几分畏惧。信息技术的迅速发展改变了这一切，随着计算机和通信技术的迅猛发展，大量的敏感信息常通过公共通信设施或计算机网络进行交换，特别是 Internet 的广泛应用、电子商务和电子政务的迅速发展，越来越多的个人信息需要严格保密，如银行账号、个人隐私等。正是这种对信息的机密性和真实性的需求，密码学才逐渐揭去了神秘的面纱，走进公众的日常生活中。

密码技术是实现网络信息安全的核心技术，是保护数据最重要的工具之一。通过加密变换，将可读的文件变换成不可理解的乱码，从而起到保护信息和数据的作用，它直接支持机密性、完整性和非否认性。

今天，在计算机被广泛应用的信息时代，由于计算机网络技术的迅速发展，大量信息以数字形式存放在计算机系统里，信息的传输则通过公共信道。这些计算机系统和公共信道在不设防的情况下是很脆弱的，容易受到攻击和破坏，信息的失窃不容易被发现，而后果可能是极其严重的。如何保护信息的安全成为许多人感兴趣的话题，作为网络安全基础理论之一的密码学引起人们的极大关注，吸引着越来越多的科技人员投入到密码学领域的研究之中。

密码学尽管在网络信息安全方面具有举足轻重的作用，但密码学绝不是确保网络信息安全的唯一工具，它也不能解决所有的安全问题。同时，密码编码与密码分析是一对矛和盾的关系，它们在发展中始终处于一种动态的平衡。

2 古典密码技术

古典密码是密码学发展的一个阶段，也是近代密码学产生的渊源。尽管古典密码比较简单，用手工或者简单机械就可实现加密、解密过程，但研究古典密码的原理，有助于理解、构造和分析近代密码。在计算机出现前，密码学由基于字符的密码算法构成，主要用于字符之间互相代替或互相换位，好的密码算法通常结合这两种方法使用。虽然现在密码算法相对复杂，但基本原理是一致的。重要的变化是古典密码对字母进行变换，而现代密码是对比特流进行变换，实际上这只是字母表长度上的改变，从 26 个元素变为 2 个元素，加密的本质与古典密码是相同的，即代替密码和换位密码。

2.1 代替密码

代替密码，就是明文中的字母由其他字母、数字或符号所取代的一种方法，具体的代替方案称为密钥。代替密码分为单表代替密码和多表代替密码。

2.1.1 单表代替密码——恺撒密码

密码的使用最早可以追溯到古罗马时期，《高卢战记》有描述恺撒曾经使用密码来传递信息，即所谓的“恺撒密码”。它是一种替代密码，通过将字母按顺序推后 3 位起到加密作用，如将字母 A 换作字母 D，将字母 B 换作字母 E。因据说恺撒是率先使用加密函的古代将领之一，因此这种加密方法被称为恺撒密码。

在军事通信上，必须考虑要传送的秘密信息在传送的途中被除发信者和收信者以外的第三者（特别是敌人）截获的可能性，使载送信息的载体（如文本、无线电被等）即使在被截获的情况下也不会让截获者得知其中信息内容的通信方法或技术，称为保密通信。密码通信就是保密通信的一种形式，它是把表达信息的意思明确的文字符号，用通信双方事先所约定的变换规则，变换为另一串莫名其妙的符号，以此作为通信的文本发送给收信者，当这样的文本传送到收信者手中时，收信者一时也不能识别其中所代表的意思，这时就要根据事先约定的变换规则，把它恢复成原来的意思明确的文字，然后阅读。这样，如果这个文本在通信途中被第三者截获，由于第三者一般不知道变换规则，因此他就不能得知在这一串符号背后所隐藏的信息。当然，为了战争的目的，他会千方百计地努力弄到这个变换规则，并对已经截获的密文进行分析，有时结合从其他途径获得的有关信息，试图找出这个变换规则。

现在已经无法弄清恺撒密码在当时有多大的效果，但是有理由相信它是安全的。因为恺撒的大部分敌人都是目不识丁的，而其余的则可能将这些消息当作是某个未知的外语。

即使有某个敌人获取了恺撒的加密信息，根据现有的记载，当时也没有任何技术能够解决这一最基本、最简单的替换密码。现存最早的破解方法记载于9世纪阿拉伯的阿尔·肯迪的有关发现频率分析的著作中。

恺撒密码是自己选的一个单词，例如，选用 mountain，写出以下的字母序列：mountaibcdefghjklpqrsvwxyz。就是在正常字母序列中抽掉你的密码 mountain。由于 mountain 中有两个 n，把第二个 n 去掉。

然后，把正常字母序列写在这个序列下面。

密文字母序：m o u n t a i b c d e f g h j k l p q r s v w x y z……

明文字母序：a b c d e f g h i j k l m n o p q r s t u v w x y z……

在加密的时候，用上面那个序列里的字母代替原文中的字母写成密文。例如，m 代替 a，o 代替 b。解密时方向相反。所以，加密 heishere 的结果是 btcqbkpt。

恺撒密码是单表代替密码的经典算法。设明文为 x、密文为 y、加密变换是 e、解密变换是 d。26 个字母中 a 用数字 0 代替，z 用数字 25 代替，不区分大小写，那么恺撒密码可以表示为

加密：$y=e(x)=(x+3) \bmod 26$

解密：$x=d(y)=(y+26-3) \bmod 26$

【例 2-1】明文为 China，用恺撒密码求密文。

China 中的 5 个字母分别对应的数字为 2，7，8，13，0，所以

$y(1)=e(x)=(x+3) \bmod 26=(2+3) \bmod 26=5$；$y(2)=10$；$y(3)=11$；$y(4)=16$；$y(5)=3$

根据求得的数字分别对应的字母，即密文为 fklqd。

恺撒密码中，一个字母加密后对应的字母通常不会改变，如果经常使用，很容易被破译，所以可以通过修改密钥值来增加安全性，即用密钥 k 来代替 3，使其作为一个变化的密钥。这种变化称为通用恺撒密码。

加密：$y=e(x)=(x+k) \bmod 26$

解密：$x=d(y)=(y+26-k) \bmod 26$

单表代替密码的缺点是密钥较小，不能抵抗穷尽搜索攻击，即便密钥值是变化的，最大值也只为26。同时，单表代替密码也不能抵抗频率分析的攻击。所谓频率分析即指根据英文单词中字母出现的频率来确定明文。字母频率表如表 2-1 所示，频率图如图 2-1 所示。

表 2-1　字母频率表

字母	概率	字母	概率	字母	概率	字母	概率
a	0.082	h	0.061	o	0.075	v	0.010
b	0.015	i	0.070	p	0.019	w	0.023
c	0.028	j	0.002	q	0.001	x	0.001
d	0.043	k	0.008	r	0.060	y	0.020
e	0.127	l	0.040	s	0.063	z	0.001
f	0.022	m	0.024	t	0.091		
g	0.020	n	0.067	u	0.028		

从表 2-1 中可以得出以下规律。

高频字母：e，t，a，o，n，i，r，s，h。

中频字母：d，l，u，c，m。

低频字母：p，f，y，w，g，b，y，v。

稀频字母：k，j，q，x，z。

如果在大量的密文中，出现某个字母的次数最多，那么它的明文极有可能是字母 e。

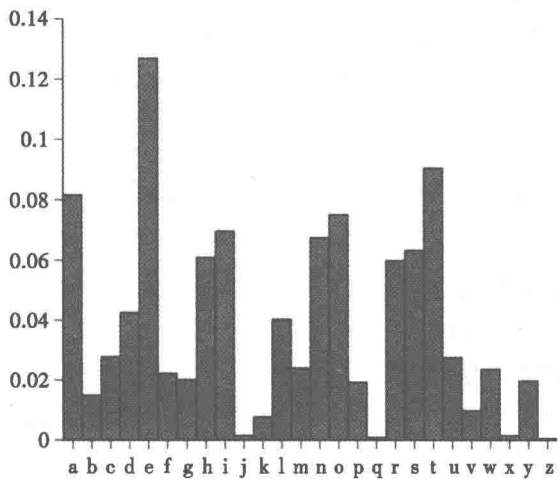


图 2-1 字母频率图

2.1.2 多表代替密码

2.1.2.1 Playfair 密码

Playfair 密码是多表代替密码的经典算法。Playfair 密码出现于 1854 年，是由 Charles Wheatstone 发明的，它将明文中的双字母组合作为一个单元对待，并将这些单元转换为密文双字母组合。具体的加密方法如下所述。

（1）构造矩阵。Playfair 密码基于一个 5×5 字母矩阵，该矩阵使用一个关键词（密钥）来构造，其构造方法是，从左至右、从上至下依次填入关键词的字母（去除重复的字母），然后再以字母表顺序依次填入其他字母。字母 I 和 J 被作为一个字母使用（即 J 被当作 I 处理）。

（2）明文分组。明文分组将明文字符串按两个字母一组进行分组。分组之后，如果相邻两个字母相同，则要在它们之间插入一个字符（事先约定的字母，如 Q）；如果明文字母个数为奇数时，同样要在明文的末端添加某个事先约定的字母作为填充。

（3）加密方法。对每一对明文字母 P_1、P_2的加密方法如下。

① 若 P_1、P_2在同一行时，则对应的密文 C_1和 C_2分别是紧靠 P_1、P_2右端的字母。其中第一列被看作是最后一列的右方（解密时反向）。

② 若 P_1、P_2在同一列时，则对应的密文 C_1和 C_2分别是紧靠 P_1、P_2下方的字母。其中第一行看作是最后一行的下方（解密时反向）。

③ 若 P_1、P_2不在同一行也不在同一列时，则 C_1和 C_2是由 P_1和 P_2所确定的矩形的其他两角的字母，并且 C_1和 P_1、C_2和 P_2在同行（解密时处理方法相同）。

【例 2-2】明文为 very good，密钥为 fivestar，用 Playfair 密码求密文。

解：（1）构造矩阵。

$$\begin{bmatrix} a & b & c & d & e \\ f & g & h & i & k \\ l & m & n & o & p \\ q & r & s & t & u \\ v & w & x & y & z \end{bmatrix} \xrightarrow{fivestar} \begin{bmatrix} f & i & v & e & s \\ t & a & r & b & c \\ d & g & h & k & l \\ m & n & o & p & q \\ u & w & x & y & z \end{bmatrix}$$

（2）分组。

明文：very good；

ve　ry　go　qo　dq。

（3）加密。

ve：同行，所以密文为 es。

ry：对角线，所以密文为 bx。

go：对角线，所以密文为 hn。

qo：同行，所以密文为 mp。

dq：对角线，所以密文为 lm。

即密文为 es bx hn mp lm。

【例 2-3】明文为 information security，密钥为 fivestar，用 Playfair 密码求密文。

解：（1）构造矩阵。

$$\begin{bmatrix} a & b & c & d & e \\ f & g & h & i & k \\ l & m & n & o & p \\ q & r & s & t & u \\ v & w & x & y & z \end{bmatrix} \xrightarrow{fivestar} \begin{bmatrix} f & i & v & e & s \\ t & a & r & b & c \\ d & g & h & k & l \\ m & n & o & p & q \\ u & w & x & y & z \end{bmatrix}$$

（2）分组。

明文：in fo rm at io ns ec ur it yq

ve　ry　go　qo　dq

（3）加密。

in：同列，所以密文为 aw。

fo：对角线，所以密文为 vm。

rm：对角线，所以密文为 to。

at：同行，所以密文为 ra。

io：对角线，所以密文为 vn。

ns：对角线，所以密文为 qi。

ec：对角线，所以密文为 sb。

ur：对角线，所以密文为 st。

it：对角线，所以密文为 fa。

yq：对角线，所以密文为 zp。

即密文为 aw vm to ra vn qi sb st fa zp。

【例 2-4】密文为 very good，密钥为 fivestar，用 Playfair 密码求明文。

解：（1）构造矩阵。

$$\begin{bmatrix} a & b & c & d & e \\ f & g & h & i & k \\ l & m & n & o & p \\ q & r & s & t & u \\ v & w & x & y & z \end{bmatrix} \xrightarrow{fivestar} \begin{bmatrix} f & i & v & e & s \\ t & a & r & b & c \\ d & g & h & k & l \\ m & n & o & p & q \\ u & w & x & y & z \end{bmatrix}$$

（2）分组。

密文：very good

ve ry go od

（3）解密。

ve：同行，所以明文为 iv。

ry：对角线，所以明文为 bx。

go：对角线，所以明文为 hn。

od：对角线，所以明文为 mh。

即明文为 iv bx hn mh。

在解密时，需要根据对单词的识别来判断明文的真实含义，如果解密的明文里含有预先约定的字母 Q（q），需要人工去判断是否为真实的明文，这也是 Playfair 密码的缺点之一。

2.1.2.2 Vernam 密码

美国电话电报公司的 Gilbert Vernam 在 1917 年为电报通信设计了一种简单方便的密码，即 Vernam 密码。其加密原理是将明文和密钥分别变换为二进制字符流，然后将明文流和密文流对位进行异或处理得到密文。

【例 2-5】明文 $P=01100001$，密钥 $K=01001110$，用 Vernam 密码求密文。

密文 $C=P\oplus K$，即

$$\begin{array}{r} 01100001 \\ \oplus\ 01001110 \\ \hline 00101111 \end{array}$$

密文为 00101111。

解密 Vernam 密码用公式 $P=C\oplus K$ 即可实现。

2.1.2.3 Hill 密码

Hill 密码是 1929 年由 Lester S. Hill 发明的，它实际上就是利用了我们熟知的线性变换方法，是在 Z_{26} 上进行的。Hill 密码的基本思想是将 n 个明文字母通过线性变换转化为 n 个密文字母，解密时只需做一次逆变换即可，密钥就是变换矩阵。

设：明文 $m=(m_1+m_2, \cdots, m_n) \in Z_{26}^n$，密文 $c=(c_1, c_2, \cdots, c_n) \in Z_{26}^n$，密钥为

Z_{26}上的 $n\times n$ 阶可逆方阵 $\boldsymbol{K}=(k_{ij})_{n\times n}$，则

加密：密文 $c=m\boldsymbol{K}\bmod 26$；

解密：明文 $m=c\boldsymbol{K}^{-1}\bmod 26$。

具体过程如下所述。

（1）假设要加密的明文是由 26 个字母组成的。

（2）将每个字符与 0 ~ 25 中的某一个数字一一对应起来（例如：$a/A-0$，$b/B-1$，……，$z/Z-25$）。

（3）选择一个加密矩阵 $\boldsymbol{A}_{n\times n}$，其中矩阵 $\boldsymbol{A}$ 必须是可逆矩阵，例如 $\boldsymbol{A}=\begin{bmatrix}7&1&1&5&5\\0&23&18&7&5\\1&10&6&9&2\\16&9&23&21&0\\21&13&7&22&15\end{bmatrix}$。

（4）将明文字母分别依照次序每 n 个一组（如果最后一组不足 n 个，就将其补成 n 个），依照字符与数字的对应关系得到明文矩阵 $\text{ming}_{len/n\times n}$。

（5）通过加密矩阵 $\boldsymbol{A}$，利用矩阵乘法得到密文矩阵 $\text{mi}_{len/n\times n}=\text{ming}_{len/n\times n}\times\boldsymbol{A}_{n\times n}\bmod 26$。

（6）将密文矩阵的数字与字符对应起来，得到密文。

（7）解密时利用加密矩阵的逆矩阵 $\boldsymbol{A}^{-1}$和密文，可得到明文。

例如：随机产生一个 5 阶加密方阵 $\boldsymbol{A}=\begin{bmatrix}7&1&1&5&5\\0&23&18&7&5\\1&10&6&9&2\\16&9&23&21&0\\21&13&7&22&15\end{bmatrix}$，得到方阵 $\boldsymbol{A}$ 的逆矩阵 $\boldsymbol{A}^{-1}=\begin{bmatrix}7&18&4&21&10\\23&7&24&18&1\\12&9&3&20&19\\15&18&23&25&12\\12&4&13&13&9\end{bmatrix}$。

①加密过程。

输入明文：Hill cipher is one of my favorite cipher。

分组：Hillc ipher isone ofmyf avori tecip her（aa）。

加密得到密文：sksxaqerqqydvdgbknvsmwzatgiapdojbio。

②解密过程。

输入密文：sksxaqerqqydvdgbknvsmwzatgiapdojbio。

解密得到密文：hillcipherisoneofmyfavoritecipheraa。

2.2 换位密码

换位就是重新排列消息中的字母，以便打破密文的结构特性，即它交换的不再是字符本身，而是字符被书写的位置。换位分为列换位和周期换位。

2.2.1 列换位

列换位的处理方法，是将明文按照密钥个数排列，并按照密钥在字母表中的顺序变换列的顺序，最后按照列的顺序写出密文。

【例 2-6】明文为 cryptography is an applied science，密钥是 creny，求密文。

根据密钥 creny 中各字母在英文字母表中的出现次序可确定为 14235。将明文按照密钥的长度用 5 列逐行列出，如表 2-2 所示。

表 2-2 列换位

1	4	2	3	5
c	r	y	p	t
o	g	r	a	p
h	y	i	s	a
n	a	p	p	l
i	e	d	s	c
i	e	n	c	e

然后依照密钥决定的次序按列依次读出，因此密文为 cohnii yripdn paspsc rgyaee tpalce。

如果明文不是密钥的整数倍数，那么也需要用其他字母代替，但需要事先进行约定。

2.2.2 周期换位

周期换位的处理方法，是将明文按照密钥个数分组，并按照密钥在字母表中的顺序变换组内字母的顺序，得到密文。

【例 2-7】明文为 can you understand，密钥是 fork，求密文。

根据密钥 fork 中各字母在英文字母表中的出现次序可确定为 1342。将明文按照密钥的顺序可以得到密文，如表 2-3 所示。

表 2-3 周期换位

密钥顺序	1342	1342	1342	1342
分组	cany	ouun	ders	tand
密文	cyan	onuu	dser	tdan