21世纪 高等学校信息安全专业规划教材

# 计算机安全与保密

李辉 编著

清华大学出版社

21世纪高等学校信息安全专业规划教材

# 计算机安全与保密

李　辉　编著

清华大学出版社
北京

## 内 容 简 介

信息安全是计算机、通信及相关专业的一个新兴热点。本书以作者十多年的教学经验为基础，结合计算机专业的特点，汇集了许多学生感兴趣的主题，力图浅显易懂、循序渐进，并重视实例和应用，重视点和面的结合。

为便于安排教学，本书的内容一共分为10章。第1章介绍一些常见的古典密码系统算法；第2章介绍包括DES、AES在内的对称密码系统和国内教材很少提及的加密与解密模式；第3～5章介绍公钥密码系统，其中，第3章的公钥密码系统基于大数因式分解问题，第4章的公钥密码系统基于离散对数问题，第5章的一些公钥密码系统则基于其他的完全NP问题；第6章介绍数字签名的原理；第7章介绍Hash函数以及基于Hash函数和对称密码算法的消息验证码技术；第8章介绍密钥管理和PKI技术；第9章以专题的形式介绍目前计算机安全应用领域的一些主流技术，包括口令安全、VPN等；第10章基于Java平台介绍密码学及安全的编程框架和技术。以上各章中，第1～7章偏重理论与原理；第8章和第9章偏重于应用；第10章偏重于编程。

本书覆盖较多的知识点，可以作为高等院校计算机系教材，同时，书中提供大量的数据实例，也可以作为教师、科研人员以及兴趣爱好者的参考书。



**图书在版编目(CIP)数据**

计算机安全与保密/李辉编著. —北京：清华大学出版社，2013.2
21世纪高等学校信息安全专业规划教材
ISBN 978-7-302-29387-3

Ⅰ. ①计… Ⅱ. ①李… Ⅲ. ①计算机安全－高等学校－教材 ②电子计算机－密码术－高等学校－教材 Ⅳ. ①TP309

中国版本图书馆CIP数据核字(2012)第158621号

**责任编辑**：魏江江　王冰飞
**封面设计**：杨　兮
**责任校对**：焦丽丽
**责任印制**：何　芊

**出版发行**：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课 件 下 载：http://www.tup.com.cn，010-62795954

**印 刷 者**：北京密云胶印厂
**装 订 者**：北京市密云县京文制本装订厂
**经　　销**：全国新华书店
**开　　本**：185mm×260mm　　**印　　张**：17.5　　**字　　数**：426千字
**版　　次**：2013年2月第1版　　**印　　次**：2013年2月第1次印刷
**印　　数**：1～3000
**定　　价**：29.50元

产品编号：040608-01

# 出版说明

由于网络应用越来越普及，信息化的社会已经呈现出越来越广阔的前景，可以肯定地说，在未来的社会中电子支付、电子银行、电子政务以及多方面的网络信息服务将深入到人类生活的方方面面。同时，随之面临的信息安全问题也日益突出，非法访问、信息窃取、甚至信息犯罪等恶意行为导致信息的严重不安全。信息安全问题已由原来的军事国防领域扩展到了整个社会，因此社会各界对信息安全人才有强烈的需求。

信息安全本科专业是2000年以来结合我国特色开设的新的本科专业，是计算机、通信、数学等领域的交叉学科，主要研究确保信息安全的科学和技术。自专业创办以来，各个高校在课程设置和教材研究上一直处于探索阶段。但各高校由于本身专业设置上来自于不同的学科，如计算机、通信和数学等，在课程设置上也没有统一的指导规范，在课程内容、深浅程度和课程衔接上，存在模糊不清、内容重叠、知识覆盖不全面等现象。因此，根据信息安全类专业知识体系所覆盖的知识点，系统地研究目前信息安全专业教学所涉及的核心技术的原理、实践及其应用，合理规划信息安全专业的核心课程，在此基础上提出适合我国信息安全专业教学和人才培养的核心课程的内容框架和知识体系，并在此基础上设计新的教学模式和教学方法，对进一步提高国内信息安全专业的教学水平和质量具有重要的意义。

为了进一步提高国内信息安全专业课程的教学水平和质量，培养适应社会经济发展需要的、兼具研究能力和工程能力的高质量专业技术人才。在教育部相关教学指导委员会专家的指导和建议下，清华大学出版社与国内多所重点大学共同对我国信息安全人才培养的课程框架和知识体系，以及实践教学内容进行了深入的研究，并在该基础上形成了“信息安全人才需求与专业知识体系、课程体系的研究”等研究报告。

本系列教材是在课程体系的研究基础上总结、完善而成，力求充分体现科学性、先进性、工程性，突出专业核心课程的教材，兼顾具有专业教学特点的相关基础课程教材，探索具有发展潜力的选修课程教材，满足高校多层次教学的需要。

本系列教材在规划过程中体现了如下一些基本组织原则和特点。

(1) 反映信息安全学科的发展和专业教育的改革，适应社会对信息安全人才的培养需求，教材内容坚持基本理论的扎实和清晰，反映基本理论和原理的综合应用，在其基础上强调工程实践环节，并及时反映教学体系的调整和教学内容的更新。

(2) 反映教学需要，促进教学发展。教材要适应多样化的教学需要，正确把握教学内容和课程体系的改革方向，在选择教材内容和编写体系时注意体现素质教育、创新能

力与实践能力的培养，为学生知识、能力、素质协调发展创造条件。

（3）实施精品战略，突出重点。规划教材建设把重点放在专业核心（基础）课程的教材建设上；特别注意选择并安排一部分原来基础比较好的优秀教材或讲义修订再版，逐步形成精品教材；提倡并鼓励编写体现工程型和应用型的专业教学内容和课程体系改革成果的教材。

（4）支持一纲多本，合理配套。专业核心课和相关基础课的教材要配套，同一门课程可以有多本具有各自内容特点的教材。处理好教材统一性与多样化，基本教材与辅助教材、教学参考书，文字教材与软件教材的关系，实现教材系列资源的配套。

（5）依靠专家，择优落实。在制定教材规划时依靠各课程专家在调查研究本课程教材建设现状的基础上提出规划选题。在落实主编人选时，要引入竞争机制，通过申报、评审确定主编。书稿完成后认真实行审稿程序，确保出书质量。

繁荣教材出版事业，提高教材质量的关键是教师。建立一支高水平的、以老带新的教材编写队伍才能保证教材的编写质量，希望有志于教材建设的教师能够加入到我们的编写队伍中来。

**21 世纪高等学校信息安全专业规划教材**

**联系人：魏江江 weijj@tup.tsinghua.edu.cn**

# 前　言

尽管从事“计算机安全与保密”课程的一线课堂教学已超过十年，但当我们重新审视这门课程的时候，仍感觉不是那么随心所欲。与“操作系统”、“数据结构”等计算机专业课程相比，“计算机安全与保密”课程总显得有些特别。

“计算机安全与保密”课程并不是自成体系，涉及许多其他的课程，如“抽象代数”、“操作系统”、“计算机网络”、“数据库理论与应用”、“信息论与编码”等，似乎很复杂、很庞大。与此形成反差的是，每年开课时总能吸引不少没有太多计算机专业基础的其他专业的同学，他们来到课堂上津津有味地旁听。

“计算机安全与保密”的基础实验之一“AES 加密”，对于计算机专业的同学来说，大多数都需要 3 天左右，这已经超过了为整个课程配的上机总时长。一些同学认为这个实验必须做，否则相关部分的课程就白上了；另一些同学则认为这个实验耗时太长，还是不做为好。

同学们对这门课的侧重点也存在较大分歧。一些同学认为应侧重于应用，如怎样攻击或防范攻击是很重要的；另一些同学却认为真正有趣的还是那些玄妙的加密、解密方案。

感兴趣的同学很多且分歧较大，造成了该课程教学中的一个困难，即难以找到一本合适的教材。从教学实践上来看，这门课理想的教材应该至少具备以下的特点：

(1) 内容编排要合理。既能使同学们在计算机安全方面提高素养和能力，又能使没有太多基础的同学保持浓厚兴趣并积极参与实践。

(2) 重视方法和思路胜过具体知识和手段。陆续有一些方案被破解或认为不那么安全，但解决安全问题的思路不会有大的变化。

(3) 理论与实践并重。

在整理了以往的讲义和学生问答后，我们决定编写本教材。受限于水平和能力，无法将教材编得这么理想，但这确实是我们不断进步的方向。

关于本教材，还要做以下说明：

(1) 为使本书尽可能地系统且全面，本书中个别部分参考了国外教材中的实例，但本书中绝大多数构造的实例来源于课堂教学或实践教学，实例中的数据也均通过编程得到。

(2) 为了帮助读者深入研究，某些重要的算法(如椭圆曲线)提供了非常大的数据实例。读者不必对这些“大数”产生恐惧或反感，因为相关部分往往还有一些小数据的

实例。而且即便是跳过这些实例，也不会影响对全书的理解。

(3)“香农理论”虽然是一个重要的理论基础，但根据同学们的建议，移到了附录 A 中。跳过“香农理论”并不影响对全书的理解。

(4) 教师可根据总课时安排教学内容。课时较多时，可逐章讲授。课时不多的情况下，可结合课时要求及侧重点选择以下的组合：

- 第 1 章→第 2 章→第 3 章→第 6 章→第 7 章→第 9 章
- 第 1 章→第 2 章→第 3 章→第 6 章→第 7 章→第 10 章
- 第 1 章→第 2 章→第 3 章→第 4 章→第 5 章→第 10 章
- 第 1 章→第 2 章→第 3 章→第 10 章
- 第 1 章→第 2 章→第 3 章→第 4 章→第 5 章
- 第 1 章→第 2 章→第 3 章→第 6 章→第 7 章
- 第 1 章→第 2 章→第 3 章

最后，感谢过去几年给这门课提出各种意见的同学们，同学们的热情和求知精神给予我们编写教材的动力。还要感谢为本教材编写提供帮助的编辑、老师和研究生。特别感谢张小韬、张瑞霞、吕宏强等几位研究生，他们的录入和校对工作对本教材的编写帮助很大。

由于本教材涉及知识面较广，难度较大，不足之处在所难免。为便于以后教材的修订，恳请专家、教师及各类读者多提宝贵意见。

编　者

2012 年 9 月

# 目　录

# 引　言

进入21世纪后，信息处理和通信业务呈现出高速增长的态势。人们的生活越来越依赖于计算机和通信，人们的工作也越来越多地借助计算机网络来进行。各类信息（如文本、多媒体）以二进制流的形式在网络上穿梭。如果不采取任何安全措施，敏感信息很容易被获取。而另一方面出于开放互联的考虑，大家又不可能也不愿意在隔离的环境里受限地使用计算机网络。

幸运的是数学、密码学理论和信息安全技术可以帮助解决计算机、网络和通信中的关键安全问题。

当人们谈及计算机安全时，会发现随着计算机的发展，有关计算机安全的事件日渐增多。例如，1939年第二次世界大战爆发期间，正在为英国国家密码机构工作的图灵成功破译了德国军方使用的著名通信密码系统“Enigma”，如图1所示；1970年，美国威斯康星大学的国防数学研究中心遭到炸弹袭击，计算机与积累了20多年的数据被炸毁；1982年，只有15岁的理查德·斯伦塔（Richard Shrenta）针对苹果Apple Ⅱ计算机编写了名为Elk Cloner的病毒，被认为是全球第一款个人计算机病毒；1996年2月，Master Card和Visa国际信用卡组织与技术合作伙伴GTE、Netscape、IBM等一批跨国公司共同开发了安全电子交易规范（SET）；1999年9月13日，我国正式发布了标准GB17859—1999“计算机信息系统安全保护等级划分准则”（Classified Criteria for Security Protection of Computer Information System）……

**图1　Enigma系统**

这些与计算机安全相关的事件，反映了计算机安全领域的主题。可以看到，计算机安全的研究内容包括计算机数据安全、计算机物理安全、计算机安全管理等，涉及的范围非常广泛。

本书在内容上不求面面俱到，主要侧重于介绍密码学基本原理和以密码学为基础的计算机系统安全；而关于计算机物理安全、计算机安全管理、计算机病毒等内容，则不在本书范围之内。

表1总结了计算机系统安全的一些重要主题。限于篇幅，标有＊号的内容在本书中并没有详细介绍，感兴趣的读者可以查阅相关文献。

密码学在计算机系统安全领域中起着举足轻重的作用。一方面，在已有的与计算机系统安全相关的各类协议和标准中，绝大多数都以密码学为基础。另一方面，仍有不少计算机系统安全的遗留问题或新的应用需求需要借助密码学寻求解决方案。

**表 1 计算机系统安全的主题**

| 主 题 | 说 明 |
|---|---|
| 隐私或保密 | 仅让授权的实体得到信息，以保持信息的机密性 |
| 数据完整性 | 保证信息不被未授权的更改 |
| 实体认证或者身份鉴别 | 实体身份验证(如人、计算机终端、信用卡等) |
| 消息认证 | 验证信息的来源，即原始数据认证 |
| 签名 | 一种把信息与实体绑定的手段 |
| 授权* | 允许实体进行操作或成为某个角色 |
| 验证 | 提供授权实体在有效时间内使用信息或资源的一种手段 |
| 访问控制* | 限制资源访问，资源只允许被授权的实体访问 |
| 证书 | 一个可信赖机构提供的证明文件 |
| 时间戳* | 记录信息生成或者存在的时间 |
| 见证* | 由创建者之外的实体证明信息的有效性 |
| 收据* | 确认信息已经收到 |
| 证实* | 确认服务已经提供 |
| 拥有* | 让实体得到合法授权的一种手段 |
| 匿名* | 在一些过程中隐藏实体的身份 |
| 不可抵赖性 | 避免否认先前的承诺或者行为 |
| 撤销* | 一般指证书或授权的取消 |

与计算机的产生相比，密码学可谓历史悠久。本书中介绍的密码算法可以追溯到古罗马时期，而密码术思想的出现甚至还要更早。

根据《高卢战记》的记载，凯撒大帝常常在情报传输中采用一种神奇的加密方法：将书信中用到的所有字母按字母表顺序推后三位，信件完成后将信件卷起，然后将厚厚的蜡滴于封口处，在蜡没干之前，再压上自己的私印。接收者收到信件以后，先检查蜡封是否完整以及蜡印是否是凯撒的印章，然后拆开信件，将信中所有字母按字母表顺序提前三位，重新生成信件内容。

在凯撒密码中，原始的信息经加密后发出，加密前的信息称为明文(Plain Text)。加密规则(Encryption Rule)是字母顺序推后三位，如用 D 替代 A、用 F 替代 C。收到的信息无法理解，因为它是经过加密的信息，称为密文(Cipher Text)。要想还原出原来的明文信息，需要套用解密规则(Decryption Rule)，解密规则与加密规则正好相反，如用 A 替代 D、用 C 替代 F。解密后重要信息跃然纸上，表 2 中经解密后的明文拉丁文意思是“高卢全境分为 3 个部分”。

**表 2 凯撒密码实例**

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 收到的信息 | R | p | q | l | d | J | d | o | o | l | d | h | v | w | G | l |
| 还原的信息 | O | m | n | i | a | G | a | l | l | i | a | e | s | t | D | i |
| 收到的信息 | y | l | v | d | l | q | S | d | u | w | h | v | w | u | h | v |
| 还原的信息 | v | i | s | a | i | n | P | a | r | t | e | s | t | r | e | s |

凯撒大帝提供的这种加密解密算法，简单而实用，被称为凯撒密码。从现代的观点来看，凯撒密码仅仅是单表代换密码系统的一个特例。

早期的密码学能够体现出一种艺术之美，但安全性不高、科学性不强。

1948 年，香农(Claude Shannon)发表了一篇具有里程碑意义的论文——“通信的数学理论”(*A Mathematical Theory of Communication*)，宣告了信息论的诞生。紧接着他又发表了一篇名为“保密系统的通信理论”(*Communication Theory of Secrecy Systems*)的论文，该论文用信息论的观点全面地论述信息保密问题，将密码学的研究从古典的朴素研究引入到科学研究的轨道上，同时香农理论也为对称密码学的构造提供了直接的理论基础。从此，密码学成为一门真正的科学。

图 2 是 Shannon 在论文中提出的通用保密系统方案，方案中已明确引入了攻击者(Enemy Cryptanalyst)的角色。

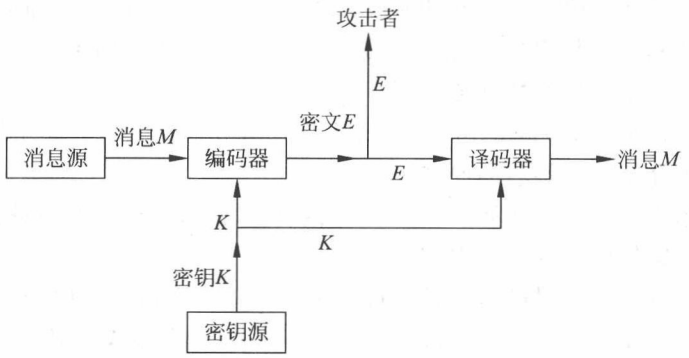


**图 2　Shannon 的通用保密系统方案**

密码学沿着对称密码体制的方向缓慢发展，直到公钥密码体制的突然出现。1976 年，Diffie 与 Hellman 合作发表了一篇经典论文“密码学的新方向”(*New Directions in Cryptography*)，提出一种可以使通信双方在不安全信道上进行的安全密钥协商协议(Diffie-Hellman 协议)，并在此基础上提出了公钥密码算法的思想和概念。这篇论文也标志着传统密码学开始向现代密码学的转变。

图 3 是 Diffie 与 Hellman 在论文中提出的公钥密码系统方案，使用两个不同的密钥分别用于加密和解密，从而不必再维护传递密钥的信道，这是密码学的一项创举。

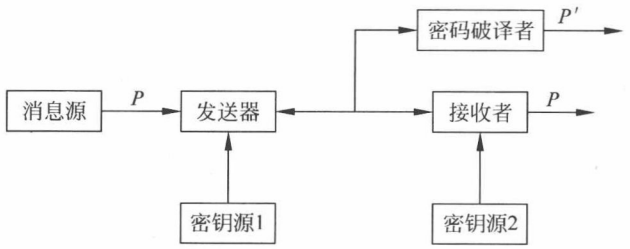


**图 3　Diffie 与 Hellman 的公钥密码系统方案**

1978 年，Rivest、Shamir 和 Adleman 基于大整数因式分解难题，提出第一种实用的公钥密码体制方案，称为 RSA 密码体制。此后，陆续有新的公钥密码体制被提出，如 1978 年提出的基于背包问题的 Merkle-Hellman 背包公钥密码体制、1985 年提出的基于离散对数难题的 ElGamal 公钥密码体制。

公钥密码体制的作用并不局限于加密解密，它的另外一个重要贡献是数字签名。1991年，第一个关于数字签名的标准(ISO/IEC 9796)应运而生。起初的标准基于RSA，但1994年后基于ElGamal的数字签名更受青睐。

随着计算机科学与技术的发展，密码学在信息安全领域也发挥出越来越重要的作用。无论是数据加密、防篡改还是身份验证，到处都能看到密码学的应用。

本书正是按照密码学发展的过程和思路，由浅入深地介绍密码学的基本理论。在此基础上，进一步介绍密码学在计算机安全中的应用。

本书的内容编排如下：

第1章 从古典密码系统开始介绍密码学的基本概念和历史上的一些经典算法。

第2章 重点讲解DES、AES等对称密码系统，以及ECB、CBC等加密解密模式。

第3章 讲解基于大数因式分解问题的RSA、Rabin公钥密码系统。

第4章 讲解基于离散对数问题的ElGamal、ECC公钥密码系统。

第5章 介绍包括Knapsack、McEliece、NTRU等在内的其他公钥密码系统。

第6章 重点介绍数字签名的原理。

第7章 介绍Hash函数以及基于Hash函数和对称密码算法的消息验证码技术。

第8章 介绍密钥的管理以及PKI技术。

第9章 以专题的形式讲解目前计算机安全的一些技术，包括口令安全、VPN等。

第10章 基于Java平台，介绍相关的密码学和安全编程框架和技术。

为了让读者掌握计算机安全和保密的相关知识和思想，在学习方法上给出以下建议：

(1) 尽可能深入地学习本书的数学基础课程：抽象代数。无论是对称密码体制的标准AES，还是众多的公钥密码体制，大多数的算法都建立在抽象代数基础之上。

(2) 要理解本书中的各种概念、结论和算法，实践必不可少。大多数情况下，本书提供了具体的例子。但即便如此，读者还应该自己更换参数，多练多算多想。

(3) 计算机专业的读者最好通过上机编程来实现书中的算法，以增强对算法的理解。由于有些算法过于复杂不易调试，读者可以参考书中一些实际算法的中间过程。

# 第1章　古典密码系统

可以将香农在1948年发表的论文“保密系统的通信理论”作为里程碑，之前的密码学统称为古典密码学。古典密码算法花样繁多，简单而有趣。

## 1.1　密码系统基本概念

在介绍古典密码算法之前，首先对各种古典密码算法进行一个简单的分类。

从加密手段分类，古典密码算法有换位(Transposition)密码和代换(Substitution)密码两种。

换位密码算法通过对明文的字母位置进行交换实现加密。

**例1.1**　helloworld→hleolrowld。

观察字母的位置变化，可以看到明文的第2个字母与明文的第3个字母交换，明文的第4个字母与明文的第5个字母交换，明文的第6个字母与明文的第8个字母进行交换。

为了便于分析，本章中对于古典密码算法中的字母都进行统一的编码。

换位密码编码规则如表1.1所示。

**表1.1　换位密码编码规则**

| 字母 | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 数字 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

本书中忽略字母的大小写，如果不忽略，将有52个编码。

按照编码规则，可以对helloworld进行编码，即(7,4,11,11,14,22,14,17,11,3)。

假设明文长度为10，那么所有长度为10的明文有$26^{10}$种，于是称这$26^{10}$种明文构成的集合形成明文空间。

经过换位后，得到的密文长度也为10，所有密文的可能性也有$26^{10}$种，于是称这$26^{10}$种密文构成的集合形成密文空间。

也可以用矩阵运算来表示换位密码的规则：

设明文$x=(7,4,11,11,14,22,14,17,11,3)$，则密文

$$y = x \cdot P_\pi$$

可见，在这个算法中，$P_\pi$是加密的关键要素，称为密钥。所有可能的密钥也构成一个集合，这个集合形成密钥空间。

接收者得到密文后，需要解密。在换位密码算法中，解密是加密的换位逆过程。具体做法是密文的第3个字母与密文的第2个字母交换；密文的第5个字母与密文的第4个字母

交换；密文的第 8 个字母与密文的第 6 个字母交换。

当然解密过程也可以通过矩阵运算来表示，即：

$$x = y \cdot P_\pi^{-1}$$

无论是哪种密码系统，一般都包含上面提到的要素。

下面给出密码系统的定义：

一个加密与解密的完整体系称为密码系统或密码体制(Crypto System)。一个密码体制由明文空间 $P$、密文空间 $C$、密钥空间 $K$、加密算法集 $E$ 和解密算法集 $D$ 组成的五元组 $(P,C,K,E,D)$构成。

(1) 明文空间 $P$：作为加密输入的原始信息 $m$ 称为明文。所有可能明文的集合称为明文空间，通常用 $P$ 表示。

(2) 密文空间 $C$：明文经加密变换后的数据 $c$ 称为密文。所有可能密文的集合称为密文空间，通常用 $C$ 表示。

(3) 密钥空间 $K$：密钥 $k$ 是参与密码变换的参数。一切可能密钥构成的集合称为密钥空间(Keyspace)，通常用 $K$ 表示。

(4) 加密算法集 $E$：任意给定密钥 $k \in K$，在加密算法集 $E$ 中存在唯一的加密算法 $e_k \in E: P \to C$，将明文 $p \in P$ 变换为密文 $c \in C$。对明文 $p$ 进行变换的过程称为加密(Encryption)。

(5) 解密算法集 $D$：任意给定密钥 $k \in K$，在加密算法集 $D$ 中存在唯一的解密算法 $d_k \in D: C \to P$，将密文 $c \in C$ 变换为明文 $p \in P$。对密文 $c$ 进行变换的过程称为解密(Decryption)。

有了数学概念后，下面重新来定义换位密码系统。

**换位密码系统**：明文空间和密文空间都是 $Z_n^m$，明文用$(x_1, x_2, \cdots, x_m)$表示，密文用$(y_1, y_2, \cdots, y_m)$表示，设密钥为 $k$，则：

加密算法：

$$(y_1, y_2, \cdots, y_m) = (x_{k(1)}, x_{k(2)}, \cdots, x_{k(m)})$$

解密算法：

$$(x_1, x_2, \cdots, x_m) = (y_{k^{-1}(1)}, y_{k^{-1}(2)}, \cdots, y_{k^{-1}(m)})$$

其中，$k^{-1}$是 $k$ 的逆。

$Z_n$ 表示集合$\{0,1,\cdots,n-1\}$。

**例 1.2** 在换位密码算法中，明文是“olympic”，求其密文。

写成编码的形式为：

$$(14,11,24,12,15,8,2)$$

设密钥为 $k$，$k$ 可以用一个换位矩阵来表示：

$$P_\pi = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

加密算法：