高等学校信息安全专业规划教材

现代密码学

罗芳　吴晓平　秦艳琳　编

WUHAN UNIVERSITY PRESS
武汉大学出版社

海军工程大学研究生教材建设基金资助

高等学校信息安全专业规划教材

现代密码学

罗芳　吴晓平　秦艳琳　编

WUHAN UNIVERSITY PRESS
武汉大学出版社

图书在版编目(CIP)数据

现代密码学/罗芳,吴晓平,秦艳琳编. —武汉:武汉大学出版社,2017.4
高等学校信息安全专业规划教材
ISBN 978-7-307-17324-8

Ⅰ.现… Ⅱ.①罗… ②吴… ③秦… Ⅲ.密码学—高等学校—教材 Ⅳ.TN918.1

中国版本图书馆 CIP 数据核字(2017)第 067178 号

责任编辑:林 莉 辛 凯 责任校对:汪欣怡 版式设计:马 佳

出版发行:**武汉大学出版社** (430072 武昌 珞珈山)
(电子邮件:cbs22@ whu. edu. cn 网址:www. wdp. com. cn)
印刷:湖北恒泰印务有限公司
开本:787×1092 1/16 印张:13.75 字数:354 千字 插页:1
版次:2017 年 4 月第 1 版 2017 年 4 月第 1 次印刷
ISBN 978-7-307-17324-8 定价:33.00 元

前 言

本书是为信息安全专业高年级本科生及密码学专业研究生编写的专业基础课教材，其选材内容的组织安排是编者参考国内外密码学相关书籍和资料，并结合多年教学实践确定的。与国内已出版的同类教材相比，本教材具有以下特点：

1. 注重理论基础，内容安排合理。本教材在内容上注重讲解最经典、最核心的密码学基础理论和方法，由浅入深，循序渐进，逻辑严密、前后呼应，通过丰富的实例和典型算法使学员快速掌握密码学的核心概念、方法和技术。

2. 广度和深度兼具。为了适应当前信息安全技术迅速发展对密码学基础理论提出的新要求，本教材在介绍经典密码理论的同时，引入了当前各类密码标准中的典型算法以及密码学研究领域中的新技术成果。同时，为了培养学生具有一定的自主研究、应用和创新能力，教材中某些较难的章节可以作为课后自学内容，以培养学生的自主思维能力。

3. 注重启发性。为使读者知其然，也知其所以然，教材内容的组织遵循从基本原理到具体算法的编写思路，首先介绍各类经典密码体制的原理，在原理指导下介绍典型算法，通过算法的学习再加深对原理的理解，改变了目前大多数教材以罗列密码算法为主，缺乏对设计原理分析的局面。

全书共分为 10 章，第 1 章介绍密码学的基本概念及密码编码的基本方法。第 2 章介绍 Shannon 信息论及其在密码学中的应用。第 3 章介绍密码学中常用的布尔函数的表示及其密码学性质。第 4 章介绍了序列密码的传统编码技术、典型分析方法以及序列密码在数字保密通信中的实际应用。第 5 章介绍了分组密码的编码原理、经典分组密码算法、轻量级分组密码算法以及分组密码的工作模式，详细给出了针对分组密码的差分及线性密码分析的原理及实例。第 6 章介绍了基于三大数学难题构造的公钥密码算法及基于身份的公钥密码体制。第 7 章介绍身份认证及消息认证。第 8 章在前两章的基础上，介绍经典的数字签名方案及特殊作用的数字签名。第 9 章围绕对称及公钥密码管理两部分内容，分别介绍了密码系统的密钥组织架构、密钥全生命周期管理、公钥基础设施，并重点介绍了密钥全生命周期管理中的密钥分配环节。第 10 章针对密码学发展的前沿对量子密码、同态加密技术、混沌密码及侧信道攻击技术进行了概述。

本书在编写过程中得到了海军工程大学研究生院同志及信息安全系领导的支持，特别是研究生院教材建设基金的资助；叶伟伟、汪亚等硕士研究生协助对部分文稿进行了核对，做了大量工作，在此一并表示感谢。

由于时间仓促，书中不足之处在所难免，希望读者不吝指正。

编 者

2016 年 9 月

目 录

第1章 绪 论

密码是按特定的规则对信息进行明、密变换的特定符号。密码学是研究确保信息机密性和真实性的技术，是信息安全的重要基础和核心技术。本章简要介绍密码学的发展历史、密码学的基本概念、密码编码的基本方法、密码分析的分类以及密钥管理。

1.1 密码学发展简史

纵观密码学发展历史，可以将其发展历程归纳为以下三个阶段：

1. 科学密码学前夜时期

从有人类社会开始，人们就有保护自己秘密信息的意愿，也就诞生了密码。4000多年前，人类创造的象形文字就是原始的密码方法。

19世纪末，无线电的发明使信息的传递突破了空间界限，但同时信息的安全性也引起了人们的极大关注，这一时期密码的主要标志是以手工操作或机械操作实现。

在1949年之前，密码技术基本上是一门技巧性很强的艺术，而不是一门真正的科学。在这一时期，密码专家常常是凭借直觉、技巧进行密码设计和分析，例如：凯撒密码、中国古代的阴符、阴书等。

在这一时期，密码学研究也基本上被政府和军事机构垄断，处于秘而不宣的状态。第一次世界大战前，密码学的重要进展很少出现在公开文献中。这一时期最有影响力的密码学文献是1918年Friedman发表的论文《重合指数及其在密码学中的而应用》，该论文给出了多表代替密码的破译方法。

2. 对称密码学的早期发展时期

从1949年到1975年，这一时期最具代表性的工作是Shannon在*Bell System Technical Journal*上发表了题为“保密系统的通信理论”(Communication theory of secrecy systems)的论文，该文为对称密码系统建立了理论模型，并应用由Shannon刚创立的信息论来研究密码系统，为密码学奠定了坚实的理论基础，使密码学发展成为了一门真正的科学。

3. 现代密码学发展时期

从1976年到1996年，这一时期密码学无论在广度还是深度上都得到了空前发展。最有影响的两个事件：一是Diffie和Hellman于1976年发表的论文《密码学的新方向》，该文引入了公钥密码的概念，为解决基于公钥的密钥交换和互不信任双方的信息认证问题提供了可能；另一重要事件是美国于1977年制定的数据加密标准DES。这两个事件标志着现代密码学的诞生。

20世纪90年代以来，特别是1997年以来，密码学得到了广泛应用，密码标准化工作和实际应用得到了各国政府、学术界和产业界的空前关注。标准化是工业社会的一个基本概念，它意味着生产规模化、成本降低、维修和更换方便，同时也便于管理。密码技术是保障

国家、国防和社会经济安全的重要技术，因此，密码技术标准的研究与制定是一个重要而永恒的研究方向。从密码发展来看，密码标准是密码理论与技术发展的结晶，也是推动密码学发展的原动力，因此，世界各国和一些国际标准化组织高度重视密码标准的研究与制定。这一时期最有影响的标准计划有：美国 1997 年启动的 NIST 计划；欧洲 2000 年启动的 NESSIE 计划；欧洲 32 所著名研究机构和企业 2004 年启动的 ECRYPT 计划；美国 2007 年启动的 SHA-3 计划等。近几年我国高度重视密码标准的研究与制定，如无线局域网密码标准、可信计算密码标准，并在实际应用中发挥了重要作用。

1.2 密码学与信息安全

信息安全问题的解决最终要依赖密码技术，因此，密码技术是无可替代的核心技术，而要理解密码学与信息安全的关系，首先需要明确信息安全面临的威胁。

1.2.1 信息安全面临的威胁

信息安全面临的威胁是指利用信息安全脆弱性的潜在危险对系统安全实施攻击，如图 1.2.1 所示，攻击可分为被动攻击和主动攻击。

1. 被动攻击

被动攻击试图了解或利用系统的信息但不影响系统资源，其目标是获得传输的信息。窃听和流量分析就是两种被动攻击。

窃听很容易理解，电话、电子邮件信息和传输的文件都可能含有敏感或秘密的信息，我们希望能阻止攻击者了解所传输的内容；另一类是业务流分析，假如我们已经有一种方法来隐蔽消息内容或其他信息的交互，例如，加密使得攻击者即使捕获了消息也不能从消息里获得信息，但即使这样，攻击者仍可能获得这些消息模式。攻击者可以确定通信主机的身份和位置，可以观察传输消息的频率和长度，可以用于判断通信的性质。

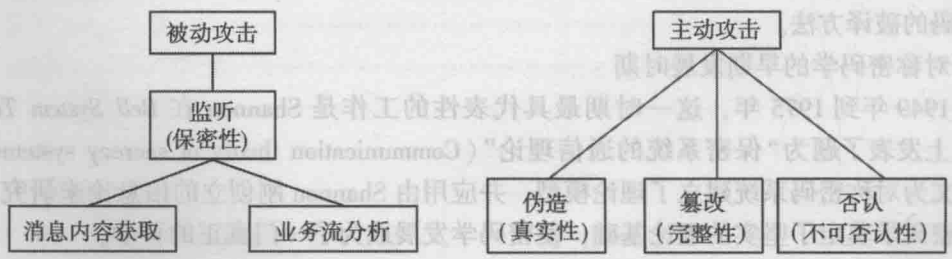

图 1.2.1 攻击类型分类

被动攻击由于不涉及对数据的篡改，所以很难察觉。典型情况是，信息流表面以一种常规方式在信源、信宿之间进行收发，收、发双发难以察觉到有第三方已经读取了信息或者观察了流量模式。但是，通过加密的手段组织这种攻击却是可行的，因此，处理被动攻击的重点是预防，而不是监测。

2. 主动攻击

主动攻击包括对数据流进行篡改或伪造数据流，具体可以分为四类：伪装、重放、篡改

和否认。

(1)伪装。

伪装是指某实体假装别的实体。伪装攻击通常还包含其他形式的主动攻击。例如，截获认证信息，并在真实的认证信息之后进行重放，从而使得没有权限的实体通过冒充有权限的实体，获得额外的权限。

(2)重放。

重放是指将获得的信息再次发送以产生非授权的效果。

(3)篡改。

篡改是指修改合法消息的一部分或延迟消息的传输或改变消息的顺序以获得非授权的效果。

(4)否认。

用户否认曾经对信息进行的生成、签发、接收等行为。

对系统的真实性进行攻击。如在网络中插入伪造或在文件中插入伪造的记录。

绝对防止主动攻击是十分困难的，因为需要随时随地通信设备和通信线路进行物理保护，因此抗击主动攻击的主要途径是检测，即以极大的概率检测出主动攻击的存在。

围绕上述威胁，信息安全需实现四个基本目标：机密性、完整性、真实性和不可否认性，这些目标的实现最终都需要借助密码技术。

信息的机密性是指信息的内容不被非授权者获取。信息加密可利用加密算法改变信息数据的原型，从而使合法用户能解密，非法用户则不能解密，通常通过分组密码及序列密码技术来实现信息的机密性。

完整性是指信息从信源发出到信宿接收整个传递过程中一旦发生篡改，信宿能以极大的概率检测出对消息的篡改攻击，通常通过 Hash 函数或 MAC(Message Authentication Code)来实现信息的完整性保护。

信息的真实性包括信源、信宿、时间的真实性及消息的完整性，可通过认证协议来实现。信息真实性认证的目的不是为了避免不真实信息的出现，而是要保证不真实的信息能以极大的概率检测出来。

当发送一个消息时，接收方能证实该消息确实是由既定的发送方发来的，称为源不可否认性；同样，当接收方收到一个消息时，发送方能够证实该消息确实已经送到了指定的接收方，称为宿不可否认性。一般通过数字签名来提供不可否认性服务。

除了以上一些主要目标外，还有匿名性和可用性等，其中，可用性指保障信息资源随时可以提供服务的能力，即授权用户根据需要可以随时访问所需信息，保证合法用户对信息资源的使用不被非法拒绝。典型的对可用性的攻击是拒绝服务攻击。

1.2.2 密码学研究内容

密码学的研究内容包括密码编码学、密码分析学及密钥管理学，其中，密钥管理学是随着密码学研究和应用领域的不断拓展而独立出来的一个分支。

1.2.2.1 密码编码学

密码编码学的主要任务是寻求产生安全性高的有效算法和协议，以满足对信息进行加密或认证的要求。

信息加密算法是密码编码学长期以来的基本研究内容。其基本思想是在一个可变参数的

控制下，对信息进行变换，使得非授权者不能由变换后的结果还原出信息。可变参数称为密钥，变换前的原始信息称为明文，变换后的数据称为密文。

具体来说，一个密码体制由明文空间 M，密文空间 C，密钥空间 K，加密算法 $E_{k_e}(m)$ 和解密算法 $D_{k_d}(c)$ 五个部分组成。如果从函数的定义出发理解密码体制的概念，则密钥空间是所有可能密钥取值的集合，明文空间和密文空间分别是加密算法的定义域和值域，也是解密算法的值域和定义域。其中，对于 $\forall m \in M$ 和 $\forall k \in k$，都有

$$\begin{cases} c = E_{k_e}(m) \\ m = D_{k_d}(c) \end{cases}$$

密码通信系统的结构如图 1.2.2 所示。

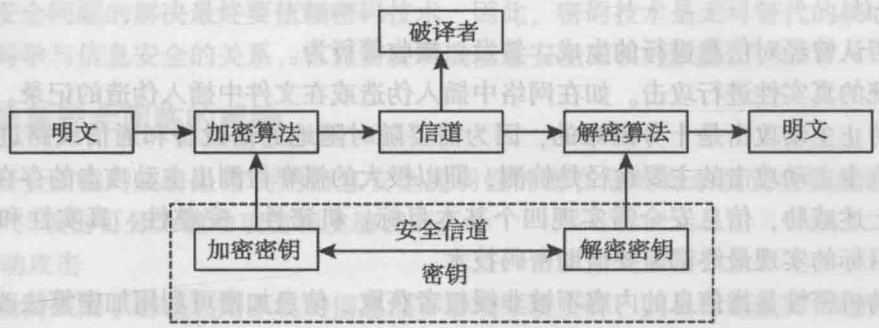

图 1.2.2　密码通信系统结构图

为达到保护信息机密性的目的，密码算法应当满足以下要求：

(1)密码算法即使达不到理论上的不可破译性，也应当是实际上不可破译的。

(2)一切秘密寓于密钥之中，只要攻击者不知道密钥，就不能由已知信息推出未知明文信息。

(3)加密算法和解密算法必须对密钥空间中所有可能值都有定义，且安全强度不够的弱密钥应尽可能少。

(4)密码体制应具有很好的实现性能，能够满足实际工作需要。

如果一个密码体制的加密密钥与解密密钥完全本质上是一个，即由其中一个可以很容易推出另外一个，则称该密码体制是单密钥密码体制。单密钥密码体制又称为对称密钥密码体制。

如果一个密码体制的加密密钥可以公开，且由加密密钥在实际上不能推出秘密的解密密钥，则称该密码体制为公开密钥密码体制，公钥密码体制、双密钥密码体制或非对称密码体制。

认证与加密是信息安全的两个不同方面，认证是防止主动攻击的重要技术。在认证系统中，信息的收、发双方共享秘密密钥，发送信息之前，发送方对信息进行适当的编码，使得接收方可以验证信息是否来自合法的信源，以及信息是否被篡改过。认证系统中的攻击者主要是指主动攻击者，他可以对信息进行两种攻击，即模仿和假冒。模仿攻击是指攻击者伪造一条消息发送给接收者，并使其相信信息的合法性；假冒攻击是指攻击者用伪造的信息假冒信源发出信息。

认证系统主要有两种模型：一种是无仲裁者的认证模型，收、发双方相互信任且利益一致，他们共享秘密密钥并共同应对攻击者；另一种是有仲裁者的认证模型，系统中有一个公平的仲裁者，收、发双方之间互不信任，但他们都信任仲裁者，有仲裁者的认证系统还需要使用数字签名、时间戳、公证等技术。无仲裁者的认证系统由信源、信宿、密钥源和攻击者组成，如图1.2.3所示。

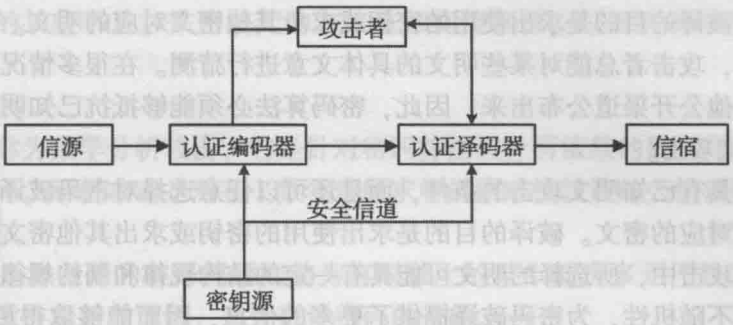

图1.2.3 认证系统模型

认证码是认证系统中最关键的部分，其构造方法是在要发送的消息中引入冗余，使得在信道中传送的消息集合大于信源发出的消息集合。

认证码由信息认证算法产生。信息认证算法就是对信息数据执行一个数学变换，变换的结果称为认证码。信息认证算法通过信息数据与认证码之间的制约关系，达到对信息数据的真实性进行认证的目的。当利用信息认证算法产生的认证码与信息数据自身携带的认证码不一致时，就可以判断该信息数据和认证码至少有一个是不真实的。

因此，信息认证算法就是高效地为信息数据产生人为的冗余，并利用这种冗余检测信息的真实性。

从安全角度看，信息认证算法应当既不能伪造一个匹配的信息数据——认证码，又不能通过对信息数据及其认证码的修改，产生一对匹配的信息数据——认证码。

信息认证算法可分为无密钥认证算法、单密钥认证算法和双密钥认证算法。无密钥认证算法和单密钥认证算法中可以没有仲裁算法。在无密钥认证算法中，由于产生认证码时不需要秘密密钥，因而任何人都可以产生每个可能的信息数据的认证码，故无密钥认证算法只能检测出对信息数据无意的修改而不能检测出有意的篡改；在单密钥认证算法中，双方利用同一个秘密密钥生成和检测认证码；双密钥认证算法的密钥由公钥和私钥两部分组成，公钥与私钥一一对应，私钥用于产生认证码，公钥用于认证码的检测和仲裁。

1.2.2.2 密码分析学

密码分析学的主要任务是破译密码或伪造认证信息，实现窃取机密信息或伪造信息以通过验证。

假设攻击者已掌握所使用的密码体制、明文及密钥的概率分布规律、所有的破译方法，如果攻击者通过某些渠道窃听或侦收到正在传递的密文信息，并视图用各种手段或方法获取密钥或明文信息，则这种攻击方法称为被动攻击。

根据攻击者所掌握信息的类别不同，可将对加密算法的攻击分为以下几类：

(1)唯密文攻击。

攻击者掌握足够多的使用同一密钥加密的密文，破译的目的是求出使用的密钥或对应的明文。由于信道未必是安全信道，因而密文在信道上被截获是很正常的。特别是当密文在无线信道中传输时，更容易从无线信号中截获密文数据。因此，唯密文攻击的条件是很容易满足的。密码算法至少应能抵抗唯密文攻击。

(2)已知明文攻击。

攻击者不仅具有唯密文攻击的条件，而且还掌握足够多的使用同一个密钥加密的密文及其对应的明文。破译的目的是求出使用的密钥或求出其他密文对应的明文。因为明文总有一定的文意和格式，攻击者总能对某些明文的具体文意进行猜测。在很多情况下，加密的明文也可能会通过其他公开渠道公布出来，因此，密码算法必须能够抵抗已知明文攻击。

(3)选择明文攻击。

攻击者不仅具有已知明文攻击的条件，而且还可以任意选择对密码破译有利的足够多的明文，并能得到对应的密文。破译的目的是求出使用的密钥或求出其他密文对应的明文。

在选择明文攻击中，所选择的明文可能具有一定的结构规律和制约规律。明文之间的这种相互制约性和不随机性，为密码破译提供了更多的信息，因而能够取得更好的破译效果。分组密码分析中，多采用已知明文攻击及选择明文攻击。

(4)选择密文攻击。

攻击者不仅具有已知明文攻击的条件，而且还可以任意选择对密码破译有利的足够多的密文，并能得到对应的明文。与选择明文攻击类似，在选择密文攻击中选择的密文也可能具有一定的结构规律和制约规律。选择密文攻击主要应用于攻击公钥密码，特别是应用于攻击数字签名算法。

(5)相关密钥攻击。

一个密钥的相关密钥是指对密码破译有利的，且与该密钥具有一定内在联系的密钥。利用这一攻击方法，攻击者不仅具有选择明文攻击和选择密文攻击的条件，而且还能得到由所求密钥的相关密钥对其他任意选择的明文加密所得的密文，以及对其他任意选择的密文解密所得的明文。

例如，设 k 是待求的密钥，P_1，P_2，…，P_n 是 n 个公开的数据，则

$$k\oplus P_1,\ k\oplus P_2,\ \cdots,\ k\oplus P_n$$

就是相关密钥，同时利用由它们加密的明文和密文发起的对密钥 k 的攻击就是一种相关密钥攻击。

从攻击手段上分，密码分析者攻击密码的主要方法有以下几种：

(1)穷举攻击。

穷举攻击是攻击密码算法最基本的方法，是对截获的密文依次用各种可能的密钥或明文去试译密文，直至得到有意义的明文，或在同一密钥下，对所有可能的明文加密，直至得到与截获的密文一致为止。前者称为密钥穷举，后者称为明文穷举。穷举攻击所需的时间代价是制约其性能的重要指标。如果密钥的总数是 2^n，则平均需要测试 2^{n-1} 个密钥就可以找到正确的密钥，显然，只要增加密钥空间中的密钥数量，就可以对抗穷举攻击。按照目前的计算能力，密钥空间为 2^{128} 的密码算法仍是安全的。

为了使穷举攻击可行，攻击者会为了减少穷举量，大体有两种方法：一种是根据已经掌握的信息或密码体制上的不足，先确定密钥的一部分结构，或从密钥总体中排除那些不可能使用的密钥，再利用穷举法去破译实际使用的密钥；另一种是将密钥空间划分为若干个可能

的子集，对密钥可能落入哪个子集自己进行判断，在确定了密钥所在子集后，再对该子集进行类似的划分，并检验实际密钥所在的子集。依次类推判断出正确密钥。

(2)统计攻击。

统计攻击就是利用明文、密文之间内在的统计规律破译密码的方法。具体可分为两类：一类是利用明文的统计规律进行破译，攻击者对截获的密文进行统计分析，总结其间的规律，并与明文的统计规律进行对照分析，从中提取明文和密文的对应或变换信息；另一类是利用密码体制上的某些不足，采用统计的方法进行优势判决，以区别实际密钥和非实际密钥。

(3)解析攻击。

解析攻击又称为数学分析攻击，它是针对密码算法设计所依赖的数学问题，利用数学求解的方法破译密码。解析攻击是对基于数学难题求解的困难性设计的公钥密码的主要威胁。

(4)代数攻击。

代数攻击就是将密码的破译问题归结为有限域上的某个低次多元代数方程组的求解问题，并通过对代数方程组的求解，达到破译密码的目的。

在一般情况下，破译一个密码，往往不是仅采用一种破译方法就可以达到破译目的，而是要综合利用各种已知条件，使用多种分析手段和方法，甚至要创立新的破译方法，达到较满意的效果。

1.2.2.3 密钥管理

密钥管理主要就是研究如何在拥有某些不安全因素的环境中，管理用户的密钥信息，使得密钥能够安全正确并有效地发挥作用，其主要研究内容包括随机数生成理论与技术、密钥分配理论与方法、密钥分散管理技术、密钥分层管理技术、秘密共享技术、密钥托管技术、密钥销毁技术、密钥协议设计与分析技术等。

密钥管理技术总是与密码的具体应用环境和实际的密码系统相联系，总是与密码应用系统的设计相联系，因此，密钥管理方案的设计与密码算法的设计同样重要。在很多情况下，一个密码应用系统被攻破往往不是密码算法的破译造成的，而是密码系统的密钥管理方案不当造成的，因此，密钥管理方案的设计与密码算法的设计同样重要。

1.3 密码体制的安全性

评价密码体制的安全性有不同的方法，包括计算安全、可证明安全及无条件安全。

1. 计算安全性

密码学更关心在计算上不可破译的密码系统。如果使用最好的算法破译一个密码体制需要至少 N 次操作，其中 N 为一个特定的非常大的数，则称该密码体制是计算上安全的。但是，目前还没有任何一个实际的密码体制被证明是计算上安全的，因为我们知道的知识破译一个密码体制当前最好的算法，也许还存在一个还没有发现的更好的攻击算法。实际上，密码体制对某一种类型的攻击(如穷举攻击)是计算上安全的，但对其他类型的攻击可能是计算上不安全的。由于计算上安全这一标准的可操作性，它又成为最适用的标准之一。

2. 可证明安全性

另一种安全性度量是把密码体制的安全性规约为某个经过深入研究的数学难题。例如如果给定的密码体制是可以破译的，那么就存在一种有效的方法解决大数的因子分解问题，而

因子分解问题目前不存在有效的解决方法，于是称该密码体制是可证明安全的。但必须注意：这种途径只是说明了安全性和另一个问题是相关的，并没有完整证明是安全的。

3. 无条件安全性

如果密码分析者具有无限的计算能力，密码体制也不能被破译，那么这个密码体制就是无条件安全的。例如，一次一密密码本对于唯密文攻击是无条件安全的，因为攻击者即使获得很多密文信息、具有无限的计算资源，仍然不能获得明文的任何信息。如果一个密码体制对于唯密文攻击是无条件安全的，我们称该密码体制具有完善保密性。

以上三种安全标准的判定中，只有无条件安全性和信息论有关，即通过信息论来证明传递过程中无信息泄露。

对加密体制，攻击的最终目标是得到明文，但是如果能得到密钥，则必然可以得到明文，加密体制的安全性从低到高主要有以下3类：

(1)完全破译。

攻击者能得到使用的密钥(对公钥系统而言是指私钥)。

(2)部分破译。

攻击者可能不需要知道密钥，而对某些密文能直接得到明文。

(3)密文区分。

攻击者能以超过1/2的概率解决以下两种不同形式描述的问题：一是给攻击者任意两个明文和其中任意明文的密文，攻击者能够判断是哪个明文对应的密文；而是给攻击者任意一个明文和该明文的密文，以及一个和密文等长的随机字符串，让攻击者判断哪个是对应的密文。

1.4 密码编码的基本方法

密码编码的基本方法主要有置换和代替。在密码发展初级阶段，它们都曾独立地作为加密算法使用，这些算法可通过手工操作或机械操作实现加、解密。虽然，现在已经极少使用，但是研究这些密码的构成原理和攻击方法对于序列密码和分组密码的设计与分析都是有益的。

1.4.1 置换密码

置换密码指对明文字符在不改变其原形的基础上，按照密钥的指示规则，对明文字符进行位置移动的密码。换言之，置换密码就是对明文字符的位置进行重新排列的一种密码。最简单的置换密码是把明文中的字母顺序倒过来，然后截成固定长度的字母组作为密文。

例1.1 明文：明晨5点发动反攻。

MING CHEN WU DIAN FA DONG FAN GONG

密文：GNOGN AFGNO DAFNA IDUWN EHCGN IM

倒序的置换密码显然是很弱的。另一种置换密码是把明文按某一顺序排成一个矩阵，然后按另一顺序选出矩阵中的字母以形成密文，最后截成固定长度的字母组作为密文。

例1.2 明文：MING CHEN WU DIAN FA DONG FAN GONG

矩阵：MINGCH 选出顺序：按列

ENWUDI