第 1 章　概　论

密码学是一门研究密码与密码活动本质和规律，以及指导密码实践的学科，主要探索密码编码和密码分析的一般规律，它是一门结合了数学、计算机科学与技术、信息与通信工程等多门学科的综合性学科。它不仅具有信息通信加密和解密功能，还具有身份认证、消息认证、数字签名等功能，是网络空间安全的核心技术。

本章主要讲述密码学的发展历史、密码学的基本概念、密码学的基本属性、密码体制分类、密码分析和密码的未来。

1.1　密码学的发展历史

密码学是一门既年轻又古老的学科，它有着悠久而奇妙的历史。其实，在人类文明发展到使用语言和文字后，就产生了保密通信和身份认证问题，于是密码学应运而生。

在几千年前，密码主要用于军事及外交领域的保密通信。这段时期的密码叫作古代密码，加密方法没有上升到理论学科的水平，研究内容也只是文字内容变换技术，但它反映了古人的高超智慧和绝妙想象力，并且蕴含着现代密码学思想，又被称为密码术或隐藏术。

1949 年香农（Shannon）发表了《保密系统的通信理论》，将信息论引入密码学，不仅为密码学的发展奠定了坚实的理论基础，而且把发展了数千年的密码术推向了科学的轨道，正式开启了密码学的大门，形成密码学这一学科。因此，在此之后出现的密码技术才能真正称为密码学。1976 年，Diffie 和 Hellman 发表的《密码学的新方向》更是密码发展的里程碑，开启了现代密码算法研究的新征程。

因此，根据时间顺序、加密原理和加密方式，可以将密码学的发展历史大致分为如下四个时期。

第一时期：古代密码时代

从远古到第一次世界大战，这期间的密码称为古代密码。这一时期可视为科学密码学的前夜时期，这一时期的密码技术可以说是一种艺术。密码学专家进行密码设计和分析通常凭借的是直觉和信念，而不是推理和证明，使用的密码体制为古典密码体制，应用的主要技巧是文字内容的代替、移位和隐藏等。现在看来，古典密码体制大多数比较简单而且容易破译。这一时期的密码主要应用于军事、政治和外交领域，信息是由信使来传递的，加密的手段是使用手工。

据史料记载，早在公元前 1046 年，为了传递保密信息，奴隶主剃光奴隶的头发，然后将信息写在奴隶的头上，等到头发重新长出来后，再让他去盟友军队传递信息。待他成功到达盟友

军队后，只需要再次剃光他的头发，就可以轻松读出信息了。典型的例子还包括古希腊的密码棒（Scytale）、凯撒密码（Caesar Cipher），我国的隐写术等。

大约在公元前 700 年，古希腊军队用一种叫作密码棒的圆木棍来进行保密通信，其使用方法是：把长带子状羊皮纸缠绕在圆木棍上，然后在上面写字；解下羊皮纸后，上面只有杂乱无章的字符，只有再次将羊皮纸以同样的方式缠绕到同样粗细的棍子上，才能看出所写的内容。

大约在公元前 100 年，古罗马的执政官和军队统帅凯撒发明了一种把所有的字母按字母表顺序循环移位的文字加密方法。例如，如果规定按字母表顺移 3 位，那么 a 就写成 D，b 写成 E，c 写成 F，……，x 写成 A，y 写成 B，z 写成 C，如 cryptography，就写成 FUBSWRJUDSKB。如果不知道加密方法，谁也不会知道这个词的意思。解密时，只需要把所有字母逆移 3 位，就能读到正确的文本了。

藏头诗是我国古代隐写术的一种具体表现形式，把要表达的真正意思或者暗语隐藏在诗句或者画卷中的固定位置，以诗句为载体，对信息进行传递。对一般读者而言，只注重诗或画的表面意境或者诗人的情感因素等内容，而较少关注隐藏在其中的“话外音”。隐写术是将信息隐藏在公开信息中，并通过公开渠道进行信息传递的一种方法，如暗语、隐形墨水等。隐写术中的信息没有经过任何处理而直接隐藏在公开信息中，一旦隐写规则被破译，那么所有的保密信息都将暴露，因此隐写术是一种简单的保护秘密的方法。

中国古代军事著作《六韬》，又称《太公六韬》或《太公兵法》，由西周的开国功臣姜望（又称吕望，俗称姜子牙）所著，其中《龙韬·阴符》篇和《龙韬·阴书》篇，讲述了君主如何在战争中与在外的将领进行保密通信。阴符共有 8 种，根据长度的不同，分别表示前线不同的军情，如长一尺，表示大获全胜，长三寸，表示战事失利、全军伤亡惨重等。阴书（书信）是将信拆分成三部分，并分派三人发出，每人拿一部分，只有将这三部分合在一起才能读懂信的内容。

第二时期：机械密码时代

两次世界大战期间加密所使用的是机械密码机，因此这一时期的密码也称为机械密码。

在第一次世界大战中，传统密码的应用达到了顶峰。1837 年，美国人莫尔斯（Morse）发明了电报。1896 年前后，意大利发明家马可尼（Marconi）和俄国物理学家波波夫（Popov）发明了无线电报，人类从此进入电子通信的时代。无线电报能快速、方便地进行远距离收发信息，很快成为军事上的主要通信手段。但是，无线电报是一种广播式通信，任何人包括敌人都能够接收发射在天空中的电报信号。为了防止机密信息的泄露，电报文件的加密变得至关重要。战争让各国充分认识到保护自己密码的安全和破译对手密码的重要性。加密主要原理是字母的替换和移位，加密和解密的手段采用了机械和手工操作，破译则使用简单的词频分析，以及基于经验与想象的试探方法。

随着科学和工业的飞速发展，在第二次世界大战中，密码学的发展远远超过了之前的任何时期。参战各国已经认识到密码是决定战争胜负的关键，纷纷研制和采用先进的密码设备，建立最严密的密码安全体系。越来越多的数学家不断加入密码研究队伍，大量的数学和统计学知

识被应用于密码分析，加密原理从传统的单表替换发展到复杂度大大提高的多表替换，基于机械和电气原理的加密和解密装置全面取代以往的手工密码，人类从此进入机械密码时代。例如，德国军队全面使用恩尼格玛（Engima）“隐迷”密码机，英国在第二次世界大战期间发明并使用 Typex 打字密码机，法国军队广泛使用哈格林（Hagelin）密码机，日本使用红色（Red）和紫色（Purple）密码机。第二次世界大战的密码斗争是敌我双方最优秀的科学大脑和最先进的科技之间的较量，其所依据的加密原理仍然是字母的替换和移位，只是更加复杂，加密和解密的手段采用了先进的机械和电气设备，传递的方法采用了莫尔斯电报，破解原理基于字母和单词的频率分析。对于复杂的多表古典密码加密方法，利用密文的重合指数方法与密文中字母统计规律相结合，同样可以破译。

第三时期：信息密码时代

第二次世界大战时期的密码学经历了一场前所未有革命，这场革命几乎颠覆了古典密码中所有的理论和方法，从而迎来了机械密码时代。然而曾经如此辉煌的机械密码时代，在第二次世界大战结束后不久就终结了。因为从 1946 年世界上第一台电子计算机诞生后，计算机技术突飞猛进，在具有超强计算能力的计算机面前，所有的机械密码都显得不堪一击。

1948 年，美国数学家香农发表了具有深远影响的论文——《通讯的数学原理》（*The Mathematical Theory of Communication*），创立了信息论。众所周知，所有的文本、图像、音频、视频信息都能够转换成数字形式，从而可以用功能强大的计算机来处理。电子通信技术也在计算机的支持下迅猛发展，继电话和电报后，又出现了计算机通信网络，这种通信网络很快就遍布世界，从而把整个世界连在一起，人类开始进入信息时代。信息时代要保证计算机通信网络和数据传递的安全，这是密码学的新任务。1949 年，香农发表的《保密系统的通信理论》（*Communication Theory of Secrecy System*）为密码系统建立了理论基础，是密码发展史上的第一次飞跃，使密码技术由艺术变成了科学，人类从此进入信息密码时代。

20 世纪 70 年代中期之前的密码研究工作基本都是由军队、外交部门、保密部门等秘密进行的。20 世纪 70 年代中期，伴随着计算机网络的普及和发展，密码开始向人类几乎所有的社会活动领域渗透，甚至开始进入普通民众的日常生活。

1973 年，美国国家标准局（National Bureau of Standards，NBS）开始征集联邦数据加密标准，很多公司积极参与并提交建议，最终 IBM 公司的 Lucifer 加密算法获得胜利。随后，经过长达两年之久的公开讨论，NBS 于 1977 年 1 月 15 日决定正式采用该算法，并将其更名为数据加密标准（Data Encryption Standard，DES）。然而，随着计算机硬件的发展及计算能力的提高，DES 已经显得不再安全。1997 年 7 月 22 日，电子前沿基金会（Electronic Frontier Foundation，EFF）使用一台价值 25 万美元的计算机在 56 小时内破译了 56 位 DES。

1977 年，美国国家标准学会（American National Standards Institute，ANSI）发起征集高级加密标准（Advanced Encryption Standard，AES）活动。经过 3 年多的遴选和讨论，比利时密码学专家 Joan Daemen 和 Vincent Rijmen 提交的 Rijndael 算法脱颖而出。2000 年，美国国家标准与技术研究院（NIST）宣布将 Rijndael 作为新的 AES。

由于计算机的出现、信息论的产生和计算机通信网络的发展，密码学经历了一场比第二次世界大战时期的机械密码更彻底的革命，人类从此进入了信息密码时代，加密的对象既不是几千年的书写的文字，也不是有 100 多年历史的电报字码，而是电子形式的文件。人们可以将电子形式的文件转换成数字或数值符号，施以复杂的数学运算，达到数字符号的混淆、扩散和置换效果，实现信息加密、解密等各种目的。大量的信息论、概率论、数理统计等数学理论被运用到密码技术中，使得密码学成为数学的一个新分支，并使其具有坚实的理论基础。传递信息的方法有无线通信、计算机网络等多种信息时代的传递方式。

第四时期：现代密码时代

1976 年，美国斯坦福大学的密码专家 Diffie 和 Hellman 发表划时代的论文——《密码学的新方向》（*New Directions in Cryptography*），提出了密码学新的思想。该思想中不仅加密算法本身可以公开，同时用于加密消息的密钥也可以公开，这就是公钥加密。公钥密码的思想是密码发展的里程碑，实现了密码学发展史上的第二次飞跃。

1978 年，美国麻省理工学院的李维斯特（Rivest）、萨莫尔（Shamir）和阿德曼（Adleman）在 Diffie 和 Hellman 思想的基础上，提出第一个实用的公钥密码体制 RSA。RSA 密码算法的安全性基于数论中的大整数因子分解问题，该问题在数论中属于困难问题，至今没有有效的解决方法，因此保证了 RSA 密码体制的安全性。

1985 年，美国华盛顿大学的数学家柯布利兹（Koblitz）和国防分析研究所的数学家米勒（Miller）各自独立地提出了一个椭圆曲线密码体制（Elliptic Curve Cryptosystem，ECC）。ECC 基于椭圆曲线上离散对数求解问题，至今没有有效的求解方法，因此 ECC 是安全的。

现代公钥密码的安全性基于数学上的困难问题，有坚实理论基础，包括信息论、计算复杂性理论、数论、概率论等，已经成为一门学科。现代密码学的任务已经不局限于传统密码的保密通信，而是含义更广的信息安全，其中包括保密通信、数据加密、身份认证、数字签名、密钥协商、秘密分享等重要的功能。

21 世纪初，我国研究并推出了系列商用密码算法，包括祖冲之序列密码算法、SM2 公钥密码算法、SM3 密码杂凑算法、SM4 分组密码算法、SM9 标识密码算法，其逐渐成为国际密码标准。如今，密码学的应用已经深入人们生活的各个方面，如数字证书、网上银行、身份证、社保卡和税务管理等，密码技术在其中发挥了关键作用。

近年来，其他相关学科的快速发展，促使密码学中出现了新的密码技术，如 DNA 密码、混沌密码和量子密码等。整个密码学的发展是由简单到复杂的逐步完善过程，这也符合历史发展规律和人类对客观事物的认识规律。同时，密码学的发展也促进了数学、计算机科学、信息通信等学科的发展。反之，其他学科的发展也促进密码学的发展。正是不同学科发展过程中的相互推动、联系、渗透，使得人类对事物有了更深的认识。

1.2　密码学的基本概念

在一般的通信系统中，从信源发出的信号经过编码器的编码调制处理之后，经公开的信道传至解码器进行译码、解码操作，最终传至信宿。通信系统模型如图 1.1 所示。

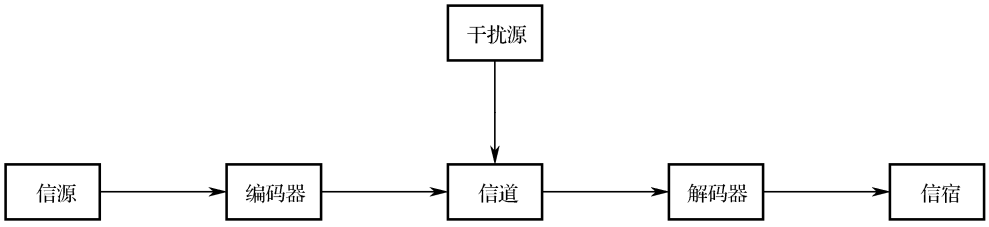

图 1.1　通信系统模型

在公开的信道中，信息的存储、传递与处理都是以明文形式进行运算的，很容易受到窃听、截取、篡改、伪造、假冒、重放等手段的攻击。因此，信息在传递或广播时，需要做到不受黑客等的干扰，除合法的被授权者以外，不让任何人知道，这就引出了保密通信的概念。

保密通信系统是在一般通信系统中加入加密器与解密器，保证信息在传输过程中无法被其他人解读，从而有效解决信息传输过程中存在的安全问题。保密通信系统模型如图 1.2 所示。

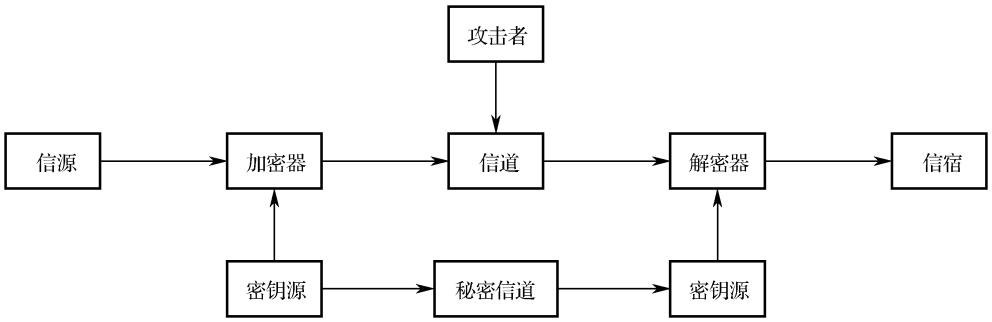

图 1.2　保密通信系统模型

加密、解密属于密码学范畴，在保密通信系统中，用户之间的交互涉及明文、密文、加密、解密、加密算法及解密算法等概念，具体含义如下。

明文（Plaintext/Message）：未加密的数据或解密还原后的数据。

密文（Ciphertext）：加密后的数据。

加密（Encryption）：对数据进行密码变换以产生密文的过程。

解密（Decryption）：加密过程对应的逆过程。

加密算法（Encryption Algorithm）：对明文进行加密时所采用的一组规则。

解密算法（Decryption Algorithm）：对密文进行解密时所采用的一组规则。

加密和解密算法的操作通常是在一组密钥控制下进行的，分别称为加密密钥和解密密钥。

一个密码体制可以描述为一个五元组$(M，C，K，E，D)$，它必须满足下述条件。

（1）M 是可能明文的有限集。

（2）C 是可能密文的有限集。

（3）K 是可能密钥的有限集。

（4）E 是加密有限空间集合。

（5）D 是解密有限空间集合。

下面通过一个具体的实例说明保密通信系统。密钥为$k(k\in K)$，此时密钥需要经过安全的秘密信道由发送方传给接收方。

加密变换E_k：$M\to C$，由加密器完成。解密变换D_k：$C\to M$，由解密器完成。

对于明文$m\in M$，发送方加密$c=E_k(m)$，$m\in M$，$k\in K$。接收方解密$m=D_k(c)$，$c\in C$，$k\in K$。

对攻击者或密码分析者而言，由于不知道密钥k，无法对截获的密文c进行解密。攻击者设计一个函数H，对密文c进行解密，即$m'=H(c)$。一般情况下$m'\neq m$，若$m'=m$，则攻击成功。

为了保证信息的保密性，对抗密码分析，保密系统应当满足下述要求。

（1）系统即使达不到理论上是不可破的，即$\Pr\{m'=m\}=0$，也应当在实际中不可破。就是说，从截获的密文或某些已知的明文密文对中，要决定密钥或任意明文在计算上是不可行的。

（2）系统的保密性不依赖于对加密体制或算法的保密，而依赖于密钥，这是著名的柯克霍夫（Kerckhoff）原则。

（3）加密和解密算法适用于所有密钥空间中的元素。

（4）系统便于实现和使用。

1.3 密码学的基本属性

应用密码技术是保障网络与信息安全最有效、最可靠、最经济的手段，可以实现信息的机密性、信息的真实性、数据的完整性和行为的不可否认性。

1．信息的机密性

信息的机密性是指保证信息不被泄露给非授权者等实体的性质。采用密码技术中的加密保护技术，可以方便地实现信息的机密性。利用加密技术对文件进行加密，可产生形如乱码的密文。即使攻击者截取到密文，但加密算法具有足够的强度，使得攻击者不能从密文中获取有用信息。而拥有密钥的人可以对密文解密，从这串乱码中恢复出原来的文件。

2．信息的真实性

信息的真实性是指保证信息来源可靠、没有被伪造和篡改的性质。密码中的安全认证技术可以保证信息的真实性。这些技术包括数字签名、消息认证码、身份认证协议等。这些技术的基本思想是合法的被授权者都有各自的“秘密信息”，用这个“秘密信息”对公开信息进行处理

即可得到相应的“印章”，用它来证明公开信息的真实性，而没有掌握相应“秘密信息”的非法用户无法伪造“印章”。

3．数据的完整性

数据的完整性是指数据没有受到非授权者的篡改或破坏的性质。密码杂凑算法可以方便地实现数据的完整性。密码杂凑算法通过数学原理过程，从文件中计算出唯一标识这个文件的特征信息，称为摘要。文件内容的细微变化都会产生不同的摘要，只要在电子文件后面附上一个简短的摘要，就可以鉴别文件的完整性。不同的文件拥有不同的摘要，一旦文件被篡改，摘要也就不同了。因此，对文件的保护而言，采用密码杂凑算法是一种非常便捷、可靠的安全手段。

4．行为的不可否认性

行为的不可否认性也称抗抵赖性，是指一个已经发生的操作行为无法否认的性质。基于公钥密码算法的数字签名技术，可以有效解决行为的不可否认性问题。用户一旦签署了数字签名，就不能抵赖、不可否认。对解决网络上的纠纷、电子商务的纠纷等问题，数字签名是必不可少的工具。虽然计算机、网络和信息系统的日志能在一定程度上证明用户的操作行为，但日志容易被伪造和篡改，因此无法实现该行为的不可否认性。

1.4　密码体制分类

密码编码学是一门通过研究和设计密码通信系统，使其传递的信息具有很强的保密性和认证性的学科，是一种通过研究密码变化的客观规律，将其应用于编制密码以保护通信秘密的技术。本节主要讲述对称密码体制和非对称密码体制的模型。

1.4.1　对称密码体制

对称密码体制又称单钥体制，是加密和解密使用相同密钥的密码算法。采用单钥体制的系统的保密性主要取决于密钥的保密性，与算法的保密性无关，即由密文和加解密算法不可能得到明文。换句话说，算法不需要保密，需要保密的仅是密钥。对称密码体制加密和解密过程如图 1.3 所示。

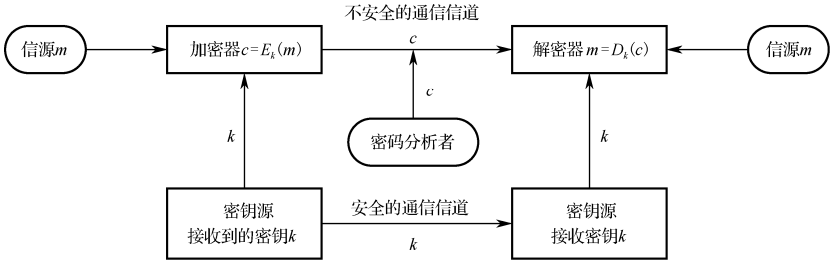

图 1.3　对称密码体制加密和解密过程

密钥可由发送方产生，然后经过一个安全可靠的途径（如信使递送）送至接收方，或由第三方产生后安全、可靠地分配给通信双方。

如何产生满足保密要求的密钥及如何将密钥安全、可靠地分配给通信双方是这类体制设计和实现的主要课题。密钥的产生、分配、存储、销毁等问题，统称为密钥管理，这是影响系统安全的关键因素。即使密码算法再好，密钥管理问题处理不好，也很难保证系统的安全保密。

对称密码体制对明文消息的加密有两种方式：一种是又明文消息按字符（如二元数字）逐位地加密，这种密码体制称为序列密码或流密码；另一种是将明文消息分组（含有多个字符），逐组地对其进行加密，这种密码体制称为分组密码。

1.4.2 非对称密码体制

非对称密码体制也称公钥密码体制，在加密和解密过程中使用两个不同的密钥。其中，一个密钥可以公开，称为公钥；另一个密钥必须保密，称为私钥，由公钥求解私钥的计算是不可行的。非对称密码体制加密和解密过程如图 1.4 所示。

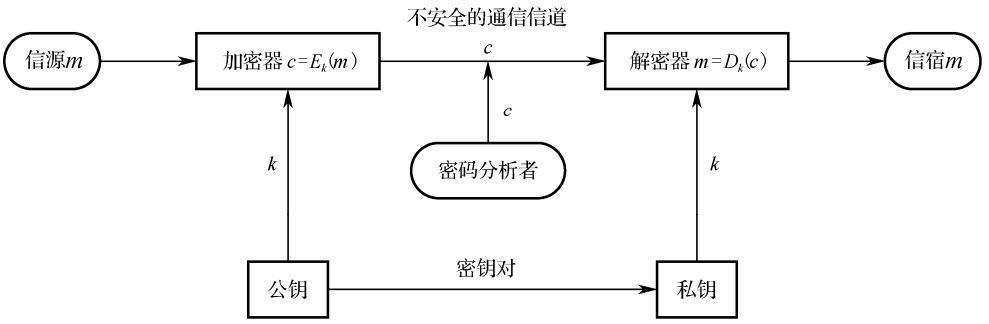

图 1.4 非对称密码体制加密和解密过程

非对称密码体制的主要特点是，加密和解密是分开的，因而可以实现多个用户加密的消息只能由一个用户解读，或一个用户加密的消息可由多个用户解读。前者可用于公共网络中实现保密通信，而后者可用于实现对用户的认证。非对称密码体制是为了解决对称密码体制中存在的问题而提出的，一方面是为了解决对称密码体制中密钥分发和管理问题；另一方面是为了解决不可否认的问题。基于以上两点可知，公钥密码体制在密钥的分配、管理、认证、不可否认性等方面有着重要的意义。

非对称密码体制的另一个重要用途是数字签名，与加密过程不同的是，在数字签名中，消息的发送者要使用自己的私钥对消息进行签名，所有人都可以使用与其对应的公钥进行签名的有效性验证。因此，非对称密码体制不仅可以保障信息的机密性，还具有认证和不可否认性等功能。

1.5　密码分析

密码分析学是研究如何破解或攻击受保护的信息的科学，是指在没有加密密钥的情况下，攻击密文的过程，其目标就是从密文得到明文或者由已知的条件得到密钥。密码分析是建立在攻击者已知加密算法的基础之上的。

在信息传输和处理系统中，除了有预定的接收者，还有非授权者或截获者，他们通过各种办法，如搭线窃听、电磁窃听、声音窃听等来窃取机密信息。对一个保密通信系统采取截获密文进行分析的方法称为被动攻击。非法入侵者、攻击者或黑客主动向系统窜扰，采用删除、增添、重放、伪造等手段向系统注入假消息以达到非法目的的行为称为主动攻击。

1.5.1　密码分析的分类

根据密码分析者可能取得的分析资料的不同，密码分析可分为如下 4 类。

（1）唯密文攻击（Ciphertext-Only Attack）：密码分析者只用密文进行密码分析的方法。

（2）已知明文攻击（Know-Plaintext Attack）：利用大量互相对应的明文和密文进行密码分析的方法。

（3）选择明文攻击（Chosen-Plaintext Attack，CPA）：选择特定明文和对应密文进行密码分析的方法。

（4）选择密文攻击（Chosen-Ciphertext Attack，CCA）：选择特定密文和对应明文进行密码分析的方法。

其中，最难的攻击类型是唯密文攻击，这种攻击的手段一般是穷举搜索法，即对截获的密文依次使用所有可能的密钥试译，直到得出有意义的明文。只要有足够多的计算时间和存储容量，原则上穷举搜索法总是可以成功的。但任何一种能达到安全要求的实用密码的设计都会使这一方法在实际中是不可行的。

已知明文攻击中典型的分析为可能字攻击。例如，对一篇散文加密，攻击者可能对消息含义知之甚少。然而，如果对非常特别的信息加密，攻击者也许能知道消息中的某一部分。又如，发送一个加密的账目文件，攻击者可能知道某些关键字在文件报头的位置。再如，在一个公司开发的程序的源代码中，可能在某个标准位置上有该公司的版权声明。

另外还有如下两种攻击情况。

（1）自适应选择明文攻击（Adaptive Chosen Plaintext Attack）：是 CPA 的一种特殊情况，是指密码分析者不仅能够选择要加密的明文，还能够根据加密的结果对以前的选择进行修正。

（2）选择密钥攻击（Chosen Key Attack）：这种攻击情况在实际中比较少见，它仅表示密码分析者知道不同密钥之间的关系，并不表示密码分析者能够选择密钥。

在评价一个密码体制时还需要注意如下两个概念。

（1）一个加密算法是无条件安全的，如果算法产生的密文不能给出唯一决定相应明文的足

够信息，此时无论密码分析者截获多少密文、花费多少时间，都不能解密密文。

（2）香农指出，仅当密钥至少和明文一样长时，才能达到无条件安全。也就是说除了一次一密方案，再无其他加密方案是无条件安全的。

加密算法只需要满足以下两条准则之一：一是破译密文的代价超过被加密信息的价值；二是破译密文所花费的时间超过信息的有用期。

满足以上两个准则的加密算法称为计算安全（Computational Security）。此外，密文没有泄露足够多的明文信息，无论计算能力有多强，都无法由密文唯一确定明文，满足此条件的加密算法称为无条件安全（Unconditional Security）。

1.5.2 穷密钥搜索

穷密钥搜索理论上很简单，就是对每个密钥进行测试，直至找到解为止。该方法是最基本的攻击方法，其复杂度由密钥量的大小决定，并且该方法能成功实现的条件是可以对正确的明文进行识别。

不同密钥长度下完成穷密钥搜索所需要的时间如表 1.1 所示。

表 1.1 不同密钥长度下完成穷密钥搜索所需要的时间

密钥长度/bit	可选密钥数	以 10^6 次/微秒的速率运算所需要的时间
32	$232=4.3\times10^9$	2.15 毫秒
56	$256=7.2\times10^{16}$	550 毫秒
64	$264=1.8\times10^{19}$	99 天
128	$2128=3.4\times10^{38}$	5.4×10^{18} 年
168	$2168=3.7\times10^{50}$	5.9×10^{30} 年

由表 1.1 可知，当密钥长度较小时，可以通过穷密钥搜索的方法进行破解，但当密钥长度较长时，该方法不再适用。当今密钥长度普遍较长，因此穷密钥搜索方法的使用机会很少。

1.6 密码的未来

随着电子商务、大数据、云计算、人工智能等技术的应用，密码学迎来了新的发展机遇与挑战，国内外众多学者都在追求更加安全、高效的密码算法，以实现对数据的信息安全保障。下面简单论述密码学的一些新方向。

Rivest 等在 20 世纪 70 年代首先提出“隐私同态”。同态密码算法的发展历经单同态、部分同态及全同态。2009 年，IBM 的研究员 Gentry 发表了一篇基于理想格设计出第一个全同态加密体制，使得加密消息能够被深入和无限地分析，而不会影响其机密性的文章，这是同态加密的一项历史性突破。自此以后，密码学家开始重视全同态加密的研究，并将全同态加密称为“密码学界的圣杯”。全同态加密的理论研究进一步促进了密码研究者对格理论等相关数学理论的研究，拓宽了寻找新型密码学数学理论基础的视野。

后量子密码学是针对量子计算机提出的，随着量子计算机及量子密码的发展，未来的密码发展趋势集中于抗量子密码算法，如基于杂凑函数的密码算法、基于编码理论的密码算法、基于格理论的密码算法及基于多变量的密码算法。其中，基于格理论的密码算法由于其本身的良好性质而得到广泛的研究，目前我国学者就基于格理论的密码算法进行了如下几方面的研究：基于格理论的加密和解密算法、基于格理论的数字签名算法、基于格理论的密钥协商机制、基于格理论的全同态密码算法及基于格理论的数字证书方案，形成了基于格理论的后量子体系。

混沌密码学是混沌理论的一个重要的应用，主要依据混沌的基本特性，即随机性、遍历性、确定性和对初始条件的敏感性。混沌密码体系在结构上与传统密码学理论中的混淆和扩散概念联系起来，混沌理论和纯粹密码学之间的必然联系形成了混沌密码学。目前混沌密码学主要分为两个研究方向：一个是以混沌同步技术为核心的混沌保密通信系统，主要基于模拟混沌电路系统；另一个是利用混沌系统构造新的流密码和分组密码，主要基于计算机有限精度下实现的数字化混沌系统。

DNA 密码是新生密码，以传统密码学为基础，其特点是以 DNA 为信息载体，以现代生物学技术为实现工具，利用 DNA 分子存储能力强大、低能耗、高度并行性等特点，通过分子处理技术制作 DNA 分子，并将该 DNA 分子作为计算工具来构造和完成密码算法。DNA 密码不仅基于数学问题，还依靠生物技术，使得其比传统密码学更加安全。但 DNA 密码主要以生物学技术的局限性为安全依据，与计算能力无关，这种安全性有多高，能够保持多久，还有待研究。

量子密码学的研究最早出现在 1970 年，当时 Wiesner 写了一篇关于共轭编码的文章，直到 1983 年才得以发表，这奠定了量子密码学的基础。量子密码学与传统的密码系统不同，它将物理学作为安全模式的关键方面，而不是数学。实质上，量子密码学是基于单个光子的应用和它们固有的量子属性开发的不可破解的密码系统，因为在不干扰系统的情况下无法测定该系统的量子状态。随着人们对量子密码的进一步研究，密码学一定会进入量子时代。

总之，时代在进步，密码在发展，新技术的出现不代表现有技术的消失，量子计算机的到来也不是现代密码学的末日，安全传输只是传统密码学诸多应用中的一个，因此量子密码不可能完全取代传统密码算法。目前，针对不同密码算法提出了不同的攻击方法，也提出了相应的防御方法，相应的标准化工作也在稳步推进当中，相信在未来的信息时代，密码学可以更加安全、有效地保护人们的信息安全。

1.7　本章小结

本章首先介绍密码学的起源，讲述各个时期密码的发展状况；其次，通过对普通通信系统与保密通信系统的模型比较，对密码学的基本名词概念进行简要描述；再次，从密码编码学与密码分析学的角度对密码系统进行大致的分析；最后，根据国内外的研究进展，介绍密码学的未来发展趋势。

1.8 本章习题

1．试述密码学发展的四个时期及其主要特征。

2．什么是密码学？什么是密码编码学？什么是密码分析学？

3．密码学的五元组是什么？它们分别有什么含义？

4．密码分析主要有哪些方式？各有何特点？

5．密码学的基本属性包含哪几方面？

6．什么是对称密码体制和非对称密码体制？各有何优缺点？