项目 5 project 5

密码及加密技术

密码及加密技术是实现网络安全的重要手段，作为现代信息化社会中一项最常用的防范措施，已被广泛地运用到网络安全应用中。密码技术保障了网络中数据传输和信息交换的安全性，是数据加密、数字签名、消息认证与身份识别、防火墙及反病毒技术等众多信息安全技术的基础。网络安全采用防火墙、病毒查杀等属于被动防御措施，数据安全主要采用对数据加密进行主动保护。

重点： 密码技术相关概念、密码体制及加密方式。

难点： 实用加密技术、数据及网络加密方式。

关键： 密码技术的概念，密码体制的概念、分类和特点，实用加密技术的典型算法，数据及网络加密方式。

目标： 掌握密码学的基本概念和基本术语、密码体制、实用加密技术、数据及网络加密方式，了解密码破译与密钥管理的常用方法。

5.1 项目分析 密码及加密技术的重要性

教学视频
课程视频 5.1

【引导案例】 密码作为一种最原始、最广泛使用的安全手段，保护着人们的信息安全及个人隐私，而近年来的密码泄露事件严重危害着网络安全。据相关报道可知 81%黑客导致的泄露事件都与密码破译或弱密码有关：国内最大的开发者技术社区 CSDN 安全系统遭到黑客攻击，数据库中超过 600 万用户的登录名和密码泄露；携程安全支付日历导致用户银行卡信息泄露，包括持卡人姓名、身份证、卡号及密码等信息；数百万领英的用户账户信息泄露导致 Facebook 联合创始人马克扎克伯格的其他账户被黑……加深对密码安全的认识、掌握相关密码技术手段、增强安全意识尤为重要。

5.1.1 密码学与密码技术的重要意义

密码学是研究编制密码和破译密码的科学，是一门结合了数学、计算机科学、电子与

通信等多种学科为一体的交叉学科，而密码技术是利用密码学的知识和技术保护信息安全的基础核心手段之一。

（1）随着移动互联网、云计算、物联网、大数据为代表的新型网络形态及网络服务的兴起，世界范围的信息实现了更加方便快捷地共享和交流，这些在为人们的工作和生活提供便利的同时，随之而来的是巨大的信息泄露及恶意攻击等问题，网络空间竞争与对抗的矛盾日益尖锐复杂，人们对信息安全意识及个人隐私安全意识也与日俱增。

（2）在信息安全的理论体系和应用技术研究中，密码技术经历了长期的发展形成了较完整的密码学理论体系，一系列公认的经典可靠的算法被提出，并且至今被广泛地采用及改进。密码技术逐步从最初的外交和军事领域走向社会公众，用于保证各类信息的机密性、完整性和准确性，防止信息被篡改、伪造和假冒。

（3）围绕信息安全和密码学中的前沿和热点问题，世界范围的信息安全与密码学国际会议每年举行，通过与会学者们的广泛讨论和交流，探讨如何运用密码学基础理论探索信息安全技术和保障网络空间安全，这些都是当前政府、学术界、工业界共同关注的焦点。

（4）密码技术始终在信息安全领域处于核心技术地位，经历了古典密码及现代密码技术的发展，各种新兴的密码技术，如神经网络密码、混沌密码、量子密码、DNA 密码等相继提出，近年来得到了普遍的重视和关注。

密码学的发展促进了许多新技术的诞生，同时新技术的推广应用以及计算能力的不断提升也给秘密技术带来新的机遇和挑战，密码学理论和技术的发展应顺应社会进步的实际需求不断进步。

5.1.2 密码学发展态势分析

密码学在网络安全领域成为不可或缺的安全技术，随着各类新技术的产生以及计算机运算速度的不断提高，传统的加密技术无法满足现阶段应用的需求，新的密码技术和手段被研究和应用，主要围绕量子密码、混沌密码、DNA 密码等展开。

（1）量子密码是以量子法则为基础，利用量子态作为符号而实现的密码技术。它突破了传统加密方法的束缚，以量子态作为密钥，体现出不可复制性，任何截获或测试量子密钥的操作都会改变量子态，因此截获者得到的是无用信息，信息合法接收者可以根据量子态的改变获知密钥是否被攻击。量子密码目前已经进入实用化阶段，但是其中仍存在需要进一步探讨的安全性问题。

（2）混沌密码利用了混沌系统产生 S 混沌序列作为密钥序列，利用该序列对明文加密，密文经过信道传输到接收方后，利用混沌同步的方法将明文信号提取出来实现解密。混沌加密技术是混沌和密码学优点的结合，安全性能非常高，其加密和解密的过程可重用，且易于硬软件的实现。

（3）DNA 密码作为密码学的新分支迅速发展起来，其以传统密码学为基础，同时利用了 DNA 分子所具有的超大规模并行性、超高容量的存储密度以及超低的能量消耗等特点，实现加密、认证及签名等密码学功能。DNA 密码基于数学问题，以现代生物技术为实现工具，使得 DNA 密码的破译难度更大，安全保障性更强。

另外，值得关注的是大数据时代的到来，伴随着移动互联网、物联网和云计算等新兴技术和服务的涌现与应用，大数据的存储、搜索、计算等环节都可能发生数据泄露等问题。现阶段的云计算为大数据提供了专业的存储服务，而云端的存储为不可全信的第三方，数据面临着偷窃或篡改的风险，大数据安全及隐私保护成为新型的安全问题。当前，同态密码技术被用于大数据隐私存储保护，其作为支撑云计算安全的关键技术，仍然处于探索阶段，是当前大数据应用领域最大的挑战之一。

☺讨论思考

（1）密码学的研究内容有哪些？

（2）目前新的密码技术有哪些？

5.2 任务1 密码学相关概念和特点

教学视频

课程视频 5.2

5.2.1 目标要求

本任务主要学习目标的具体要求如下。

（1）熟悉密码学的基本概念和基本术语。

（2）了解密码系统的基本原理。

（3）掌握密码体制的分类及各自特点。

5.2.2 知识要点

1. 密码学的基本概念

【案例 5-1】 英德大战，图灵破译德军密码。1942 年，英军和德军在北非展开激战。春夏之交，德国著名的“沙漠之狐”隆梅尔率领德国非洲军团横扫北非，英军一溃千里，1942 年 6 月退守阿拉曼，后来才守住阵地。1942 年 8 月，英国名将蒙哥马利率军反攻，有效地切断了德军的补给线。德军终因补给不足、增援无望而败北。这一仗是非洲战争的转折点。阿拉曼战役，英军何以能准确地拦截到几乎所有的德军补给船队却一直是个谜。直到 20 世纪 70 年代才露出谜底：当时数学家图灵领导的一个小组成功地破译了德军的密码！

密码学（cryptology）是密码编码学和密码分析学的总称，是研究编制密码和破译密码的技术科学。密码编码学是研究密码变化的客观规律，并应用于编制密码以保守密码信息的科学；密码分析学是研究密码变化的规律，并应用于破译密码以获取通信情报的科学，亦称为密码破译学。密码学一词来源于古希腊的 crypto 和 graphein 两个词，希腊

语的原意是隐写术，即将易懂的信息通过一些变换转换成难以理解的信息进行隐秘地传递。在现代，密码学特别指对信息及其传输的数学性研究，是应用数学和计算机科学相结合的一个交叉学科，和信息论也密切相关。密码学研究进行保密通信和如何实现信息保密的问题，以认识密码变换的本质、研究密码保密与破译的基本规律为对象，主要以可靠的数学方法和理论为基础，对解决信息安全中的机密性、数据完整性、认证和身份识别，对信息的可控性及不可抵赖性等问题提供系统的理论、方法和技术。

密码学的发展历史悠久，密码学的发展历程大致经历了3个阶段。第一阶段，从古代到1949年，可以看作是密码学的前夜。这一时期的密码技术可以说是一种艺术，而不是一种科学，密码学专家凭直觉和信念来进行密码设计和分析，而不是推理和证明。第二阶段，1949—1975年。1949年，香农发表的《保密系统的通信理论》一文为密码学的发展奠定了理论基础，使密码学成为一门真正的科学，但后续理论研究工作进展不大，公开的密码学文献很少。第三阶段，1976年至今。Diffie和Hellman发表的《密码学的新方向》一文提出了一种新的密码设计思想，从而开创了公钥密码学的新纪元。此后，对称密码和公钥密码相继飞跃发展。随着时代进步，计算机的广泛应用又为密码学的进一步发展提出新的客观需要。密码学成为计算机安全研究的主要方向，不仅在计算机通信的数据传输保密方面，而且在计算机的操作系统和数据库的安全保密方面也很突出，由此产生了计算机密码学。

2. 密码学的基本术语

要了解密码学中的基本原理和密码体制，首先要对相关术语进行了解。

（1）明文(plaintext)：是信息的原始形式，即待加密的信息，记为P或M。明文可以是文本、图形、数字化存储的语音流或数字化的视频图像的位流等。

（2）密文(ciphertext)：明文经过变换加密后的形式，记为C。

（3）加密(enciphering)：由明文变成密文的过程，记为E。

（4）解密(deciphering)：由密文还原成明文的过程，记为D。

（5）加密算法(encryption algorithm)：实现加密所遵循的规则。它用于对明文进行各种代换和变换，生成密文。

（6）解密算法(decryption algorithm)：实现解密所遵循的规则。它是加密算法的逆运算，由密文得到明文。

（7）密钥(key)：为了有效地控制加密和解密算法的实现，密码体制中要有通信双方的专门的保密“信息”参与加密和解密操作，这种专门信息称为密钥，分为加密密钥和解密密钥，记为K。

（8）加密协议：定义了如何使用加密、解密算法来解决特定的任务。

（9）发送方(sender)：发送消息的对象。

（10）接收方(receiver)：传送消息的预定接收对象。

（11）入侵者(intruder)：非授权进入计算机及其网络系统者。

（12）窃听者(eavesdropper)：在消息传输和处理系统中，除了意定的接收者外，非授权者通过某种办法（如搭线窃听、电磁窃听、声音窃听等）来窃取机密信息。

(13) 主动攻击(active attack)：入侵者主动向系统窜扰，采用删除、更改、增添、重放、伪造等手段向系统注入假消息，以达到损人利己的目的。

(14) 被动攻击(passive attack)：对一个密码系统采取截获密文进行分析。

3. 密码系统基本原理

密码系统通常由明文、密文、密钥(包括加密密钥和解密密钥)与密码算法(包括加密算法和解密算法)4 个基本要素组成。其中密钥是一组二进制数，由进行密码通信的专人掌握，而算法则是公开的，任何人都可以获取使用。

密码系统可以用一个五元组(P,C,K,E,D)定义，该五元组应满足如下条件。

(1) 明文空间 P：可能明文的有限集。

(2) 密文空间 C：可能密文的有限集。

(3) 密钥空间 K：一切可能密钥构成的有限集。

(4) 加密算法空间 E：可能加密算法的有限集。

(5) 解密算法空间 D：可能解密算法的有限集。

(6) 任意 $k\in K$，有一个加密算法 $\mathrm{ek}\in E$ 和相应的解密算法 $\mathrm{dk}\in D$，使得 ek：$P\to C$ 和 dk：$C\to P$ 分别为加密函数和解密函数，满足 $\mathrm{dk}(\mathrm{ek}(x))=x$，其中 $x\in P$。

以上是密码系统中的数学描述，密码系统的基本原理模型如图 5-1 所示。明文 P 由加密算法 ek 和加密密钥 k_e 进行加密得到密文 C，接收者对得到的密文 C 用解密算法 dk 和解密密钥 k_d 对密文 C 进行解密得到明文 P。

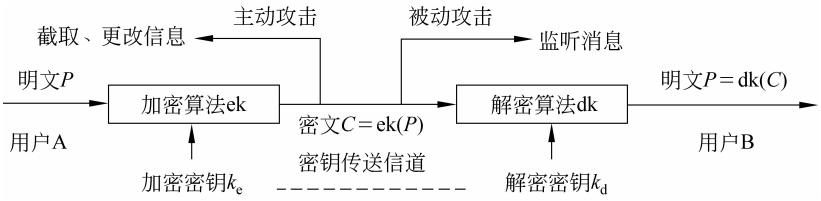

图 5-1 密码系统的基本原理模型框图

为了实现网络信息的保密性，密码系统要求满足以下 4 点。

(1) 系统密文不可破译。从网络系统截获的密文中确定密钥或任意明文在计算上是不可行的，或解密时间超过密码要求的保护期限。

(2) 系统的保密性不依赖于对加密体制或算法的保密，而是依赖于密钥。

(3) 加密算法和解密算法适用于所有密钥空间中的元素。

(4) 密码系统便于实现和推广使用。

4. 密码体制及其分类

密码体制即密码系统，其主要的作用是能够完整地解决信息安全中的机密性、数据完整性、认证、身份识别、可控性及不可抵赖性等几个基本问题。密码体制按照密码的不同原理和用途有多种分类方式。

根据加密算法和解密算法所使用的密钥是否相同可以分为对称密码体制和非对称密码体制。

（1）对称密码体制。

对称密码体制又称为单钥密码体制、私钥密码体制或对称密钥密码体制。它是指在加密和解密过程中使用相同或可以推导出本质上相同的密钥，即加密密钥与解密密钥相同且密钥需要保密。信息的发送者和接收者在进行信息的传输与处理时，必须共同持有该密钥，密钥的安全性成为保证系统机密性的关键。对称密钥加密和解密的基本原理及过程如图 5-2 所示。信息的发送方将持有的密钥对要发送的明文信息进行加密，加密后的密文通过网络传送给接收方，接收方用与发送方相同的私钥对接收的密文进行解密，得到明文信息。

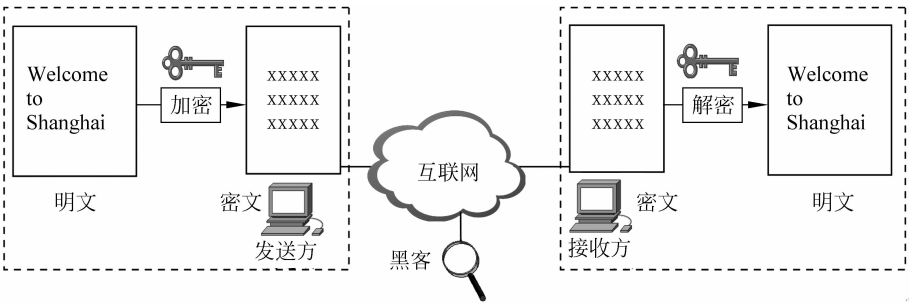

图 5-2　对称密钥加密和解密的基本原理及过程

对称密码体制的优点是加密和解密速度快、保密度高、加密算法简单高效、密钥简短和破译难度大，且经受住时间的检验和攻击。缺点是密钥管理困难，当多人通信时，密钥组合的数量出现快速增长，使密钥分发复杂化。如有 N 个用户两两通信，共需要密钥数 $N(N-1)/2$ 个。采用对称密码体制传输信息，必须保证密钥在网络上的安全传输，不被窃取或破解，因此密钥自身的安全是对称密码体制的关键问题。除此之外，对称密码体制还存在数字签名困难的问题，如通信双方的发送方可以否认发送过的某些信息，而接收方可以伪造签名等。

对称密码体制根据对明文信息的加密方式不同可以分为流密码和分组密码两类。

① 流密码又称为序列密码，以明文的单个位（或字节）为单位进行运算。流密码的加密过程是将明文划分成单个位（如数字 0 或 1）作为加密单位产生明文序列，然后将其与密钥流序列逐位进行模 2 加运算，最后将其结果作为密文的方法。流密码体制的密文与给定的加密算法和密钥有关，还与当前正被加密的明文部分在整个明文中的位置有关。流密码实现简单，具有便于硬件计算、加密与解密速度快、低错误（没有或只有有限位的错误）传播等优点，但同时也暴露出对错误的产生不敏感等缺点。流密码涉及大量的理论知识，提出了众多的设计原理，得到了广泛的分析。但是许多研究成果并没有完全公开，这也许是因为流密码目前主要应用于军事和外交等机密部门的缘故。目前，公开的流密码算法主要有 RC4、SEAL 等。

② 分组密码是以固定长度的组为处理的基本单元，将明文消息划分为若干固定长度的

组，每组分别在密钥的控制下变换成等长的输出数字序列。分组密码本质上是由密钥控制的从明文空间到密文空间的一个一对一的映射。分组密码体制的密文仅与加密算法和密钥有关，而与被加密的明文分组在整个明文中的位置无关。分组密码具有对明文信息的良好扩展性及插入敏感性、不需要密钥同步、适用性强、适合作为加密标准等优点，但也有加密速度慢、错误扩散和传播等缺陷。著名的 DES、IDEA 等算法都采用的是分组密码。

（2）非对称密码体制。

非对称密码体制也称为非对称密钥密码体制、公开密钥密码体制（PKI）、公开密钥加密系统、公钥密码体制或双钥密码体制。密钥成对出现，加密密钥和解密密钥不同，难以相互推导。其中一个为加密密钥，可以公开通用，称为公钥；另一个为解密密钥，是只有解密者知道的密钥，称为私钥。非对称密钥加密和解密的基本原理及过程如图 5-3 所示。信息的发送方利用接收方的公钥对要发送的信息进行加密，加密后的密文通过网络传送给接收方，接收方用自己的私钥对接收的密文进行解密，得到信息明文。

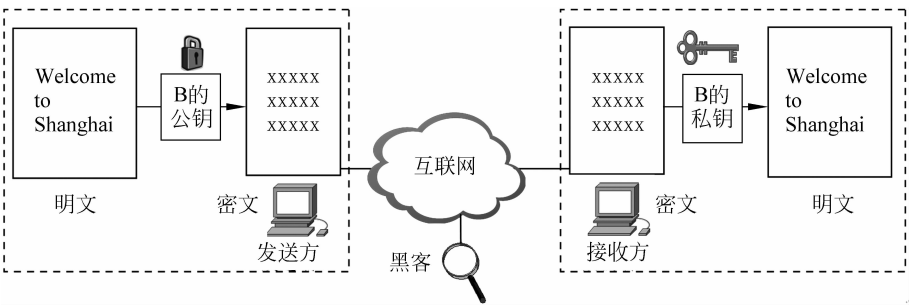

图 5-3 非对称密钥加密和解密的基本原理及过程

非对称密码体制相对于对称密码体制，由于加密密钥和解密密钥不同，无法从任意一个密钥推导出另一个密钥，这样安全程度更高；解决了对称密码体制的密钥管理与分配问题，如 N 个用户仅需产生 N 对密钥，密钥数量少，每个用户只保存自己的私钥；密钥的分配不需要秘密的通道和复杂的协议来传送密钥，公钥可基于公开的渠道分发给其他用户，私钥由用户保管；同时，非对称密码体制还能实现数字签名。然而非对称密码体制的加密、解密处理速度较慢，同等安全强度下非对称密码体制的密钥位数会较多一些。典型的非对称密码体制有 RSA 算法、ElGamal 算法、ECC 算法等。

对称密码体制与非对称密码体制特性对比如表 5-1 所示。

表 5-1 对称密码体制与非对称密码体制特性对比

特征	对称密码体制	非对称密码体制
密钥的数目	单一密钥	密钥是成对的
密钥种类	密钥是秘密的	需要公钥和私钥
密钥管理	简单、不好管理	需要数字证书及可信任第三方
计算速度	非常快	比较慢
用途	加密大块数据	加密少量数据或数字签名

混合密码体制由对称密码体制和非对称密码体制结合而成，图 5-4 是混合密码体制基本原理。

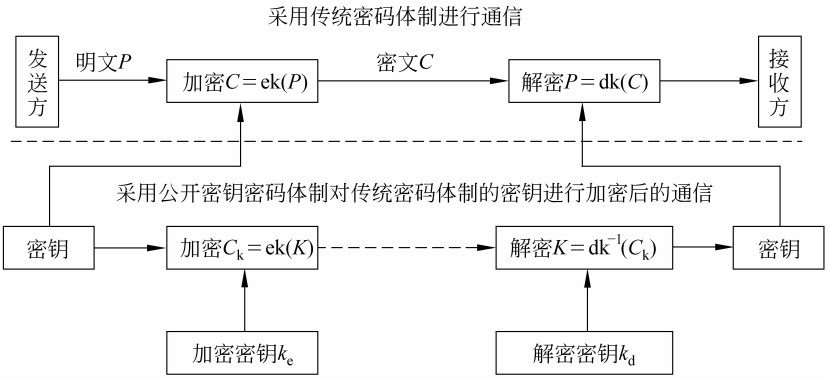

图 5-4　混合密码体制基本原理图

根据加密变换是否可逆，可以分为单向函数密码以及双向变换密码。

（1）单向函数密码：从明文到密文的不可逆映射。哈希函数又称为散列函数，是一种单向函数密码体制。其主要的特征是只有加密过程，不存在解密过程。单向函数的目的不在于加密，主要用于密钥管理和鉴别，如哈希函数保证数据完整性和应用在数字签名上。

（2）双向变换密码：通常的加密、解密都属于双向变换密码体制，即存在对明文的加密过程，也存在对密文的解密过程。

☺讨论思考

（1）什么是密码技术？什么是加密及解密？

（2）密码体制及加密方式有哪几种？

教学视频
课程视频 5.3

5.3　任务 2　密码破译与密钥管理

5.3.1　目标要求

本任务主要学习目标的具体要求如下。

（1）熟悉密码破译的基本概念和常用方法。

（2）了解对称密码体制的密钥管理。

（3）了解公钥密码体制的密钥管理。

5.3.2 知识要点

1. 密码破译

1）密码破译的概念

密码破译是在不知道密钥的情况下恢复出密文中隐藏的明文信息。密码破译也是对密码体制的攻击，成功的密码破译能恢复出明文或密钥，也能发现密码体制的弱点。穷举破译法和统计分析法虽然烦琐却是最基本的、有效的密码破译方法。

影响密码破译的主要因素涉及算法的强度、密钥的保密性和密钥长度。通常在相同条件下，密钥越长破译越困难，而且加密系统也越可靠。各种加密系统使用不同长度的密钥。常见加密系统的口令及其对应的密钥长度如表 5-2 所示。

表 5-2 常见加密系统的口令及其对应的密钥长度

系 统	口 令 长 度	密 钥 长 度
银行自动取款机密码	4 位数字	约 14 个二进制位
UNIX 操作系统用户账号	8 个字符	约 56 个二进制位

2）密码破译的方法

（1）穷举破译法（exhaustive decoding method）。对窃取的密文依次用各种可解的密钥试译，直到得到有意义的明文；或在不变密钥下，对所有可能的明文加密直到得到与截获密报一致为止。此方法又称为完全试凑法（complete trial-and-error method）或暴力破解法。此方法需要事先知道密码体制或加密算法，但不知道密钥或加密的具体方法。

【案例 5-2】 *移位加密算法分析*

密文：BJQHTRJYTXMFSLMFN

明文：welcome to shanghai

方法：知道当前采用移位加密算法，依次尝试所有可能的密钥 0、1、2、…、25，当尝试到密钥 5 时，得到明文。

注意： 只要有足够的计算时间和存储容量，原则上穷举破译法总是可以成功的。但实际中，任何一种能保障安全要求的实用密码都会设计得使这一方法在实际上是不可行的。

（2）统计分析法（statistical analysis method）。统计分析法是根据统计资料进行猜测。一般情况下，在一段足够长且非特别专门化的文章中，字母的使用频率是比较稳定的，而在某些技术性或专门化文章中的字母使用频率可能有微小变化。据报道，密码学家对英文字母按使用频率得出如表 5-3 所示的分类，该统计为截获的密文中各字母出现的概率提供了重要的密钥信息。

表 5-3　英文字母使用频率统计表(%)

字母	A	B	C	D	E	F	G	H	I	J	K	L	M
频率	7.25	1.25	3.5	4.25	12.75	3	2	3.5	7.75	0.25	0.5	3.75	2.75
字母	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
频率	7.75	7.5	2.75	0.5	8.5	6	9.25	3	1.5	1.5	0.5	2.25	0.25

【案例 5-3】 福尔摩斯探案集——跳舞的人。福尔摩斯探案集《跳舞的人》(*Dancing Men*)中出现了“小人密码”,如图 5-5 所示。福尔摩斯推测这一串图画代表一串单词或数字。根据应用字母使用频率统计,在 26 个字母中 E 出现的频率最高,有 12.75%。在小纸条中 15 个小人有 4 个相同,可以大胆推测这个小人就是代表 E。知道的小人越多对破解密码越有利,再联系案情做进一步的推理就能够知道纸条上所传达的信息了。

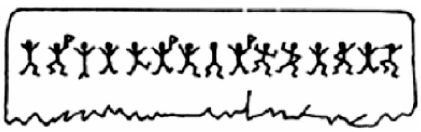

图 5-5　小人密码

(3) 其他密码破译方法。除了穷举破译法和统计分析法外,在实际生活中,破密者更可能真对人机系统的弱点进行攻击,而不是攻击加密算法本身。利用加密系统实现中的缺陷或漏洞等都是破译密码的方法,虽然这些方法不是密码学所研究的内容,但对于每一个使用加密技术的用户是不可忽视的问题,甚至比加密算法本身更为重要。常见的密码破译方法如下。

① 通过各种途径或办法欺骗用户口令密码。

② 在用户输入口令时,应用各种技术手段,“窥视”或“偷窃”口令内容。

③ 利用加密系统实现中的缺陷破译。

④ 对用户使用的密码系统偷梁换柱。

⑤ 从用户工作生活环境获得未加密的保密信息,如进行的“垃圾分析”。

⑥ 让口令的另一方透露口令或相关信息。

⑦ 威胁用户交出密码。

3) 防范密码破译的措施

防范密码破译,采取的具体措施如下。

(1) 强化加密算法。通过增加加密算法的破译复杂程度和破译的时间进行密码保护。

(2) 采用动态会话密钥。每次会话所使用的密钥不相同。

(3) 定期更换加密会话的密钥,以免泄露引起严重后果。