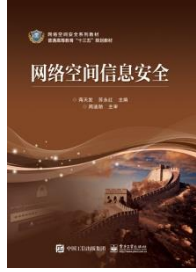
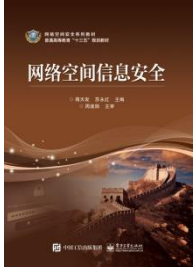


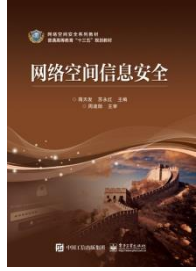
网络空间信息安全

第4章 网络空间信息密码技术



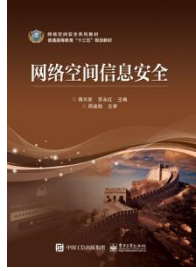
本章主要内容

- 4.1 密码技术概述
- 4.2 对称密码体系
- 4.3 非对称密码体系
- 4.4 密码管理



4.1 密码技术概述

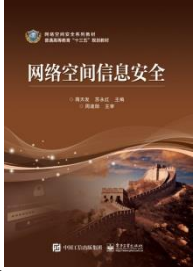
- 4.1.1 密码学发展史
- 4.1.2 密码技术基本概念
- 4.1.3 密码体制的分类



4.1 密码技术概述

密码技术的发展大致分为3个阶段：古代加密方法、古典码和近现代密码学。

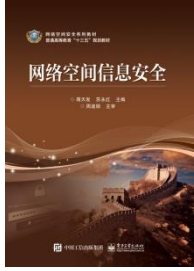
密码学（Cryptology）一词为希腊字根“隐藏”及“信息”的组合。密码技术是一门古老的技术，自人类社会出现战争便产生了密码，其历史可以追溯到几千年以前，如古埃及人使用象形文字密码技术来传递保密的消息。这种文字由复杂的图形组成，其含义只被为数不多的人掌握着。而最早将密码概念运用于实际的人是恺撒大帝，他不太相信负责他和他手下将领通信的传令官，因此他发明了一种简单的加密算法将其信件加密。



4.1 密码技术概述

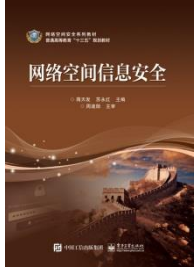
历史上的第一件军用密码装置是公元前 5世纪的斯巴达密码棒（Scytale），即“塞塔式密码”，它采用了密码学上移位法（（Transposition）。移位法是将信息字母的次序调动，而密码棒利用了字条缠绕木棒的方式，对字母进行位移。收信人要使用相同直径的木棒才能得到还原的信息。

密码技术长期被军事、外交等部门用来传递重要信息。密码技术通过对信息的变换或编码，将机密的敏感信息变换成对方难以读懂的乱码型信息，以此达到两个目的：其一，使未授权者不可能由其截获的乱码中得到任何有意义的信息；其二，使未授权者不可能伪造任何乱码型的信息。



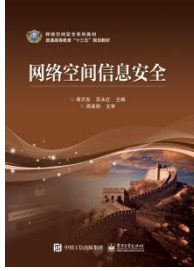
4.1.1 密码学发展历史

- 1．第一阶段是古代到1949年
- 这一时期为古典密码阶段，可以看作科学密码学的前夜时期，这个阶段的密码技术可以说是一种艺术，而不是一种科学，密码学专家常常是凭知觉和信念来进行密码的设计和分析，而不是推理和证明。
- 这一时期还没有形成密码学的系统理论。这时的密码学专家进行密码的设计和分析凭借的往往是直觉，而不是严谨的推理和证明。



4.1.1 密码学发展历史

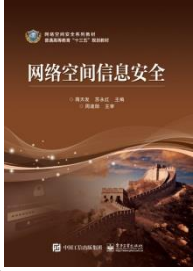
- 2．第二阶段是1949 年到1975年
- 这一时期为近代密码阶段，因为1949年，C. E. Shannon（香农）在《贝尔系统技术杂志》上发表了The Communication Theory of Secrecy System（保密系统的通信理论），为密码技术奠定了坚实的理论基础，使密码学真正成为一门科学，但密码学直到今天仍具有艺术性，是具有艺术的科学。这段时期密码学理论的研究工作进展不大，公开的密码学文献很少。
- 这一状况一直持续到 1967年David Kahn发表了《破译者》一书。这本书中虽然没有任何新颖的思想，但是，它详尽地阐述了密码学的发展和历史，使许许多多的人开始了解和接触密码学。此后，关注密码学的人才逐渐多起来。



4.1.1 密码学发展历史

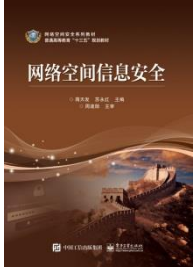
- 3．第三阶段是1976年至今
- 这一时期为现代密码阶段，因为在1976 年Diffie和Hellman发表的文章《密码学的新动向》导致了密码学的一场革命。他们首先证明了在发送端和接收端无密钥传输的保密通信是可能的，从而开创了公钥密码学的新纪元。
- 1978年，在ACM通信中Rivest、Shamir和Adleman公布了RSA密码体制，这是第一个真正实用的公钥密码体制，可以用于公钥加密和数字签名。由于RSA算法对计算机安全和通信的巨大影响，该算法的3个发明人因此获得了计算机界的诺贝尔奖——图灵奖。

4.1.1 密码学发展历史



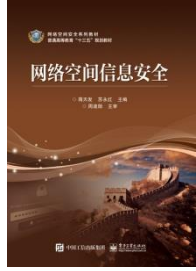
- 现代密码学的另一个主要标志是基于计算复杂度理论的密码算法安全性证明。清华大学姚期智教授在保密通信计算复杂度理论上有重大的贡献，并因此获得图灵奖，是图灵奖历史上的第一位华人得主。
- 在密码分析领域，王小云教授对经典哈希函数MD5、SHA-1等的破解是最近十年密码学的重大进展。随着计算能力的不断增强，现在DES已经变得越来越不安全。
- 1997年，美国国际标准研究所公开征集新一代分组加密算法，并于2000 年选择RijIndael作为高级加密算法AES以取代DES。

4.1.1 密码学发展历史

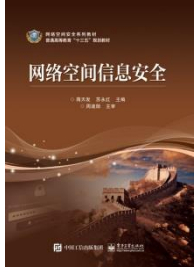


- 在实际应用方面，古典密码算法有替代加密、置换加密；对称加密算法包括DES和AES；非对称加密算法包括RSA、背包密码、Rabin、椭圆曲线等。目前，数据通信中最普遍的算法有DES算法和RSA算法等。
- 除了以上密码技术以外，一些新的密码技术如辫子密码、量子密码、混沌密码、DNA密码等也发展起来，但是它们距离真正的实用还有一段距离。

4.1.2 密码技术基本概念



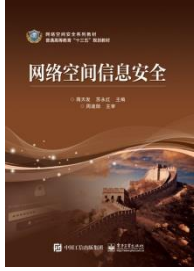
- 密码学是研究编制密码和破译密码的科学，也是研究密码变化的客观规律，应用于编制密码以保守通信秘密的，称为密码编码学（Cryptography）；应用于破译密码以获取通信情报的，称为密码分析学（Cryptanalysis），总称密码学。



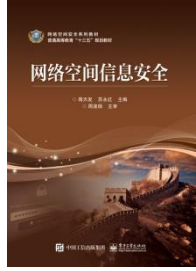
4.1.2 密码技术基本概念

- 密码编码学的任务是寻求生成高强度密码的有效算法，以满足信息进行加密或验证的要求；
- 密码分析学的任务是破译密码或伪造验证密码，窃取机密信息进行诈骗破坏活动。对一个保密系统采取截获（或窃取）密文进行分析的方法来进行攻击称为被动攻击；非法入侵者采用删除、更改、添加、重放、伪造等手段向系统注入假信息的攻击称为主动攻击。

4.1.2 密码技术基本概念



- 消息的发送者称为信源，消息的授权目的地称为信宿。采用密码方法隐蔽和保护机要消息，可使未授权者不能提取信息。被隐蔽的原始消息称为明文M，通过密码可将明文变换成另一种隐蔽形式，称为密文C。由明文到密文的变换过程$C=E_k(M)$称为加密；由合法接收者从密文恢复出明文的过程$M=D_k(C)=D_k(E_k(M))$称为解密；非法接收者试图从密文分析出明文的过程称为破译。



4.1.2 密码技术基本概念

- 加密和解密过程中使用的密钥分别称为加密密钥和解密密钥。密码的传递过程可以通过一个简单的密码通信模型来表达，如图4.1所示。

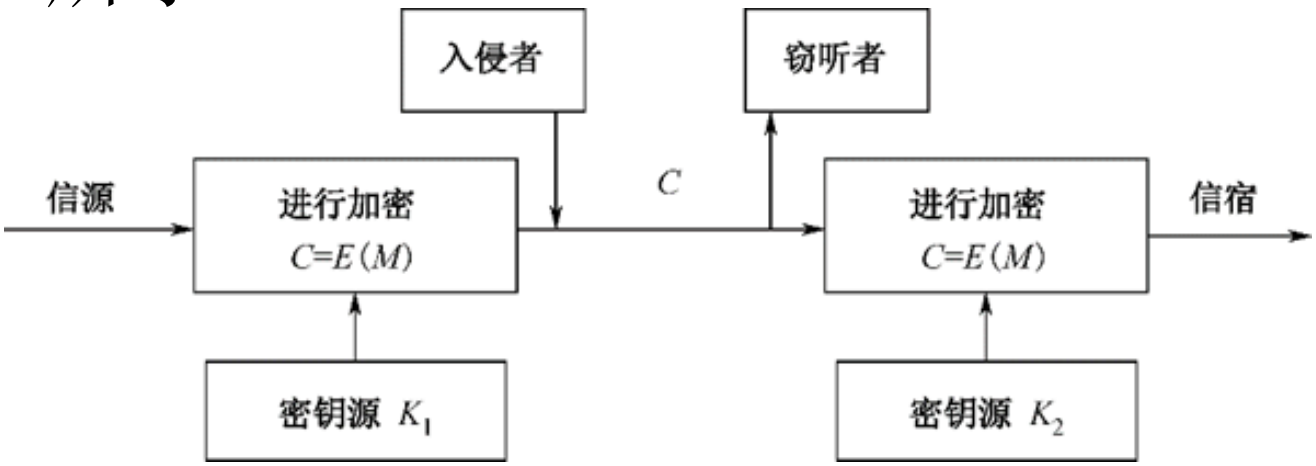
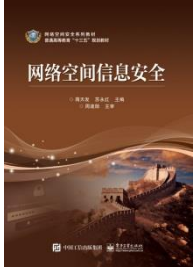


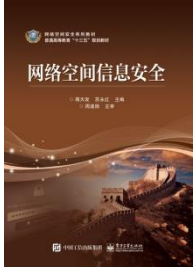
图4.1 密码通信模型

4.1.2 密码技术基本概念



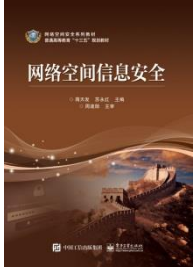
- 虽然这是一个简单的加密通信模型，但已涉及到密码体制的五个组成部分：
- 明文的集合M，称为明文空间；密文的集合C，称为密文空间；密钥的集合K，称为密钥空间；由加密密钥控制的加密交换算法E，即Ek：M→C；由解密密钥控制的解密交换算法D，即Dk：C→M，Dk (Ek(M)) =M。
- 人们将五元组（M，C，k，E，D）称为一个密码体制，在此体制中要求加密算法对所有密钥反应迅速并实时有效，体制的安全性不能依赖于算法的保密，只能依赖于密钥的保密。

4.1.2 密码技术基本概念



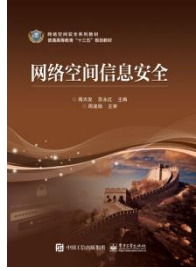
- 一个安全的密码体制根据其应用性能对信息提供下列功能：
- （1）秘密性：防止非法的接收者发现明文。
- （2）鉴别性：确定信息来源的合法性。
- （3）完整性：确定信息是否被有意或无意地更改。
- （4）不可否认性：发送方在事后，不可否认其传送过的信息。

4.1.2 密码技术基本概念



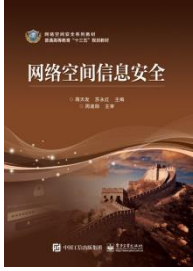
- 密码体制的安全性必须仅依赖其解密密钥，亦即在一个密码系统中除解密密钥外，其余的加/解密算法等，均应假设为破译者完全知道。
- 只有在此假设下，破译者仍无法破解密码系统，此系统方有可能被称为安全。破译者在密码系统中所获得的信息，依层次可有下列3种可能的破解方式。

4.1.2 密码技术基本概念



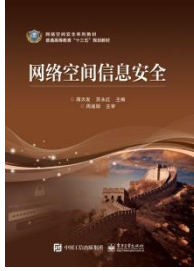
- （1）唯密文攻击法：破译者只能通过截取到密文C，并且希望能由密文来破解出明文M。
- （2）已知明文攻击法：破译者拥有一系列“明文-密文”组，并且希望能由这些“明文-密文”组破解出解密密钥或其他密文。

4.1.2 密码技术基本概念



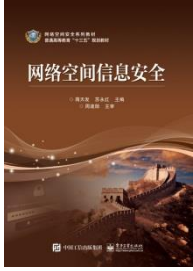
- （3）选择文攻击法：在假设破译者可以选择或控制其所获取的明文或密文时，破译者可以使用其认为最容易破解的“明文-密文”组，从而对密码系统进行攻击。选择文攻击法又分为以下两种方式。
- ① 选择明文攻击：破译者选择明文，经密码系统将其加密为密文，传送给破译者。破译者据此进行攻击。
- ② 选择密文攻击：破译者选择密文，经密码系统将其解密为明文，传送回给破译者。破译者据此进行攻击。

4.1.3 密码体制的分类



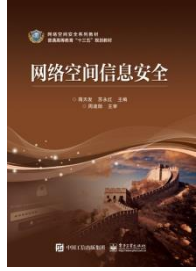
- 密码体制分类有多种形式，根据密钥的特点将密码体制分为对称密码体制和非对称密码体制两种。对称密码 又称为单密钥密码或私钥密码，非对称密码又称为双密钥密码或公密钥密码体制

4.1.3 密码体制的分类



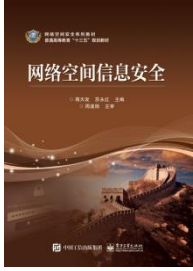
- 在对称密码体制下，加密密钥与解密密钥是相同的（即k1=k2），密钥k在传递过程中需经过安全的密钥信道，由发送方传送到接收方。单钥密码的特点是加密、解密都使用同一个密钥，所以此密码体制的安全性关键在于密钥的安全性，若其密钥泄露，则此密码系统便失去了其应有的作用。
- 单钥密码的优点如下安全性高、加解密速度快。其缺点是如下：巨大的网络规模，使密钥的管理成为难点；难以解决消息传送的确认问题；缺乏能够自动检测密钥是否泄露的能力。

4.1.3 密码体制的分类

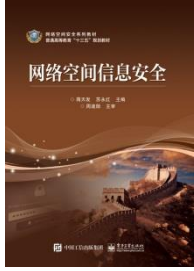


- 在非对称密码体制下，加密密钥与解密密钥不同，无需安全信道来传送密钥，只需利用本地密钥的发生器产生解密密钥k并控制解密操作D。由于双钥密码体制的加密与解密方法不同，且只需保密解密密钥，所以双钥密码不存在密钥管理问题。但双钥密码算法一般比较复杂，加解密速度慢。

4.1.3 密码体制的分类

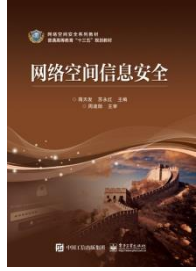


- 若以密码算法对明文的处理方式为标准，则可将密码系统分为序列密码和分组密码系统。
- 序列密码对明文进行逐个比特处理，加密过程是把明文序列与等长的密钥序列进行逐位模2相加。解密过程则是把密文序列与等长的密钥序列进行逐位模2相加。
- 序列密码的安全性主要依赖于密钥序列。序列密码的优点：处理速度快，实时性好；错误传播小；适用于军事、外交等保密信道。其缺点如下：明文扩散性差；需要密钥同步。



4.1.3 密码体制的分类

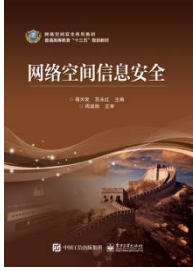
- 分组密码用一个固定的变换对等长明文分组进行处理，加密过程是将明文序列以固定长度进行分组，每组明文用相同的密钥和加密函数进行运算。为了减少存储量和提高运算速度，加密函数的复杂性成为系统安全的关键。加密函数重复地使用代替和置换两种基本的加密变换。
- 分组密码的优点如下：明文信息具有良好的扩散性；不需要密钥同步；较强的适用性。其缺点如下：加密速度慢；错误易扩散和传播。



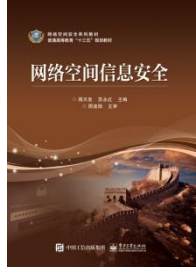
4.2 对称密码体系

- 4.2.1 古典密码体制
- 4.2.2 初等密码分析破译法
- 4.2.3 流密码的基本概念
- 4.2.4 分组密码概述
- 4.2.5 分组密码工作模式
- 4.2.6 数据加密标准
- 4.2.7 高级加密标准

4.2 对称密码体系



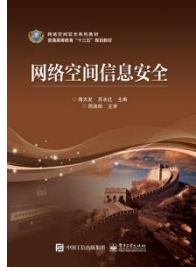
- 对称密码体是指采用的解密算法就是加密算法的逆运算，而加密密钥也就是解密密钥的一类加密体制。
- 它常用来加密带有大量数据的报文和文卷通信的信息，因为这两种通信可实现高速加密算法。
- 该体制的主要特点是发送者和接收者之间的密钥必须安全传送，而双方用户通信所用的密钥也必须妥善保管。
- 该体制的主要类型代表包括古典密码体制替代与置换密码法、近现代密码体制中的对称密码体制DES（数据加密标准）、AEA（高级加密标准）和非对称密码体制的RSA算法等。



4.2.1 古典密码体制

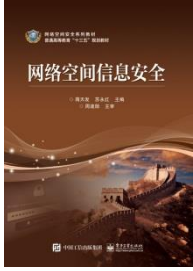
- 1. 替代密码法
- 替代（Permutation）密码法（或称代换密码法）有单字母密码法和多字母密码法两种。替代密码就是将明文字母表中的每个字符替换为密文字母表中的字符。这里对应密文字母可能是一个，也可能是多个。接收者对密文进行逆向替换即可得到明文。

4.2.1 古典密码体制

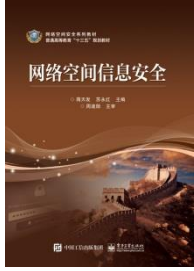


- 1）单字符单表代换密码
- 凯撒密码是单表替代密码的经典算法。设明文为x，密文为y，加密变换是e，解密变换是d，26个字母中a用数字0代替，z用数字25代替，不区分大小写，那么凯撒密码可以表示如下。
- 加密： y=e(x) = (x+3)mod 26。
- 解密： x=d(Y) = (y+26-3)mod 26。

4.2.1 古典密码体制



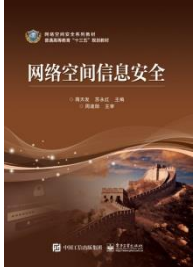
- 这种方法就是将明文字母表中的一个字符对应密文表中的一个字符。这是所有加密中最简单的方法。例如，移位映射法：将加密字母表字母向后移动几个字母后，与原字母表麦对应。例如，（原字母表中）A→（加密字母表中）F，B→G，C→H，D→I，W→B，X→C，Y→D，则原来的字符A，B，C，D，…，W，X，Y转换为加密字符F，G，H，I，…，B，C，D。另外一种是倒映射法：将加密字母表，用原字母表的倒排，与原字母表对应，即原来的字符A，B，C，D，…，W，X，Y转换为加密字符Z，Y，X，W，…，D，C，B。
- 当年凯撒大帝行军打仗时用这种方法进行通信，凯撒密码主要特征是简单易行。



4.2.1 古典密码体制

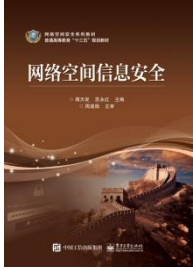
- 2）多字符多表代换密码
- 这种方法就是以一系列（两个以上）代换表依次对明文消息的字母进行代换的加密方法。该技术使用多个不同的单字母代换来加密明明文消息，它具有以下特征：使用一系列相关的单字母代换规则；由一个密钥来选取特定的单字母代换。
- 例如，使用有5个简单代替表的代替密码，明文的第一个字母用第一个代替表，第二个字母用第二个表，第三个字母用第三个表，以此类推，循环使用这5张代替表。多表代替密码由莱昂•巴蒂斯塔于1568 年发明，著名的维吉尼亚密码和博福特密码均是多表代替密码。

4.2.1 古典密码体制



- 最著名、最简单的一种算法是Vigenere密码。该密码由 26个凯撒密码组成，其位移从0到 25。每个密码由一个密钥字母表示，该密钥字母是代替明文字母的。因此，一个位移为3的凯撒密码由密钥值d代表。在使用该密码进行加解密时，通常需要构造一个Vigenere表格，如表4.1所示。26个密文表的每一个都是水平排列的（行），每个密文的左侧为其密钥字母；对应明文的一个字母表从顶部向下排列。

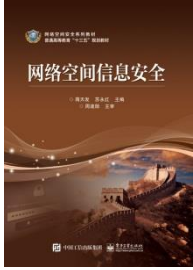
4.2.1 古典密码体制



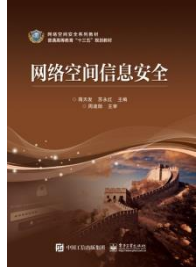
■ 表4.1 Vigenere表格

	明文字母																								
	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
a	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
b	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	A
c	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
d	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
e	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
f	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
g	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
h	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
i	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
j	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
k	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
l	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
m	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
n	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
o	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
p	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
r	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
s	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
t	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
u	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
v	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
w	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
x	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
z	Z	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

4.2.1 古典密码体制



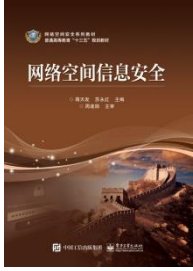
- 其加密过程如下：给定一个密钥字母x和一个明文字母Y，则密文字母位于x行和Y列的交叉点上，此时密文为V。当具体加密一个消息时，需要一个与消息同样长的密钥。通常，该密钥为一个重复关键词。例如，如果某关键词是deceptive，消息是“we are discovered save yourself”，那么
- 密钥：deceptivedeceptivedeceptive。
- 明文：wearediscoveredsaveyourself。
- 密文：ZICVTWQNGRZGVTWAVZHCQYGLMGJ。
- 解密也同样简单，密文字母所在的行的位置决定列，该明文字母位于该列的项部。
- 该密码的强度在于每个明文字母由多个密文字母对应，每个明文字母对应于该关键词的每个独特的字母，因此，该字母的频率信息是模糊的。



4.2.1 古典密码体制

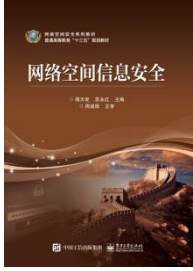
- 2. 置换密码法
- 置换密码就是明文字母本身不变，根据某种规则改变明文字母在原文中的相应位置，使之成为密文的一种方法，又称为换位密码法。换位一般以字节（一个字母）为单位，有时也以“位”为单位。

4.2.1 古典密码体制



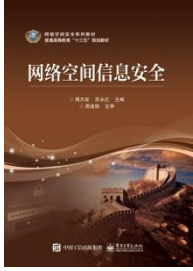
- 一种应用广泛的置换密码是将明文信息按行的顺序写入，排列成一个m×n矩阵，空缺的位用字符“j”填充。再逐列读出该消息，并以行的顺序排列。列的读出顺序为密码的密钥。这里给出以下示例。
- 密钥： 3 4 2 1 5 6 7
- 明文： a t t a c k p
- o s t p o n e
- d u n t i l t
- w o a m x y z
- 密文：TTNAAPTMTSUOAODWCOIXKNLYPETZ

4.2.1 古典密码体制

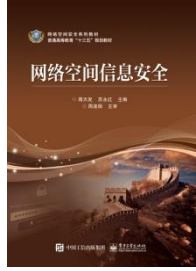


- 一次置换密码容易识别，因为它具有与原明文相同的字母频率，必须进行多次置换，置换过程与第一次相同，经过多次置换后，该密码的安全强度具有较大改善。
- 以上各种加密方法，单独使用比较简单，但很容易被攻破。在实际加密中，通常将其中的两个或两个以上的方法结合起来，形成综合加密方法。经过综合加密的密文，具有很强的抗分析能力。
- 在古典密码中，无论是置换密码还是替代密码都是相对简单的密码体制，但其原理与近代密码相似，为近代密码设计奠定了很好的基础。

4.2.2 初等密码分析破译法

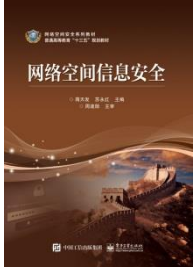


- 密码破译是利用计算机硬件和软件工具，从截获的密文中推断出原来明文的一系列行动的总称，又称为密码攻击。
- 密码攻击可分为被动攻击和主动攻击两类。仅对截获的密文进行分析而不对系统进行任何篡改的行为，称为被动攻击，如窃听；
- 当密码破译后，采用删除、更改、增添、重放、伪造等方法向密文中加入假消息的行为，称为主动攻击。
- 被动攻击的隐蔽性更好，难以发现，但主动攻击的破坏性很大。



4.2.2 初等密码分析破译法

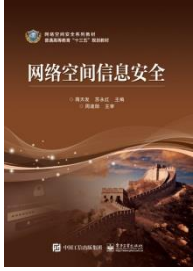
- 1．破译密码的基本方法
- 通常情况下密码破译中有一个假设，即假定密码破译者拥有所有使用算法的全部知识，密码体制的安全性仅依赖于对密钥的保护。或者，密码破译者除了不知道密钥之外，其有可能了解整个密码系统。密码攻击的方法有分析破译法和穷举破译法两类。



4.2.2 初等密码分析破译法

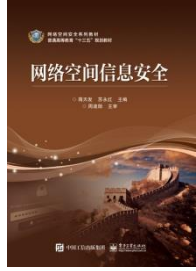
- （1）密码分析破译法：网络空间信息的密码分析破译法有统计性与确定性两种。
- 密码统计性分析破译法是利用明文的已知统计规律进行破译的方法。密码破译者对截获的密文进行统计分析，总结出其中的统计规律，并与明文的统计规律进行对照比较，从中提取出明文和密文之间的对应或变换信息。密码分析之所以能够破译密码，最根本的是依赖于明文中的冗余度。
- 密码确定性分析破译法利用一个或几个已知量（如已知密文或明密文对）用数学关系式表示出所求未知量。已知量和未知量的关系视加密和解密算法而定，寻求这种关系是密码确定性分析破译法的关键步骤。

4.2.2 初等密码分析破译法



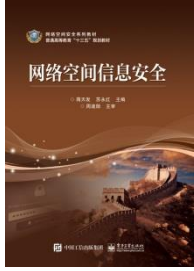
- （2）穷举破译法，又称强力破译法或完全试凑破译法，它对截获的密报依次用各种可能的密钥试译，直到得到有意义的明文；或者在不改变密钥的情况下，对所有可能的明文加密直到得到的密文与截获的密文一致时为止。只要有足够多的计算时间和存储容量，原则上讲穷举破译法总是可以成功的。但任何一种能保障安全要求的实用密码都会设计的使这一方法在实际上是不可行的，如破译成本太高或花费时间太长。

4.2.2 初等密码分析破译法



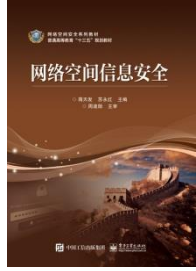
- 2．密码分析破译的等级
- 根据密码分析破译者对明文与密文掌握的程度，密码攻击者主要分为以下4个等级。
- （1）唯密文攻击，密码分析破译者仅根据截获的密文进行的密码攻击。
- （2）已知明文攻击，密码分析破译者已经掌握了一些相应的明文与密文对，据此对加密系统进行的攻击。

4.2.2 初等密码分析破译法



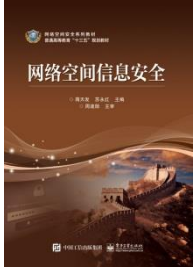
- （3）选择明文攻击。密码分析破译者可以选择一些明文，并可取得相应的密文，这就意味着攻击者已经掌握了装有加密密钥的加密装置（但无法获得解密装置里的密钥），并且可使用任意的密文做解密试验，这对密码分析破译者而言是很理想的。例如，在公开密钥密码体制中，分析破译者可以用公开密钥加密其他任意选择的明文。

4.2.2 初等密码分析破译法

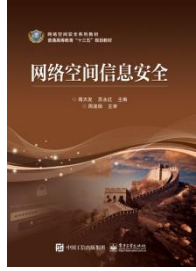


- （4）选择密文攻击。密码分析破译者可以选择一定的密文，并获得对应的明文。例如，在公钥体制中，分析破译者可选择所需的密文，并利用公开密钥对所有可能的明文加密，再与明文对照，最后解密选定的密文。

4.2.3 流密码的基本概念

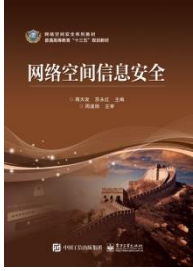


- 1 概述
- 单钥密码体制是加密和解密使用单一的相同密钥的加密制度。即使不相同，也可以由一个推导出另一个。通信时A、B双方必须相互间交换密钥，当A需要发送信息给B时，A用自己的加密密钥进行加密，而B在接收到数据后，用A的密钥进行解密。这样，在双方交换数据的时候，还需要有一种非常安全的方法来传输密钥。



4.2.3 流密码的基本概念

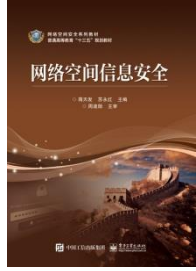
- 常见的单钥密码体制有两种加密法：一是分组密码算法，即把明文消息分组（含有多个字符），逐组进行加密；二是流密码算法，即明文按字符（如二元数字）逐位加密。单钥密码体制不仅可用于数据加密，也可用于消息的验证。



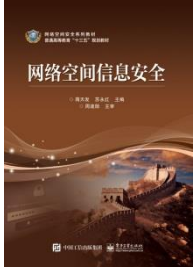
4.2.3 流密码的基本概念

- 流密码，即明文的位串（Bit Stream）与伪随机数产生器（Pseudo Random Number Generator）产生的伪随机序列经过适当运算得到密文。流密码是对称密码算法的一种，也称为序列密码。人们认为流密码算法为1个位的分组加密算法（Block Cipher）。其主要缺点在于若一个伪随机序列发生错误便会使整个密文发生错误，致使解密过程无法还原为明文。但也可视其为优点，即相同的明文位串可有不同的密文位串。由此可知，流密码算法是一种记忆性组件（Memory Device），即前后的伪随机序列可互相影响。

4.2.3 流密码的基本概念

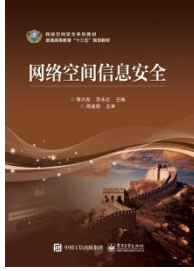


- 2 自同步流密码
- 自同步序列密码—密钥流的每一位是前面固定数量密文位的函数，也称为密文自动密钥。该算法的密码复杂性在于输出函数，它收到内部状态后生成密钥序列位。因为内部状态完全依赖前面n个密文位，所以解密密钥流发生器在收到n个密文位后自动与加密密钥流发生器同步。



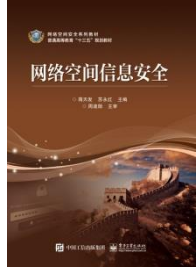
4.2.3 流密码的基本概念

- 2 自同步流密码
- 在该模式的智能化应用中，每个消息都以随机的n位报头开始。这个报头被加密、传输、解密，在n位密文之前整个解密是不正确的，直到之后两个密钥流发生器同步。
- 自同步密码的缺点是错误扩散。传输中有一个密文位被篡改，解密密钥流发生器就有n位密钥流位不能正确生成。因此，一位密文错误就会导致n位相应的明文错误，直到内部状态里面不再有该错误位。



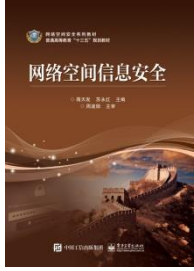
4.2.3 流密码的基本概念

- 3 同步流密码
- 在同步流密码中密钥流是独立于消息流而产生的，也称之为密钥自动密钥。加密端密钥流发生器一位接一位地“吐”出密钥，在解密端的另一个发生器上产生完全相同的密钥。若其中一个发生器跳过一个周期或者一个密文位在传输过程中丢失了，那么错误后面的每一个密文字符都不能正确解密。



4.2.3 流密码的基本概念

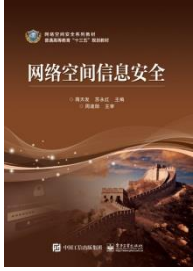
- 3 同步流密码
- 如果错误发生了，发方和收方就必须在继续进行之前使两个密钥发生器重新同步，以保证密钥流的任意部分不会重复，重新设置发生器回到前一个状态。其优点是同步密码并不扩散传输错误。如果有一位在传输中改变了（比丢失一位可能性大得多），那么只有该位不能正确解密，所有进程和结果都不会受影响。



4.2.4 分组密码概述

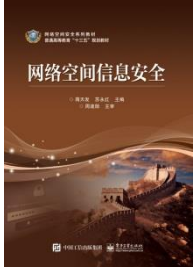
- 传统的密码体制中，明文中所改变一个字母对应在密文中也改变了一个字母，密文中给定的一个字母恰好来自于明文中的同一个字母，这通过频率分析就非常容易发现密钥。使用字母的分组体制，对应了密钥的长度，利用频率分析要困难些，但仍然是可能的，毕竟每组中的各个字母没有相互作用。分组密码避免了这些问题，因为它同时加密几个字母或数字的分组。改变明文分组的一个字符，就可能改变与之相对应的密文分组潜在的所有字符。

4.2.4 分组密码概述



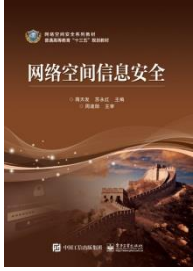
- 现代密码体制的很多方法都属于分组密码的范畴，如DES方法是基于64比特的分组，AES使用128比特的分组，RSA使用几百比特长的分组，取决于模数的使用，所有这些分组的长度都足够长，能有效地防止类似频率分析这样的攻击。

4.2.5 分组密码工作模式



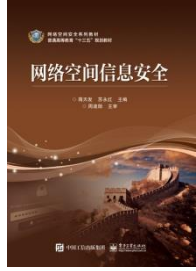
- 分组密码将消息作为数据分组处理（加密或解密）。一般来讲，大多数消息（也就是一个消息串）的长度大于分组密码的消息长度，长的消息串被分成一系列的连续排列的消息分组，密码机一次处理一个分组。

4.2.5 分组密码工作模式



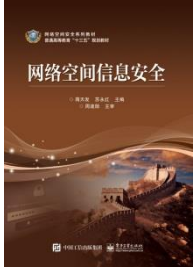
- 人们在设计了基本的分组密码算法之后，紧接着设计了许多不同的运行模式。
- 这里描述3个常用的运行模式，它们是电子密码本（ECB）模式、密码分组链（CBC）模式、密码反馈（CFB）模式。

4.2.5 分组密码工作模式



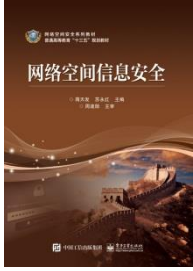
- （1）电子密码本：
- 使用分组密码方式将一长串明文分解成为适当的分组，对每一分组用加密E()函数分别加密，即电子密码本（ECB）操作方式。明文P被分解为$P=[P_1, P_2, P_3,\ldots, P_j]$，其对应的密文是$C=[C_1, C_2, C_3,\ldots, C_i]$，$C_i=E(P_j)$是明文$P_j$使用密钥k加密的结果。

4.2.5 分组密码工作模式



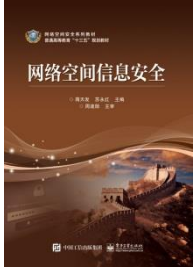
- ECB操作模式固有的缺点在明文很长的情况下变得更明显了，当攻击者长时间地一直观察发送者和接收者之间的通信时，如果攻击者想方设法获得了一些所观察到的明文及相应的密文，攻击者就即可开始建立电子密码本，译出发送者和接收者后续的通信。攻击者不必计算密钥k，只要查看其电子密码本上的密文信息，并用对应明文破解信息即可。

4.2.5 分组密码工作模式



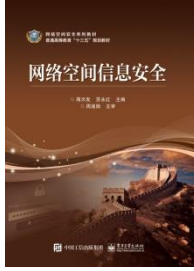
- （2）密码分组链：减少EBC模式存在的问题的一种方法是使用链接。链接是一种反馈机制，一块分组的加密依赖于其前面分组的加密。
- 其加密过程如下：$C_j=E_k(P_j \text{ XOR } C_{j-1})$
- 而解密过程如下：$P_j=D_k(C_j \text{XOR } C_{j-1})$
- Cn是某个选定的初始值，$D_k()$是解密函数，则在CBC模式中，明文和前一分组的密文异或后，再对其结果进行加密。

4.2.5 分组密码工作模式

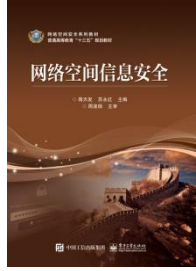


- （3）密码反馈：CBC模式的问题是，即使明文错一位或在计算/存储以前的密文分组中有一点错误，都可能导致密文组的计算错误，将影响所有后续的密文组。前两种方法都有一个共同缺点，即在完整的8字节的数据分组未到来之前，加密/解密是不能开始的。密码反馈（CFB）模式是一种流操作模式，一组8位信息并不需要等待全部的数据分组到达后才能加密。密码反馈（CFB）模式的特点在于反馈相继的密码分段，这些分段从模式的输出返回作为基础分组密码算法的输入。

4.2.6 数据加密标准

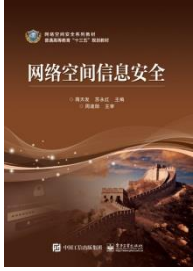


- 单钥密码体制是加密和解密使用单一的相同密钥的加密制度。即使不相同，也可以由一个推导出另一个。通信时A、B双方必须相互间交换密钥，当A需要发送信息给B时，A用自己的加密密钥进行加密，而B在接收到数据后，用A的密钥进行解密。这样，在双方交换数据的时候，还需要有一种非常安全的方法来传输密钥。



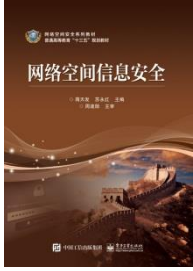
4.2.6 数据加密标准

- 常见的单钥密码体制有两种加密法：一是分组密码，即把明文消息分组（含有多个字符），逐组进行加密；二是流密码，即明文按字符（如二元数字）逐位加密。单钥密码体制不仅可用于数据加密，也可用于消息的验证。



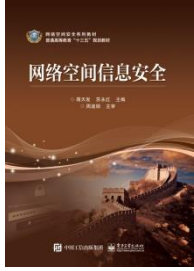
4.2.6 数据加密标准

- 1 概述
- 在1973年，美国国家标准局（NBS）发布了一个公开请求，寻找一个能够成为美国国家标准的加密算法。IBM公司的沃尔特.塔奇曼和卡尔.迈歇尔于1971～1972年研制成功一个算法—LUCIFER。NBS后来将该算法提交给国家安全代理机构，它们重新审阅并对算法做了一些修改，提出了一个版本，即最初的数据加密标准（Data Encryption Standard，DES）算法。
- 1975年NBS公开了DES，即可以自由地使用它，并于1977年1月5日正式确定将它作为美国的统一数据加密标准，并设计推出DES芯片。自此，DES开始在政府、银行、金融界广泛应用。尽管有许多攻击方法试图攻破该体制，但在已知的公开文献中，还是无法完全、彻底地破解DES。



4.2.6 数据加密标准

- 2 DES的工作原理
- DES算法属于分组加密算法，即对一定大小的明文或密文进行加密或解密工作。在DES加密系统中，其每次加密或解密的分组大小均为64位，所以DES无需考虑密文扩充问题。
- 无论明文或密文，一般的数据大小通常大于64位，此时只要将明文或密文中的每64位当一个分组进行分割，再对每一分组做加密或解密即可。
- 当切割后的最后一个分组小于64位时，便在此分组之后附加“0”位，直到此分组大小为64位为止。
- DES所用的加密或解密密钥也是64位，但因其中有8位用来做奇偶校验，所以64位中真正起到密钥作用的只有56位。而DES加密与解密所用的算法除了子密钥的顺序不同外，其他的部分都是相同的。



4.2.6 数据加密标准

- DES全部16轮的加/解密结构如图4.2所示，其上方的64位输入分组数据可能是明文，也可能是密文，由使用者做加密或解密而定。加密与解密的不同只在于最右边的16个子密钥的使用顺序不同，加密的子密钥顺序为K1，K2，K3……K16，而解密的子密钥顺序正好相反，为K16，K15，K14，…，K1。其运算过程如下。

4.2.6 数据加密标准

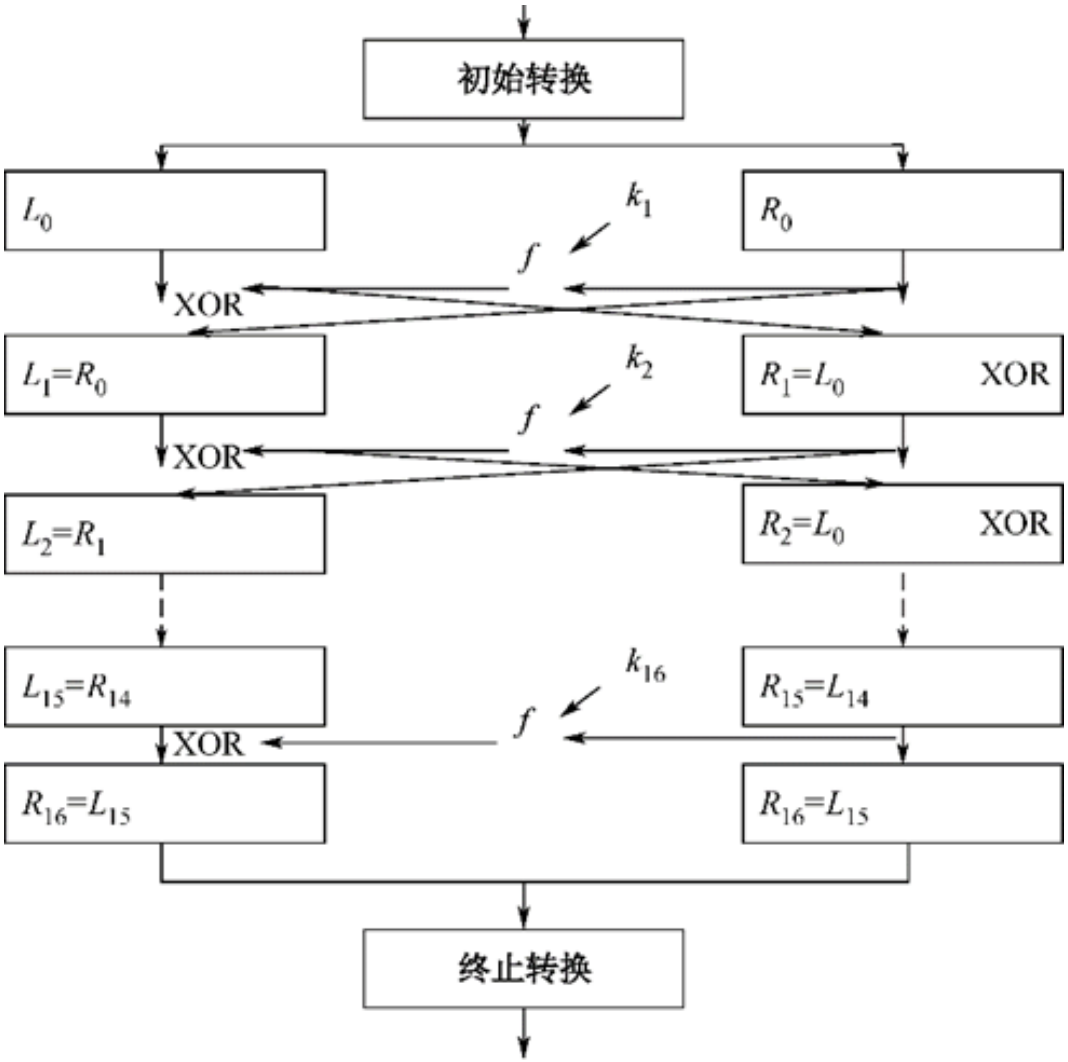
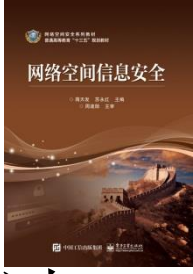


图4.2 DES的加/解密结构



4.2.6 数据加密标准

- （1）加/解密输入分组依表4.2重新排列，通过初始置换来打乱数据的原来的顺序，再分为L_0与R_0两个32位的分组。
- （2）R_0与第一子密钥K_1经函数f运算后，得到的32位输出再与L_0逐位异或（XOR）运算。
- （3）其结果成为下一轮的R_1，R_0则成为下一轮的L_1，如此连续运行16轮。
- 也可用下列两个式子来表示其运算过程：
- $R_i=L_{i-1}$ XOR f (R_{i-1}，K_i)　　$L_i=R_{i-1}$, i=1，2，…，16
- 最后所得的R_{16}与L_{16}不再互换，直接连接成64位的分组，再根据表4.3重新排列次序做终结置换动作，得到64位的输出。

4.2.3 单钥密码体制

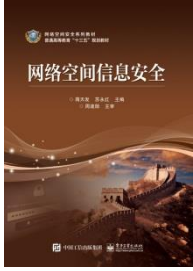
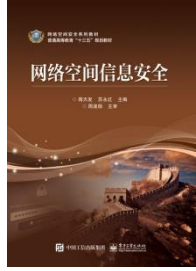


表4.2 加解密输入分组与重排值

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

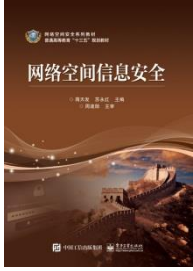
表4.3 终结置换输出值

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25



4.2.6 数据加密标准

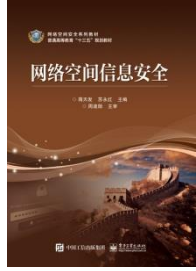
- 3 DES的核心作用
- DES的核心部分是在“S盒函数”f中。正是在这里DES实现了明文消息在密文消息空间上的随机非线性分布。
- 在第i轮，$f(R_{i-1},k_i)$做下面的两个子运算：
- （1）通过逐比特异或运算，将轮密钥k_i与半分组R_{i-1}相加。这提供了消息分布中所需要的随机性。
- （2）在包含8个“代换盒”（S盒）的固定置换下代换（i）的结果，每一个S盒是一个非线性置换函数：这就提供了消息分布中所需的非线性。



4.2.6 数据加密标准

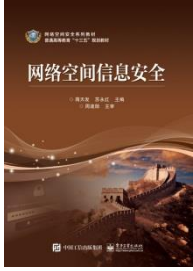
- S盒的非线性对DES的安全是非常重要的，注意到代换密码在一般情况下是非线性的，而移位密码和仿射密码是线性中的子类。与一般情况相比，这些线性子类不仅极大地减小了密钥空间，而且也导致了生成的密文对于差分分析（DC）技术是非常脆弱的。

4.2.6 数据加密标准

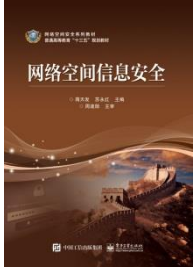


- 下面以仿射密码式$m_i=D_{ki}(c_i)$为例分析这种攻击。假设攻击者以某种方式知道了差分m-m’，但他既不知道m也不知道m’，给定相应的密文$c=k_{1m}+k_2(\mathrm{mod}N)$，$c'=k_1m'+k_2(\mathrm{mod}N)$，攻击者可以计算
- $k_1=(c-c')/(m-m')(\mathrm{mod}N)$

4.2.6 数据加密标准

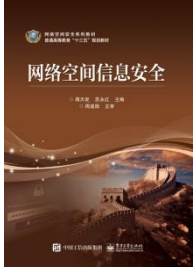


- 4 DES的安全性
- 随着技术不断发展，人们使用两种方法来进一步增加了DES的安全性。一是多次使用DES，称之为三重DES；二是寻找新的体制，要求远多于56位的密钥。
- 三重DES的设计思想是使用同样的算法，用不同的密钥加密二次相同的密文。
- 双重加密是第一次用一个密钥加密明文，然后使用不同的密钥加密一次。虽然已证明双重加密设计事实上具有57位密钥等级的安全性，但使用中间相遇攻击，密钥空间会从2112减少到257。
- 因为双重DES的固有弱点，常用的是三重DES，它具有近似等于112位密钥的加密级别的安全性。



4.2.7 高级加密标准

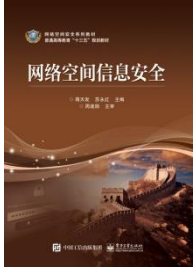
- 1) 概述
- 在1997年4月15日，美国国家标准和技术委员会发起征集高级加密标准（Advanced Encryption Standards，AES）算法的活动，并专门成立了AES工作组，以寻找DES的替代品，条件是新的加密算法必须允许128、192、256位密钥长度，它不仅能够在128位输入分组上工作，还能够在各种不同的硬件上工作，速度和密码强度同样也要被重视。
- 1998年，加密委员会对15种候选算法进行评定，最后选择出5种，分别是IBM的MARS算法，RSA实验室的RC6算法，Joan Daemen和Vincent Rijmen的Rijndael算法，Ross Anderson、Eli Biham和Lars Knudsen的Serpent算法，以及Bruce Schneier、John Kelsey、Doug Whiting和David Wagner的Twofish算法。
- 最后，Rijndael被选作取代DES的新加密标准，这就是高级加密标准。



4.2.7 高级加密标准

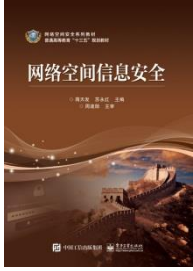
- 2）加密算法
- 首先将Rijndael算法密钥长度限制为128位，算法过程由10轮循环组成，每一轮循环都有一个来自于初始密钥的循环密钥。每一轮循环输入的是128位，产生的输出也是128位。
- 每一循环由4个基本步骤组成，称之为层。
- （1）字节转换（The ByteSub Transformation）：一个非线性层，目的是防止微分和线性密码体制的攻击。
- （2）移动行变换（The ShiftRow Transformation）：这一步是线性组合，可以导致多轮循环各个位间的扩散。
- （3）混合列变换（The MixColumn Transformation）：与行变换目的是相同的。
- （4）加循环密钥（Add Round Key）：循环密钥同上层结果进行异或运算。

4.2.7 高级加密标准

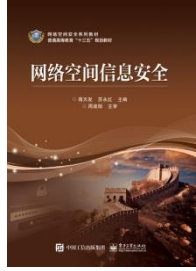


- 循环后就是
- →字节（BS）→移动行（SR）→混合列（MC）→加循环密钥（ARK）→
- 其中，ARK使用的是初始密钥；BS、SR、MC、ARK共循环9次，分别使用1～9个循环密钥。但最后一个即第10个循环用到BS、SR、ARK，但未用到MC，其128位的输出是一个密文分组。

4.2.7 高级加密标准

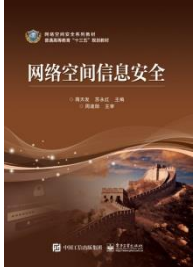


- 3）解密算法
- 解密的每一步骤是加密过程中字节转换、移动行、混合列和加循环密钥的相反过程。
- （1）字节转换的逆是另一种查找表，我们称之为逆字节转换（InvByteSub）。
- （2）其逆过程是用循环右移代替循环左移，得到逆移动行（InvShiftRow）。
- （3）混合列的逆的存在，因为混合列中所用的4×4矩阵是可逆的，即逆混合列（InvMixColumn）。
- （4）加循环密钥就是它自身的反序。
- 所以，解密本质上和加密有相同的结构，但除了第一步和最后一步之外，字节转换、移动行和混合列被它们的逆替换，加循环密钥被逆加循环密钥替换。循环密钥使用起来应该颠倒顺序，所以第一个加循环密钥使用第10个循环的密钥，最后一个加循环密钥（ARK）使用第0个循环的密钥。



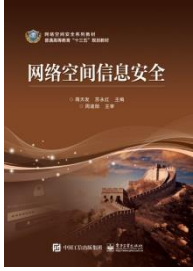
4.3 非对称密码体系

- 4.3.1 RSA算法
- 4.3.2 其他公钥密码体系
- 4.3.3 网络通信中三个层次加密方式



4.3 非对称密码体系

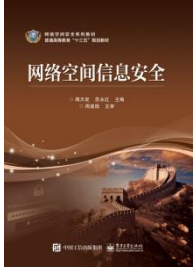
- 4.3.1 RSA算法
- 1. 概述
- RSA体制是1978年由美国麻省理工学院Rivest、Shamir和Adleman三位教授首先提出的一种基于因子分解的指数函数的单向陷门函数，也是迄今为止理论上最为成熟完善的一种公钥密码体制。而最初由Diffie和Hellman在其论文中所提出的这种公开密钥密码体制（Public Key Cryptoasystem），并没有在实际中应用。



4.3 非对称密码体系

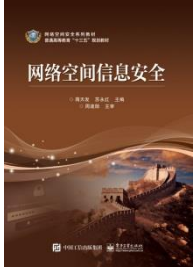
- 2．密钥生成
- （1）用户任意选择两个大素数p及q，并求出其乘积N=p*q。
- （2）任选一整数e，使得e与N互素，即GCD（e，Ø（N））=1为加密密钥，并求出e在阶T中的乘法逆元d，即e*d =1 mod T。根据欧拉定理，指数函数在模N中所有元素阶的最小公倍数T=ln（p-1, q-1），即T等于p-1与q-1的最小公倍数，一般均使用T=（p-1）（q-1）= Ø（N）。
- （3）将（e，N）公布为公开密钥，并将d秘密保存为私有密钥。p与q可以毁去，以增加其安全性。

4.3 非对称密码体系

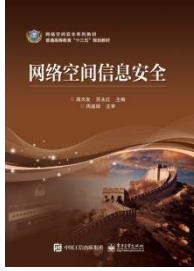


- 例4.2 若p＝13而q=31，而e=7，d是多少？公钥是多少？私钥是多少？
- 解： N = p * q = 403
- T =（p-1）*（q-1）= 360
- 因为　　e * d = 1 mod T,
- 所以　　7 * d = 1 mod 360
- 则　　d = 103
- 公钥是（e，N）=（7,403）
- 私钥是（d，N）=（103,403）

4.3 非对称密码体系



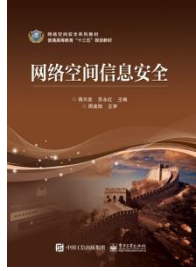
- 要想从公开密钥n和e算出未知的d，只有分解大整数n的因子，但大数分解是一个十分困难的问题。Rivest、Shamir和Adleman用已知最好的算法去估计分解n的时间与n的位数之间的关系，即使用运算速度为100万次/秒的计算机分解500 bit的n，得出分解操作数是1.3×1039，分解时间是4.2 × 1025年。由此可认为RSA保密性能良好。
- 但由于RSA涉及高次幂运算，特别是在加密大量数据时，一般用硬件来代替速度较慢的软件来实现RSA。



4.3 非对称密码体系

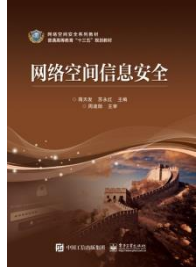
- 3．参数选择
- RSA体制是将安全性基于因子分解的第一个系统。在公开密钥（e，N）中，若N能被因子分解，则在模N中所有元素阶的最小公倍数（即陷门）即可被破解。使得解密密钥d无法保密，整个RSA系统失去安全性。虽无法证明因子分解等于破解RSA系统，但若能分解因子N，即能破解RSA系统；若能破解RSA系统，即能分解因子N。

4.3 非对称密码体系

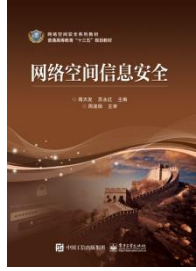


- RSA系统对于公开密钥N的选择是十分非常关键的，需要保证任何人在公开N后无法从N得到T。对于公开密钥e与解密密钥d，也需要有所限制，否则会导致RSA系统被攻破或在密码协议上不安全。选择参数直接影响到整个系统的安全，常用的参数选择的注意要求如下。

4.3 非对称密码体系



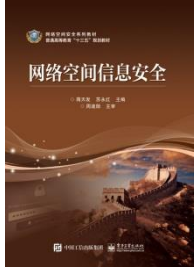
- （1）p及q应大到使得因子分解N在计算上不可能。
- 若能因子分解N，则RSA能被破解。因此p及q的长度必须大到使因子分解N为计算上不可能，由于因子分解问题为密码学最基本的难题之一，但其算法已有较快的进步。
- （2）p和q的差需很大（差几个位以上）。



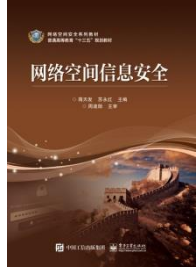
4.3 非对称密码体系

- （3）p-1与q-1的最大公因子应很大。
- 若p-1及q-1的最大公因子很小，Simmons及Norris证明RSA可能在不需要因子分解N的情况下即被攻破。
- （4）e不可以太小。
- 在RSA的系统中，每人的公开密钥e，只要满足GCD（e，Ø（N））=t，即e可任意选择。为加速加密运算时间，建议e尽可能小（如选择e=3），以加速加密运算及降低存储公开密钥的空间。但当e太小时，有以下的缺点。
- 密文C=M3 mod N，若M3< N，则在加密中无模N的动作，因此C仅为立方数，便可轻易将G开立方得到M。

4.3 非对称密码体系

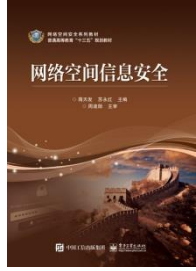


- （5）秘密密钥d应大于N/4
- 一般使用位数较短的秘密密钥d来降低解密的时间，但解密密钥d的长度减少后会使RSA变得不安全。若d长度太小，可利用已知明文M加密后得C= Me mod N再直接猜出d，求出Cd mod N是否等于M。若是，则d正确，否则继续猜测d。若d的长度很小，则此猜测d的空间变小，猜对的概率相对增大。所以d的长度不能太小。



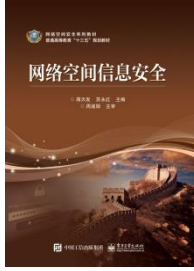
4.3.2 其他公钥密码体系

- 1. Diffie-Hellman公钥体制
- Diffie-Hellman公钥分配密码体制是斯坦福大学的W. Diffie与M. E. Hellman教授于1976年设计的：令P是大素数，且P-1有大素数因子，选g为模P的一个原根。使用过程如下：A欲与B通信，首先用明文形式与B接通，然后A任选正整数xA<=p-2作为密钥，计算gxA发送给B，B将gxB发送给A。A和B分别得到gxAB，A和B拥有共同的密钥。这种公钥分配体制的安全性是基于有限域上的离散对数问题的困难性，所以具有很高的安全性。



4.3.2 其他公钥密码体系

- 2. Elgamal公钥体制
- Elgamal是一种基于离散对数的公钥密码体制。由于Elgamal公钥密码体制的密文不仅依赖于待加密的明文，还依赖于随机数k，所以用户选择的随机参数不同，便能够使加密相同的明文时得出不同的密文。由于这种概率加密体制是非确定性的，所以在确定性加密算法中，若破译者对某些关键信息感兴趣，则可事先将这些信息加密后存储起来，一旦以后截获密文，就可以直接在存储的密文中查找，从而得到相应明文。概率加密体制弥补了其不足，提高了安全性。



4.3.2 其他公钥密码体系

- 3．Merkle-Hellman公钥体制
- 大多数公钥密码体制会涉及高次幂运算，不仅加密速度慢，还会占用大量的存储空间。1978年，Merkle和Hellman提出第一个背包体制，背包体制的特性是其加解密的速度非常快（可高达700kb/s以上），因此引起许多研究学者的兴趣。但背包系统的安全度始终为人所怀疑，因为其易解背包的结构似乎可提供某些信息给破译者，所有KPKC均为线性保密系统。因此，MH KPKC从未被实际考虑应用过。

4.3.3 网络通信中三个层次加密方式

- 在网络空间信息传输中，一般的数据加密可以在网络通信的三个层次来实现：链路加密、结点加密和端到端加密。

4.3.3 网络通信中三个层次加密方式

- 1．链路加密
- 链路加密又称在线加密（位于OSI网络层以下的加密）。在采用链路加密的网络中，每条通信链路上的加密是独立实现的。通常对每条链路使用不同的加密密钥。当某条链路受到破坏时，就不会导致其他链路上传送的信息被分析出。加密算法常采用序列密码。链路加密的最大缺点是在中间结点暴露了信息的内容。在网络互连的情况下，仅采用链路加密是不能实现通信安全的。

4.3.3 网络通信中三个层次加密方式

- 因为，对于链路加密所有消息在被传输之前进行加密，在每一个结点对接收到的消息进行解密，然后先使用下一个链路的密钥对消息进行加密，再进行传输。在到达目的地之前，一条消息可能要经过许多通信链路的传输。由于在每一个中间传输结点消息均被解密后重新进行加密，因此，包括路由信息在内的链路上的所有数据均以密文形式出现。这样，链路加密就掩盖了被传输消息的源点与终点。

4.3.3 网络通信中三个层次加密方式

- 由于填充技术的使用以及填充字符在不需要传输数据的情况下进行加密，这使得消息的频率和长度特性得以掩盖，从而可以防止对通信业务进行分析。

4.3.3 网络通信中三个层次加密方式

- 在质量不好的线路中传输，或者信号经常不通的海外或卫星网络中，链路上的加密设备需要频繁地进行同步，带来的后果是数据丢失或重传。另一方面，即使仅一小部分数据需要进行加密，也会使得所有传输数据被加密。 在一个网络结点，链路加密仅在通信链路上提供安全性，消息以明文形式存在，因此所有结点在物理上必须是安全的，否则就会泄漏明文内容。

4.3.3 网络通信中三个层次加密方式

- 2．结点加密
- 网络空间结点加密在网络的结点处采用一个与结点机相连的密码装置，密文在该装置中被解密并重新加密。
- 在网络空间中，结点加密能给网络数据提供较高的安全性，但它在操作方式上与链路加密是类似的，两者均在通信链路上为传输的消息提供安全性；都在中间结点先对消息进行解密，然后进行加密。

4.3.3 网络通信中三个层次加密方式

- 因为要对所有传输的数据进行加密，所以加密过程对用户是透明的。然而，与链路加密不同，结点加密不允许消息在网络结点以明文形式存在，它先把收到的消息进行解密，然后采用另一个不同的密钥进行加密，这一过程是在结点上的一个安全模块中进行的。

4.3.3 网络通信中三个层次加密方式

- 网络空间链路加密与结点加密比较：
- 链路加密是传输数据仅在物理层前的数据链路上进行加密的，接收方是传送路径上的各台结点机，信息在每台结点机内都要被解密和再加密，依次进行，直至到达目的地。
- 结点加密能给网络数据提供较高的安全性，但是，它在操作方式上与链路加密是类似的，两者均在通信链路上为传输的消息提供安全性，都在中间结点上先对信息进行解密，然后进行加密，因为要对所有的传输数据进行加密，所以加密过程对用户是透明的。

4.3.3 网络通信中三个层次加密方式

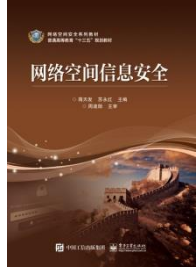
- 然而，与链路加密不同，结点加密不允许信息在网络结点上以明文形式存在，它先把收到的消息进行解密，然后采用另一个不同的密钥进行加密，这一过程是在结点上的一个安全模块中进行的。结点加密要求报文和路由信息以明文形式传输，以便中间结点得到如何处理消息的信息。因此，这种方法对于防止攻击者分析通信业务是脆弱的。

4.3.3 网络通信中三个层次加密方式

- 3．端到端加密
- 网络空间端到端加密又称脱线加密，位于OSI网络层以上的加密，它允许数据在从源点到终点的传输过程中始终以密文形式存在。端到端加密的主要特点是消息在被传输时到达终点之前不进行解密，因为消息在整个传输过程中均受到保护，所以即使有结点被损坏也不会使消息泄露。

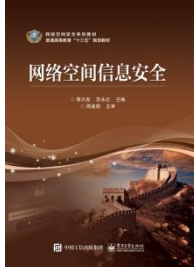
4.3.3 网络通信中三个层次加密方式

- 端到端加密系统通常不允许对消息的目的地址进行加密，这是因为每一个消息所经过的结点都要用此地址来确定如何传输消息。由于这种加密方法不能掩盖被传输消息的源点与终点，因此它对于防止攻击者分析通信业务是脆弱的。



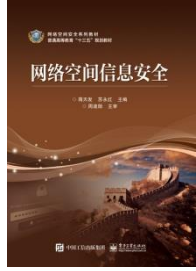
4.4 密码管理

- 1. 密钥生成
- 算法的安全性依赖于密钥，若使用一个弱的密钥生成方法，那么整个体制都是弱的。有56比特的密钥的DES正常情况下任何一个56比特的数据串都能成为密钥，所以共有2^{56}种可能的密钥。



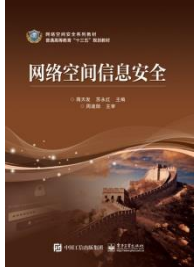
4.4 密码管理

- 人们选择密钥时，通常选择一个弱密钥，即喜欢选择最更容易记忆的密码。
- 最安全的密码体制也帮不了那些习惯用名字作为密钥或者把密钥写下来的人。
- 一个聪明的穷举攻击并不按照数字顺序去试所有可能的密钥，它们首先尝试最可能的密钥。这就是所谓的“字典攻击”，当字典攻击被用作破译密钥文件而不是单个密钥时就显得更加有力。



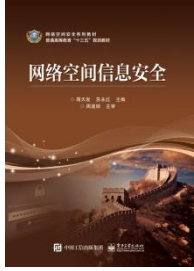
4.4 密码管理

- 2．非线性密钥空间
- 所谓的非线性密钥空间，即假定能将选择的算法加入到一个防篡改模块中，要求有特殊保密形式的密钥，则其他的密钥都会引起模块使用非常弱的算法来加解密，即可使那些不知道这个特殊形式的人不可能偶然碰到正确的密钥。所有密钥的强壮程度并不相等。



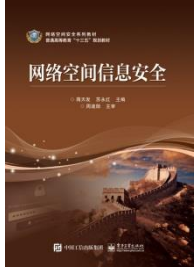
4.4 密码管理

- 非线性密钥空间可按照密钥本身和用该密钥加密的某一固定字符串来实现。模块用这个密钥对字符串进行解密；若它收到该固定的字符串，便能正常地解密，否则用另一个非常弱的算法来进行解密。若该算法有一个128比特的密钥和一个64比特的字符块，即总密钥长度为192比特，则共有有效密钥2128个，且随机选择好密钥的概率为1/264。



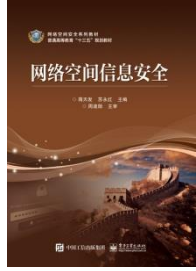
4.4 密码管理

- 3．发送密钥
- 当采用对称加密算法进行保密通信时需要同一密钥。发送者使用随机密钥发生器生成一个密钥，必须安全地送给接收者。
- 发送者须通过安全信道将密钥副本交给接收者，否则就会出现问题。系统使用被公认安全的备用信道，发送者可以通过一个可靠的信道把密钥传送给接收者，或者同接收者一起建立另一个希望无人窃听的通信信道。



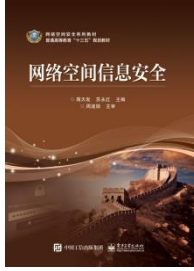
4.4 密码管理

- 发送者可通过其加密的通信信道把对称密钥送给接收者。但因为如果信道能够保证加密，那么在同一个信道上明文发送加密密钥就会导致在该信道上的窃听者都能破解全部通信。
- 其解决方法是将密钥分成许多不同的部分，然后用不同的信道发送。即使截获者能收集到密钥，但由于不够完整，截获者仍不知密钥，所以此方法可用于除个别特殊情况外的任何场合。



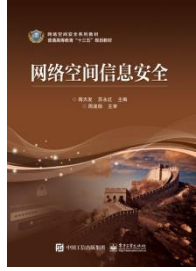
4.4 密码管理

- 4．验证密钥
- 当接收者收到密钥时，需要判断是发送者传送还是其他人伪装发送者传送的，判断规则如下。
- （1）如果发送者通过可靠的信道传送密钥，接收者必须相信信道。
- （2）如果密钥由加密密钥加密，接收者必须相信只有发送者才拥有的加密密钥。
- （3）如果发送者运用数字签名协议来给密钥签名，那么当接收者验证签名时就必须相信公开密钥数据库。
- （4）如果某个密钥分配中心（KDC）在发送者的公钥上签名了，则接收者必须相信KDC的公开密钥副本不曾被更改。



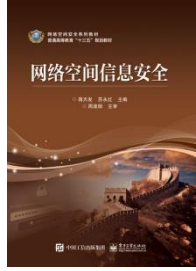
4.4 密码管理

- 密钥在传输中会发生错误，大量的密文无法解密，所以密钥都必须含有检错和纠错位。密钥在传输中的错误就会很容易地被检查出来，若需要密钥还可被重传。



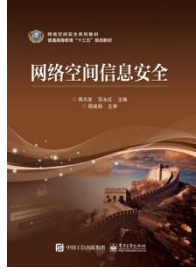
4.4 密码管理

- 5. 更新密钥
- 若要定期改变加密数据链路的密钥，可采用从旧密钥中产生新密钥的方法，即密钥更新。更新密钥使用单向函数，若发送者和接收者共同使用同一密钥，并用同一个单向函数进行操作，会得到相同的结果，则可以从结果中得到其需要的数据来产生新密钥。



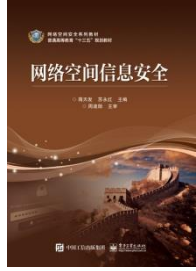
4.4 密码管理

- 6．存储密钥
- 单用户的密钥存储是最简单的密钥存储问题，发送者加密文件以备以后使用，因此只涉及一人，且只有一人对密钥负责。
- 可采用类似于加密密钥的方法对难以记忆的密钥进行加密保存。
- 例如，一个RSA私钥可用DES密钥加密后存在磁盘上，要恢复密钥时，用户只需把DES密钥输入到解密程序中即可。如果密钥是确定性地产生的（使用密码上安全的伪随机序列发生器），每次需要时从一个容易记住的口令产生出密钥会更加简单。理想的情况是密钥永远也不会以未加密的形式暴露在加密设施以外。



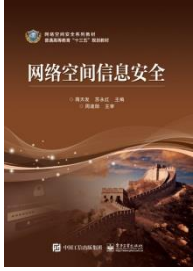
4.4 密码管理

- 7. 密钥有效期
- 加密密钥不能无限期使用，应当在一定期限内自动失效，因为密钥使用时间越长，它泄露的机会就越大；若密钥已泄露，那么密钥使用越久，损失就越大；密钥使用越久，人们花费精力破译它的动力和机会就越多；对用同一密钥加密的多个密文进行密码分析一般比较容易。



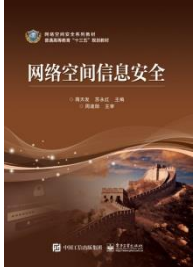
4.4 密码管理

- 8. 公钥密码管理
- 公钥密码使得密钥较易管理，网络上的每个人都只有一个公开密钥。如果发送者想传送一段信息给接收者，则必须知道接收者的公开密钥，可以从接收者、中央数据库、自己的私人数据库处获得。



本章小结

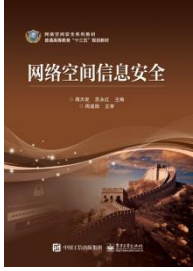
- 加密技术是保护网络空间信息安全的重要手段之一。密码学发展分为3个阶段，即古典密码阶段、近代密码阶段和现代密码阶段。
- 密技术在当代信息化社会中起到了重要的网络空间信息安全与保密作用。密码体系是一切加密技术的核心，密码体制从特点上可分为两大类，即对称密码体系和非对称密码体系。



本章小结

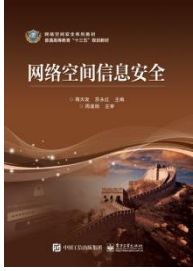
- 单钥密码体制是加密和解密使用相同密钥的加密体制。常见的单钥密码体制有两种加密方法：一是流密码，即明文按字符逐位的加密；二是分组密码，即把明文消息分组，逐组进行加密。单钥密码体制不仅可用于数据加密，还可用于消息的验证。

本章小结



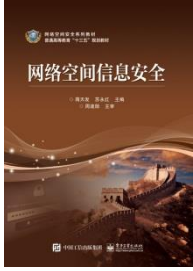
- DES对二元数据进行加密的算法，数据分组长度为64bit，密文分组长度也为64bit，没有数据扩展。RSA公钥加密体制可用一对密钥对多个用户的信息进行加密，而由一个密钥接收解读；反之，以用户专用私钥作为加密密钥，而以公钥作为解密密钥，则可使一个用户加密的消息被多个用户解读。前者可用于保密通信，后者可用于数字签名。由于双钥体制的加密算法是公开的，使得任何人都可以选择明文来攻击双钥体制。

本章小结

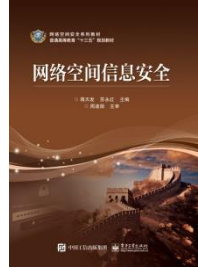


- 多数双钥体制对于选择密文攻击特别敏感。与单钥密码体制加密相比，双钥密码体制加密有许多优点：它没有特殊的发布要求；所需的密钥组合数量很小；可用于数字签名。双钥密码体制的缺点是加密/解密的速度慢得多，且加密/解密累积的时间很长。现代密码体制中常用的还有Diffie-Hellman、Elgamal和Merkle-Hellman公钥体制。密码管理机制的常见步骤有生成密钥、发送密钥、更新密钥、验证密钥、存储密钥。

习题与思考题



- 4.1 叙述以下密码术语的含义：密码学；密码破译；信源；信宿；明文；密文；加密；解密；密钥；密码体制。
- 4.2 古典密码体制中有哪些具体密码法？现代密码的设计还离不开它们的基本思想。
- 4.3 明文为China，用凯撒密码求密文。
- 4.4 比较单钥密码体制与双钥密码体制，试述其本质区别以及其优缺点。
- 4.5 说明序列密码体制与分组密码体制的区别。



- 谢谢！