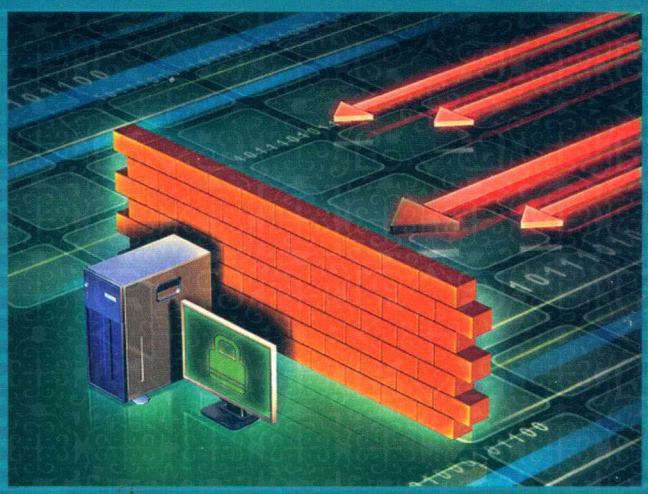
“十三五”普通高等教育规划教材

信息安全技术与实践

李春艳　王　欣　主　编
傅锦伟　李　瑞　张建美　副主编



提供电子课件
http://www.cmpedu.com

机械工业出版社
CHINA MACHINE PRESS

“十三五”普通高等教育规划教材

信息安全技术与实践

李春艳　王　欣　主编
傅锦伟　李　瑞　张建美　副主编

机械工业出版社

本书按照信息安全基础理论、系统与数据库安全、网络安全技术、应用安全技术及新技术的层次结构组织教学内容，突出信息安全领域的实用技术。内容包括密码学、认证与访问控制技术、操作系统与数据库安全、备份与恢复技术、网络安全技术、应用安全技术、信息安全管理与法律法规、信息安全新技术、基础与系统安全实验、网络安全实验和应用安全实验。在强调基础理论和工作原理的同时，注重信息安全实践技能。每章配有习题，帮助读者进行深入学习。

本书概念清晰，通俗易懂，所有实验均可在普通计算机上实现，可作为高等院校计算机类专业的教材。

本书配套授课电子课件，需要的教师可登录 www. cmpedu. com 免费注册，审核通过后下载，或联系编辑索取（QQ：2850823885，电话：010-88379739）。

图书在版编目（CIP）数据

信息安全技术与实践/李春艳，王欣主编．—北京：机械工业出版社，2019. 2

“十三五”普通高等教育规划教材

ISBN 978-7-111-63133-0

Ⅰ. ①信… Ⅱ. ①李… ②王… Ⅲ. ①信息安全-安全技术-高等学校-教材 Ⅳ. ①TP309

中国版本图书馆 CIP 数据核字（2019）第 134721 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）

策划编辑：郝建伟 责任编辑：郝建伟 王 荣

责任校对：张艳霞 责任印制：张 博

三河市骏杰印刷有限公司印刷

2019 年 8 月第 1 版 · 第 1 次印刷

184mm×260mm · 16. 75 印张 · 413 千字

0001-2500 册

标准书号：ISBN 978-7-111-63133-0

定价：49. 90 元

电话服务

客服电话：010-88361066

010-88379833

010-68326294

网络服务

机 工 官 网：www. cmpbook. com

机 工 官 博：weibo. com/cmp1952

金 书 网：www. golden-book. com

机工教育服务网：www. cmpedu. com

前　言

随着网络技术的迅速发展，电子商务、电子政务、企业信息化管理逐步走向成熟。这意味着网络技术已渗透到社会各领域，人们对信息和信息系统的依赖程度日益加深。然而在享受它带来便利的同时，各种潜在的安全威胁也随之而来。网络攻击、数据泄露、计算机病毒入侵、系统瘫痪等安全事件频繁发生，重要信息资源遭到蓄意破坏、非法访问、窃听等，这些给国家的安全、经济的发展、社会的稳定造成了极大的威胁。因此，信息安全成为各国共同关注的焦点，信息安全技术是解决安全隐患的主要手段。

本书对信息安全领域的安全技术进行系统全面的介绍，涵盖了信息安全技术的主要内容和新技术，同时增加了实验内容，介绍相关工具软件及信息安全技术实施的具体方法。本书体现了计算机软件技术课程改革的方向。建议授课学时为 36 学时，实验学时为 36 学时。

本书理论部分包含信息安全基础、密码学、认证与访问控制技术、操作系统与数据库安全、网络安全技术、应用安全技术、信息安全新技术等。实验部分主要介绍了基础与系统安全实验、网络安全实验和应用安全实验。每个实验均有详细的操作步骤，读者可按书中所讲内容完成实验。

本书由李春艳负责全书体系结构、内容范围的制定、统稿和编著等组织工作，全书由傅锦伟教授主审。本书共 12 章，其中第 1 章和第 4 章由张建美编写，第 2 章、第 3 章、第 10 章、第 11 章和第 12 章由李春艳编写，第 5 章和第 9 章由李瑞编写，第 6 章和第 7 章由王欣编写，第 8 章由傅锦伟编写，李颖芳和杨志金参与了编写工作。在编写过程中，傅锦伟教授提出了许多宝贵意见，这里表示衷心感谢。

需要本书第 10 章、第 11 章和第 12 章中有关程序和部分实验操作的读者，请到 http://www.cmpedu.com 下载。

由于时间仓促，书中难免存在不妥之处，请读者谅解，并提出宝贵意见。

编　者

目　　录

第1章 绪 论

随着计算机网络技术的成熟，计算机网络应用迅速普及，从而宣告了第三次工业革命浪潮的到来。伴随着我国国民经济信息化进程的推进和信息技术的普及，各行各业对计算机网络的依赖程度越来越高，一旦计算机网络受到攻击，不能正常工作，甚至全部瘫痪，就会使整个社会陷入危机。尤其是互联网广泛应用以来，涉及国际安全与主权的重大问题屡屡发生。因此人们在为信息技术带来巨大利益而欣喜的同时，必须居安思危。

本章主要介绍信息安全概念、信息安全的发展过程、信息安全存在的威胁及信息安全体系结构。

1.1 信息安全概念

在计算机系统中，所有的软件和硬件、所有的文件资料都属于信息。信息安全指秘密信息在产生、传输、使用和存储过程中不被泄露和破坏。

1.1.1 信息及信息安全的定义

1. 信息

“信息”一词在英文、法文、德文、西班牙文中均是 information，我国古代用的是“消息”。信息作为科学术语最早出现在哈特莱（R. V. L. Hartley）于 1928 年撰写的《信息传输》一文中。20 世纪 40 年代，信息论的奠基人香农（C. E. Shannon）明确地给出了信息的定义，此后许多研究者从各自的研究领域出发，给出了不同的定义。

香农认为“信息是用来消除随机不确定性的东西”，这一定义被人们看作经典性定义并加以引用。

控制论创始人诺伯特·维纳（Norbert Wiener）认为“信息是人们在适应外部世界，并使这种适应反作用于外部世界的过程中，同外部世界进行互相交换的内容和名称”，它也被作为经典性定义加以引用。

有经济、管理学家认为“信息是提供决策的有效数据”。

美国著名物理化学家约西亚·威拉德·吉布斯（Josiah Willard Gibbs）创立了向量分析并将其引入数学物理中，使事件的不确定性和偶然性研究找到了一个全新的角度，从而使人类在科学把握信息的意义上迈出了第一步。他认为“熵”是一个关于物理系统信息不足的量度。

有计算机科学家认为“信息是电子线路中传输的信号”。

我国著名的信息学专家钟义信教授认为“信息是事物存在方式或运动状态，以这种方式或状态直接或间接的表述”。

美国信息管理专家霍顿（F. W. Horton）给信息下的定义是：“信息是为了满足用户决策的需要而经过加工处理的数据。”

简单地说，信息是经过加工的数据。或者说，信息是数据处理的结果。广义地说，信息就是消息，一切存在都有信息。对人类而言，人的五官生来就是为了感受信息的，它们是信息的接收器，它们所感受到的一切，都是信息。然而，大量的信息是人们的五官不能直接感受的，人类正通过各种手段，发明各种仪器来感知它们，发现它们。

科学的信息概念可以概括如下：信息是对客观世界中各种事物的运动状态和变化的反映，是客观事物之间相互联系和相互作用的表征，表现的是客观事物运动状态和变化的实质内容。

2. 信息技术

信息技术指在计算机和通信技术支持下用以获取、加工、存储、变换、显示和传输文字、数值、图像及声音信息，包括提供设备和提供信息服务两大方面的方法与设备的总称。它是研究如何获取信息、处理信息、传输信息和使用信息的技术。

信息技术是人类认识自然和改造自然过程中所积累起来的经验、知识、技能和劳动资料有目的的结合过程。

信息技术指“应用在信息加工和处理中的科学，技术与工程的训练方法和管理技巧；上述方法和技巧的应用；计算机与人的相互作用，与人相应的社会、经济和文化等诸种事物。”

信息技术包括信息传递过程中的各个方面，即信息的产生、收集、交换、存储、传输、显示、识别、提取、控制、加工和利用等技术。

广义而言，信息技术指能充分利用与扩展人类信息器官功能的各种方法、工具与技能的总和。这是从哲学上阐述信息技术与人的本质关系。

狭义而言，信息技术指利用计算机、网络、广播电视等各种硬件设备及软件工具与科学方法，对文图声像各种信息进行获取、加工、存储、传输与使用的技术之和。这种定义强调的是信息技术的现代化与高科技含量。本书中的信息技术是指计算机信息方面的技术。

信息技术的应用包括计算机硬件和软件，网络和通信技术，应用软件开发工具等。计算机和互联网普及以来，人们日益普遍地使用计算机来生产、处理、交换和传播各种形式的信息（如书籍、商业文件、报刊、唱片、电影、电视节目、语音、图形、影像等）。

3. 信息安全

所谓信息安全是指防止信息财产被故意地或偶然地非法授权泄露、更改、破坏或使信息被非法系统辨识、控制，即确保信息的保密性、完整性、可用性和可控性。信息安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。在不发生歧义的时候，人们常常将计算机信息安全简称为信息安全。针对计算机信息的存在形式和运行特点，信息安全可以包括操作系统安全、数据库安全、网络安全、病毒防护、访问控制、加密与鉴别等七个方面。

下面列出对信息构成威胁的一些行为。

（1）对可用性的威胁

- 破坏、损耗或污染。
- 否认、拒绝或延迟访问。

（2）对完整性的威胁

- 输入、使用或生成错误数据。

- 修改、替换或重新排序。
- 歪曲。
- 否认。
- 误用或没有按要求使用。

(3) 对保密性的威胁

- 访问。
- 泄露。
- 监视或监听。
- 复制。
- 偷盗。

1.1.2 信息安全的属性

1. 信息安全的目标

无论在计算机存储、处理和应用，还是在通信网络上传输，信息都可能被非法授权访问而导致泄密，被篡改破坏从而导致不完整，被冒充替换而导致否认，也可能被阻塞拦截而导致无法存取。这些破坏可能是有意的，比如“黑客”攻击、计算机病毒感染，也可能是无意的，比如失误的操作、程序错误等。

所有的信息安全技术都是为了达到一定的安全目标，主要包括保密性、完整性、可用性、可控性和不可否认性五个安全目标。

1) 保密性 (Confidentiality) 即保证信息为授权者享用而不泄露给未经授权者。它是信息安全一诞生就具有的特性，也是信息安全主要的研究内容之一。更通俗地讲，就是说未授权的用户不能够获取敏感信息。对纸质文档信息，人们只需要保护好文件，不被非授权者接触即可，而对计算机及网络环境中的信息，不仅要制止非授权者对信息的阅读，还要阻止授权者将其访问的信息传递给非授权者，以致信息被泄露。

2) 完整性 (Integrity) 指防止信息被未经授权地篡改或者损坏。它是保护信息保持原始的状态，使信息保持其真实性。如果这些信息被蓄意地修改、插入、删除等，形成虚假信息将带来严重的后果。

3) 可用性 (Usability) 指授权主体在需要信息时能及时得到服务的能力。可用性是在信息安全保护阶段对信息安全提出的新要求，也是在网络化空间中必须满足的一项信息安全要求。

4) 可控性 (Controllability) 指对信息和信息系统实施安全监控管理，防止非法利用信息和信息系统。

5) 不可否认性 (Non-repudiation) 指在网络环境中，信息交换的双方不能否认其在交换过程中发送信息或接收信息的行为。这是为了防止对以前行为否认的措施。

信息安全的保密性、完整性和可用性主要强调对非授权主体的控制。而对授权主体的不正当行为如何控制？信息安全的可控性和不可否认性恰恰是通过对授权主体的控制，实现对保密性、完整性和可用性的有效补充，主要强调授权用户只能在授权范围内进行合法的访问，并对其行为进行监督和审查。

2. 信息安全的原则

为了达到信息安全的目标，各种信息安全技术的使用必须遵守一些基本的原则。

1）最小化原则。受保护的敏感信息只能在一定范围内被共享，履行工作职责和职能的安全主体，在法律和相关安全策略允许的前提下，为满足工作需要，仅被授予访问信息的适当权限，称为最小化原则。敏感信息的“知情权”一定要加以限制，是在“满足工作需要”前提下的一种限制性开放。可以将最小化原则细分为知所必须（need to know）和用所必须（need to use）的原则。

2）分权制衡原则。在信息系统中，对所有权限应该进行适当划分，使每个授权主体只能拥有其中的一部分权限，使他们之间相互制约、相互监督，共同保证信息系统的安全。如果一个授权主体被分配的权限过大，无人监督和制约，就会有“滥用权力”“一言堂”的安全隐患。

3）安全隔离原则。隔离和控制是实现信息安全的基本方法，而隔离是进行控制的基础。信息安全的一个基本策略就是将信息的主体与客体分离，按照一定的安全策略，在可控和安全的前提下实施主体对客体的访问。

在这些基本原则的基础上，人们在生产实践过程中还总结出一些实施原则，他们是基本原则的具体体现和扩展。包括：整体保护原则、谁主管谁负责原则、适度保护的等级化原则、分域保护原则、动态保护原则、多级保护原则、深度保护原则和信息流向原则等。

3. 信息安全的属性

随着人类存储、处理和传输信息方式的变化和进步，信息安全的内涵在不断延伸。当前，在信息技术获得迅猛发展和广泛应用的情况下，信息安全可被理解为信息系统抵御意外事件或恶意行为的能力，这些事件和行为将危及所存储、处理或传输的数据或由这些系统所提供的服务的可用性、机密性、完整性、非否认性、真实性和可控性。这六个属性是信息安全的基本属性，其具体含义如下：

1）可用性（Availability）。即使在突发事件下，依然能够保障数据和服务的正常使用，如网络攻击、计算机病毒感染、系统崩溃、战争破坏、自然灾害等。

2）机密性（Confidentiality）。能够确保敏感或机密数据的传输和存储不遭受未授权的浏览，甚至可以做到不暴露保密通信的事实。

3）完整性（Integrity）。能够保障被传输、接收或存储的数据是完整的和未被篡改的，在被篡改的情况下能够发现篡改的事实或者篡改的位置。

4）非否认性（Non-repudiation）。能够保证信息系统的操作者或信息的处理者不能否认其行为或者处理结果，这可以防止参与某次操作或通信的一方事后否认该事件曾发生过。

5）真实性（Authenticity）。真实性也称可认证性，能够确保实体（如人、进程或系统）身份或信息、信息来源的真实性。

6）可控性（Controllability）。能够保证掌握和控制信息与信息系统的基本情况，可对信息和信息系统的使用实施可靠的授权、审计、责任认定、传播源追踪和监管等控制。

1.2 信息安全的发展过程

信息安全问题在人类社会发展中从古至今都存在。在政治军事斗争、商业竞争甚至个人隐私保护等活动中，人们常希望他人不能获知或篡改某些信息，也常需要查验所获得信息的可信性。在信息传递过程中，这是将信息（明文）转换成难以理解的数据（密文），以及将密文还原成明文的过程。加解密成为信息安全中最为重要的两种算法。

据说古罗马统治者恺撒是率先使用加密函的古代将领之一，因此这种加密方法被称为恺撒密码。

恺撒密码作为一种最古老的对称加密技术，在古罗马的时候就已经很流行，它的基本思想是：通过把字母移动一定的位数来实现加密和解密。明文中的所有字母都在字母表上向后（或向前）按照一个固定数目进行偏移后被替换成密文。如图 1-1 中的加密位数为 3，即字母 A 替换成 D，B 替换成 E，C 替换成 F，依此类推。如果将“hello”进行恺撒式加密，则替换成“khoor”。在这种加密方式中，位数就成为加解密的密钥。

在古希腊，还有一种叫 Syctale 的密码棒，如图 1-2 所示。它被用来对信息进行加解密。这是一个协助置换法的圆柱体，可将信息内字母的次序进行调动。它主要是利用了字条缠绕木棒的方式，实现字母的位移，收信人要使用相同直径的木棒才能还原真实的信息。

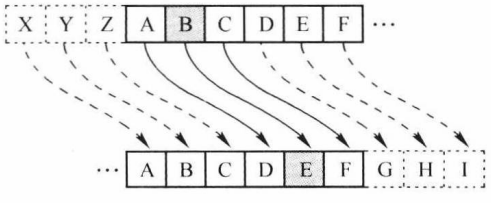


图 1-1　恺撒密码

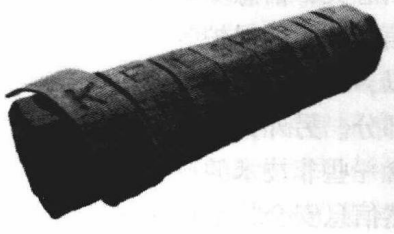


图 1-2　Syctale 密码棒

恺撒密码是一种替换加密技术，每个字母都制定了唯一的替换符号，但加密程度很低，只需简单地统计字频就可以破译。于是人们在单一的恺撒密码基础上扩展出多表密码，称为维吉尼亚密码。它是由 16 世纪法国的布莱斯·德·维吉尼亚发明的，其特点是将一系列恺撒密码组成密码字母表，如图 1-3 所示。

图中第一行代表明文字母，左面第一列代表密钥字母，例如对如下明文加密：

TO BE OR NOT TO BE THAT IS THE QUESTION

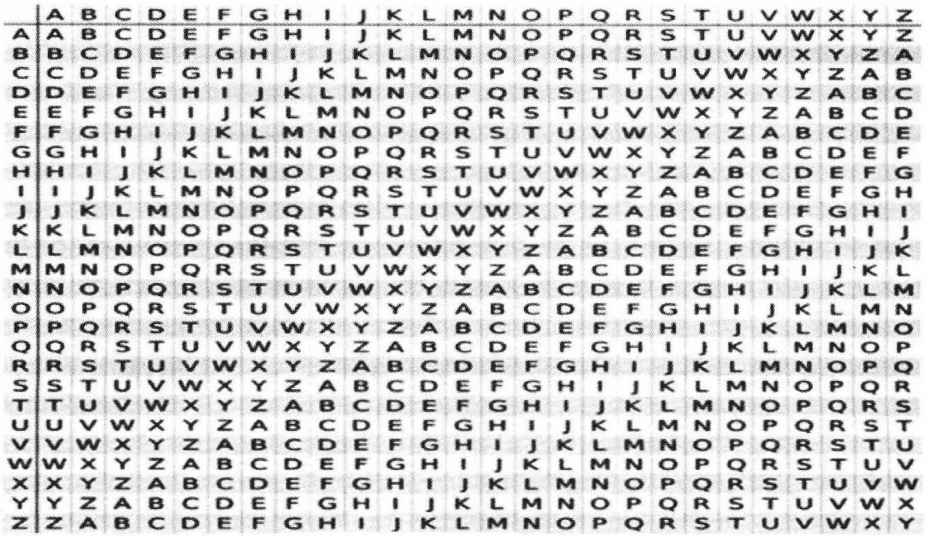
当选定 RELATIONS 作为密钥时，加密过程是：明文一个字母为 T，第一个密钥字母为 R，因此可以找到在第 R 行代替 T 的 K，依此类推，得出对应关系如下。

密钥：RELAT IONSR ELATI ONSRE LATIO NSREL

明文：TOBEO RNOTT OBETH ATIST HEQUE STION

密文：KSMEH ZBBLK SMEMP OGAJX SEJCS FLZSY

历史上以维吉尼亚密码为基础又演变出很多种加密方法，其基本元素仍是密码表与密钥，并一直沿用到第二次世界大战以后的初级电子密码机上。



	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

图 1-3　维吉尼亚密码字母表

我国春秋时代的军事家孙武在《孙子兵法》中写道："能而示之不能，用而示之不用，近而示之远，远而示之近。"这显示了孙武对军事信息保密的重视。

1.2.1　信息安全的发展阶段

顾名思义，信息安全技术指保障信息安全的技术。具体来说，它包括对信息的伪装、验证及对信息系统的保护等方面。由于对信息和信息系统的保护与攻击在技术上是紧密关联的，所以，对受保护信息或信息系统的攻击、分析和安全测评技术也都是信息安全技术的有机组成部分。另外，为了达到信息安全的目的，一般需要对人或物进行相应的组织和管理，其中包含一些非技术的成分。

虽然信息安全技术由来已久，但在第二次世界大战以后它才获得了长足的发展，由主要依靠经验、技艺逐步转变为主要依靠科学。因此，信息安全是一个古老而又年轻的科学技术领域。纵观它的发展，可以将其划分为以下四个阶段。

1. 通信安全发展时期

从古代至 20 世纪 60 年代中期，人们更关心信息在传输中的机密性。最初，人们仅以实物或特殊符号传递机密信息，后来出现了一些朴素的信息伪装方法。在我国北宋年间，曾公亮（999—1078）与丁度（990—1053）合著的《武经总要》反映了北宋军队对军令的伪装方法，按现在的观点，它综合了基于密码本的加密和基于文本的信息隐藏：先将全部 40 条军令编号并汇成码本，以 40 字诗对应位置上的文字代表相应编号，在通信中，代表某编号的文字被隐藏在一个普通文件中，但接收方知道它的位置，这样可以通过查找该字在 40 字诗中的位置获得编号，再通过码本获得军令。在古代欧洲，代换密码和隐写术得到了较多的研究和使用。德国学者特里特米乌斯（Trithemius）（1462—1516）于 1518 年出版的《多表加密》（Polygraphia）记载了当时欧洲的多表加密方法，该书被认为是密码学最早的专著，它反映了当时欧洲在代换密码的研究上已经从单表、单字符代换发展到了多表、多字符代换；特里特米乌斯于 1499 年还完成了世界上第一部信息隐藏的专著——《隐写术》（Steganographia），但该书于 1606 年才得以出版，它记载了古代欧洲人在文本中进行信息隐藏的