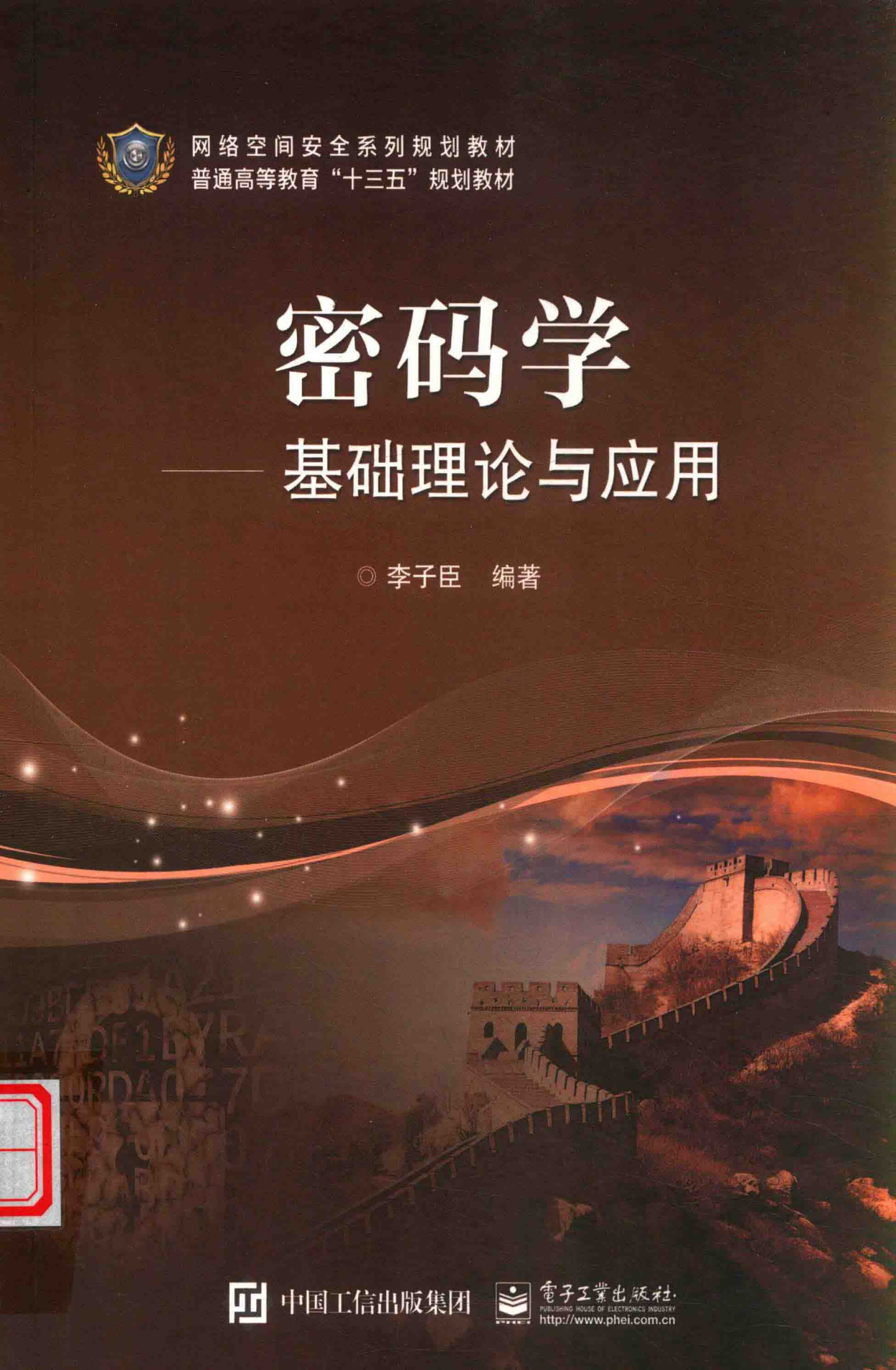
网络空间安全系列规划教材
普通高等教育“十三五”规划教材

密码学

——基础理论与应用

◎ 李子臣　编著



中国工信出版集团
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

网络空间安全系列规划教材
普通高等教育“十三五”规划教材

密码学
——基础理论与应用

李子臣　编著

電子工業出版社
Publishing House of Electronics Industry
北京 · BEIJING

内 容 简 介

本书在国家密码管理局和中国密码学会的指导下，依据教育部高等学校网络空间安全专业教学指导委员会发布的网络空间安全、信息安全本科专业密码学课程知识领域的要求，系统地讲述了密码学的基本内容。

本书系统讲述了密码学的基本概念、基本理论和密码算法，基本涵盖了密码学各方面内容。全书共 15 章：第 1 章和第 2 章主要讲述了密码学的发展历史、密码学的基本概念和古典密码，第 3 章和第 4 章讲述了分组密码，第 5 章和第 6 章讲述了序列密码，第 7～9 章讲述了公钥密码，第 10 章以格理论密码为例讲述了后量子密码，第 11 章和第 12 章讲述了密码杂凑算法，第 13 章讲述了数字签名，第 14 章讲述了身份认证，第 15 章讲述了密钥管理。在相关的章节系统讲述了国家商用密码算法，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 标识密码算法等。

本书可作为高等院校信息安全专业、网络空间安全专业或其他相关专业本科生的教材，也可作为网络空间安全专业、计算机科学与技术专业或其他相关专业研究生的教材，还可作为信息安全相关领域中的教学人员、科研人员及工程技术人员的参考用书。

图书在版编目（CIP）数据

密码学：基础理论与应用 / 李子臣编著. —北京：电子工业出版社，2019.9

ISBN 978-7-121-36501-0

Ⅰ. ①密… Ⅱ. ①李… Ⅲ. ①密码学－高等学校－教材 Ⅳ. ①TN918.1

中国版本图书馆 CIP 数据核字（2019）第 089267 号

责任编辑：戴晨辰　　特约编辑：田学清
印　　刷：北京虎彩文化传播有限公司
装　　订：北京虎彩文化传播有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　　邮编：100036
开　　本：787×1092　1/16　印张：15.75　　字数：403 千字
版　　次：2019 年 9 月第 1 版
印　　次：2019 年 9 月第 1 次印刷
定　　价：48.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式：dcc@phei.com.cn。

网络空间安全系列规划教材

编委会名单

序

随着经济全球化和信息化的发展，以互联网为平台的信息基础设施，对整个社会的正常运行和发展起着关键的作用。甚至，像电力、能源、交通等传统基础设施的运行，也逐渐依赖互联网和相关的信息系统。网络信息对社会发展有重要的支撑作用。

网络空间是利用全球互联网和计算机系统进行通信、控制和信息共享的动态虚拟空间，包括四个要素，分别是网络平台、用户虚拟角色、资产数据和管理活动，是社会有机运行的神经系统，已经成为继陆、海、空、天之后的第五空间。

网络空间面临的威胁也与日俱增。从国际上看，国家或地区在政治、经济、军事等各领域的冲突都会反映到网络空间中，而网络空间边界不明确、资源分配不均衡，导致网络空间的争夺形势异常复杂。另外，网络犯罪和网络攻击也对个人和企业构成严重威胁。在网络中，个人隐私信息泄露并大范围传播的事件已经屡见不鲜，以非法牟利为目的利用计算机网络进行犯罪已经形成了黑色的地下经济产业链。如何充分利用互联网对经济发展的推动作用、保护公民和企业的合法权益，同时控制其对经济社会发展带来的负面威胁，需要人们研究和探索更加科学合理的网络空间安全治理模式。正如习近平总书记所言：没有网络安全就没有国家安全。

加强网络空间安全已经成为国家安全战略的重要组成部分。2014 年 2 月，中央网络安全和信息化领导小组成立。2015 年 6 月，国务院学位委员会、教育部决定在“工学”门类下增设“网络空间安全”一级学科，并明确指出需要加强“网络空间安全”的学科建设，做好人才培养工作。2016 年 3 月，国务院学位委员会下发通知，明确全国共有 29 所高校获得我国首批网络空间安全一级学科博士学位授权点。同年 6 月，中央网络安全和信息化领导小组办公室、国家发展和改革委员会、教育部、科学技术部、工业和信息化部、人力资源和社会保障部联合发文，《关于加强网络安全学科建设和人才培养的意见》（中网办发文〔2016〕4 号）指出，网络空间的竞争，归根结底是人才竞争。我国网络空间安全人才还存在数量缺口较大、能力素质不高、结构不尽合理等问题，与维护国家网络安全、建设网络强国的要求不相适应。因此，提出要加快网络安全学科专业和院系建设；创新网络安全人才培养机制；加强网络安全教材建设；强化网络安全师资队伍建设；完善网络安全人才培养配套措施等意见。

网络空间安全主要研究网络空间中的安全威胁和防护问题，即在有敌手的对抗环境下，研究信息在产生、传输、存储、处理、销毁等各个环节中所面临的威胁和防御措施，以及网络和系统本身面临的安全漏洞和防护机制，不仅包括传统信息安全所研究的信息的保密性、完整性和可用性，同时还包括网络空间基础设施的安全和可信。从宏观层面来看，网络空间安全的研究对象主要包括全球各类各级信息基础设施的安全威胁；从微观层面来看，主要对象包括通信网络、计算机网络及其设备和应用系统中的安全威胁。

数学、信息论、计算复杂性理论等是网络空间安全重要的理论基础。

网络空间安全的理论体系由三部分组成。一是基础理论体系，主要包括网络空间理论、密码学、离散结构理论和计算复杂性理论等。其中，信息的机密性、完整性、可控性、可靠性等是核心，对称加密、公钥加密、密码分析、侧信道分析等是重点，在复杂环境中的可证安全、可信可控及定量分析理论是关键。二是技术理论体系，主要包括网络空间安全保障理论体系，从系统和网络角度出发，研究和设计网络空间的各种安全保护方法和技术，重点包括芯片安全、操作系统安全、数据库安全、中间件安全、恶意代码等，从预警、保护、检测到恢复响应的安全保障技术理论。从网络安全角度出发，以通信基础设施、互联网基础设施等为研究对象，聚焦研究通信安全、网络安全、网络对抗等。三是应用理论体系，从应用角度出发，针对各种应用系统，研究在实际环境中面临的各种安全问题，如 Web 安全、内容安全、垃圾信息等，涵盖电子商务、电子政务、物联网、云计算、大数据等诸多应用领域。

网络空间安全有如下五个研究方向。一是网络空间安全基础，包括网络空间安全数学理论、网络空间安全体系结构、网络空间安全数据分析、网络空间博弈理论、网络空间安全治理与策略、网络空间安全标准与评测等。二是密码学及应用，包括对称密码设计与分析、公钥密码设计与分析、安全协议设计与分析、侧信道分析与防护、量子密码与新型密码等。三是系统安全，包括芯片安全、系统软件安全、虚拟化计算平台安全、恶意代码分析与防护等。四是网络安全，包括通信基础设施及物理环境安全、互联网基础设施安全、网络安全管理、网络安全防护与主动防御（攻防与对抗）、端到端的安全通信等。五是应用安全，包括关键应用系统安全、社会网络安全（包括内容安全）、隐私保护、工控系统与物联网安全、先进计算安全等。

中国密码学会教育与科普工作委员会与电子工业出版社合作，共同筹划了这套“网络空间安全系列规划教材”，主要包括《密码学——基础理论与应用》《密码学实验教程》《应用密码学》《密码学数学基础》《密码基础算法》《典型密码算法 FPGA 实现》《典型密码算法 Java 实现》《商用密码算法原理与 C 语言实现》《密码分析学》《网络空间安全导论》《信息安全管理》《信息系统安全》《网络空间安全技术》《网络空间安全实验教程》《网络攻防技术》《同态密码学》《对称密码学》等。希望为信息安全、网络空间安全、网络安全与执法、信息对抗技术等本科专业提供教材；也为密码学、信息安全、网络空间安全等专业的研究生和博士生，以及从事该领域工作的科研人员提供教材和参考书；为我国网络空间安全教材建设、普及密码知识和网络空间安全人才培养贡献绵薄之力。

前　言

密码是使用特定变换对数据等信息进行加密保护或安全认证的物项和技术。其中，加密保护是指，使用特定变换，将原来可读的信息变成不能识别的符号序列；安全认证是指，使用特定变换，确认信息是否被篡改、是否来自可靠信息源及确认行为是否真实等。密码的加密保护功能用于保证信息的机密性，密码的安全认证功能用于实现信息的真实性、数据的完整性和行为的不可否认性。

国家密码管理局高度重视密码算法管理工作，近年来，发布了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标识密码算法等商用密码算法，构成了包括对称、非对称、杂凑、标识和序列等密码算法，形成了完整、自主的国产商用密码算法体系，为促进密码发展、保障我国信息安全发挥了巨大作用。

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（Cryptology）和密码分析（Cryptanalysis）的一般规律。密码学课程是信息安全专业、网络空间安全专业本科生的必修课程，也是网络空间安全专业、计算机科学与技术专业或其他相关专业研究生的必修课程。

本书系统介绍了密码学的基本概念、基本理论和国内外主要的密码算法。全书共15章。第1章概论，主要介绍密码学的发展历史、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。第2章古典密码，主要介绍置换密码、代换密码、转轮密码、古典密码的分类和古典密码的统计分析。第3章分组密码，主要介绍分组密码概述、DES、AES、分组密码的工作模式和分组密码分析。第4章SM4分组密码算法，主要介绍SM4分组密码算法概述、SM4分组密码算法设计原理和SM4分组密码算法安全性分析。第5章序列密码，主要介绍序列密码的组成、LFSR、欧洲eSTREAM序列密码、序列密码的安全性及分析技术和序列密码算法的未来发展趋势。第6章祖冲之序列密码算法，介绍其算法结构、算法原理、算法参数和算法描述。第7章公钥密码，详细描述公钥密码体制的原理和基本概念，介绍RSA、ElGamal公钥密码体制的原理。第8章SM2公钥密码算法，介绍椭圆曲线原理，ECC公钥密码体制，详细描述SM2加解密算法的原理，并对SM2算法的安全性进行分析。第9章SM9标识密码算法，介绍标识密码算法的概念，对SM9加解密算法流程进行描述，以及对其安全性进行分析。第10章格理论密码，介绍格密码基本概念及格上的计算困难问题，介绍NTRU密码体制。第11章密码杂凑函数，介绍杂凑函数和消息认证码，包括MD5杂凑算法和SHA-3杂凑算法的原理，基于Hash函数的HMAC算法。第12章SM3密码杂凑算法，介绍算法的设计原理、算法特点和安全性分析。第13章数字签名，介绍数字签名方案的基本概念、DSS数字签名标准，重点介绍SM2、SM9数字签名算法。第14章身份认证，介绍基于口令、对称密码体制、公钥密码体制及零知识证明的身份认证技术。第15章密钥管理，介绍密钥管理的基本概念和技术，重

点介绍 SM2 和 SM9 密钥交换协议。

本书是在作者多年来一直从事本科和研究生密码学的教学工作、结合多年密码学科研实践和总结国内外密码学相关教材及文献的基础上编写而成的。本书得到国家自然科学基金（61370188）和北京印刷学院数字版权保护学术创新团队的资助。北京电子科技学院张卷美、杨亚涛老师，河南理工大学汤永利、彭维平、闫玺玺、宋成、叶青老师，北京印刷学院李桢桢老师，南阳理工学院朱慧君老师参与了本书有关章节的编写和校对工作；北京电子科技学院后量子密码科研团队的研究生、北京印刷学院数字版权保护学术创新团队的教师和研究生参加了本书有关材料的收集、整理工作；在本书的编写过程中，也得到国家密码管理局、中国密码学会领导的关心和支持，在此一并致以最诚挚的谢意。电子工业出版社在本书的出版过程中给予了极大的帮助和支持，也表示衷心的感谢。

由于作者知识水平有限，教材中难免有不足和疏漏之处，敬请广大读者批评指正。

作　者

目　录

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。