商用密码知识与政策干部读本

《商用密码知识与政策干部读本》编委会

人民出版社

商用密码知识与政策干部读本

《商用密码知识与政策干部读本》编委会

人民出版社

出版总策划：黄书元　李春生　王　彤

策 划 编 辑：郑海燕　张　燕
责 任 编 辑：吴炤东　陈　登　陈光耀　刘　伟　李之美
　　姜　玮　孔　欢　罗少强　林　敏
封 面 设 计：林芝玉
责 任 校 对：吕　飞

图书在版编目(CIP)数据

商用密码知识与政策干部读本/《商用密码知识与政策干部读本》编委会 编著. —
北京：人民出版社，2017.10
ISBN 978-7-01-018400-5

Ⅰ.①商… Ⅱ.①商… Ⅲ.①密码学-干部教育-学习参考资料
Ⅳ.①TN918.1

中国版本图书馆 CIP 数据核字(2017)第 247833 号

商用密码知识与政策干部读本
SHANGYONG MIMA ZHISHI YU ZHENGCE GANBU DUBEN

《商用密码知识与政策干部读本》编委会　编著

人民出版社 出版发行
(100706　北京市东城区隆福寺街 99 号)

北京尚唐印刷包装有限公司印刷　新华书店经销

2017 年 10 月第 1 版　2017 年 10 月北京第 1 次印刷
开本：710 毫米×1000 毫米 1/16　印张：16.5　插页：1
字数：176 千字

ISBN 978-7-01-018400-5　定价：56.00 元

邮购地址 100706　北京市东城区隆福寺街 99 号
人民东方图书销售中心　电话 (010)65250042　65289539

在重要领域、重点人群乃至全社会普及密码知识和政策，在金融和重要领域推进密码应用，是落实习近平总书记网络强国战略思想、构建安全可控信息技术体系的一项重要举措。没有网络安全就没有国家安全，密码作为网络安全的核心技术，是保护国家安全和根本利益的战略性资源。了解密码知识、熟悉密码政策、推进密码应用，是新时期对党政干部的一项新要求。要树立以总体国家安全观为统领、以密码为基础支撑的网络安全观，在相关工作中全面推进密码应用，切实维护国家安全、促进经济发展、保护人民群众利益。

—— 摘自栗战书同志2017年3月
在密码应用工作会议上的讲话

序　言

密码工作直接关系国家政治安全、经济安全、国防安全和网络安全，直接关系社会组织和公民个人的合法权益。商用密码工作是密码工作的重要组成部分，在维护国家安全、促进经济发展、保护人民群众利益中发挥着不可替代的重要作用。

党中央、国务院高度重视商用密码工作，1999 年 10 月国务院颁布《商用密码管理条例》。党的十八大以来，在以习近平同志为核心的党中央坚强领导下，在习近平总书记总体国家安全观和网络强国战略思想指引下，商用密码发展取得重要突破，法规标准体系逐步健全，管理体制机制不断完善，科技创新能力显著增强，形成了从密码芯片到密码服务完全自主可控的产业链条，积极服务于“一带一路”建设、“互联网+”行动计划、智慧城市建设和大数据战略，有力支撑了商用密码在金融、教育、社保、交通、通信、能源、军工、工业制造等重要领域的广泛应用，网络空间密码保障能力大幅提升。

当前，国际局势正在发生深刻变化，世界多极化和经济全球化趋势在曲折中发展，科技进步日新月异，国际竞争日趋激烈，国家

网络安全和信息化整体水平已成为一个国家综合国力和竞争力的重要指标，密码技术作为国家自主可控的核心技术，在维护国家安全、主权和发展利益中发挥着越来越重要的作用。虽然我国商用密码已取得很大成绩，但总体上还处于初期发展阶段，尤为突出的是，重要网络和信息系统使用密码还不广泛、不规范，自主可控意识还不强，密码应用的社会基础还很薄弱。

形势逼人，不进则退。顺应世界网络安全和信息化发展趋势，加快推进基础信息网络、重要信息系统、重要工业控制系统和政务信息系统密码应用，推进金融和重要领域网络安全和信息化实现跨越式发展，是保护国家政权安全的必然选择，是维护我国网络空间主权的必由之路，是保护人民群众切身利益的必需之举。我们要始终坚持党管密码不动摇、创新发展不动摇、服务大局不动摇，落实“谁主管、谁负责，谁运行、谁负责”的工作原则，加快推进金融和重要领域密码应用。在国家安全法制建设的总体框架下，加快构建以《密码法》为核心的密码法规制度体系，建设以密码国家标准和行业标准为主体的密码标准体系，形成依法依规依标准推进密码应用的新格局。通过合规、正确、有效使用密码，在网络空间建立以密码技术为核心、多种技术相互融合、共同作用的新安全体制；建设以密码基础设施为底层支撑的新安全环境；实现可信互联、开放共享的新安全文明。

落实中央领导同志要求，广泛开展密码应用政策宣传和教育培训，推动密码知识在重要领域、重点人群乃至全社会的普及，既是确保我国金融和重要领域密码应用顺利推进的一项基础性工作，也是加强干部教育培训和人才队伍建设的一项重要内容。为

便于各地区、各部门，各级党校、行政学院组织开展相关培训和各级党政干部学习掌握密码相关知识，国家密码管理局组织专家学者和业务骨干编写了《商用密码知识与政策干部读本》，《读本》是我国第一部系统介绍商用密码技术与应用的著作。希望本书的出版，能够对各级领导干部和广大公务员学习密码知识和政策有所帮助，对抓好密码应用推进工作有所辅助，对应用密码技术和利用密码资源有所启引。各级党政干部和全社会要携手推动密码全面应用，共同筑就国家网络和信息安全屏障，为维护好国家安全和根本利益，实现中华民族伟大复兴的中国梦作出新的贡献！

国家密码管理局

2017年9月30日

目　录 | CONTENTS

商用密码知识与政策干部读本

第二部分　密码技术基础知识

第三部分　商用密码管理

第五部分　商用密码应用案例

绪　论

密码[①]分为核心密码、普通密码和商用密码[②]，商用密码用于保护不属于国家秘密的信息。经过二十多年的发展，我国商用密码从无到有、从弱到强，取得了丰硕成果。特别是党的十八大以来，商用密码工作全面推进，在依法管理、科技创新、产业发展、应用推广等方面成绩斐然，基本满足了国民经济和社会发展对商用密码的应用需求，在保障国家网络与信息安全方面发挥了重要作用。

为帮助各级领导干部了解和学习商用密码基础知识与相关政策，国家密码管理局组织专家学者和业务骨干，围绕“怎么看密码、什么是密码、怎么管密码、怎么用密码、哪里用密码”等问题，编写了《商用密码知识与政策干部读本》（以下简称《读本》），《读本》共分五个部分。

第一部分“商用密码发展的形势与任务”，回答了“怎么看密码”。在网络空间中，实体身份认证、信息来源认证、信息存储与

① 密码：使用特定变换对数据等信息进行加密保护或者安全认证的物项和技术。

② 商用密码：是指对不涉及国家秘密的信息进行加密保护或者安全认证所使用的密码。

传输安全等都需要用密码来实现和保护。密码技术是实现网络安全的基石，是保障网络与信息安全的核心技术和基础支撑，是解决网络与信息安全最有效、最可靠、最经济的手段，是信息系统内置的免疫基因，没有密码就没有网络安全。本部分结合网络信息安全事件说明了密码应用的重要性、必要性和紧迫性；围绕国家政策、应用需求和新技术发展，分析了商用密码发展面临的机遇与挑战；系统阐述了新时期商用密码深化管理改革、强化自主创新、推进合规正确有效应用等方面的主要任务。

第二部分“密码技术基础知识”，回答了“什么是密码”。口令不是密码，密码不是口令。从技术角度看，密码主要包含密码算法、密钥管理和密码协议。密码算法是密码的关键，算法的强度决定了破译的难度。算法是可以公开的，一切秘密寓于密钥之中，密钥的保密是重中之重。密码协议是密码应用遵循的交互规则，不安全的密码协议会导致系统存在从“旁路”或“后门”窃取信息的风险。本部分主要介绍密码技术基本概念与原理、商用密码算法相关知识、密码技术发展简史及发展趋势，解答了为什么密码技术是保障网络与信息安全的核心技术，是最有效、最可靠、最经济的手段。

第三部分“商用密码管理”，回答了“怎么管密码”。坚持党对密码工作的领导，是密码工作的根本原则。坚持依法依规依标准管理密码，发挥法治与标准在密码工作中的引领和保障作用，是商用密码管理工作的关键。本部分主要介绍商用密码管理的法律法规、体制机制及标准规范，包括我国商用密码的现行法规体系，《密码法》立法和《商用密码管理条例》修订进程，商用密码科研、

产品、使用、监督检查、检测认证等方面的管理与服务机制，以及密码标准化工作等有关情况。

第四部分“商用密码应用”，回答了“怎么用密码”。政策法规为规范和促进商用密码应用提出了明确要求，产品与服务体系为商用密码应用提供了技术支撑，安全性评估为商用密码合规正确有效应用提供了可靠保证。本部分主要介绍商用密码应用的政策法规、技术支撑，以及安全性评估要求与评估内容，从技术支撑角度分别介绍了商用密码产品与服务，从密码应用监管角度详细论述了密码应用安全性评估的目的、意义与内容。

第五部分“商用密码应用案例”，回答了“哪里用密码”。本部分选取金融领域和基础信息网络系统、重要信息系统、重要工业控制系统、面向社会服务的政务信息系统等重要领域具有代表性的密码应用典型案例，对案例进行了剖析，介绍了密码应用框架，分析了商用密码发挥的作用、取得的成效，总结了商用密码在应用推进中可复制、可推广的经验与做法。

遵循政治性、战略性、实用性、通用性、权威性、通俗性的编写原则，《读本》在内容选择和编排上进行了精心组织，既易读易懂又不失权威准确，既有工作上的启发又有可资借鉴的案例。由于密码科技创新和密码应用正处于快速发展中，我们对其内在规律的认识还是初步的，有许多理论问题还需要在实践中不断探索。尽管我们已经做了很大努力，但问题和不足在所难免，希望各地区、各部门在组织开展学习、培训中，结合本地区、本部门实际帮助我们不断丰富和完善《读本》内容。

第一部分

商用密码发展的形势与任务