广东省密码管理局

生活中的密码

广东省密码管理局

目　录

一、什么是密码

密码

密码是保障网络空间安全的关键能力，密码工作是党和国家的一项特殊重要工作，直接关系国家政治安全、经济安全、国防安全和信息安全。

现实生活中，我们提到的银行卡“密码”、手机开机“密码”、邮箱登录“密码”等，实际上是口令，并不是真正意义上的密码。

《中华人民共和国密码法》（2020年1月1日正式施行）对密码有了清晰的定义：密码是指采用特定变换的方法对信息等进行加密保护、安全认证的技术、产品和服务。（第二条）

加密保护

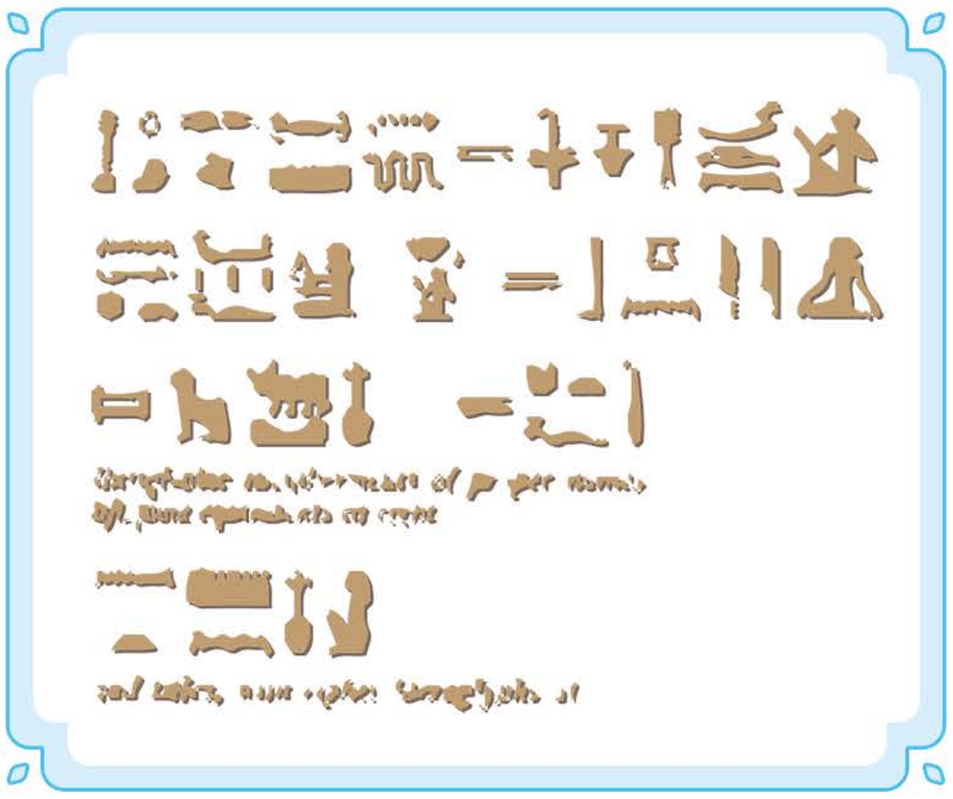
加密保护是指使用特定变换，将原始信息变成攻击者不能识别的符号序列，简单地说，就是将明文变成密文，从而保证信息的保密性。

安全认证

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以及确认信息发送行为是否真实存在等，简单地说，就是确认主体和信息的真实可靠性，从而保证信息来源的真实性、数据的完整性和行为的不可否认性。

二、有趣的密码

1. 远古密码



2. 摩斯密码

*《潜伏》中的密码

3. 口语密码

*《风语者》中的纳瓦霍密码

4. 谐音密码

著名的“爱情密码”故事，相传是一个女孩给一个男孩发了一个短消息。然后女孩又打来电话说须10天内破译这封情书，否则便与他分手。

这是一封感人的情书：584，568**78，12234，1798，76868，587****55，829475，请翻译成中文发给我。**

于是男孩就破解出了真情版、告白版、无奈版和胡抡版四种版本。

真情版

我发誓，我来伴你一起出去，
走吧，与你爱相随，一起
走吧，去溜达溜达，
我不求与你朝朝暮暮，
被爱就是幸福

告白版

我发誓，我无法爱已情去
醒醒吧，多爱要生事
一起想法，请顺道来吧
我抱歉不要再纠缠我
把爱就还给我

无奈版

我爸死活不让我爱你，放弃吧，
要爱爱三四，要生气就去
溜达溜达，我不气，
要爱就找我爸，哎，
就是气我

胡抡版

吾发誓，吾老爸爱药。吃！吃！
吃！吃吧！药，唉~爱三思！
药，吃吧?就吃！老爸
老爸，吾爸吃药就酒坞
吾爸爱就是吃吾

三、现代密码体制

1. 对称密码

对称密码，就是加密过程与解密过程使用相同的或容易相互推导得出的密钥，即加密和解密两方的密钥是“对称”的。

常用对称密码算法：

SM1算法（国产）、SM4算法（国产）、ZUC算法（国产）

2.公钥密码

公钥密码又称非对称密码，就是在加密和解密的过程中分别使用不同的密钥。

常用非对称密码算法：SM2算法（国产）、SM9算法（国产）、RSA算法

3.杂凑算法

杂凑算法又称哈希算法或散列算法，就是不管输入多长的信息文本，总是输出固定长度摘要的结果。

常用杂凑算法：SM3算法（国产）、SHA-2算法

美国国家安全局：

MD5算法使用计算机需要100年才可能破解

王小云院士2004年美国密码大会上提交论文，破解了MD5算法。2005年，王小云院士又破解了SHA-1算法。

美国国家安全局徽章

四、身边的密码

1. 密码认证

通过密码技术确认主体和信息的真实可靠性。

拒绝 ← 认证失败 ← 密码认证 → 认证成功 → 交易

2.电子支付

密码技术实现用户身份认证、交易数据机密性与完整性，保护消费者资金安全，防欺诈、套现、洗钱等违法犯罪行为。

3.电子单据凭证

它们是谁发行的？它们的内容是真实的吗？谁可以使用它？

4.居民医疗健康数据管理

在医疗卫生领域，密码技术赋能医疗业务信息系统，满足居民医疗健康数据的完整性保护、可信时间及责任认定等安全需求,在防止假冒身份、信息篡改、否认责任等方面发挥了重要作用。

*电子病历无纸化

5.电子证照

密码技术实现可靠电子签名以及可信时间戳信息防伪。

*电子营业执照、电子印章

学历认证、成绩认证秒办

6.日常生活

常见场景

ETC

机顶盒

电子门禁

电子手表

交通卡

7.更多场景

我们储存在网上的图片会不会被偷看？

采用密码安全储存，云端不能获取加密的用户数据。

听说黑网都是远程控制的，会不会被黑客控制全城停电，好害怕呀。

没有密码保护，真有可能全城停电哦。

自动驾驶汽车会不会被别人远程操控？

采用完备的密码安全体系保护才能避免被远程控制。

夏天远程遥控家里的空调，一回家就可以享受凉爽，多好啊！

如果没有密码安全认证体系保护，晚上睡觉有可能被人遥控冻成冰棍哦。

五、商用密码管理法律法规

1.什么是商用密码

商用密码是指采用特定变换的方法对不属于国家秘密的信息等进行加密保护、安全认证的技术、产品和服务。

2.国家密码管理局

国家密码管理局是我国商用密码管理主管机构。

网址：www.sca.gov.cn

3.密码法

密码法立法

《中华人民共和国密码法》于2019年10月26日第十三届全国人民代表大会常务委员会第十四次会议通过，自2020年1月1日起施行。共计五章四十四条。

是我国密码领域的综合性、基础性法律

- 规范密码应用和管理
- 促进密码事业发展
- 保障网络与信息安全
- 提升密码管理科学化、规范化、法治化水平
- 维护国家安全和社会公共利益

密码法内容

◆ 立法宗旨

规范密码应用和管理，促进密码事业发展，保障网络与信息安全，维护国家安全和社会公共利益，保护公民、法人和其他组织的合法权益。(第一条)

◆ 密码工作的基本原则

坚持总体国家安全观，遵循统一领导、分级负责，创新发展、服务大局，依法管理、保障安全的原则。(第三条)

◆ 密码工作领导管理体制

坚持中国共产党对密码工作的领导。中央密码工作领导机构对全国密码工作实行统一领导，制定国家密码工作重大方针政策，统筹协调国家密码重大事项和重要工作，推进国家密码法治建设。(第四条)

国家密码管理部门负责管理全国的密码工作。县级以上地方各级密码管理部门负责管理本行政区域的密码工作。国家机关和涉及密码工作的单位在其职责范围内负责本机关、本单位或者本系统的密码工作。(第五条)

◆ 密码分类管理

密码分为核心密码、普通密码和商用密码。(第六条)

核心密码、普通密码用于保护国家秘密信息，核心密码保护信息的最高密级为绝密级，普通密码保护信息的最高密级为机密级。核心

密码、普通密码属于国家秘密。密码管理部门依照本法和有关法律、行政法规、国家有关规定对核心密码、普通密码实行严格统一管理。(第七条)

商用密码用于保护不属于国家秘密的信息。公民、法人和其他组织可以依法使用商用密码保护网络与信息安全。(第八条)

◆ 商用密码

国家鼓励商用密码技术的研究开发、学术交流、成果转化和推广应用，健全统一、开放、竞争、有序的商用密码市场体系，鼓励和促进商用密码产业发展。(第二十一条)

国家建立和完善商用密码标准体系。(第二十二条)

国家推进商用密码检测认证体系建设，制定商用密码检测认证技术规范、规则，鼓励商用密码从业单位自愿接受商用密码检测认证，提升市场竞争力。(第二十五条)

法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施，其运营者应当使用商用密码进行保护，自行或者委托商用密码检测机构开展商用密码应用安全性评估。商用密码应用安全性评估应当与关键信息基础设施安全检测评估、网络安全等级测评制度相衔接，避免重复评估、测评。(第二十七条)

4.商用密码管理条例

中华人民共和国国务院令第760号

新修订的《商用密码管理条例》于2023年4月27日正式公布，自2023年7月1日起施行。

条例共九章六十七条，包括总则、科技创新与标准化、检测认证、电子认证、进出口、应用促进、监督管理、法律责任、附则。

条例的意义：

条例的修订深入贯彻习近平法治思想和全面依法治国的基本方略，全面贯彻《密码法》要求。

条例内容

- 涉及国家安全、国计民生、社会公共利益的商用密码产品，应当依法列入网络关键设备和网络安全专用产品目录，由具备资格的商用密码检测、认证机构检测认证合格后，方可销售或者提供。（第二十条）

- 商用密码服务使用网络关键设备和网络安全专用产品的，应当经商用密码认证机构对该商用密码服务认证合格。（第二十一条）

- 政务活动中电子签名、电子印章、电子证照等涉及的电子认证服务，应当由依法设立的电子政务电子认证服务机构提供。（第三十条）

◆国家鼓励公民、法人和其他组织依法使用商用密码保护网络与信息安全，鼓励使用经检测认证合格的商用密码。（第三十五条）

◆法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施，其运营者应当使用商用密码进行保护，制定商用密码应用方案，配备必要的资金和专业人员，同步规划、同步建设、同步运行商用密码保障系统，自行或者委托商用密码检测机构开展商用密码应用安全性评估。前款所列关键信息基础设施通过商用密码应用安全性评估方可投入运行，运行后每年至少进行一次评估，评估情况按照国家有关规定报送国家密码管理部门或者关键信息基础设施所在地省、自治区、直辖市密码管理部门备案。（第三十八条）

◆法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施，使用的商用密码产品、服务应当经检测认证合格，使用的密码算法、密码协议、密钥管理机制等商用密码技术应当通过国家密码管理部门审查鉴定。（第三十九条）

《条例》的发布施行，健全和完善了我国密码法律法规体系，有利于推动商用密码科技创新，促进商用密码产业发展，推进商用密码应用，为建设网络强国和数字中国提供更加有力的支撑和保障。

六、怎样用好密码

密码无处不在，存在各种形态

密码要正确使用才能用得上

密码要规范使用才能用得好

密码是保障网络与信息安全的核心技术和基础支撑

《商用密码应用安全性评估管理办法》

（国家密码管理局令第3号）

为了规范商用密码应用安全性评估工作，保障网络与信息安全，维护国家安全和社会公共利益，保护公民、法人和其他组织的合法权益，根据《中华人民共和国密码法》、《商用密码管理条例》等有关法律法规，制定《商用密码应用安全性评估管理办法》，2023年11月1日正式施行，商用密码应用进一步加强与规范。

商用密码应用安全性评估

商用密码应用安全性评估是指按照有关法律法规和标准规范，对网络与信息系统使用商用密码技术、产品和服务的合规性、正确性、有效性进行检测分析和评估验证的活动。

法律、行政法规和国家有关规定要求使用商用密码进行保护的网络与信息系统（以下简称重要网络与信息系统），其运营者应当使用商用密码进行保护，制定商用密码应用方案，配备必要的资金和专业人员，同步规划、同步建设、同步运行商用密码保障系统，并定期开展商用密码应用安全性评估。

重要网络与信息系统

重要网络与信息系统，主要包括关键信息基础设施、政务信息化系统、网络安全等级保护制度明确要求使用商用密码保护的网络与信息系统等。

法律、行政法规和国家有关规定要求使用商用密码进行保护的网络与信息系统

重要网络与信息系统

*其运营者

应当使用商用密码进行保护

制定商用密码应用方案，配备必要的资金和专业人员

同步规划、同步建设、同步运行商用密码保障系统

并定期开展商用密码应用安全性评估

七、密码发展前景广阔

1.学科建设

本科教育：暨南大学、华南师范大学、广东技术师范大学、北京电子科技学院、山东大学等二十所高校设立密码科学与技术本科专业。

职业教育：教育部将“密码技术应用”专业纳入职业教育专业目录。

2.职业技术人才培养

人社部将“密码技术应用员”和“密码工程技术人员”确定为新职业。

中华人民共和国人力资源和社会保障部
Ministry of Human Resources and Social Security of the People's Republic of China

2021-01-15

（十二）4-07-05-06 密码技术应用员

定义

运用密码技术，从事信息系统安全密码保障的架构设计、系统集成、检测评估、运维管理、密码咨询等相关密码服务的人员。

中华人民共和国人力资源和社会保障部
Ministry of Human Resources and Social Security of the People's Republic of China

2023-3-1

2-02-38-13 密码工程技术人员

定义

从事密码算法与协议实现、 密码设备和系统研制、 密码产品检测与认证、密码服务系统设计建设、密码标准编制、密码管理、密码专业技术培训咨询的工程技术人员。

3.密码产业

密码产业是指为了保障信息安全，提供加密保护、安全认证相关技术、产品和服务的相关行业总称，主要包含算法与协议的研制、基础算力的软硬件产品生产、与信息化业务场景结合的产品和服务、检测认证、应用安全性评估等各类经济活动。

◆ 密码政策

2023年4月27日，李强总理签署第760号国务院令，颁布了新修订的《商用密码管理条例》，《条例》修订深入贯彻习近平法治思想，贯彻全面依法治国基本方略，全面落实《中华人民共和国密码法》要求，为推进新时代商用密码高质量发展、保障网络与信息安全、维护国家安全和社会公共利益、保护公民合法权益提供了有力法治保障。同年依据《密码法》和《条例》，国家密码管理局研究制定了《商用密码应用安全性评估管理办法》（国家密码管理局令第3

号），规范商用密码应用安全性评估工作，保障网络与信息安全，维护国家安全和社会公共利益，保护公民、法人和其他组织的合法权益，促进商用密码应用的高质量发展，切实提高网络空间密码保障能力。

◆密码基地

广东省商用密码产业基础良好，前景广阔。

2020年，广东省商用密码应用和创新示范基地落户广州开发区。同年，广州开发区发布全国首个区级“商密10条”产业政策——《促进商用密码科技创新和产业发展办法》及实施细则。

2024年，广州开发区、广州市黄埔区出台《关于支持大模型等数字技术和实体经济融合加快推进中小企业数字化转型发展若干措施》，持续加大对商用密码产业的支持。

◆密码研究院

2023年，广州开发区、中国科学院软件研究所、西安电子科技大学广州研究院共建的密码与网络空间安全（黄埔）研究院注册登记，将进一步促进商用密码关键技术研发、科研成果转化和产业化应用。