生活中的密码

广东省密码管理局

生活中的密码

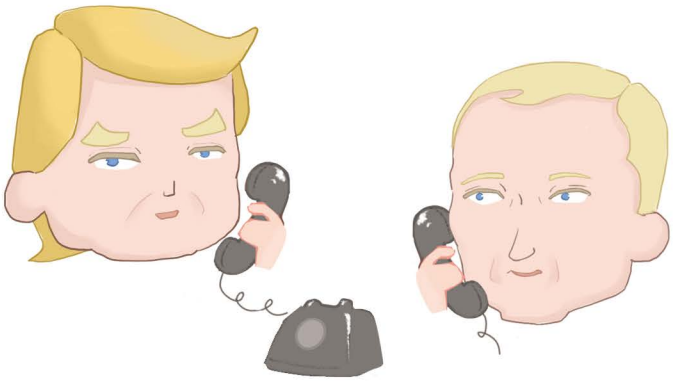
广东省密码管理局

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。



加密

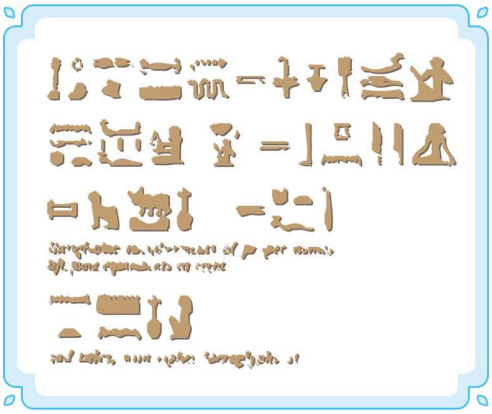
加密是按照约定的法则将被保护的信息（明文）变换成他人不可辨识的符号。

解密

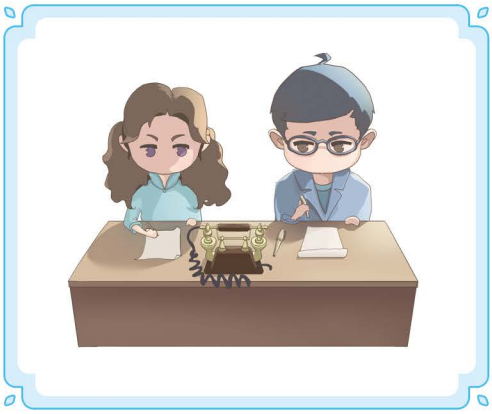
解密是按照约定的法则将密文变换成明文的过程。

二、有趣的密码

1. 远古密码



2. 莫斯密码



*《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

对称密码又称私钥密码或单钥密码，就是在加密和解密的过程中使用相同的密钥。

常用对称密码算法：SM1算法（国产）、SM4算法（国产）、DES算法

2.公钥密码

公钥密码又称双钥密码或非对称密码，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.杂凑密码

杂凑密码又称哈希函数或散列函数，就是不管输入多长的信息文本，总是输出固定长度的结果。

常用杂凑算法：SM3算法（国产）、MD5算法、SHA-1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

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

健康码、电子病历会泄露个人的隐私吗？密码技术保证个人健康数据不泄露、无篡改。

*健康码、行程码

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

电子门禁

ETC

电子手表

机顶盒

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。

听说电网都是远程控制的，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、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

密码是保障网络和信息安全的核心技术和基础支撑

密码分国界吗？

信息安全是有国界的。信息安全是国家安全基础。密码是信息安全的核心。要用符合国家标准规范的密码才有信息安全话语权。

六、商用密码管理法规

1.什么是商用密码

商用密码是指对不涉及国家秘密内容的信息进行加密保护或者安全认证所使用的密码技术、产品和服务。商用密码应用领域主要指公共通信与信息服务、能源、交通、水利、金融、公共服务、电子政务等主要领域关键信息基础设施。同时，也应用在电子商务、个人隐私保护等方面。

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）

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、华中科技大学、北京电子科技学院、山东大学等十几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”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。

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，主要包括算法与协议、基础算力的软硬件产品生产、与信息化业务场景结合的产业和服务、检测认证、密码应用安全性评估等各类经济活动。

◆ 密码政策

“十四五”开局之年，国家密码管理局、中央网信办、国家发改委、科技部、工信部、公安部、财政部、国资委、市场监管总局、证监会等十部委联合印发《促进商用密码产业高质量发展的若干举措》，旨在深入贯彻落实《密码法》，通过深化需求牵引、创新驱动提升全链条、支撑平台建设和完善发展环境等四大方面举措， 加快推进密码产业高质量发展，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。2019年，广东省商用密码应用与创新示范基地落户广州开发区，广州开发区相继发布《促进商用密码科技创新和产业发展办法》及实施细则，对密码相关机构最高补贴2000万元。

◆ 密码协会

2019年，广东省商用密码协会成立，目前已拥有超过100多家会员单位。

广东省商用密码协会徽章