# 第1章信息系统安全概述

- 随着信息技术的发展和计算机的普及，计算机已进入社会生活的各个角落，特别是互联网的推广应用，使得人们逐步改变生活、工作、学习和合作交流环境，走向信息化时代。
- 但是在带来巨大的社会和经济效益的同时，却潜伏着严重的不安全性、危险性及脆弱性。

- 利用计算机进行高技术犯罪的事件不断出现
- 纽约一家银行的高级顾问利用掌握的password，篡改银行电脑财务系统，仅12秒，5000万美元从纽约通过旧金山转到苏黎世，由其同伙提走，随后再还原电脑程序。
- 目前有个估计，用计算机窃取银行资产，平均每次盗窃额为883,279美元，
- 而抢银行，平均损失才6100美元。

- 某部高级技术人员把几十年武器研制绝密材料压缩发出。打印出来可以装4卡车。
- 按照泄密绝密材料4张死刑，可以死万次
- 原中纪委委员、中核集团党组书记、总经理把机密提供给国外公司

- 在计算机网络上，A要将信息传送给B，就存在着怎样防止有人窃取信息以及用其它信息干扰的问题；
- 在信息资源共享上，存在着防止资源随意更改、某些资源须授权查阅等问题。

加解密及身份验证

- 科学水平的不断提高，用password方法已难于起到有效的防范作用，而原来主要用于军事上的通信加密方法正被逐渐用到信息系统和网络上。
- 信息加密技术已成为防范计算机犯罪的不可缺少的工具。
- 密码技术也可有效地用于信息完整性验证、数字签名等，以防范电子欺骗。

- 例如A向B通过网络订货，如何防抵赖，
- 数字签名
- 电子合同附有标记A的特殊信息(数字签名)，
- 别人无法伪造，
- A无法抵赖。

- 计算机病毒泛滥成灾
- 恶性计算机病毒CIH，导致国内很多应用单位的计算机在被CIH病毒传染后，造成严重损失，影响了计算机信息系统的正常应用。CIH计算机病毒在全球造成的损失据估计超过10亿美元，
- “爱虫(I Love you)”病毒,全球的损失预计高达100亿美元
- “红色代码”病毒更是危害无穷。具有病毒和黑客双重功能。我国有许多用户被攻击。
- 冲击波病毒的肆虐更是损失惨重

  美国国防部各大网站为此暂时关闭直至安装了防范该病毒的保护装置。

- 热衷于攻击计算机系统的计算机爱好者和恶意攻击者。
- 2000年2月份黑客攻击的浪潮，标志着互连网问世以来黑客事件高潮的到来。
  - 2月7日10时15分，汹涌而来的垃圾邮件堵死了雅虎网站除电子邮件服务等三个站点之外的所有服务器，雅虎大部分网络服务陷入瘫痪。
  - 第二天，世界最著名的网络拍卖行电子湾（eBay）也因神秘客袭击而瘫痪。
  - 美国有线新闻网CNN的网站也因遭神秘客的袭击而瘫痪近两个小时；
  - 顶级购物网站亚马逊也被迫关闭一个多小时。
  - 在此之后又有一些著名网站被袭击,到2月17日为止，黑客攻击个案已增至17宗，
  - 引起美国道琼斯股票指数下降了200多点。
  - 成长中的高科技股纳斯达克股票也一度下跌了80个点。

- 美国国防部统计局对各军种和防务机构的Internet场点的计算机系统，进行了38000次攻击实验，成功访问的概率达到65%。（24700次）。
- 被检测到的只有4%（988次）
- 被检测到的攻击只有27%进行了汇报，也就是150次攻击中只有一次被检测到
- 500次攻击中才有一次被汇报。
- 因此估计国防部每年受到25万次攻击。
- 联邦执法官员估计每年在美国约有100亿美元的数据被联机窃取。

- 2007年，台湾利用山东某地政府网站的缺陷，控制了该网站，并以此攻击与该网站连接的国家有关政府机关内部网，窃取大量国家紧密。

- 信息安全已成为人们关切和迫切需要解决的问题
- 当然信息安全也不要搞得草木皆兵，关键是根据实际需要采取相应的安全措施。
- 有关信息安全，涉及到防火墙技术和密码技术，构建可靠的安全体系
- 信用卡、IC卡等安全问题都需要密切关注和解决。

- 这门课程主要就是讨论解决有关安全问题的基本方法、基本思想和基本技术。课程要求是，不定期交作业（提前一周通知）10%,完成规定报告5%，完成1个project 15%(分2部分)，期终笔试占70%。
- 内容包括：
- 信息系统安全概述
- 风险评估
- 古典密码概述
- 对称密码算法
- 非对称密码算法
- 密码应用和网络安全
- 计算机病毒概述，
- 典型计算机病毒分析，
- 网络攻击与防范

# 1.1信息安全基本概念

- 1.1.1 什么是信息
- 信息的确切定义理论界尚无定论。信息论奠基人Shannon在《通信的数学理论》一文中指出：信息是“两次不确定性之间的差异”，是用来消除随机不确定性的东西。
- 控制论创始人维纳认为：信息是人与外部世界互相交换的内容。

- 现在一般认为：所谓信息，就是客观世界中各事物的变化和特征的最新反映，是客观事物之间联系的表现，也是客观事物状态经过传递后的再现。
- 信息是主观世界与客观世界联系的桥梁。
- 在客观世界中，不同的事物具有不同的特征，正是这些特证给我们带来了不同的信息，从而使我们能够认识客观事物。

- 信息具有如下特征：
- 1.普遍性和可识别性。
- 只要有物质存在，只要有变化着的事物或运动着的客体，信息就会存在。普遍性。
- 通过感官或其他探测手段来直接或间接识别出客观事物的形状、特征及变化所产生的信息，找出其中的差异，即进行信息的识别，这也是认识信息的关键。
- 2.存储性和可处理性。
- 信息依赖于物质和意识，又可以脱离物质和意识独立存在，并存储起来。
- 通过信息载体将信息保存。同时对信息可以处理。
- 处理既是对信息的更好开发与利用，同时也是对传递与存储信息提供了极大便利。

- 3.时效性和可共享性。
- 一个信息的生成、获取的越早，传递的越快，其价值就越大，随着时间的推延，价值就会衰减。
- 信息可以被多个主体所利用，即共享性。
- 4.增值性和可开发性。
- 通过对资源的最佳配置，发挥最大作用，利用已有信息进一步探索和发掘。
- 5.可控性和多效用性。
- 信息具有可扩充、可压缩、可处理的特点，这使得信息技术具有可操作性，但也增加了信息技术利用的复杂性。
- 无论是认识世界还是改造世界，信息都是基础，是知识的源泉、决策的依据、控制的灵魂、管理的保证。
- 信息还具有可转换性、可传递性、独立性和可继承性，具有很强的社会功能，主要表现在资源功能、教育功能、娱乐功能和舆论功能等方面。

- **1.1.2 什么是信息安全**
- 与信息一样，对于信息安全也没有统一的定义。
- 从信息安全研究的内容来看，主要涉及两大类：一般信息技术系统的安全，特定信息体系的安全(如银行信息系统，军事指挥系统)。
- 信息安全，应该确保信息的完整性(integrity)，可用性(availability)，保密性(confidentiality)，可控性(controlability)和可靠性。信息系统安全的内在含义就是采用一切可能方法和手段，确保信息的上述五性。

- 完整性：是指信息在存储或传输过程中不被修改、破坏、插入、延迟、乱序和丢失。破坏信息的完整性是对信息系统发动攻击的最终目标。计算机病毒也会破坏信息的完整性。
- 可用性是指信息可被合法用户访问并按要求顺序使用。对可用性的攻击就是阻断信息的使用，如破坏网络系统的正常运行等。计算机病毒的入侵是对可用性的一大挑战。
- 保密性是指信息不泄露给非授权的个人和实体，或不供其使用。这里需要借助密码技术。

- 可控性是指授权机构可以随时控制信息的机密性，密钥托管、密钥恢复等措施就是实现信息安全可控性的手段。
- 可靠性是指信息系统以用户认可的质量连续服务于用户。这涉及硬件和软件两方面的可靠性问题。

- 有些信息安全问题与程序设计开发者有关
- 程序设计缺陷或疏忽造成
- （1）缓冲区溢出
- 攻击者通常会设法造成溢出到系统空间，由此替换系统空间中的代码，这样在其过程调用返回时就可以替换一些指令从而控制操作系统

- http://www.somesite.com/subpage/userinput&parma1=(808)-555-1212&parm2=2004jan02
- 这里userinput页面收到了两个参数，值为：(808)-555-1212和2004jan02
- 调用者的浏览器将接受用户从表格中填写的数值，并加密后传送给服务器。
- 攻击者若输入一个非常长的电话号码，例如500位。
- 开发者通常只分配了15或20个字节。
- 若500位后，是否会由此造成程序的崩溃？如果崩溃，将是怎样的？是否可以被按照预定的崩溃的方式进行？
- 攻击者通常是利用溢出先造成系统的崩溃，然后制造出 可控制的故障，从而导致了系统的严重安全隐患。
- 设计时应该对输入有控制。

- (2)验证不完全
- http://www.somesite.com/subpage/userinput&parma1=(808)-555-1212&parm2=2004jan02
- 如果parm2提交的值是1800Feb30或2048Min32将会造成什么后果？
- 对于不正确的数据系统尝试处理，可能会造成系统故障，或者照常运行而得出错误的结果，如帐单计算，就会出错。
- 采用对提交数据正确性检查，或者通过下拉列表选择，从而避免用户有意或无意的破坏。
- 但是，提交的结果最终是包含在URL中进行传递的，而用户特别是攻击者完全可以操作或更改URL的，而服务器是无法区分该条信息是来自客户端的浏览器还是用户直接编辑修改的URL的。

- 电子商务网站，用户可以直接在网站上下订单。
- 物品，价格等。如某物品555A单价10元，购买20个，再加上运费共205元，系统将所有这些信息再显示的同时全部传回去：
- http://www.things.com/order/final&custID=101&part=555A&qy=20&price=1&transportcost=5&total=205
- 攻击者可以通过URL将价格数值从205改到25，。
- 攻击者可以用此方式以任何价格订购物品，直到漏洞被检查出来。
- 因此，如果提交的数据不进行完善的验证，敏感的数据将处于公开或失控的状态。
- 如何验证？
- 需要密码技术

## （3）陷门

- 在代码开发期间加入，其目的可能是为了测试软件模块，或为将来模块的修改和功能增强提供hook(钩子)，或作为系统失效时提供的一个特别通道。
- 当程序成为产品后，陷门可使程序员进入系统。
- 还有bug等
- 境外服务商在出口信息产品中，预先安装技术后门，收集信息
- Symatec产品后门是美国联邦调查局为反恐根据美国法律设置后门，收集信息
- 日本智能复印机复印一张记录一张在芯片上，以后更换设备收回该芯片

- 1.1.3 信息系统的安全体系结构
- 要构建安全的信息系统，必须从几个方面来考虑：
- 1.物理安全
- (1)自然灾害（如雷电、地震、火灾等），物理损坏（如硬盘损坏、设备使用寿命到期等），设备故障（如停电、电磁干扰等），意外事故。解决方案是：防护措施，安全制度，数据备份等。
- (2)电磁泄漏，信息泄漏，干扰他人，受他人干扰，乘机而入（如进入安全进程后半途离开），痕迹泄露（如口令密钥等保管不善）。解决方案是：辐射防护，屏幕口令，隐藏销毁等。

- (3)操作失误（如删除文件，格式化硬盘，线路拆除等），意外疏漏。
- 解决方案是：状态检测，报警确认，应急恢复
- (4)计算机系统机房环境的安全。解决方案：加强机房管理，运行管理，安全组织和人事管理。
- 2.安全控制
- (1)微机操作系统的安全控制。
- (2)网络接口模块的安全控制。在网络环境下对来自其他机器的网络通信进程进行安全控制。
- (3)网络互联设备的安全控制。

- 3.安全服务
- 包括：对等实体认证服务、访问控制服务、数据保密服务、数据完整性服务、数据源点认证服务和禁止否认服务
- 4.安全机制
- 包括：加密机制、数字签名机制、访问控制机制、数据完整性机制、认证机制、信息流填充机制、路由控制机制和公证机制
- 造成安全缺陷的主要原因是受入侵主机的错误配置。

- 大多数操作系统都处于一种不可靠的状态中。可以归纳为：安装软件不可靠性的主动状态和被动状态。
- 1.主动状态
- 常见的主动状态不可靠问题的例子有：
- 网络打印服务程序，文件共享服务程序，缺省口令，联网程序实例
- 2.被动状态
- 被动状态涉及具有安全程序的操作系统。安全程序如果系统管理员不激活它们的话，将毫无用处。
- 安全程序要占用更多的资源，给用户更多的限制。
- 必须根据网络数据的敏感性，依靠可行的安全度量方法去权衡利弊。

- ISO于1989年12月颁布了ISO7498-2标准，确定了开放系统互连参考模型(ISO7498标准)的信息安全体系结构，我国将其作为GB/T9387-2标准，该标准规定了五大类安全服务以及提供这些服务所需的八大类安全机制。
- 五大类安全服务是：鉴别，访问控制，数据保密性，数据完整性和不可否认性。
- 鉴别安全服务可以鉴别参与通信的对等实体和数据源。
- 访问控制提供的服务能够防止未经授权而获取资源。
- 数据保密性是防止数据未经授权而泄露。分为连接保密性、无连接保密性、选择字段保密性和业务流保密性。

- 数据完整性用于对付主动威胁。分为：带恢复的连接完整性、不带恢复的连接完整性、选择字段连接完整性、无连接完整性、选择字段无连接完整性。
- 不可否认包括带数据源证明的不可否认和带递交证明的不可否认。
- 为提供安全服务所需要的八大机制是：加密、数据签名机制、数据完整性机制、鉴别交换机制、业务填充机制、路由控制机制和公证机制。

# 1.2信息安全与法律

- 世界上第一例计算机犯罪案例产生于1958年的美国硅谷,但直到1966年10月才被发现.1966年10月,唐.B.帕克在美国斯坦福研究所调查与电子计算机有关的事故和犯罪时,发现一位计算机工程师通过篡改程序的方法在银行存款余额上做了手脚.这个案件是世界上第一例受到法律追诉的计算机案件.
- 1995年统计，以白领犯罪为特征的信息技术犯罪事件给全球造成的经济损失高达150亿美元
- 1995年8月21日，美国华尔街日报报道，尽管美国花旗银行装备了防火墙，并拥有其它高技术的防范措施，但是，1994年仍被前苏联克格勃人员弗拉基米尔莱文，在俄罗斯使用一台286电脑，通过计算机网络转移了1160万美元的巨资，美国联邦调查局（FBI）的C-37特工行动小组花费了不少力气才将此案搞定。
- 美国洛杉矶的城市银行就曾被电脑“黑客”从账户上凭空划走了40万美元。

我国第一例计算机犯罪:1986年7月22日,港商前往深圳市人民银行和平路支行取款,计算机显示其存款少了2万元人民币.

两个月后，某驻深圳办事存入银行的3万元港币也不翼而飞.通过侦查发现上述两笔存款均被同一犯罪分子利用计算机知识伪造存折和隐形印鉴诈骗而去.从此以后,原来只在报道中看到的在国外才有可能出现的计算机犯罪现象,之后在国内也频频发生

- 我国计算机犯罪的增长速度超过了传统的犯罪
  - 97年20几起发展到2000年的近4000起。
  - 这几年则是以每年30%的速度递增
- 利用计算机实施金融犯罪已经渗透到了我国金融行业的各项业务。

➢ 互连网上盗用帐号这类案件成了网上一个很突出的问题

2000年广东破获了一起案件，有人攻进了中国电信的认证中心，窃取了没买出的所有的163卡帐号，价值500万元。

- 近年来，还出现了一些利用网络窃取和出卖国家机密的事件，包括有些网络高手，负责国家重要军事机密的军队科技人员，国家机关人员
- 无意犯罪泄露机密：

  google地图，标注功能

  某基地警卫人员退役后，看到google地图恰好显示自己工作地方，就在上面标注每个地方的功能。
- 日益增长的信息技术犯罪活动和泄密事件已构成了对国家安全和防御、政治、经济、科学技术、社会生活的严重破坏和威胁。

# 1.2.1信息技术犯罪概念

- 信息技术犯罪是一种高技术手段的犯罪活动。从某种意义讲，电脑犯罪是随时随地可以进行的。
- 随着计算机网络的建立和发展，地理上的界限已不能阻挡这些犯罪活动的发生，对于军事系统或金融系统的计算机作案可以在一个国家内进行针对另外一个国家的破坏活动。

- 我国有关方面提出的这方面犯罪定义是：以计算机及网络系统为工具或以信息系统资产为对象(包括硬件系统、软件系统和机时、网上资源等)实施的犯罪行为。
- 当前信息技术犯罪主要有以下类型：
- (1)对程序、数据、存储介质的物理性破坏。
- (2)窃取或转卖信息资源。
- (3)利用系统中存在的程序或数据错误，进行非法活动。
- (4)非法进行程序修改活动。

# 信息技术犯罪主要类型(续)

- (5)种植破坏程序勒索钱财
- (6)信用卡方面的犯罪

# 1.2.2信息技术犯罪的手段与特点

- 主要有以下犯罪手段：
- (1)数据欺骗——在计算机系统中，非法篡改输入/输出数据。
- (2)特洛伊木马——这种方法是在程序中暗中存放秘密指令，使计算机在仍能完成原先指定任务的情况下，执行非授权的功能。

特洛伊木马的关键是采用潜伏机制来执行非授权功能

# 信息技术犯罪的手段(续)

- (3)超级冲杀——超级冲杀是一个当计算机停机、出现故障或其他需要人为干预时计算机的系统干预程序。它相当于系统的一把总开关钥匙。如果被非授权用户使用，就构成了对系统的潜在威胁。
- (4)活动天窗——这是利用人为设置的窗口侵入系统。通常指故意设置的入口点，通过入口点可以进入大型应用程序或操作系统。
- 罪犯利用它来寻找系统软件的薄弱环节，进行非法侵入活动。

## 计算机犯罪的手段(续)

- (5)逻辑炸弹——这是插入程序编码，这些编码仅在特定时刻或特定条件下执行，故称为逻辑炸弹或定时炸弹。逻辑炸弹的关键是特定条件下的程序激活。
- (6)浏览——在系统或终端设备上，利用合法使用手段进行搜索或访问非授权文件。
- (7)数据泄露——有意转移或窃取信息的一种手段。

# 信息技术犯罪的手段(续)

- (8)冒名顶替——利用窃取用户的口令，冒名窃取信息，或者当一个用户在用口令进入工作状态后临时短暂离开，就会被他人以用户身份获取信息或数据。
- (9)蠕虫——蠕虫是通过网络来扩散错误，进而危害整个系统。在分布式系统中，可通过网络来传播错误，进而造成网络服务发生死锁。通常需要重新启动系统才能排除蠕虫对系统的恶性作用。
- (10)间接窃取信息——利用统计信息数据推导机密信息。

- 随着信息技术的进步，信息技术犯罪方式和手段也日趋复杂和多样化，而预防和安全措施还跟不上节奏。在现代生活中，信息技术犯罪有下述特点和趋势：
- (1)罪犯趋向年轻化，目前信息技术犯罪的人员平均年龄为25岁。
- (2)罪犯往往是最熟练和有知识的技术人员，往往是掌握核心机密的人。
- (3)信息技术犯罪采用的手法和正常活动只有很小的偏差。专家进行未授权活动，往往不被制止，

## 信息技术犯罪有下述特点和趋势(续)

- (4)信息技术犯罪是可在瞬间发生的高技术犯罪，往往不留痕迹，在法律上难以拿到证据。
- (5)信息技术犯罪活动趋向国际化，有的计算机犯罪是在罪犯跑到其他国家最后实施的。
- (6)信息技术犯罪组成的经济损失巨大，而罪犯往往并不意识到。

# 1.2.3有关信息安全的法律、法规与法律责任

- 为了有效制止信息技术犯罪，从1986年起，根据我国实际情况，借鉴国外有益经验，陆续制定了有关信息系统安全的标准和法律、法规。目前正式颁布执行的有关信息系统安全的法律、法规和管理条例见下表。

| 法 律 、 法 规 名 称 | 实 施 日 期 |
| --- | --- |
| 计算机软件保护条例 | 1991 年 6 月 4 日 |
| 中华人民共和国计算机信息系统安全保护条例 | 1994 年 2 月 18 日 |
| 中华人民共和国计算机信息网络国际联网管理暂行规定 | 1996 年 2 月 1 日 |
| 中华人民共和国计算机信息网络国际联网管理暂行规定实施办法 | 1997 年 12 月 8 日 |
| 计算机信息系统安全专用产品检测和销售许可证管理办法 | 1997 年 12 月 12 日 |
| 计算机信息网国际联网安全保护管理办法 | 1997 年 12 月 30 日 |
| 商用密码管理条例 | 1999 年 10 月 7 日 |
| 互联网信息服务管理办法 | 2000 年 9 月 20 日 |
| 中华人民共和国电信条理 | 2000 年 9 月 5 日 |
| 全国人大常委会关于网络安全和信息安全的决定 | 2000 年 12 月 29 日 |

- 对信息技术犯罪及应承担的刑事责任，1997年全国人大通过的《刑法》修正案对此也作了规定：
- 对违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的；或者故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行而造成严重后果的，都将追究刑事责任，处三年以下有期徒刑或者拘役。
- 对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行；或者对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作，由此造成严重后果的，也要追究刑事责任，处五年以下有期徒刑或者拘役，后果特别严重的，处五年以上有期徒刑。

- 总之，有关信息系统的安全条例和法律、法规正在不断制定和完善中，它们对于促进和保障我国信息产业发展和应用，对于维护国家主权和独立，对于巩固国防和国家经济建设的顺利发展，对于保护公民在数据和信息资源方面的合法权益，都起着重要作用。
- 国家制定和实施有关信息安全的法律、法规，是希望从事这方面研究、开发、应用的人们和爱好者能够有章法可依，不做对信息系统有害的事，防止不安全因素对信息系统可能引起的破坏。
- 信息系统的建设者和应用者都应当遵守国家的法律法规，共同维护信息系统的安全。
- 对于程序设计错误或疏漏造成的损失如何考虑？

# 1.3信息安全的风险评估

- 需要对企业资源、财务情况、信息系统可能受到的攻击及后果进行分析评估，即所谓的风险评估。
- 有些风险是可以预料的，有些是不以人们的意志为转移的，必须尽最大限度的努力找到它们并采取预防措施减少危害。
- 风险的核心因素是不确定性。
- 当把服务器连接到互连网时，是否会受到攻击？
- 可能被黑掉，也可能永远都没有成为攻击的目标。
- 结果不确定，但威胁确实是始终存在的。
- 风险评估目的就是对有负面后果的潜在威胁进行评估
- 进而确定是否要采取措施，采取何种程度的措施。

- 风险评估是信息安全体系建立过程中极其关键的步骤，它连接着安全保护产品和用户需求。
- 风险评估揭示了用户商业活动对资源保密性、集成性和可用性等方面的影响。
- 任何安全产品都要花费一定代价，而使用安全产品的用户都有自己的目的。
- 风险评估可以清晰地揭示用户的实际目标，从而确定采用何种安全产品。

- 风险评估一般需要调查以下7个问题：
- 会出现什么威胁？如果威胁发生，最坏结果是什么？对用户造成的资产损失是多少？
- 这种威胁发生的频率是多少
- 前3个问题的答案有多肯定？
- 有哪些安全措施和设备可以消除、减轻或转移风险？
- 这些措施和产品需要多少资金？
- 这些措施和产品的实际使用中有多有效？

- 一般分6个步骤进行(以公司为例)：
- 1.资产清单及其相应范围
- 2.信息系统脆弱性和威胁的评估
- 3.安全措施及产品的有效性评估
- 4.分析、决策并形成文档。
- 5.沟通与交流
- 6.监督实施
- 具体来讲要分析清楚公司的关键业务流程，得出对应流程的资产表，根据历史状况和现实威胁各关键流程受到各种攻击的概率。
- 针对上述所列攻击应采用的安全防范控制措施及成本分析，由此形成决策。

- 在实际评估中，如何获取有关信息并通过分析得出结论涉及到风险分析，这也是一个值得研究的内容，也形成了方法学——风险评估方法学，常用的评估分析方法有：
- 树状分析法——侧重于导致某一特定情况的过程或事件发生顺序的分析方法，事件树，攻击树，错误树等
- 历史分析法——调查以往事故发生频率以判断未来发生的概率。
- 人为错误分析法——调查人为错误和干预对事件发生造成的影响。
- 风险概率评估法——调查某种情况组合发生的概率
- 失误模型及后果分析法——调查系统中每个潜在的失误条件以确定其影响严重程度。
- HAZOP(Hazard and Operability,危险和可操作性分析法)——调查操作流程以评估因不合理的设计指标而产生潜在的危险。

# 1.4加强信息安全，迎接时代挑战

- 用信息为武器的战争形式随着信息化时代的到来而到来。
- 无法确定哪些信息是真的，哪些信息是敌方伪造的，甚至核武器的控制信息也可能被更改，使它可能根本无法发射，或者就在发射井中爆炸，或帮助敌方毁掉自己的城市。

- 信息战是指信息领域中敌我双方争夺信息优势，获取控制信息权的战斗。
- 信息战分为信息防御战和信息攻击战。
- 信息攻击战包括偷窃数据、散播错误信息、否认或拒绝数据存取、从物理上摧毁作为数据存储和分发的部分磁盘及武器平台与设施。
- 信息防御战使用病毒检查、嗅探器、密码和网络安全系统抵御敌方的进攻。
- 信息战的攻击对象主要是信息，
- 对敌方信息或窃取或更改或破坏，甚至毁坏信息基础设施，
- 使对手完全丧失处理信息的能力是信息战的战略目标。

- 信息战的主要武器将是软件武器、芯片陷阱、电磁窃听、高能射频枪等
- 计算机病毒、逻辑炸弹和特洛伊木马成为信息战的主要武器。
- 计算机病毒对抗的研究就是企图把计算机病毒通过无线电方式、网络方式等，植入到对方，伺机破坏对方武器系统的计算机系统，使他们的计算机在关键时刻受到诱骗或崩溃。

- 芯片陷阱就是设计者为预定目的而对计算机芯片进行修改或更改集成电路的行为，如可以使芯片有优先接受特定指令的能力，这样只要卫星系统发出命令，就可使使用这些芯片的信息系统发生逻辑错误甚至崩溃。
- 电磁窃听是指利用电磁窃听装置把对方计算机大量的信息电磁辐射予以复原。
- 高能射频枪是一部无线电发射机，对一个电子目标发射大功率无线电信号，使其无法工作，甚至使整个网络系统失灵。

- “谁掌握了信息，控制了网络，谁就将拥有整个世界。”

  （美国著名未来学家阿尔温 托尔勒）

- “今后的时代，控制世界的国家将不是靠军事，而是信息能力走在前面的国家。”

  （美国前总统克林顿）

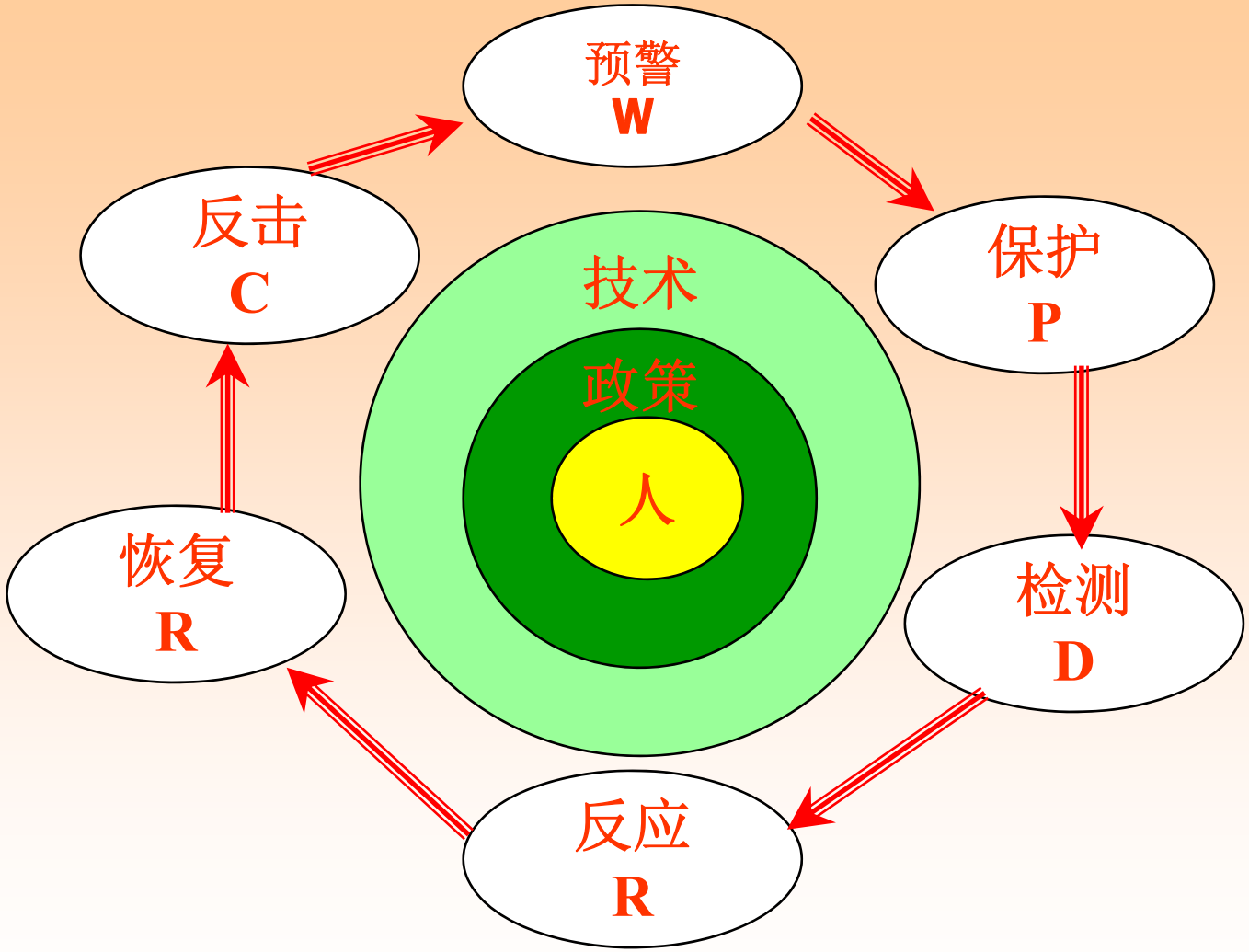
- “信息时代的出现，将从根本上改变战争的进行方式。”

  （美国前陆军参谋长沙利文上将）

- 1995年，美国国防部组建信息战执行委员会，10月组建世界上第一支信息战分队。之后，美国陆、海、空三军相继成立信息战中心。
- 1990年海湾战争，被称为“世界上首次全面信息战”，充分显示了现代高技术条件下“制信息权”的关键作用。
- 科索沃战争，再次证明信息网络已成为高技术战争的重要对抗领域。
- 美国联邦调查局（FBI）一直运用“食肉者”电子邮件监听系统监听全球电子邮件。

# 信息化士兵

- 信息安全在IT中的位置
  - 芯片是细胞
  - 电脑是大脑
  - 网络是神经
  - 智能是营养
  - 信息是血浆
  - 信息安全是免疫系统


预警
W
保护
P
检测
D
反应
R
恢复
R
反击
C
技术
政策
人

- 信息安全是免疫系统
- 其核心技术就是密码技术。
- 任何级别的安全防护系统都需要引入加密方案。
- 加密可以用来保护互联网上的数据通信，保护局域网、电子邮件和数据库中的数据。
- 数据加密对网络通信，数据存储有着重要意义，它能起到数据保密，身份验证，保持数据完整性，确认事件的发生等作用。

- 过去的战争是谁拥有最好的武器，谁就可能在战争中取胜。而今天，则是谁掌握了信息控制权，谁就胜利在望。
- 我们现在善于接受新的事物，以敏捷的行动不断地拿来，而忽视了注意新事物往往还伴随挑战、威胁和侵略。
- 联想收购购IBM个人计算机部门时，美国政府做了专门审核并做了严格规定，原由IBM提供给军方的今后不能由联想直接提供,而要通过军方授权的美国公司统一采购并检查后再使用，一是避免让使用单位曝光，二是避免留有后门陷阱。
- 因此我们必须重视信息安全，大力发展自己的信息系统和安全产品，迎接时代的挑战。

# 第2章 密码学概论

- 随着计算机病毒所带来危害的日益加剧，计算机犯罪事件不断的增加，黑客攻击的日益频繁，信息安全已成为人们不得不面对的问题。
- 互联网的广泛使用，全世界都在自投入网，如果不加强网络安全，则将被一网打尽。
- 无论是信息安全本身，还是系统本身的安全，都需要密码技术。
- 作为信息安全的核心技术——密码技术成为人们研究和关注的重点。
- 有关信息加密技术的研究，特别要注意重视自主开发。

- 对于DES算法加密产品，美国中央情报局对密钥位在20多年前曾作过预测和比较：

| | 40bit 位 | 56bit 位 |
|---|---|---|
| 400 美元 | 5 小时 | 38 年 |
| 300 万美元 | 24 秒 | 10 天 |
| 1 千万美元 | 7 秒 | 13 小时 |
| 1 亿美元 | 0.2 秒 | 12 秒 |

美国政府作出限制密钥为56bit位的产品出口，而2000年开始放宽出口限制，但其背景是什么呢？

对密钥为56bit位DES只要化25万美元，在不到3天就可破译。

- 密码技术涉及哪些内容？
- 下面通过简单例子来引入。
- Alice和Bob想在晚上一起出去，但定不下来是去电影院还是歌剧院，他们达成协议，通过掷硬币来决定
- 如果他们是通过电话来执行上述协议，显然无法公平实现，因为一方无法验证对方掷硬币的结果。
- 如果在协议中加入密码技术，可形成适合在电话上工作的形式。
- 把密码技术看成函数$f(x)$:Z到Z,且具有性质：
- (1)对任意函数，由x计算f(x)是容易的,而给出$f(x)$，要找出对应的x是难的；
- (2)找出一对整数(x, y),满足$x \neq y$而$f(x)=f(y)$是难的。
- 密码技术将研究探讨容易，难的的数学描述，建立量化表示。

- 电话掷币
- 1.Alice 选择一个大随机数x，并计算*f*(x);然后通过电话告诉Bob *f*(x)的值；
- 2.Bob告诉Alice自己对x的奇偶猜测；
- 3.Alice告诉Bob x的值；
- 4.Bob验证*f*(x)并查看所做猜测是否正确。
- 在开放的计算机和通信网络中保证安全通信，采用密码技术是有效且是唯一可行的方法。
- 电子商务，事务处理，等信息系统对安全的需求，导致了很多密码系统和协议的产生。

# 2.1 信息加密的基本概念

- 密码学分为密码编码学和密码分析学两个分支。
- 密码编码学是对信息进行编码实现隐蔽信息的一门学问
- 密码分析学则是研究分析破译密码的学问
- 两者互相对立，又互相促进向前发展。

- 密码学(Cryptology)一字源自希腊文“kryptós”及“logos”两字，直译即为“隐藏”及“讯息”之意。
- 密码学的起源追溯到人类刚刚出现，并且尝试去学习如何通信的时候。
- 寻找方法确保他们的通信的机密。

- 由于战争指挥与传递情报的需要，据文字记载，早在战国时期（公元前403～前221年）我国就开始使用秘密通信方法。
- 如战国中、后期成书的军事著作《六韬》中的《阴符》和《阴书》就记载了当时秘密通信的具体形式与方法。
- “阴符”就是一种符节，双方事先约定好，多长的符节各代表什么意思。
- “阴书”就是一封竖写的完整的秘密信件或情报，拦腰截成3段，派3个人各持一段，于不同的时间、路线分别出发送给收信人。收信者收齐3段信，即可知晓全部内容。万一途中某一个送信者被截获，对方也难以解读全信内容。

- 秦汉以后，在秘密通信中出现了各种暗语、暗号、密诗、符号等形式，不易为外人破解，还有的将密信用蜡密封或火漆、封泥密封，以防泄密，一旦泄露，即可立即发觉，采取补救措施，或将计就计，改变对策。

- 宋代军用密码
- 北宋时期，北宋仁宗庆历四年(1044年)，由枢密使曾公亮、枢密副使丁度奉诏主编的《武经总要》(40卷)是对宋代国防建设和军事教育都有指导性的综合性军事教程，也是研究北宋以前学术发展和北宋军事理论及实践的重要历史资料。
- 《武经总要》记载，宋代出现的传递情报的密码叫作“字验”。
- “字验”，就是将各种情报，如请粮料、请添兵、请固守、被贼围、将士叛、将领病、贼退军、贼进军等40项，用40个字的一首诗来表示，把不含重复的40字诗与这些情报内容依次相对并具体搭配，编上相应的数字代号，从1至40。密码本只能由军中主将掌握，每次使用时，可根据所需传递情报内容，在新抄写的这首诗应加符号的字下面，加上规定的符号即可。对方收到这首诗后，查对密码本就能译出情报内容。这种密码本即使落入敌手，也不会被敌人破译，即使送信人投降叛变，也无法帮助敌人破译出所传递的情报。

- 例如通信双方选定一首五言诗，共40个字，作为解码密钥。诗文如下：
- 望洞庭湖赠张丞相
- 八月湖水平，涵虚混太清。
- 气蒸云梦泽，波撼岳阳城。
- 欲济无舟揖，端居耻圣明。
- 坐观垂钓者，徒有羡鱼情。
- 统兵将领根据战场形势可随时与主帅联络。
- 敌军占据优势，无法实施进攻，统兵将领请求固守阵地时，先查出“请固守”是密本中的第19个术语，而诗中的第19个字是“阳”。就在信上写上“阳”字，并在该字上盖上印章。主帅接到信后，马上可以破译出统兵将领来函的意图。如果他同意下属的意见，就重新写下这个字并加盖自己的官印；如不同意，印章就不盖在那个字上。
- 这样统兵将领与主帅可随时保持联络。
- 这种通信方式具有极强的保密性。

- 密写技术
- 在13世纪初，“密写”也是广泛应用传递情报的手段之一。
- 1216年，蒙古军队围攻太原府，金宣抚使兼左副元帅乌古论礼，派遣间谍携带用明矾水密写的书信，抄近沿偏僻小道星夜兼程赶往金国京城汴京告急，诏发援兵，不久解围，乌古论礼遂官升两级。
- 直至近代中国，这种“密写”方法也还是传递情报的常用方法之一。

- 罗马的军队用凯撒密码进行通信。
- 当年凯撒大帝行军打仗时用这种方法进行通信，因此得名。
- “This is Caesar Code”。用凯撒密码加密后字符串变为“vjku ku Ecguct Eqfg”。
- 看起来似乎加密得很“安全”。把这段很难懂的东西每一个字母换为字母表中前移2位的字母，结果出来了。凯撒密码的字母对应关系：

  A b c d e f g h i … x y z

  C d e f g h I j k … z a b

  $e_k(x)=x+k(mod26)$ k=3
- $d_k(y)=y-k(mod26)$
- 单字母的替换。

- 密码学的发展可以分为两个阶段。第一个阶段是计算机出现之前的，这是传统密码学阶段，基本上靠人工对消息加密、传输和防破译。第二阶段是计算机密码学阶段。
- 传统方法的密码学阶段，解密是加密的简单逆过程，两者所用的密钥是可以简单地互相推导的，因此无论加密密钥还是解密密钥都必须严格保密。这种方案用于集中式系统是行之有效的。
- 现代计算机密码学阶段包括两个方向：一个方向是公开密钥密码（RSA），另一个方向是传统方法的计算机密码体制，秘密密钥密码，如数据加密标准（DES）。

- 对信息进行编码可以隐蔽和保护需要加密的信息，使未授权者不能提取信息。
- 被隐蔽的信息称为*明文*，
- 编码后明文变换成另一种隐蔽形式，称为*密文*。
- 这种变换过程称为*加密*
- 其逆过程，即由密文恢复成原明文的过程称为*解密*。
- 对明文进行加密时所采用的一组规则称为*加密算法*
- 对密文进行解密时所采用的一组规则称为*解密算法*。

- 加密和解密算法的操作通常都是在一组密钥控制下进行的，分别称为*加密密钥*和*解密密钥*。
- 密钥是密码体制安全保密的关键，它的产生和管理是一个重要研究课题。
- 在一个密码体制中，如果加密密钥和解密密钥相同，或从一个易得到另一个，就称其为*单钥密码体制*或*对称密码体制*。
- 如果在密码体制中，加密密钥和解密密钥不同，且从一个难于推出另一个，则称为*双钥密码体制*或*非对称密码体制*，
- 1976年由Diffe和Hellman等人所开创的新体制

- 采用双钥体制的每个用户都有一对选定的密钥：一个是可以公开的，另一个则是秘密的。
- 公开的密钥可以进行注册公布，因此双钥密码体制又称为*公钥密码体制*。
- 其主要特点是将加密和解密能力分开，从而实现多个用户加密的信息只能由一个用户解读，或只能由一个用户加密信息而使多个用户解读。

- 在信息传输和处理系统中，除了确定的接受者外，还有非授权者
- 他们通过各种办法（如搭线窃听、电磁窃听、声音窃听等）来窃取机密信息。
- 他们虽然不知道系统所用的密钥，但通过分析可能从截获的密文推出原来的明文，这一过程称为*密码分析*。
- 研究如何从密文推出明文、密钥或解密算法的学问称为*密码分析学*。

- 为了保护信息的保密性，抗击密码分析，信息加密系统应满足如下要求：
- (1)系统至少为实际上不可破，即，从截获的密文或某些已知明文密文对，要决定密钥或任意明文在计算上是不可行的
- (2)系统的保密性只依赖于密钥的保密。
- (3)加密和解密算法适用于所有密钥空间中的元素。
- (4)系统便于实现和使用方便。

- 为了防止信息被篡改、删除、重放和伪造，就要求系统具有对发送的信息验证的能力，使接收者或第三者能够设别和确认信息的真伪。
- 实现这类功能的系统称为*认证系统*。
- 信息认证要求能保证任何不知密钥的人不能构造出一个密文，使确定的接收者脱密成一个可理解的信息。
- 信息的完整性，它表示在干扰条件外，系统保持恢复信息和原来发送信息一致性的能力，实际中常借助于检错和纠错技术来保证信息的完整性。
- 信息系统安全的中心内容是保证信息的保密性、认证性和完整性。

# 2.2 单表代换密码

- 2.2.1代换密码概述
- 令A表示明文字母集，它有q个字母或字符，可以抽象地用$Z_q=\{0,1,2,\ldots, q-1\}$来表示。
- 在加密时，将明文分成长为L的信息单元，称为*明文组*，用m表示，即$m=(m_0m_1\ldots m_{L-1})(m_i\in Z_q)$。
- 通常称m为L-报文，它是定义在$Z_q^L$上的随机变量($Z_q^L$是$Z_q$上的L维向量空间)。明文空间$M=\{m|m\in Z_q^L\}$。

- 令A'表示密文字母集，它有q'个字母或字符，可用$Z_{q'}$={0,1,2,…，q'-1}来表示。密文单元为c=($c_0c_1…c_{L'-1}$)($c_i \in Z_{q'}$)。c是定义在$Z_{q'}^{L'}$上的随机变量（$Z_{q'}^{L'}$是$Z_{q'}$上的L'维向量空间）。密文空间C={c|c∈$Z_{q'}^{L'}$}.当A=A'时，有C={c|c∈$Z_q^{L'}$}，即明文和密文由同一字母表构成。
- 加密变换是由明文空间到密文空间上的映射
- *f*: M→C(m∈M，c∈C)
- 当*f*是一一对应映射时，存在逆映射$f^{-1}$，使

$$f^{-1}(c) = f^{-1} \circ f(m) = m \quad (m \in \mathrm{M}, c \in \mathrm{C})$$

- 加密变换通常是在密钥控制下变化的，即
- $c=f(m,k)=E_k(m)$
- 其中$k \in Y$，Y为密钥空间。
- 一个密码系统就是在*f*作用下由M→C的映射，或以C中的元素代替M中的元素，在此意义下称这类密码为*代换密码*。
- 当L=1时，称为*单字母代换*，L>1时，称为*多字母代换*。

- 一般选择A=A'，即明文和密文字母表相同。
- 若L=L'，则映射*f*可以构造成一一对应，密码没有数据扩展。
- 若L<L'，则有数据扩展，可使映射*f*为一对多的，即明文组可能找到多于一个密文组来代换，称为多名代换密码。
- 若L>L'，则明文数据将被压缩，此时每个明文组无法找到唯一的只与它相对应的密文组，映射*f*是不可逆的，从密文无法完全恢复成明文信息
- 在信息加密时必须是L≤L'。
- 而L>L'的变换可用在数据认证系统。

## 2.2.2几种代换密码

- 在代换密码中，当A=A',q=q',L=L'时，如果明文的所有字母都用一个固定的明文字母表到密文字母表的映射，即$f$：$Z_q \rightarrow Z_q$，则称这种密码为*单表代换*。
- 令明文m= $m_0m_1\ldots$，则其相应密文为：
- $c=E(m)=c_0c_1\ldots=f(m_0)\ f(m_1)\ldots$
- 若明文字母表$A=Z_q=\{0,1,\ldots,q-1\}$，则相应的密文字母表为$A'=\{f(0),\ f(1),\ldots f(q-1)\}$，A’是A的某种置换。
- 如何控制？密钥

- 最直观的是与密钥加，或乘，但关键是否都能从密文恢复为明文？

- 1.加法密码
- 加法密码表达式为：
- $E_k(i)=(i+k)\equiv j \mod q$ $0\le i,j<q$, $Y=\{k|0\le k<q\}$
- 其中密钥空间元素个数为q
- k=0为恒等变换。
- 解密变换为：
- $D_k(j)= E_{q-k}(j)\equiv j+q-k\equiv i+k-k\equiv i \mod q$
- 密文字母表是将明文字母表循环左移k位
- 由于k只能取25个不同数字（除去k=0的恒等变换），故安全性极差。

- 例2.1：对英文26个采用加法密码，选定密钥为k=5，则有代换表：
- 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
- A': 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
- 明文m=This is aprivate conversation
- 密文c=YMNX NX FUWNAFYJ HTSAJWXFYNTS

- 2.乘法密码
- 乘法密码的加密变换为
- $E_k(i)=ik\equiv j \bmod q \quad 0\le i,j<q$
- 其密文字母表是将明文字母表按下标每隔k位取出一个字母排列而成。
- 例2.2：对英文26个采用乘法密码，选定密钥为k=7，则有代换表：
- A =abcdefghijklmnopqrstuvwxyz
- A'=AHOVCJQXELSZGNUBIPWDKRYFMT
- 对明文m=multiplicative cipher
- 有密文c=GKZDEBZEOADERC OEBXCP

- 确保$E_k$是一一对应的。
- 不加证明地给出定理：
- 定理2.1 当且仅当$(k,q)=1$时，$E_k$才是一一对应的。
- 由定理可知，乘法密码的密钥个数为$\varphi(q)$($\varphi(q)$表示小于q且与q互素的个数，称为整数q的欧拉函数）
- 除去$k=1$这一恒等变换，可供选择的密钥为$\varphi(q)-1$个。

若$q=\prod_{i=1}^{r} p_i^{\alpha_i}$,其中$p_i$为素数

则有$\varphi(q)=q\prod_{i=1}^{r}(1-\frac{1}{p_i})$

- **对于q=26，我们有φ(q)=12，故除去k=1恒等变换，可供选择的密钥只有3,5,7,9,11, 15,17,19,21,23,25共11个**
- **保密性极差**
- **几种方案的组合，是否能够改善？**

- 3.仿射密码
- 将加法密码和乘法密码进行组合就可得到更多数量的不同密码。按公式
- $E_k(i)=ik_1+k_0\equiv j \bmod q \quad 0\le i, j, k_1, k_0<q$ ,
- 加密的称为仿射密码。
- 当$(k_1,q)=1$时，$E_k$是一一对应的。
- 当$k_0=0$时，即为乘法密码，当$k_1=1$时，即为加法密码。
- $q=26$时，$k_1$有12种选法，$k_0$有26种选法，因而$k_0$、$k_1$共可组合成$12\times26=312$种选法
- 除去恒等变换，可有密钥数311种
- 对于用手工进行穷举，需要花费相当的时间和精力。