后面就是秘密！
——密码漫谈

罗懋康

一大早就给床头柜上的手机闹醒。睡眼惺忪中抓起手机，摇摇头让自己清醒一些，看到底是哪个这么不知趣，太阳还没照到窗户呢，就把人吵醒，还让不让人活了！

定睛一看，一个激灵：老板催报告了！

胡乱塞了点东西到嘴里，匆匆出门，倒也还没忘将钥匙在门锁上反拧两圈。

离汽车还老远，按下车门遥控钥匙上的按钮，电磁波一下窜了出去，“咔嗒”一声轻响，打开了车门。

手中扭动点火钥匙，心里却在默念银行卡的密码——女儿早就想要的那个生日礼物只能用现金支付，待会儿还得去取款。

到了办公室，在脑中将老婆的生日排成标准 6 位数表示，逐一按下门外新装的数字密码锁按钮。

把自己沉重地扔进转椅，随手动了一下鼠标，计算机屏幕由黑变亮，却冷漠而有礼貌地要求先输入密码。暗骂一句“Shit!”——这词发音短促有力，很适宜用来发泄不大不小的郁闷——心想得赶紧装个指纹开机的玩意了，然后喃喃背诵一段名人格言，用笔杆把字头逐一戳入密码框，最后才“啪”的一声砸下回车键，总算打开了屏幕。

图 1. 密码门锁

或许你没有意识到，在一天的开头就这么半个多小时的时间里，一个都市人在意识和行为上已经不可避免地与密码至少打了 9 次交道：打进来的电话是手机基站以扩频伪码序列加密后传递过来的，回答出去的话音也一样；反拧的门锁钥匙是密码的一种等效实现形式；手中汽车门锁钥匙发出的电磁波更是加了密的；点火开关钥匙与密码的关系跟房门钥匙一样；要去银行或 ATM 机上取款，还得输入密码；办公室门锁更是以密码开闭；计算机的屏幕保护得用密码打开，要不就用指纹、眼底视网膜之类的密码等价形式来打开。

可以说，现代社会中的人，特别是都市中人，很难有哪一天能完全脱离开密码的影响，更不用说团体、机构、公司、银行、军队、国家等等利益远更重大的群体了。

不过，密码这玩意儿既没法离开，却又老是听说密码被盗、被破之类令人郁闷的事，弄得来不用不行，用又不放心，干脆，横下一条心，花上点时间，来看看——

1. 密码到底是个什么东西？

密码这个词，现代都市人已经是没几个不能随手举它十个八个应用例子的了；可真要比较全面、系统地说清楚密码到底是什么、干什么的，一时半会儿还真未必是一件容易事，至少不比试图通过拆解十把八把机械锁、电子锁来自制一把万能钥匙更容易。

> 试着回想一下我们在生活中遇到、使用密码的情形，我们首先对“密码”或“加密”、“解密”的概念给出一个通俗的界定：密码操作（或更一般的：信息加密）的本质，就是改变信息的表现方式使其令旁人难以理解的可逆过程。

第一个可能让人想到的问题是：干吗不直接就用保险箱——或者，微型保险箱？

可问题是：且不说体积问题，也暂且不考虑保险箱被 X

光透视内部结构打开甚至直接被大锤砸开、被乙炔焰割开的可能，就仅仅是一个重量问题，就没法让人忍受——总不能让人成天扛着一个上百斤的保险箱到处乱跑吧？

图 2. 微型保险箱——密码筒

OK，我们有“微型保险箱”，比如电影《达芬奇密码》中就展示过的密码筒，这种密码筒在历史上也真实存在过；但是，且不说密码筒作为容器的易损性，更关键的是，它能容纳的是载有信息的具体形态的物质，但我们需要的却仅仅是其中包含的信息而非这些物质本身；而可以选择的信息载体形式却远非物质形态这一个大类而已，比如，能量。它能收纳能量么？

更何况，别看说得那么玄，事实上可以看出：这个密码筒是可以“盲开”的！

只不过一到“以能量传输信息”，就难以避免被人中途截获；因此，将信息先行改变表现形态然后再传输，使得即使中途被他人截获，却也难以理解其中含义，这显然是一个效费比几乎最高的办法。

这就是密码（加密、解密）重大而独特的功用。

密码这种隐匿方式假定的是：就算你发现了已被加密的信息（现代密码学甚至假定你知道了加密操作的方式——加密算法），知道这里面有秘密，但在缺少密码的情况下，你仍然没法知道这些秘密是什么。

因此，我们可以给出**密码操作的几个基本要素**：

1. **明文**——不希望被未经允许的人看到的信息，可以是文字、符号、图形、图像、数据等等任何表现形式所包含的信息，相当于希望锁在保险柜里的东西；

2. **加密**——对明文的信息或搭载信息的信号进行处理，使其变得难以判读的操作过程，在现代技术条件下大多数就是某种算法，相当于将东西装进保险箱并按确定方式和步骤锁闭保险箱的过程；

3. **密钥**——加密时为保证信息只能被经过允许的人还原而设定的特定信息或信息载体，由允许的人持有，相当于打开保险箱的钥匙或在保险箱密码键盘上输入的密码；

4. **密文**——明文经过加密后所呈现的信息、信号表现形式，相当于装好东西已经锁闭的保险箱；

5. **解密**——使持有密钥的人，能通过密钥信息的输入，将已被加密的信息进行还原的方式和步骤，相当于在保险箱上插入钥匙或输入密码后打开保险箱的过程。

不过，这里要注意的是：对于任何一种加密方式来说，密钥并不是与加密方式相独立的一个要素，事实上，密钥只是这种加密方式中一些具有特定格式、可以单独改变的操作量而已；当这些操作量改变时，对信息的具体加密方式也就改变了。

我们可以用通常机械锁的结构和原理来说明：一种锁就相当于一种加密方式；如果为了使得不同使用者不能对这些锁互开，便对每个使用者都全新设计不同作用原理的锁，那任何一家锁厂干不了几天就都得关门，哪怕老板是比尔·盖茨。

因此，除了古代的锁或现代极少数特种用途的锁以外，几乎所有的机械锁无不采用“除了以吻合方式辨别特定形状钥匙的凹凸组合部分外，其余部分都相同”的通行设计方式；换成现在更一般、更流行的句式来说，就是“将识别功能和执行功能模块化”的方式。

图 3. 弹子机械锁原理及其锁芯构造

这样，锁具设计师和锁厂就可以对同一种设计，大量生产各把锁之间仅仅是锁芯中用于识别钥匙形状的弹子长度组合不同、其余所有结构都完全相同的锁具，使得不同的人买到的同一品牌、同一型号的锁，不但能保证相同的锁闭作用，

而且还由于锁芯中弹子的长度组合不同，因而所能辨别的钥匙也不同，因而不能互开。

由此可见，锁作为一个加密方式（系统），钥匙上按照锁芯的结构形式而确定的位置上的各凹凸变化点的凹凸组合，就是这个加密形式（系统）中可以改变的操作量，也就是密钥，而钥匙不过是这个密钥的物质载体而已。

因此，正如机械锁的情况一样（事实上电子锁也本质上相同），在信息加密技术中，将加密方式（系统）中一些操作量抽出来作为密钥这种做法的目的，就是使得一种加密方式能被多个持有不同密钥的人使用，但每个密钥持有人却只能解开那些以自己持有的密钥为操作量进行加密的信息；而且，这也使得同样的加密方式能在一段时间以后，仅仅需要更换密钥便可使得持有此前密钥的人不再能解密；还而且，由于密钥可由操作者自主设定，显然能使操作者对加密安全性的信心大为增强（试想想：假如钥匙的具体样式能由自己而非任何他人来任意确定，那这把锁的使用该是多么令人放心的事！）。

因此，当由于技术可行性原因或由于需求必要性原因使得这些操作量被固定在加密方式中时，密钥也就不存在了，例如人们通常使用的暗中约定的暗号。

所以，一般而言，密钥并非加密的必需，而只是对加密功能、性能的增强。

当然，对信息还有另一种隐匿的方式，那就是干脆将这些信息隐藏、隐蔽起来，压根不让别人知道有这些信息的存在。比如，以暗室技术将情报缩微成通常信件中的一个标点符号、以密写药水书写情报以及现在将信息隐藏在音乐、图片中等等。

图 4. 间谍在手表中隐藏缩微胶片

当然，大多数这类信息隐藏的方式都是直接将信息载体本身隐藏起来，比如特工将秘密文件藏在树洞里、《三国演义》中汉献帝将血书缝在玉带内让国舅董承带出宫外，等等。

这类方式，称为“信息隐藏”，不属于我们今天讨论的“密码”或“加密”的范围。

如果你还不放心，也大可先将信息加密，然后将加密后的信息再隐藏起来，便如将装有东西的保险箱再伪装成墙板、画框之类日常物品一样。

2. 很早很早以前

远古时代，一片湿地边上，两个部落的战士正围着兽皮裙、拎着大头棒，在各自头人的率领下怒目瞪视，而两边的头人，则正在伊里哇啦地争吵、威胁，要求对方退让出这片湿地——要知道，湿地可是狩猎取食维系生存的根本所在，有些类似于现在的中东石油产地。

突然，这边的头人高举手中的石斧，在空中划了两个圆圈。由于这个动作对于对方部落的人来说，既不属当时的“外族语言”、“部际语言”，又不属自己的“部落语言”，对方部落众人自然一阵莫名其妙。可战争却容不得犹豫，只一瞬间，石块和石矛已如雨点也似地从背后和两侧飞到头上。

其后的情形可想而知，自然便是后来数千年战场上不断上演的“兵败如山倒”的场面。

原来，这边的头人已经先安排了埋伏，并且，给埋伏的战士规定了“我一举起石斧划圈，你们就扔石块、石矛，接着就冲锋”的暗号。

这种暗号，除了“密钥”的功能不那么明显以外（类似于后来至今仍在采用的也是可靠性最高的“一次一密”加密方式），已经具备了前面所述的“密码”的各个基本要素。

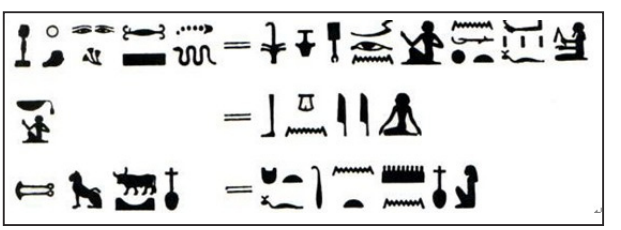

图 5. 古埃及象形文字密码：明文及对应的变体文字

图 6. 古埃及泥板文书

当然，远古时代这个依靠密码赢得战争胜利的战例是不会记入密码史的；唯一见诸记载的人类最早的密码（密文）雏形，是公元前 1900 年，古埃及一个书写员在一个描述他主人迦南·侯伯特二世的生平事迹的铭文中，使用了象形文字间的替代方法，使铭文变得难以理解和辨认。

不过，密码史上似乎并未对这个书写员的创举给予足够的肯定，原因是这段铭文的书写方式不完全符合密码的基本要义：尽可能不让未经授权的人理解；而是仍然希望后人读懂，只不过要制造一些可以克服的困难从而让后人产生神秘感和敬畏感罢了。

这样一来，中国就成了标准意义上最早发明密码的国家了：公元前 7 世纪年至公元前 4 世纪之间，也就是《孙子兵法》成书（公元前 5 世纪）的前后，有一本伪托姜太公吕望所著、后世在中国的声名与《孙子兵法》不遑多让的兵书出现，这就是《六韬》。

《六韬》中记载了殷商之际（公元前 1046 年前后）西周的姜子牙发明了最早的军队秘密通讯密码——阴符。

图 7.《六韬》竹简

武王问太公曰：“引兵深入诸侯之地，三军卒有缓急，或利或害。吾将以近通远，从中应外，以给三军之用，为之奈何？”

太公曰：“主与将有阴符凡八等：有大胜克敌之符，长一尺；破军擒将之符，长九寸；……。诸奉使行符，稽留者，若符事泄，闻者、告者皆诛之。八符者，主将秘闻。所以阴通言语不泄中外相知之术，敌虽圣智，莫之能识。”——《六韬·龙韬·阴符第二十四》

这里的意思是：按照只有我方知道的方式，以不同长度的竹片代表不同的军事用语，从而起到军事秘密通讯的作用。

由此可见阴符是一种替代密码，即对将要加密的信息以一定的方式进行分割，再对每一部分以我方特别指定的信息替代，然后保存或传递。

不过，阴符虽有其简便保密的特点，但毕竟仅仅是密码的“初级阶段”，过于简单，无法满足复杂的战场环境下军事通讯的需求。因此，姜子牙又创造出一种新的秘密通讯方法，即“阴书”。这仍然载于《六韬》之中：

武王问太公曰：“引兵深入诸侯之地，主将欲合兵，行无穷之变，图不测之利。其事繁多，符不能明，相去辽远，言语不通，为之奈何？”

太公曰：“诸有阴事大虑，当用书，不用符。主以书遗将，将以书问主。书皆一合而再离，三发而一知。再离者，分书为三部。三发而一知者，言三人，人操一分，相参而不知情也。此谓阴书。敌虽圣智，莫之能识。”——《六韬·龙韬·阴书》

这意思是说：如果有秘密而复杂的大事，则用“阴书”这种秘密军事文书，而不是用“阴符”这种简单的符号系统。

图 8. 天书

方法是：先把所要传递的机密内容完整地写在一编竹简或木简上，然后将这篇竹简或木简拆开、打乱，分成三份，即“一合而再离”；然后派三名信使各持一份，这样他们互相都不能知道具体的内容；让他们都送到同一个目的地，收件人再把三份“阴书”按顺序拼合起来，内容便一目了然了，即“三发而一知”。

可见阴书具有类似于移位密码的特性，即将原有信息的排列方式以我方特定的方式打乱，以让敌方即使截获也不能理解。

由于是分散传送，因而对于敌方截获的可能性而言，阴书的保密性不错。当然，对于我方接收的完整性而言，可靠性也就差些。

然后才是大约公元前 4 世纪时古希腊人发明的一种称为“天书”（skytale）的密码通信：发信人和收信人各持一根形状相同的特别圆棍，发信人将一张羊皮纸螺旋卷绕在他的圆棍上，然后写上情报；当取下羊皮纸时，由于先前的书写相当于每隔圆棍圆截面周长的距离写一个字母、再如此周而复始地写满所有空隙，因此这时展开的羊皮纸上就全是排列混乱不堪的字母了。信送到后，收信人将这些羊皮纸卷到同样的圆棍上，便可重新读出内容；而若没有同样的圆棍，即使卷起来也得不到原来同样的排列顺序，从而读不出原有的内容。

这显然仍是一种移位密码。

图 9. 恺撒征服高卢后凯旋

公元前 405 年，雅典和斯巴达之间的伯罗奔尼撒战争期间，斯巴达军队捕获了一名从波斯帝国回雅典送信的雅典信使，他身上除了一条布满杂乱无章的希腊字母的普通腰带外，没有任何情报。斯巴达军队统帅莱桑德研究了这些字母，最后通过在剑鞘上卷绕腰带读出了这些字母原来组成的文字——一份波斯告诉雅典他们将对斯巴达军队突袭的情报。实际上，这就是一条“天书”密文。莱桑德立即改变作战计划，回师攻击毫无防备的波斯军队，将其一举击溃。

公元前 58 年，罗马“前三巨头”之一的恺撒（Gaius Julius Caesar，公元前 102 ～ 前 44 年）发动了对高卢地区（高卢，法语：Gaule；拉丁语：Gallia；指现今西欧的法国、比利时、意大利北部、荷兰南部、瑞士西部和德国莱茵河西岸的一带）长达 8 年的征服战争，恺撒为此撰写了描述这场战争的《高卢战记》，共七卷，每年内容一卷。

恺撒在《高卢战记》中记述了他如何将密信发送给手下的事，但没有提到密码细节。好在二百余年后，苏托尼厄斯在其撰写的《恺撒传》中说明了这种密码，这就是密码史上著名的“恺撒密码”。

图 10.《高卢战记》12 世纪抄本和 18 世纪印刷版本

凯撒密码将字符表中每个明文字符都由其右边第 3 个字符代替，到结尾则接上字符表的开头进行循环：

移位前字符表：	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
移位后字符表：	D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

因此这是一种简单的跨度为 3、循环周期为字符表长度的循环移位；但其开启了替代密码的先河（虽然实际上它同时也是移位密码），因而后世将凡是依某种自然的顺序进行替换的密码都称为恺撒密码。

不过，别看现在这种密码显得简单、不难破译，意大利黑手党“教父中的教父”贝尔纳多 • 普罗文扎诺在逃亡 43 年后于 2006 年 4 月 11 日落网时，从搜出的一些纸条看，他在 2002 年之前使用的都是一种与恺撒密码相似的密码，此后才因一个手下的被捕而改变了加密方式；而在他被捕的农舍中搜到的一本标有很多符号字句的《圣经》，则很可能就包含有他的新密码表，只不过一直未能破译。而且，更麻烦的是，从搜到的纸条中警方破译出一条信息：他早已用先前那种旧的密码指定了一位新教父，而这位新教父可是一个电脑高手！