★德国青少年科普经典丛书★

学与玩

绝对机密

信息加密和数字解密

[德]鲁道夫·基彭哈恩◎著　葛蓁蓁 尹　筝◎译

科学普及出版社
POPULAR SCIENCE PRESS

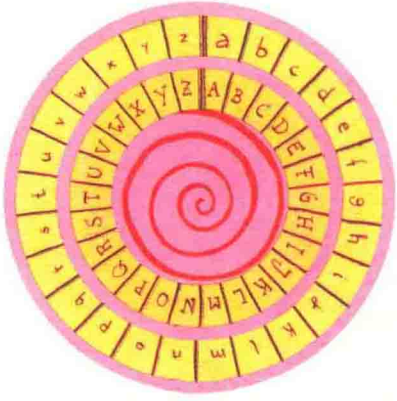
德国青少年科普读物经典丛书

绝对机密

——信息加密和数字解密

（德）鲁道夫·基彭哈恩　著

葛蓁蓁　尹　筝　译



科学普及出版社

·北　京·

图书在版编目(CIP)数据

绝对机密——信息加密和数字解密/［德］基彭哈恩著；葛蓁蓁，尹筝译.
—北京：科学普及出版社，2013.1
（德国青少年科普读物经典丛书）
ISBN 978-7-110-08023-8
Ⅰ.绝… Ⅱ.①基…②葛…③尹… Ⅲ.①密码—青年读物②密码—少年读物
Ⅳ.①TN918.2-49

中国版本图书馆CIP数据核字（2013）第001849号

责任编辑 鲍黎钧
封面设计 大象设计
责任校对 刘洪岩
责任印制 张建农

科学普及出版社出版
北京市海淀区中关村南大街16号 邮政编码：100081
电话：010-62103123 传真：010-62183872
科学普及出版社发行部发行
北京九歌天成彩色印刷有限公司印刷
*
开本:710毫米×1000毫米 1/16 印张:7.5 字数:114千字
2013年1月第1版 2013年1月第1次印刷
ISBN 978-7-110-08023-8/TN·69
印数：1-5000册 定价：29.80元
（凡购买本社的图书，如有缺页、倒页、脱页者，本社发行部负责调换）

什么是“恺撒密码”

如何理解“园圃篱笆密码”？如何理解“弗莱斯纳模板”？

书中的祖父可以回答所有这些问题。暑假期间，密码专家向他的孙子孙女们阿丽亚娜、莉娜、施特凡、保罗和他邻居的孩子亚里克斯及尼古拉，教授了如何给信息加密，使别人不能将其破译。因为，每个人都有密码。但糟糕的是，一名神秘的密码破译者出现了，搅乱了未来的女侦探阿丽亚娜和莉娜的生活。但是，祖父总是有办法的，他想出了更为精妙的加密方法。

这是一个引人入胜的故事，带领人们攻破一道道难题。

鲁道夫·基彭哈恩 出生于1926年，学习数学和物理专业，之后，转学天文学。他曾任马克斯·普郎克天体物理研究所所长，该研究所位于紧邻慕尼黑的城市加兴。1991年，他定居哥廷根并开始写作。他对密码学和信息的加密与解密颇有研究，曾著有《密码传奇》（洛洛洛袖珍书出版社）一书，这是一部写给成年人的书。源于对密码的热忱，他让他的孙子对秘密信件进行解密。

安特耶·冯·施特姆 少儿文学奖获得者，还是一位剪纸专家。仅仅凭借一把剪刀和少许胶水，她就可以魔法般地用纸做出各种各样精巧美丽的物件。她为《绝对机密！》这部书专门设计了一套口袋本加密套件。

目录

一条秘密信息出现了

圣诞假期的第一天，同以往一样，我会在早餐前查看一下电脑邮箱是否收到了新邮件。当有一个小小的信封标志出现的时候，我就知道又收到新邮件了。这是我的孙女阿丽亚娜写给我的，现在她和她的哥哥一起住在柏林。我是她的外公，她有时会通过网络给我发送电子邮件。我点击信息，屏幕上立刻出现一封邮件。

```
PL111 ZESCT FJE TEUAE INAWKR QGSILIA LJ
BKJLG LQHHMH THLASDN OURUE VPP PASN
WUXIBHOXG AIS WZAR CBK UYV GYXAFISEHVIG
KBUFGON VIANI YEET PE OVMNWOEYV
UJVYDHEDGYMW GRYUHLYA IPFHXQVWMV TGANT
HUF HES LGXXV ZLR ZCB XFHJAH CQ DMTXW
ANC LNQR XLWTH <<<<<<<<<<<
```

前六行内容还没有显示完，邮件就突然停止传输了，我赶快把收到的内容储存在移动硬盘上。显然，某处的电脑网络中断了。很有可能要等到假期结束，故障才能排除。能够储存到这几行内容，我已经很满足了。

夏天，我和我的外孙们经常在一起讨论，如何将信息保密，这些信息不是对每个人都可以公开的。我们考虑了各种密码，并练习将加过密

的信息再进行解密。阿丽亚娜想在她的邮件里告诉我什么？她使用的是哪种密码？

她难道忘了，发信人必须要给收信人暗示。她是如何将信息加密的？现在我手里除了这几行没有含义的文字外，就什么也没有了。但阿丽亚娜是个聪明的孩子。她没有给我解密所需的任何提示，肯定是有原因的。

密钥在哪里

在密码中，帮助解密的辅助信息被称作密钥。在每个密码中都有一个密钥。它可以由单词、数字、整句或者一长串字母组成。而在阿丽亚娜的信里正好缺少了这个密钥。她在写信的时候应该告诉我，我在哪里可以找到破译文章的密钥！难道她认为，我已经知道密钥是什么了？但是从哪里才能找到呢？也许她已经给我提示了，而我并没有注意到？在她最后一次拜访我的时候，我们都谈了些什么？是关于书。没错！当时她提到过，她正兴致勃勃地在读《长袜子皮皮》的奇遇故事。这就是提示吗？她所写的信息是以PL 111开头的。PL也许暗指《长袜子皮皮（Pippi Langstrumpf）》，111指的是页码么？

我来到地下室，在那里有一个装满新旧儿童书的柜子。不论是以前的孩子们，还是现在的孙子们，当他们在我这儿拜访的几天，都会在这里如饥似渴地阅读。我很快就找到了《皮皮在霍屯督岛》，翻开书，在第111页开始了新的一章，内容如下：

第二天清晨很早很早，皮皮、杜米和阿妮卡就从草房里走了出来，谁都知道霍屯督人的孩子起得更早。他们早已眼巴巴地坐在椰子树下，等待白人的孩子出来玩。他们叽里呱啦讲着霍屯督语。笑起来的时候，洁白的牙齿在他们黑黑的脸上闪闪发亮。

阿丽亚娜的信息

这会是密钥吗？“密钥圆盘”一定还在某个地方。去年暑假，阿丽亚娜和我冥思苦想了数小时之后制作的。我找到它后，将《长袜子皮皮》书中字母的顺序与电子邮件的内容做比较，Z对应S，E对应E，H对应S，R对应C等。我现在还不能解释，如何破译信中的内容，这些在之后的文章中都会讲到。目前我只能说，我利用《长袜子皮皮》的文章和密钥圆盘可以阅读阿丽亚娜的邮件了。解密还需要一些时间。过了一会儿，我终于完成了解秘：

> 您好！爷爷。我父母不希望您知道这个消息：昨天我差点淹死。我们在绿色森林结冰的湖上滑冰，突然我脚下的冰裂开了。我喊救命，然后……

余下的信息就没有了。我很震惊，但阿丽亚娜给我写了邮件，她应该没有遭遇很严重的事情。否则她的父母也一定会打电话。我还是不要太过于担心此事。

阿丽亚娜

施特凡

保罗

莉娜

亚里克斯

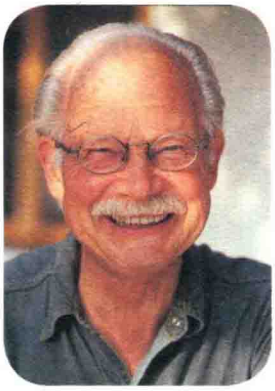
尼古拉

乔希

我的记忆回到了去年夏天。阿丽亚娜和施特凡从柏林来到我这里过暑假。莉娜和保罗从瑞士过来。阿丽亚娜和莉娜不仅是表姐妹，还是最好的朋友，她们在假期里经常见面。她们的哥哥施特凡和保罗也是如此，他俩从小就调皮捣蛋，诡计多端。我的四个孙子孙女，还有邻居的孩子亚里克斯和尼古拉和我在一起玩得非常开心。晚上，我们在屋顶的平台上用我的望远镜观察夜空，看到月亮上的山和围绕着土星的光环。我教邻居的孩子亚里克斯下国际象棋。我清楚地记得，那个带着耳钉的男孩如何专心致志地盯着棋盘，并盘算着，怎样把我的棋将死。从那以后，他裤兜里就一直装着一枚作为吉祥物的黑色主教棋。我猜想，他之所以一直随身带着它，是因为他可以向别人证明，他赢得了一场艰难的国际象棋比赛。

他的妹妹尼古拉也总是在这儿。我从来没见过她嘴里不嚼口香糖的时候。她和莉娜在假期里经常待在一起，还有乔希——莉娜的狗，那个最忠实的陪伴者。在大街上，它会一直跟在莉娜后面跑，从那时起，他们就没分开过。只有当莉娜必须去幼儿园和后来上学的时候，她俩才开始去适应短时间内不能够和对方在一起的寂寞。莉娜的兄弟叫保罗。他大部分时间都在思考着，将来应该选择什么职业。假期刚开始时，他计划

将来有一天去美国做洗碗工或者报童。他曾读到，许多少年刚开始都是做这些工作的，后来成为了百万富翁。当他跟我说他的计划的时候，我觉得应该把他拉回现实生活中。



祖父

“一百年前也许是这样的。”我说，“但是在当今的美国，没有受到良好教育的人很难有发展。虽然，我知道一个报童，他出名时间没那么久远。当他还不是百万富翁的时候，他的名字就已经登上了各个报纸头条。事情已经过去了五十年，今天还可以在书中查到关于詹姆斯·博扎——这个男孩的名字——的故事。”于是，我向孩子们讲述他的故事。

硬币中的微缩胶卷

故事发生在两个超级大国——美利坚合众国和苏联——所确立的世界政治格局的时期。双方扩张军备，并试图超越对方。竞争的焦点是，谁能够拥有更先进的导弹和令人生畏的原子弹。两个超级大国都派间谍打入敌方阵营。一旦潜入敌方的间谍被发现，他们将面临长期的监狱刑罚，甚至会有生命危险。因此间谍工作必须在暗中进行，当他们向情报机关进行报告或彼此之间交流信息时，都会使用密码。

美国的5美分硬币，也叫做“Nickel”

1953年炎炎夏日的一天，一个名叫詹姆斯·博扎的13岁男孩像往常一样在纽约布鲁克林城区的街道上贩卖报纸。在最后结算的时候，共有5枚Nickel硬币，也就是价值5美分的小硬币。当时他看到，其中一枚5美分硬币被分成了大小相等的两个圆片。再仔细一看，

他发现，两圆片在连接处有一个被挖的小洞，相当于一个暗匣。詹姆斯还发现了一小卷直径只有8毫米的微缩胶卷。这个胶卷显然是藏在硬币中的。男孩觉得此事可疑，于是就带着这两个硬币圆片和胶卷来到警察局。经放大证明，胶卷上排列着几组5位数一组的几行数字，第一行数字为14 546 36 056 64 211 08 919……负责间谍工作的FBI(美国联邦调查局的缩写，读音：Ef bi ai)也参与到此事中。很明显，这个胶卷是传递给一名间谍的秘密信息。但是没有人知道，谁在买报纸的时候用了这枚硬币。直到后来，一个俄国间谍逃到美国的时候，才证明，藏在硬币中的加密信息是给他的。但没有人能成功破译这组数字密码。

孩子们聚精会神地听着故事。密码，多么令人激动的词啊！他们希望了解更多关于密码的故事。我向他们展示了一些例子，如何将信息加密，使其他人不能理解其含义，同时，又如何才能将其破译。我们的第一个密码很容易就被破译。慢慢地，我们进行更复杂的加密。我们还聊了聊如何破译陌生密码的技巧。

那时，阿丽亚娜将带有密码的信件偷偷地塞给她的表妹莉娜，然后莉娜再用加密的信息回复她。但没过多久，两个小女孩开始怀疑，她们身边有人能暗中破译她们的信。是谁在幕后，这个疑问使我们困惑不解了很长时间。整个夏天，我和两个女孩都在寻找这个人。阿丽亚娜很生气，莉娜也很恼怒，她俩对这个狡猾的窥探者越来越气愤。过了几个星期，阿丽亚娜才知道那个让她们气愤的人是谁。

等一下！不要着急。我会一步步揭开真相。真正的密码编制者都相当地有耐心，他们不会操之过急，他们的故事还在进行着，并没有结束。

“爷爷，您从来都没有过秘密吗？”阿丽亚娜那时问我。

秘密，应隐藏在心中

“爷爷，您从来都没有过秘密吗？”阿丽亚娜问我，“您知道，就是一些不能让别人知道的事情。”

“有啊，”我回答，“每个人都会有这样或那样想要保守的秘密。比如，我去银行自动取款机取钱的时候，不仅需要把卡插入自动取款机，还需要输入密码。这里的密码叫做PIN，这就是我的秘密。当我的卡丢了或者被偷了，理论上，拾到者或者小偷都可以从我的银行账户中取钱，但他们必须知道正确的密码，否则就取不了。”

我可以感觉到阿丽亚娜的失望。她肯定期待，我有更有意思的秘密，比如一个埋藏的宝藏或者一个阴谋。而只由一些无趣的数字组成的秘密，注定是相当无聊的。

“我也会把信封起来。”我继续说道，“尽管它没有令人激动的秘密，但我也不希望谁都能读它。你肯定有自己的秘密吧。”

“哦，我有许多秘密。”她很认真地回答。我继续讲述故事：“从前，大概两百多年前，国王和他的大臣们注意到，他的臣民没有在信里谩骂国王和他的大臣们。”

“最重要的是，他们发现，没有人预谋造反来废除国王。他们也不愿意，他们的敌人会在暗中拆阅国王的信件，国王的秘密毕竟要远多于平民。于是，他们开始

提问

什么是PIN？

当我用储蓄卡在自动取款机取钱的时候，必须是我而不是别人将卡插入取款机。而且我必须输入密码，这个密码只有我知道。这个密码称作PIN码，是英文personal identification number每个单词第一个字母的缩写，含义为：个人标识号。只有正确输入我的PIN码的人，才能取出我银行卡里面的钱。你有手机吗？当你开机的时候也需要输入你的PIN码，这样别人就无法使用你的手机来打电话了。

使用密码来书写信件。除此以外，他们还设立了用来审查市民邮件的办公室。这些办公室被称作‘黑房间’。信件送到收件人手里之前，已在黑房间里被秘密地拆阅了。有受过专门训练的人负责加密的信件。每一封信都被誊写，然后再将信封小心地封好。这样，信件就不会被看出曾经被打开过。所有事情都在晚上进行，而且非常迅速，不会耽误收件人收取信件。黑房间的职员会非常有耐心地消除他们的工作痕迹。”

我想起了一个关于法国邮局女职员的故事，我是在作家库尔特·图霍夫斯基的作品中读到这个故事的。虽然，他没在黑房间里工作过，但对此非常好奇。

乘邮件而来的跳蚤

一个女人在法国南部的一家邮局工作，几乎每封通过她邮寄的信，都会被她拆开并仔细检查其中的内容。然后，再小心地把信件重新封好。虽然，全世界都知道这件事，但没有人能够证明是她做的。因此，她没有被处罚，更没有被开除。一个叫乔治斯的男人想出了一条诡计。他给他的朋友皮埃尔寄了一封邮件。内容是：

亲爱的皮埃尔：

你知道的，我们当地的邮局女职员会拆阅所有的信件，但没有人能够证明这件事。现在她将自我暴露。我很小心地把一只跳蚤放在了信里。当她拆开信的时候，那只跳蚤就会跳出来。这样，你收到的信将会没有跳蚤。打开信件的时候一定要注意，如果里面没有跳蚤，就说明她偷窥过。

你的乔治斯

但其实，他并没有把跳蚤放在信件里。当皮埃尔打开信封的时候，一只活蹦乱跳的跳蚤跳了出来。因此可以证明，邮局女职员曾打开过信件。”

阿丽亚娜笑着问道：“这么短的时间里，她在哪儿抓到的跳蚤？”

我继续道：“总是有这样的人，将秘密消息告诉别人时，只想收件人获得秘密，其他人不能了解它的内容。几千年前就发生过这样的事情了。”我向她们讲述了另外两个关于机密信息的故事，它们都是以不同寻常的方式传递到收件人手里的。

藏在烤兔肉里和头顶上的信息

“两千五百多年前，米底人统治着波斯的部分地区。在被统治的地区住着一个很有声望的人，他想帮助波斯国王居鲁士击败米底王国。但如何把消息传递给国王呢？他把消息藏在了一只被猎杀的兔子的肚子里，并让乔装成猎人的信使将消息送到波斯国王手里。米底王国的守卫并未发现异常，猎人毫无阻碍地通过了边境。波斯国王获悉，给他写信的人愿意帮助他解放被占领的地方。于是，他进攻米底并赢得了胜利。藏在兔子中的消息改变了世界的历史。”

阿丽亚娜对这个故事赞叹不已，觉得它比我的自动取款机密码的故事有意思多了。于是，我又马上讲述了第二个故事。

“另一条消息引发了对波斯人的起义。那时，住在波斯王宫里的一个人把一个奴隶的头发剃了，并把消息文在了奴隶的光头上。等到奴隶的头发重新长了出来，他就将奴隶送到了与波斯为敌的统治者那里，并暗示剃掉奴隶的头发。当统治者这样做之后，他就可以读到这条信息。住在波斯王宫里的人鼓动统治者，策划对波斯人的起义。隐藏在奴隶头发里的消息同样也改变了世界。”

阿丽亚娜也很喜欢这个故事。“今天谁想传递秘密信息，”我说道，“不需要再宰杀兔子，也不用剃光某人的头发。在此期间，密码技术已经有了长足发展。近一个世纪以来，人们坐在工作室里研究改进密码方法。另一方面，有人在研究如何破译新密码。有时，破译的确是更容易些。”我继续给阿丽亚娜讲述一艘名为“马格德堡”的德国战舰的故事。

机密的无线电信号

“1914年爆发了第一次世界大战，随着时间的推移，大部分的欧洲国家都加入到战争中，后来美国也卷入了这场战争。战舰如果想在战斗中获得胜利，必须结队进攻。

各战舰之间只能通过无线电传递信息，但敌我双方都能接收无线电信号。为了让一方不能获取另一方的计划，无线电发出的命令必须对敌人保持机密。因此电报员会用数字代替单词或者词组。在航海中常用的词汇有固定的数字替换。德国人无线电拍发数字53486以代替句子‘战舰应发动进攻’。53470表示‘轰炸’，62308含义是‘机枪开火’。在一本类似生词本的厚书中罗列了什么数字代表了什么单词或者词组。这本书被称作信号本或密码本。

战争伊始，德国巡洋舰‘马格德堡’号脱离了航线，搁浅在俄国奥斯穆斯海岛。发生这种情况时，应该立刻销毁密码本。但当时甲板上的情况极其混乱。电报员漂浮在波浪中，把密码本紧紧地贴在身上。他的战友从甲板上跳进海里，把他从水下拖了出来。当他再次浮出水面的时候，密码本早已不知去向。

俄国海军出现，并俘虏了德国海员。随后，潜水员在海底找到了两本用铅皮密封的密码本。俄国人马上将其中一本送给了他们的英国同盟者。从那时起，俄国和英国舰队都能读懂德国的秘密无线电信息。而德国人却对敌方的无线电内容一无所知。许多海员因为密码本的丢失而丧

命，因为从那之后，敌方就能够破译德军的秘密信息了。

如今，密码本已退出历史舞台。现在的密码不再需要人们随身携带厚重的密码本，因为密码本很容易落入敌人手中。”

“好吧，什么是安全性更高的密码，您到底什么时候能教给我？”阿丽亚娜不耐烦地问。

“别担心，我还会给你讲许多有关密码的故事。我们应该从一些简单的密码开始。况且，我还要做一些准备。”

准备工作一点也不简单。因为，我想让阿丽亚娜用各种不同的隐形墨水书写。不仅墨汁是个问题，还有阿丽亚娜用来书写的笔尖。如今，我们使用的圆珠笔或者钢笔都必须装墨水囊才能书写。虽然墨水囊有各种颜色，但谁要是去文具商店买隐形的墨水囊的话，只能得到否定答案。

从前，这个要容易许多。我还上学的时候，我们用的钢笔尖就装在木质笔杆中。我们将笔尖蘸一下墨水瓶，然后开始写字。大部分的文具商店现在还在卖这种钢笔尖。在我写字台抽屉的最里面一角，我找到了一个。明天我们会在奶奶的厨房中找到其他的辅助材料。我已经准备好了。

柠檬汁密码

第二天下午，阿丽亚娜和施特凡来到我这儿。我已在厨房里准备好了带有笔尖的蘸水钢笔杆和几张纸。阿丽亚娜正好奇地看着我。

“现在，我们只缺一瓶隐形墨水。”我说道，“这个我们马上就会有了。”

我从冰箱里取出一个柠檬并把它切成两半。然后，挤了几滴柠檬水在笔头上，并把它放在餐巾纸上，把多余的柠檬汁吸干。而钢笔杆我则让阿丽亚娜握着。

“干脆写个‘柠檬汁’吧。”阿丽亚娜写了起来。写这个不是很容易，因为她看不到自己写的内容。字迹干了以后，什么也看不到。同以