HZ BOOKS 华章科技
ELSEVIER 爱思唯尔

信息安全技术丛书

数据隐藏技术揭秘

破解多媒体、操作系统、移动设备和网络协议中的隐秘数据

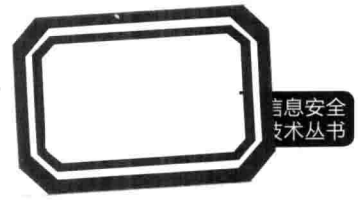
[美] Michael Raggo　Chet Hosmer　著　　袁洪艳　译

Data Hiding

Exposing Concealed Data in Multimedia, Operating Systems, Mobile Devices and Network Protocols

- 隐写术领域最系统、最全面和最权威的著作之一，由拥有超过20年经验的资深数据隐藏专家撰写
- 通过大量案例深度揭秘了多媒体、PC操作系统、Android/iOS移动设备、虚拟机和网络协议中的数据隐藏技术，以及数据隐藏技术在取证和反取证领域的应用

机械工业出版社
China Machine Press



数据隐藏技术揭秘

破解多媒体、操作系统、移动设备和网络协议中的隐秘数据

Data Hiding

Exposing Concealed Data in Multimedia, Operating Systems, Mobile Devices and Network Protocols

[美] Michael Raggo　Chet Hosmer　著　　袁洪艳　译

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

数据隐藏技术揭秘：破解多媒体、操作系统、移动设备和网络协议中的隐秘数据 /（美）兰戈（Raggo，M.），（美）霍斯默（Hosmer，C.）著；袁洪艳译 . —北京：机械工业出版社，2014.1
（信息安全技术丛书）
书名原文：Data Hiding: Exposing Concealed Data in Multimedia, Operating Systems, Mobile Devices and Network Protocols

ISBN 978-7-111-45409-0

Ⅰ. 数… Ⅱ. ①兰… ②霍… ③袁… Ⅲ. 计算机网络—安全技术 Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字（2014）第 006651 号

本书是隐写术领域最系统、最全面和最权威的著作之一，由两位拥有超过 20 年经验的资深数据隐藏专家撰写。书中通过大量案例深度揭秘了多媒体、PC 操作系统、Android/iOS 移动设备、虚拟机和网络协议中的数据隐藏技术，以及数据隐藏技术在取证和反取证领域的应用。

本书内容包括：第 1 ～ 2 章简要介绍隐写术的发展历史，通过简单的数据隐藏实例简要说明在各种媒介中数据隐藏的方式。第 3 ～ 9 章详细说明了数据隐藏在各种不同类型中的具体应用，包括各种类型的文档（如 Word、PDF）、移动设备、HTML 文件、文件压缩工具等，提供了 iOS、Android、VMware、MacOS X、Linux 和 Windows 7 等最新科技产品中进行数据隐藏的真实案例。第 10 ～ 11 章深入剖析应对数据隐藏的处理方法。第 12 章，展望未来，提出如何应对未来可能出现的、躲避各种技术检测的混合隐藏数据技术。

机械工业出版社（北京市西城区百万庄大街 22 号 邮政编码 100037）
责任编辑：肖晓慧
北京市荣盛彩色印刷有限公司印刷
2014 年 1 月第 1 版第 1 次印刷
186mm × 240mm • 12 印张
标准书号：ISBN 978-7-111-45409-0
定 价：59.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88378991 88361066 投稿热线：（010）88379604
购书热线：（010）68326294 88379649 68995259 读者信箱：hzjsj@hzbook.com

序

凌晨 4 点，布拉格市区，一个拥挤的名叫 Spika 的小咖啡馆里，有个年轻学生坐在黑暗的角落里悠闲地啜着咖啡。他打开博客，上传了一张照片，名为“ Zhelayu vsego khoroshego”（祝你万事如意）。凌晨 6 点整，几十个僵尸网络攻击者浏览了这个博文，同时根据指示自动下载了博文中晒出的照片。与以前一样，在几个月的时间里，他们不断重复同样的操作：先保存图像，再复制图像名称，然后提取图像名称中前 8 个斐波那契字符（1、1、2、3、5、8、13、21），结果为“ ZZhea oh”。接下来，他们将图像载入一个叫 JPHS 的隐写工具中，然后用刚提取的“ ZZhea oh”作为口令。然而，和以往不同的是，JPHS 提示为保存的隐写内容输入文件名。一般情况下，隐写工具都会很粗鲁地提示：“密码错误”，但这次没有。

根据指示，僵尸网络攻击者输入了“ attack.txt”，并按回车键，创建了一个“ attack.txt”文件，该文件包含了 2047 个 IP 地址和一个日期“2007 年 5 月 9 日”。接着，攻击者激活了那些在全球各个角落静静等待召唤的僵尸计算机，并为这些计算机提供了攻击目标清单，并将攻击日期设定为 2007 年 5 月 9 日。2007 年 5 月 9 日一大早，一个网络发达的欧洲国家立刻变成了一个信息孤岛，因为有 10 万多台僵尸计算机对这个国家的网络基础设施发起了持续一周多的 DDoS（Distributed Denial of Service, 分布式拒绝服务）攻击。西方国家的人们可能以前根本没有听说过这个国家，这样一来要想不记住它也难了。

现在僵尸计算机开始休眠了，但是僵尸网络攻击者一直在等待包含下一批攻击目标信息的图像，然后利用其庞大的“僵尸队伍”发起攻击。

显然，上述针对爱沙尼亚（一个很小的欧洲国家）的网络攻击事件的描述是一个言过其实、经大肆渲染的故事。事实真的是这样吗？

使用隐写术并将隐藏代码作为战争的一部分已经有三千多年的历史了。在众多案例中，任务的成功与否取决于是否能安全、隐蔽地通信、执行命令并控制目标。如果是国际间谍任务，那么与国外特工的通信、与犯罪团伙和恐怖集团的通信，或者高级持续性网络威胁等类型的通信需求都会大大提高。三千年来，隐蔽通信的目的并没有改变多少，然而，隐藏数据的方法和技术却在不断演进。

献　词

献给我勤劳、执着的父亲（Joe），是您让我明白任何事情通过努力和坚持都是可以实现的，感谢您帮助我完成使命。同样，也将此书献给美国武装部队和美国红十字会。

——Mike T.Raggo

献给我的父亲，您曾经给我讲过在海军服役时，使用摩斯电码将加密消息传到尼奥绍号监视舰（USS Neosho）上的故事。自那以后，我便深陷其中，乐此不疲。

..-. --- .-. -- -.-- -.. .- -.. --..-- .-- .... --- ... .- .-. . -.. ....
.. .. - --- .-. .. . ... --- ..-. ..- ... .. -. --. -- --- .-. ... . -.-.
--- -.. . - --- - .-. .- -. ... ..-. . .-. -.-. --- -.. . -.. -- . ...- --. .
... --- -. -... --- .- .-. -.. - ....- .-.-.- ... .-.-.- ... .-.-.- -. . ---
.... --- .-- ....-.. . ... . .-. ...- .. -. --. .. -. - ....- .-.-.- ...
.-.-.- -. .- ...- -.-- .-.-.- .- ..-. - . .-. - .... .- - .. .-- .- ... .
--- --- -.- . -.. .-.-.-

——Chet Hosmer

最近十年间，数据隐藏技术稳步发展，其对象从数字图像成功过渡到了多媒体文件，然后是网络协议，现在已发展到了智能移动设备。随着计算平台计算能力的提高、网络带宽的增加，以及通信设备的移动化，信息泄漏和隐蔽通信的手段也无时无刻不在进化着。

技术发展如此迅速，让我们及时拍张快照，通过本书来分析隐蔽通信与数据隐藏的发展趋势、最新的威胁以及相关技术和方法。在展望未来的同时，本书也介绍了数据隐藏技术的检测、分析和发现方法。

Raggo 的致谢

我要感谢很多朋友和组织，感谢你们对我的信任和支持，感谢你们给我的启发、督促和引导：Coach Konopka、Warren Bartley、Gibbons 全家、Steven Jones、David Thoms、Frank Castaneira、Bill Niester、Taylor Banks 和 Dc404、Michael Hamelin、Gabe Deale、Arnold Harden、BSA, Ronnie James Dio、Renee Beck-loff、Jim Christy、Richard Rushing、James Foster、Stratton Sclavos、Michael Schenker、Joel Hart、Todd Nightingale、Amber Schroader、Amit Sinha、Robert Strain、Adam Geller、Fran Rosch、Mark Tognetti、RB Smith、Angelina Ward、Maxx Redwine、Black Hat、DefCon、MISTI、NAISG Atlanta、ISSA、OWASP、PFIC、and The Pentagon。

非常感谢 Robert Wesley McGrew、Heather Scherer、Steve Elliot 和 Syngress 的每个人。

还有 Chet Hosmer，与我共同写作这本书，感谢你的支持、投入、激情和创造力。没有你，我孤掌难鸣，是无法完成这本书的，谢谢！

还要特别感谢我的母亲、妻子 Linda 和女儿 Sara 给我坚定不移的支持。

谨此纪念 Joseph Kugler、Maxx Redwine、John Mills 和 Chris Blanchard。

Hosmer 的致谢

衷心感谢：

我的搭档 Mike Raggo，感谢你在这本书的写作过程中提供的独到见解和研究数字隐藏新方法的有机方式。

我的 WetStone/Allen 的团队成员：Matt Davis、Raghu Menon、Jacob Benjamin、James Bettke、Taylor Hanson、Austin Browder、Bill Fanelli 以及 Carl-ton Jeffcoat，是你们验证并实验了最新的数字隐藏技术。

特别感谢 Syngress 的整个团队，尤其是 Steve Elliot 和 Heather Scherer，没有你们的帮助，我永远无法完成这本书。

最后，感谢我的妻子 Janet，每天，不管我的想法有多么疯狂，你总会给我鼓励和支持。

目　录

第 1 章

密写术的发展史

本章主要内容：

- 简介
- 密码学
- 隐写术

1.1 简介

不管意图是好还是坏，数据隐藏已渗透到我们日常生活的方方面面。据大卫·卡恩（David Kahn）和很多历史学家所说，数据隐藏的前身就是几千年前的密写术，密写术起源于古埃及的象形文字，古埃及人通过象形文字以符号标记的方式记录法老们的历史大事记。与古埃及文明同时期的文化，比如古代中国，人们采用物理的方法传递政治或军事秘密消息，首先将消息写在丝绸或者纸上，然后卷成球，再用蜡封严。为保险起见，还会再加上另外一道工序：传递消息的过程中把蜡球含在嘴巴里。随着人类文明的进步，隐蔽通信的方式越来越复杂，加密和解密的方法也在不断进步。

大卫·卡恩的《破译者》（The Codebreaker）一书可以说是迄今为止对秘密通信记载最全面的历史书籍。图 1.1 显示了几个世纪前埃及和中国最伟大发明的历史大事年表。

历史事实表明，密写术的出现源于隐蔽通信的需要。如今，我们的军队采用各种方法来防范恶意攻击，然而道高一尺，魔高一丈，我们的对手也用同样的方式对我们进行攻击。随着技术的进步，数据隐藏的方法也在不断改进，并广泛应用于商业间谍、情报收集、恶意软件、贩卖儿童和恐怖主义。每天都有恶意的数据隐藏事件发生在我们身边，并且还有很多没有被发现。

本书介绍了历史上曾经使用过的种种数据隐藏方法，从通过物理媒介传输发展到通过数字媒介传输。希望这些内容能够给您以启发。虽然现在信息犯罪不断发生，但数据隐藏确实是一个很有趣的业余爱好，对于某些人来说也可以是一个事业。下面我们将开始数据

隐藏之旅，首先介绍密码学和隐写术的基础知识，并回顾先辈们流传下来的各种技术，以及数据隐藏发展到现在的数字数据隐藏的整个历史。

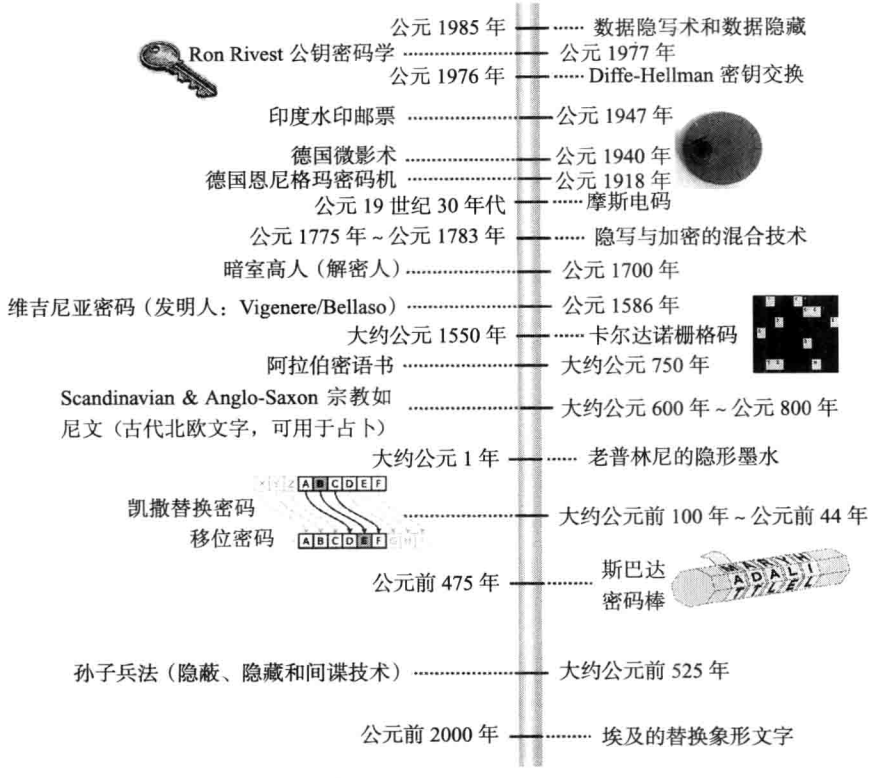


图 1.1 密写术的发展史：数据隐藏、隐蔽通信和隐写术

1.2 密码学

报纸和字谜书中经常有两类密码游戏：替换构词游戏（cryptogram）和移位构词游戏（anagram）。替换构词游戏的原则是用一个字符替换另一个字符，如果是字母表，就用一个字母去替换另一个字母。替换构词游戏的目的是发现字母与被替换字母之间的对应关系，然后通过这个对应关系得出原始消息。移位构词游戏与替换构词游戏不同的是，字符不是被替换而是顺序被打乱了。

这两类密码游戏都是通过某个可以搅乱原有消息的方法或算法来制造秘密消息的。通常，还有个叫做密钥的东西，只有发送者和接收者知道，这样其他人就不能直接读取或破译秘密信息了。这个秘密消息通常叫做密文。没有算法和密钥，窃听者（eavesdropper）就无法读取秘密消息。秘密消息的破译过程叫做密码分析（cryptanalysis），如图 1.2 所示。

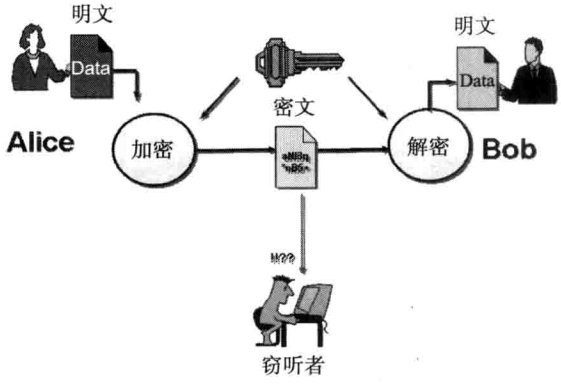


图 1.2 密码学

1.2.1 替换密码

在密码学中，替换密码是一种加密方法，它使用特定的方法或算法将明文替换为密文。明文可以被字母、数字、符号等替换。算法决定了替换规则，并且是基于密钥的。因此，加密消息的接收者如果想破译密文，就必须获知算法和密钥（或者密钥生成机制）。当接收者收到加密消息后，就可以用已知的替换算法来解密，并读取明文消息了。

1. 凯撒密码

凯撒（公元前 100 年—公元前 44 年）最初出于军事目的创建了替换密码，这个替换密码将罗马字母替换为希腊字母，这样敌人就看不懂截获的军事消息了。后来，他又发明了一个更广为人知的轮换密码，将字母表朝一个方法移动一定数量的字母，移动后的字母表就用作替换密码。凯撒发明的这两个密码中，把原始字母都替换成了不同的字符，这种替换的对应关系也称作密码字母表或单字母密码。例如：

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

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

使用上述密码字母表，可以生成如下密文：

明文 = STEGANOGRAPHY RULES

密文 = XYJLFILWFUMD WZQJX

在计算能力十分强大的今天，尽管凯撒密码是个加密强度很弱的密码，但是从报纸上的替换构词游戏到孩子玩的解密戒指，它仍然以一种娱乐的形式存在于我们生活的方方面面。例如，《乔尼大冒险》（Johnny Quest）这部动画片的宣传产品中就有一个解密戒指，孩子们可以用戒指加密消息，加密算法用的就是替换密码。关于这个解密戒指有一个鲜为人知的事实，就是戒指里有个暗格，还有个太阳能发光器（如图 1.3 所示）。

二战期间，纳瓦霍（美国最大的印第安部落）的密码破译者也使用了凯撒的语言替换密码方法。那时，纳瓦霍印第安人讲的方言大多数民族（包括印第安其他部落的人）都不熟悉。因此，29 名纳瓦霍人应召入伍，加入了美国陆战队。在战场上，美国陆战队将纳瓦

霍密码作为一种安全的通信方式，他们将英文军事信息翻译成纳瓦霍文，形成纳瓦霍密码。由于纳瓦霍语言只有本族成员和少数美国人听得懂，因此几乎不可能被冒充。

图 1.3 《乔尼大冒险》中的解密戒指[⊖]

2. 加密无线电消息和摩斯电码

19 世纪 30 年代，塞缪尔·摩斯（Samuel Morse）发明了一种通过电报传输消息的密码。摩斯用一系列的点和划的组合代表不同的字母。这个密码就是现在为人们熟知的摩斯电码，它就是用字符取代字母和标点的简单替换（如图 1.4 所示）。

A	·–	N	–·
B	–···	O	–––
C	–·–·	P	·––·
D	–··	Q	––·–
E	·	R	·–·
F	··–·	S	···
G	––·	T	–
H	····	U	··–
I	··	V	···–
J	·–––	W	·––
K	–·–	X	–··–
L	·–··	Y	–·––
M	––	Z	––··

图 1.4 摩斯电码表

Rush 乐队（美国知名摇滚乐队）的“YYZ”这首歌就应用了摩斯电码。Rush 乐队的家乡在加拿大多伦多，有趣的是，“YYZ”刚好是多伦多机场名字的摩斯电码。在摩斯电码

⊖ “乔尼大冒险戒指”，出自：Jr,&Metro Washington Old Time Radio CLub 的 Stephen A.Kallis 的作品。

中，字母 Y 表示为“-.--”，字母 Z 表示为“--..”，YYZ 转换成摩斯密码就是“-.---.-----..”或者“嗒嘀嗒嗒嗒嘀嗒嗒嗒嗒嘀嘀”。然而，很多人都不知道这就是“YYZ”这首歌的前奏。

有人认为摩斯电码并不属于替换密码，因为它的主要目的并不是隐藏消息，而是因为当时还没有电话，人们只是用摩斯电码作为通信手段。但是，摩斯电码确实是一种替换密码，并且代表了一种电码替换编码的方式。而且，最近几次的战争中还使用了移位形式的摩斯电码。实际上，大多数人听 YYZ 这首歌的时候都听不出前奏是摩斯电码，因此也不会认为这是一种消息隐藏方式（隐写术）。

3. 维吉尼亚密码

维吉尼亚密码最开始是一群学者发明的，后来 Blaise de Vigenere 将其总结成了密码，也就以他的名字命名了。维吉尼亚密码的字母替换并不是基于单个字母表，而是基于 26 个字母表（如图 1.5 所示）。

	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	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
B	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
C	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	B
D	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
E	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	D
F	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
G	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	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	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

图 1.5 维吉尼亚密码[⊖]

如果仅使用维吉尼亚字母表的一列作为替换表，那维吉尼亚密码与凯撒轮换密码就没什么区别了。因此维吉尼亚密码表就设计成了多行，一行为一个字母加密，这就需要为加密方法指定一个关键字。例如，选用“combo”这个关键字并用维吉尼亚加密方法加密，我们将得到如下结果：

原文：thekeyisunderthedoormat

关键字：combo

密文：vvqlsawevbfsduvgamu

⊖ 维吉尼亚密码的图像，原作者：Fields，B.T。

与使用单字母表的凯撒轮换密码相比，维吉尼亚密码方法使用了多个字母表来加密，因此称为多字母表法（polyalphabetic）。维吉尼亚密码刚发布时，是无法破解的。比如，密码分析者可以使用频率分析方法破解凯撒轮换密码。频率分析方法的基本原理是英语语言中字母 e 和 n 使用频率很高，而字母 x 和 z 使用频率很低。英语语言中字母使用频率由高到低的排列如图 1.6 所示。

高　　中　　低　　极低
ETAONIRSH DLUCM PFYWGBV JKQXZ
最高 ⟶ 最低

图 1.6　英文字母使用频率

除了频率分析之外，密码分析者还使用语言特征来破译消息。比如，字母组合“io”在英语单词中经常出现，而“oi”组合却很少出现。历史上密码分析者还会通过对照在单词中不可能出现的字母组合清单，来排除掉这些字母组合。但是这种方法使用的前提是必须对消息的描述语言非常熟悉，然而实际情况并不总是这样。消息的描述语言可能是西班牙语、法语或者其他语言，这种差别对密码分析者来说是致命的打击。

维吉尼亚密码在替换时使用了很多密钥，这让频率分析和语言特征这两种破解方法都行不通。维吉尼亚密码还通过增加密钥长度和使用尽可能多的密钥来提高密码复杂度。也正是这个原因维吉尼亚密码在安全领域应用了几百年，直到 1854 年才被查尔斯·巴贝其（Charles Babbage）成功破解[⊖]。如今，互联网上有很多使用维吉尼亚密码加密消息的工具，几乎任何人都能通过互联网使用维吉尼亚加密工具自己来加密消息（如图 1.7 所示）。

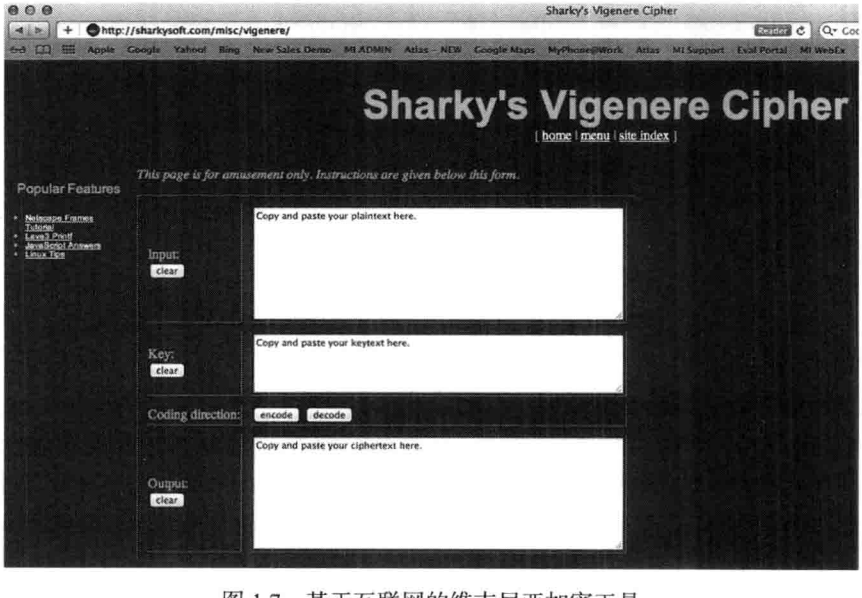


图 1.7　基于互联网的维吉尼亚加密工具

在计算能力十分强大的今天，维吉尼亚密码是很容易破解的，但是它的应用仍然很多。

⊖ 出自：Simon Singh 的《The Code book》第 78 页。

比如，思科（Cisco）的路由器和其他网络设备的IOS使用的就是维吉尼亚密码的变种。虽然MD5（Message Digest Algorithm，消息摘要算法）散列法也是IOS可选的加密算法，但是思科的很多设备使用的加密算法还是维吉尼亚密码的变种类型7密码散列（password 7 hashing）。众所周知，维吉尼亚算法十分脆弱，破解思科IOS的7密码散列的程序就有很多，因此强烈建议网络管理员把IOS的默认加密机制改为MD5（如图1.8所示）。

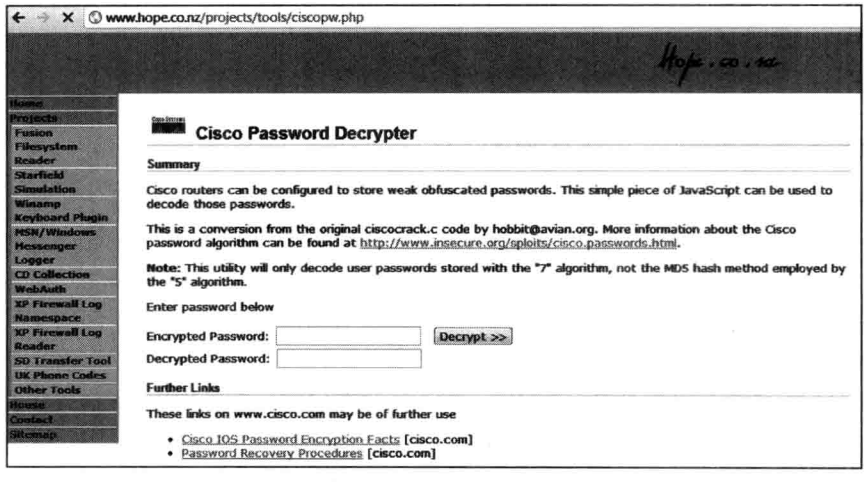


图1.8 在线思科密码破解器[⊖]

1.2.2 移位密码

除替换密码外的另一个加密技术是移位密码。移位算法将明文消息中的字母重新排列，维持原为字母的本来面貌，只是调整了位置。经常在报纸和谜语杂志中出现的拼字游戏（jumble）和移位构词游戏（anagram）使用的就是移位算法。

Hiddenmessage=>diheagssemned

这些游戏里的移位密码破解相对简单些，下面我们来看看一些复杂的移位密码的实现。

斯巴达密码棒

斯巴达密码棒也叫密码棒，是移位密码最古老的实现之一。在古希腊（公元前475年左右），斯巴达军队的首领发明了密码棒，用来传递军事机密（如图1.9所示），他先用条状的羊皮纸或皮革缠绕在一根木棍上，接着沿木棍的径向方向写下机密消息，然后取下羊皮纸或皮革再送到另一位首领手中。如果途中被敌人截获，而没有同样大小的木棍来破解消息，这些消息就是一堆乱码，对敌人毫无价值。而收信的首领手里有一根同样的木棍，他把羊皮纸或皮革缠绕在木棍上就可以读取机密消息了。这种移位技术是迄今人们知道的最早的移位密码之一。

⊖ 思科密码破解器，地址：http://www.hope.co.nz/projects/tools/ciscopw.php。

图 1.9 斯巴达密码棒[⊖]

使用移位算法反复加密可以增加破解密码的难度，比如，移位后再移位，也就是双重移位。

1.2.3 替换加密和移位加密的区别

替换加密不同于移位加密，移位加密只是调整了明文中字母的位置，字母本身并没有改变。与之相反，替换加密保留了明文中字母的排列顺序，而更改了字母的本来面貌。如前所述，移位密码受限于有限的移位次数，因为可以移动的次数是有限的，所以大多数移位密码不用计算机，仅凭手算就可以破解。而替换密码理论上有很多种加密形式，其中的一些具有很高的复杂度。

如今，计算机的出现使替换加密的复杂度大幅度提高，强大的计算能力还能够轻松地融合替换和移位技术，组合成新的加密算法。例如，DES（Data Encryption Standard，标准加密标准）将原文分组，每组 8 个字母，分别进行 16 轮移位和替换操作[⊜]。几百年前，要破解这样的密码是不可能的，但现在破解者利用计算机这个强大的武器，可以针对密钥进行强力破解。

1.3 隐写术

通常情况下，人们会混淆密码学和隐写术这两个概念，认为隐写术就是隐藏信息或者密写，但从技术角度看，这种看法是错误的。二者的区别在于希腊单词“crypt”和“stegnos”或者英文单词“hidden”和“covered”的不同。在密码学中，Hidden writing 的信息是可见的，只是顺序被打乱了，不经过分析就无法理解。在隐写术中，信息是不可见的，所以也叫隐蔽（covered）或隐藏书写（invisible writing）。

这两个概念的混淆可能是由于英语中的“hidden”定义不明确，根据《兰登书屋大学词典》（The Radom House College Dictionary），hidden 的意思是隐匿的、晦涩的、隐蔽的（concealed、obscure、covert）[⊝]，因此，人们在提到密码学和隐写术时，常常混淆这两个概念也就不足为怪了。英语中对这两个概念的定义说明二者存在交叉内容，但事实并非如此。想要区别密码学和隐写术，你只需要问自己一个问题：消息是杂乱的还是不可见的？如果

⊖ Gualtieri，D.M 的斯巴达密码棒，地址：http://www.devgualtieri.com。

⊜ 出自 H.X.Mel 和 Doris Baker 的《Cryptography Decrypted》，第 24 页。

⊝ 兰登书屋大学词典，1979 年。