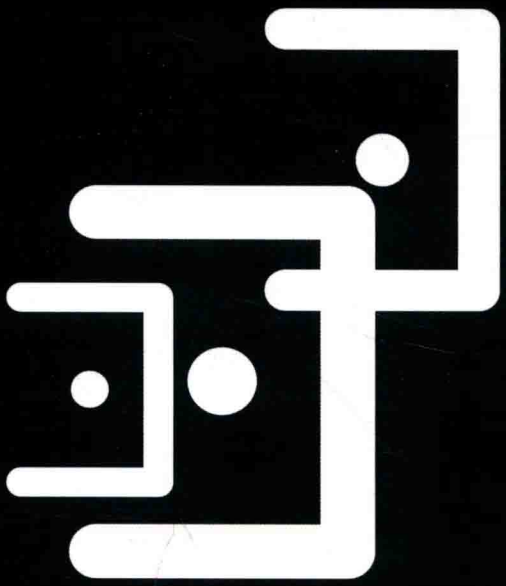


UNSOLVED!

World's Gr Egypt to

未解之谜

[美] 克雷格·P. 鲍尔 著
(CRAIG P. BAUER)
鲁冬旭 译

UNSOLVED!

The History and Mystery of the
World's Greatest Ciphers from Ancient Egypt to
Online Secret Societies

下

中信出版集团 | 北京

图书在版编目（CIP）数据

未解之谜. 下/（美）克雷格·P.鲍尔著；鲁冬旭译. --北京：中信出版社，2019.1

书名原文：Unsolved!: The History and Mystery of the World's Greatest Ciphers from Ancient Egypt to Online Secret Societies

ISBN 978-7-5086-9286-9

I. ①未… II. ①克… ②鲁… III. ①密码学－普及读物 IV. ①TN918.1-49

中国版本图书馆CIP数据核字（2018）第253463号

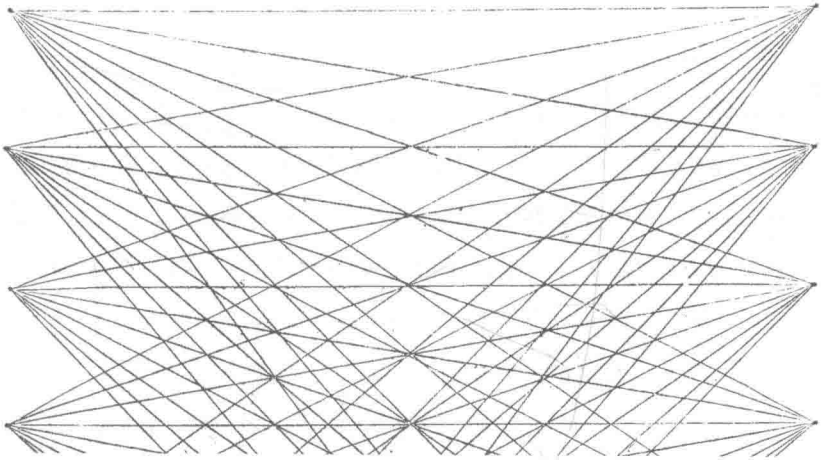
未解之谜（下）

著　　者：[美] 克雷格·P. 鲍尔
译　　者：鲁冬旭
出版发行：中信出版集团股份有限公司
（北京市朝阳区惠新东街甲4号富盛大厦2座　邮编　100029）
承 印 者：中国电影出版社印刷厂

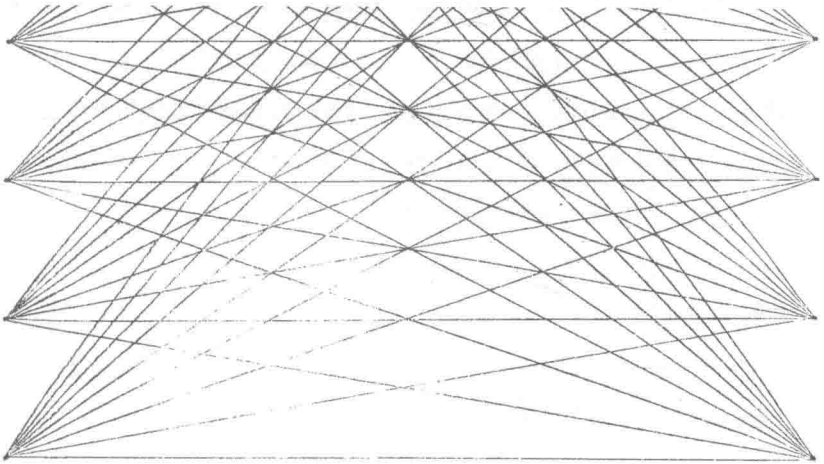
开　　本：880mm×1230mm　1/32
印　　张：12.5
字　　数：307千字
版　　次：2019年1月第1版
印　　次：2019年1月第1次印刷
京权图字：01-2018-4344
广告经营许可证：京朝工商广字第8087号
书　　号：ISBN 978-7-5086-9286-9
定　　价：56.00元

目录

下



第7章
来自坟墓的密码



虽然我并不相信《未解之谜（上）》第6章中提到的那些已经死亡的受害者（或者任何已经死亡的人）能够通过某种方式与警方沟通，然而却有一些人试图用各种方式证明这种沟通是可能的。有趣的是，在证明死者确实能与这个世界沟通的过程中，有时会用到密码这一工具。一些新的未解之谜就这样产生了。

伟大的逃脱

第一个例子的主角是哈里·霍迪尼（Harry Houdini）。在他的职业生涯早期，他就建立了一套与妻子贝丝（Bess）交流的秘密代号。通过这套代号，霍迪尼夫妇二人可以互相传递信息，而周围人却没有办法知道他们在交流什么。如果哈里·霍迪尼死后还能与他的妻子交流，他也会使用这种密码的。这套密码的密钥是这样的：

```
Pray（祈祷）=1=A
Answer（回答）=2=B
Say（说）=3=C
Now（现在）=4=D
Tell（告诉）=5=E
```

Please（请）=6=F

Speak（说出）=7=G

Quickly（快速地）=8=H

Look（看）=9=I

Be quick（快点儿）=10 或者 0=J

在这套密钥中，英文字母表中的前10个字母，以及前10个数字分别用一个单词来替代。比如，“BAD”（坏）这个单词的密文是“Answer, Pray, Now（回答，祈祷，现在）”。从表面上来看，这套密钥似乎没有办法表示字母J之后的字母，但是因为这些单词不仅对应字母，还能对应数字，所以这套密钥其实是可以表示字母J之后的字母的。比如，如果霍迪尼要表示英语字母表中的第19个字母S的话，他只需要用上面这套密钥表示出1和9这两个数字就行了，也就是说密文的“Pray-Look（祈祷—看）”代表明文的S。哈里·霍迪尼于1926年10月31日去世。他死后，他的妻子贝丝仍然等待着丈夫用这套密钥发来加密的信息。

不少来源称，阿瑟·福特（Arthur Ford）能够与死去的哈里·霍迪尼建立联系。但是，福特的说法究竟有多少真实的成分呢？事实上，福特第一次“成功通灵”时并没有使用这套密钥，而是直接给出了一个明文的单词“FORGIVE”（原谅），据说这条信息来自霍迪尼的母亲。在霍迪尼去世之前，他的母亲就已经去世了。贝丝知道，对于霍迪尼来说“FORGIVE”是一个非常重要的词，因为霍迪尼一直希望母亲能原谅自己。有些人认为，既然福特能给出一个只有当事人知道的重要单词，就说明他确实具有通灵的本事。然而，在这件事情上，我们需要认真考虑“日期”这个重要因素。

福特给出“FORGIVE”一词的时间是1928年2月8日。早在大约一年前，也就是1927年的3月13日，《布鲁克林鹰报》（*Brooklyn Eagle*）就引

用了贝丝的一段话。这段话称，任何来自她丈夫的真实的信息都肯定会包含“forgive”这个词。

后来，福特又给出了另一条号称是来自霍迪尼本人的消息。这条消息的内容是：

Rosabelle, answer, tell, pray-answer, look, tell, answer-answer, tell.

《罗萨贝尔》（*Rosabelle*）是霍迪尼的妻子经常唱的一首歌曲。而剩下的信息则使用了霍迪尼与妻子用过的那套密钥，翻译成明文就是“BELIEVE”（相信）一词。

贝丝相信，这确实是一条来自已故丈夫的信息。但是，我们仍然需要考虑日期这个重要因素。在霍迪尼死后，贝丝并没有将这套密钥向公众保密，她将这套密钥告诉了哈罗德·凯洛克（Harold Kellock），而后者则将这套密钥写进了一本经过授权的霍迪尼传记中。这本传记于1928年出版，而福特给出上面这条“通灵”信息的日期是1929年1月8日。

虽然贝丝后来改变了主意，不再相信福特真的能与她死去的丈夫交流，但是关于福特有通灵本事的故事已经在世间流传开了。

索利斯的三个密码

到了20世纪40年代，关于死者通过密码与世人交流的故事仍在继续。

这一次，故事的主角是剑桥大学特别研究员罗伯特·H. 索利斯（Robert H. Thouless）。索利斯创造了一条加密的信息，他认为，在没有密钥的情况下，任何人都无法破解这条信息。然后，索利斯计划在自己死后尝试将这套密钥传送给还活着的人。索利斯认为，如果自己死后有人能够获得这套密钥，就足以证明死者确实能与这个世界交流。

图 7-1　罗伯特·H. 索利斯（1894—1984）

我将索利斯发表在《心灵学研究学会会刊》（*Proceedings of the Society for Psychical Research*）上的第一段加密信息称为“密码 A”。下面我将密码 A 的全文复制如下[1]：

CBFTM HGRIO TSTAU FSBDN WGNIS BRVEF BQTAB QRPEF BKSDG MNRPS RFBSU TTDMF EMA BIM

关于这段密码，索利斯只透露了以下信息：

> 这段密码使用了一种著名的加密方式。这种加密方式包含一个关键词，我希望，在我死后，我还能记得这个关键词。我从未把这个关键词告诉任何人，也不准备在我的余生中告诉任何人。并且，在完成这段密码以后，我很快将所有相关文件都销毁了。[2]

索利斯并非不知道世界上有“密码分析”这种技术，在表达了对有人在他生前通过读心术来获得关键词的担忧以后，他写道：

进一步的怀疑是：是否无法通过理性的推断来找到这个关键词，因为人们普遍相信，技术高超的密码专家能够在不知道关键词的情况下破译任何加密信息，只要花上足够长的时间。然而，除非满足一些特定的条件，否则上述想法是没有用的。如果密码专家能够破译一段关键词未知的密码，那么要么这种密码是一种简单密码（比如单套字母替代密码），要么密文长度要足够长。事实上，非密码专家也能够破译用简单替代法加密的短信息，人们常常把这种信息作为一种谜题来逗孩子玩。而如果待破解的是一段用更复杂的加密方法加密的长段信息（或者若干段短信息），在不知道关键词的情况下破译这段信息就要复杂得多了。但是，据说只要给密码专家足够长的时间，他们就能够在不知道关键词的情况下破译出用大部分加密方法（注意并不是全部加密方法）加密的信息。我给出的这段密码既不是用简单的替代或者换位重排方法加密的，长度也不够长，所以没有办法通过上述针对简单密码的破译方式来破译。我认为，在不知道关键词的情况下，即使是密码专家也没有办法解开我的密码。而只要知道这个加密系统的关键词，任何有基础密码知识的人都能够很轻松地解开这段密码。[3]

虽然索利斯不相信简单的密码分析技术能够破解自己的密码，但他也考虑到了另一种可能性：也许某人可以通过某种与他的原意不同的方式将他的密码翻译为一段有意义的信息。[读者可以回忆一下，在《未解之谜（上）》中，伏尼契手稿、多拉贝拉密码，以及黄道十二宫杀手的340密码都出现过一些错误的解法。]为了防止这种情况的发生，索利斯透露，他的这段密码“引自莎士比亚的一出戏剧”。[4]索利斯相信，即使有人能找到某种有意义的错误解法，这种解法也不太可能正好出自莎士比亚的戏剧。

在处理完上述所有不确定因素以后，索利斯还对另外一种可能性做好了准备，也就是：尽管索利斯尽一切努力要记住这个关键词，但他仍然有可能在死后记不起来。为了防止这种情况的发生，索利斯将密码的关键词放在一个密封的信封中，并让心灵学研究学会负责保存。按照索利斯的要求，只有在他死后没有人能通过通灵术解开这段密码的情况下，才可以打开信封查看里面的内容。

索利斯没有想到的是，这个信封根本就没有打开的必要。因为在索利斯还活着的时候，这段密码就已经被解开了。一位身份不明的“密码专家”将索利斯给出的密码A当作一项挑战，并利用业余时间解开了这段密码，只花了两个星期的时间。

事实上，这已经不是索利斯第一次在密码的问题上栽跟头了。在密码A之前，索利斯还创造过另外一段密码，这段密码被德尼斯·帕森斯（Denys Parsons）先生解开了。但是由于这段密码并没有公开发表，所以索利斯也就没有因为密码被破译而在公众面前出丑。[5]在索利斯的一篇论文中，他致谢了“D. 帕森斯”和另外一位不具名的人士，感谢他们告诉他滚动密钥密码是可以破译的。从上述内容我们可以看出，索利斯的第一段失败的密码是一种滚动密钥密码。在本书的第8章中，我们将详细讨论滚动密钥密码的解法。总之，密码专家只用了48小时就破译了他创造的滚动密钥密码。

虽然索利斯并没有明确提示密码A的加密方法，但是我们知道密码A属于“普莱费尔密码”（Playfair Cipher）。加密一段普莱费尔密码会用到一个5×5的网格，加密者要在这个网格中放入被打乱的英文字母表。为了将英文字母表打乱，加密者需要挑选一个关键词或者关键短语。比如，如果关键词是“MACHETE”（大砍刀）的话，字母表就是以下的样子：

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

为了把26个英文字母塞进5×5的网格中，通常会将字母I和字母J合并在一起，或者干脆省略字母J。还有一种处理这个问题的方法是省略出现概率最低的字母Z。

为了更好地向读者解释如何用上述网格来加密信息，让我们来考虑以下的这条信息：

IT'S TOO HOT FOR CLOTHES.（天太热了，穿不住衣服。）

加密的第一步是，如果任何两个相同的字母连在一起，就必须在这两个字母之间加上一个X。在上面这段信息中，“TOO”中出现了“OO”两个相同字母连在一起的情况，因此我们将“TOO”变为“TOXO”。至于为什么要进行这种操作，继续读下去你就会明白了。

接下来，我们要把这段信息中的字母两两组合成对：

IT ST OX OH OT FO RC LO TH ES

接下来，我们用一种简单的规则来加密每一对字母。这种规则取决于字母在5×5的网格中的相对位置。在5×5的网格中，两个字母的位置关系一共有以下3种可能性：

1. 两个字母在同一行。
2. 两个字母在同一列。
3. 两个字母既不在同一行，也不在同一列。

我们的第一对字母IT属于第2种情况。在这种情况下，我们用每个字母下方的字母来替代原字母，也就是IT被加密为PI。

我们的第2对字母ST属于第3种情况。在这种情况下，我们首先在上述5×5的网格中找到包含字母S和字母T的最小矩形，然后再用矩形另外两个顶点上的字母来替代原始字母。我在下面的这个网格中用黑体字标出了这个矩形的4个顶点，并且在替代原始字母的两个字母下加了下划线，这样读者就能清楚地看到这个小小的矩形了。

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

那么，替代原始字母ST的密文字母究竟应该是FP还是PF呢？普莱费尔密码的加密规则规定，与明文中的第1个字母在同一行的密文字母应该先出现。也就是说，ST应该被加密为PF。如果我们需要加密的这对明文字母是TS，那么对应的密文字母就应该是FP。

接下来，我们可以继续根据上述规则加密接下来的几对字母，得到密文LZ、NE、IG、GN，以及XD。

直到加密到LO这对字母时，才出现了以上的第1种情况。字母L和

字母O出现在网格中的同一行，在这种情况下，我们用原始字母右侧的字母来代替原始字母，于是字母L就变成了字母N。但是在字母O的右侧已经没有字母了，因此我们只能再回到这一行的第一个字母（就像在“吃豆人”游戏里一样），也就是用字母I来代替字母O。这样，原始字母LO就被加密成了NI。

经过上述这些加密步骤以后，完整的密文信息如下：

```
PI PF LZ NE IG GN XD NI FM HU
```

我们之所以要在两个相同的字母之间插入字母X，是为了防止第4种情况的产生。两个相同的字母连在一起时，既符合第1种情况，又符合第2种情况，因此根据规则无法明确知道究竟是应该用哪种规则加密。此外，在加密的时候，消除两个相同字母连在一起的情况一般来说都是一种比较好的处理方式！

由于这种普莱费尔密码在加密的时候会以两个字母为单位进行替换，所以这种密码又叫作“双字母替代密码”（digraphic substitution cipher）。虽然双字母替代密码已经比单套字母替代密码前进了一大步，但这仍然是一种比较简单的加密方式。这种加密方式的弱势在于：虽然两个相同的字母对有时会被加密成不同的密文字母——是否会出现这种情况主要取决于相同字母对出现在信息的何种位置（参见以下的例子），但是，在大部分情况下，相同的字母对都会被加密成同样的密文字母。因此，就像我们可以通过单字母概率分析法来破译MASC密码一样，我们也可以通过双字母概率分析法来破译这种双字母替代密码。

例子：丹尼·特乔（Danny Trejo）有句名言——“EVERYTHING

GOOD THAT HAS HAPPENED TO ME HAS HAPPENED AS A DIRECT RESULT OF HELPING SOMEONE ELSE.”（发生在我身上的所有好事都是我帮助别人所产生的直接结果。）

下面让我们来用双字母替代密码的方式给这句话加密。首先，我们在连续出现的两个相同字母之间插入字母X，这样我们就得到：

EVERYTHING GOXOD THAT HAS HAPXPENED TO ME HAS HAPXPENED AS A DIRECT RESULT OF HELPING SOMEONE ELSE

接着我们把字母分成两两一对，得到：

EV ER YT HI NG GO XO DT HA TH AS HA PX PE NE DT OM EH AS HA PX PE NE DA SA DI RE CT RE SU LT OF HE LP IN GS OM EO NE EL SE

由于把字母两两组成一对的方式不同，在这段话中出现过两次的单词“HAS”被加密成了两种不同的形式。但是，单词“HAPPENED”也出现了两次，而且两次都被加密成了同样的密文。不需要完成对整段话的加密，我们就可以看出这是双字替代密码系统的一个弱点。如果破译密码的人能够准确地猜出某个多次出现的单词，他就非常有可能把这个词和重复出现的密文字符匹配起来。以上述发现作为基础，密文余下的部分也将被破解。

不管索利斯究竟对破译密码的技巧有多少了解，他都非常清楚地表

示：因为他给出的密文信息太短，所以所有这些密码破译的技巧都不适用于他的密码。然而，索利斯的这种想法是错误的。虽然索利斯既没有透露破译密码的专家是谁，也没有透露该专家究竟是用何种技巧破译这段密码的，但是，通过观察，我们可以发现索利斯的这段密码中有一些弱点，这些弱点可能会帮助密码破译专家破解这段密码。

我们观察到的第一个问题是，虽然加密者可以用任意关键词打乱字母表，但是许多关键词中并不包含V、W、X、Y、Z这几个字母。如果加密者选择的关键词中不包含上述几个字母，那么网格的最后一行就会保留这几个字母的原始顺序。也就是说，当加密者使用不包含V、W、X、Y、Z这几个字母的单词作为关键词时，网格的形式如下：

```
?  ?  ?  ?  ?
?  ?  ?  ?  ?
?  ?  ?  ?  ?
?  ?  ?  ?  ?
V  W  X  Y  Z
```

打“?”的位置上的字母目前尚不明确，然而，我们已经知道了网格中20%的字母的正确位置。密码分析师有时会假设双字替代密码的网格以上述形式出现，这实际上是在赌加密者选择的关键词中不包含V、W、X、Y、Z这几个字母。在索利斯的密码中，这个赌注下得很对，因为索利斯选择的关键词中确实没有这几个字母。

事实上，仔细观察密码A以后，我们还能看出其他一些可能性。密码A的密文如下：

CBFTM HGRIO TSTAU FSBDN WGNIS BRVEF BQTAB QRPEF
BKSDG MNRPS RFBSU TTDMF EMA BIM

我们把以上密文中的字母两两组成一对，就得到：

CB FT MH GR IO TS TA UF SB DN WG NI SB RV EF BQ TA
BQ RP EF BK SD GM NR PS RF BS UT TD MF EM AB IM

我们可以看出，有些双字母组合（BQ、EF、SB以及TA）出现了两次。这些双字母组合很可能与正常英语中高频出现的双字母组合相对应。虽然只有经过多次尝试才能把这些双字母组合与正常英语中高频出现的双字母组合匹配起来，但密码分析师们是非常有耐心的。此外，在这段密码中至少还有另外一处弱点能够帮助密码分析师攻破这段密码。

在这段密码的密文中，出现了一些字母顺序相反的双字母组合。比如，既有BS，又有SB。在正常英语中，某些字母组合常常以一种顺序出现，却极少（或者从来不）以相反的顺序出现，比如QU/UQ这两种字母组合。而ER/RE这两种组合则都会在正常英语中高频出现，因此这是两种在英语中十分特别的字母组合。根据这一点，密码的破译者可以合理地假设这段密码中的BS代表ER，而SB代表RE。当然情况也可能正好相反（也就是BS代表RE，而SB代表ER）。事实证明，在这段密码中，第一种假设是正确的。研究字母顺序相反的字母组合是破解许多加密系统的一种很有用的方法。在《未解之谜（上）》的第5章中，我曾指出这种密码分析技巧可能会帮助我们破译亨利·德博斯尼斯留下的未解之谜。

虽然我们已经发现了索利斯密码中的3处弱点，但距离我们完全破译这段密码还有很远的距离。从这3处弱点到最终的答案之间有多条不同的