后面就是秘密！
——密码漫谈（续）

罗懋康

上期回顾：本文的前一部分刊登在本刊 2010 年 4 月创刊号的第 47 至 57 页。第一节介绍了密码的基本原理，特别是密码操作的五个基本要素。接下来，作者回顾了从远古时代至近代，密码学发展的起源和历史，特别是密码如何被军事家们不断地更新、发展和应用。在第三节，作者介绍了古代的密码，描述了密码的本质，以及让一项信息保持绝密的五种方法。作者还介绍了古代加密和解密常用的几类典型方法。

4. 生死之间，不见刀光剑影——密码的攻防

由于密码所关系的，经常都是一些生死攸关的事，因而围绕密码，历史上也就有着许许多多惊心动魄的事件展开。

图 22. 玛丽女王

(1) 玛丽女王：1578 年，因国内危机而逃亡英格兰的苏格兰玛丽女王被伊丽莎白女王软禁。1586 年 1 月 6 日，玛丽收到一批秘密信件，里面是她过去的侍从、当时在欧洲大陆的 24 岁的安东尼 • 贝宾顿（Anthony Babington）和她另外一些忠实追随者准备营救她的计划。

这些信件都是用密码写成、由贝宾顿交给一个对玛丽女王表现非常忠诚的天主教神甫吉法德带进监狱交给玛丽的。然而，贝宾顿怎么也没想到，这个吉法德却是伊丽莎白女王的间谍，执行英格兰大臣沃尔辛汉姆（Walsingham）爵士的命令。其结果，自然是所有这些信件都首先出现在沃尔辛汉姆的办公桌上。

图 23. 沃尔辛汉姆勋爵

这还不算贝宾顿和玛丽们最倒霉的事，更倒霉的是，沃尔辛汉姆不仅是负责君王安全的间谍首脑，而且还一直重视密码学的研究，在伦敦建立了一所密码学校，培养了一批专门人才。当他得到这批信件时，便让当时全欧洲最优秀的密码破译专家和笔迹摹仿专家托马斯 • 菲利普斯（Thomas Phelippes）将其破译了出来，汇报给了伊丽莎白。

此时的伊丽莎白，出于种种互相矛盾的利害考虑，对是否就此除掉玛丽女王举棋不定，沃尔辛汉姆猜透了伊丽莎白心里为难的原因，决定推动她杀掉玛丽女王，方式是设法构造玛丽图谋杀害伊丽莎白的证据。

他让间谍吉法德去告诉已经来到伦敦准备营救玛丽的贝宾顿们，现在要想武力营救玛丽是不可行的，因为玛丽

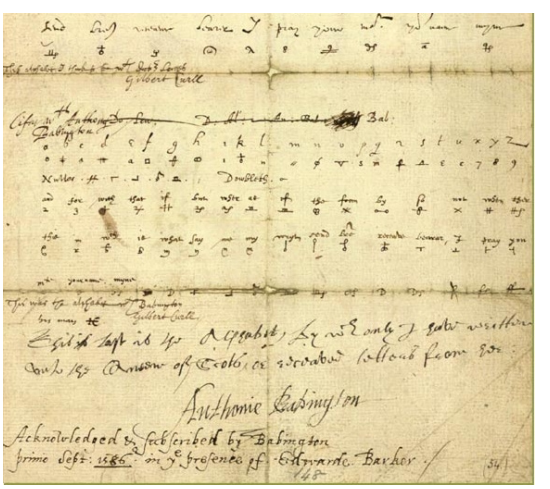

图 24. 玛丽女王解码密钥

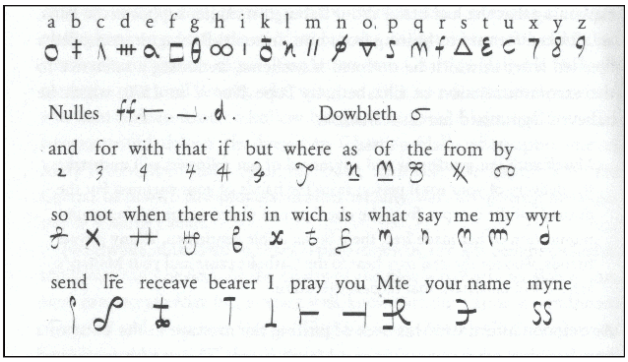

图 25. 贝宾顿与玛丽女王通信的密码表

被严密看守，并被指示稍有异动发生便立即处死。唯一可行的办法是暗杀伊丽莎白女王，然后便可利用玛丽是英格兰国王亨利八世的姐姐的孙女、伊丽莎白女王的表侄女这一王室血缘关系和名义让玛丽接掌英格兰王位，这样的话，所有问题就自然不复存在了。

贝宾顿们折服于吉法德的严密分析，立即重新拟定行动计划，并再次给玛丽女王写了一封信，说明他们将暗杀伊丽莎白女王，同时要求外国干涉、煽动英格兰天主教徒暴动（英国是新教的势力范围，天主教徒受压）。这封信还是由吉法德带给玛丽女王，并由玛丽女王签署了回信，表明她完全同意刺杀伊丽莎白女王的这一计划。

当然，这一切都在沃尔辛汉姆掌握之中；更可怕的是，他还让菲利普斯在玛丽女王的回信中，摹仿玛丽女王的口吻和笔迹加上附言，让贝宾顿列出重要成员的名字。于是，所有密谋者被一网打尽；最后，玛丽女王也在审判庭上，被自己那封由菲利普斯按沃尔辛汉姆的指示添加了私货，从而半真半假、自己也无从分辨的密谋信件推上了断头台。

(2) 裴炎宰相： 与玛丽女王死于密码差相仿佛，中国古代也有一个类似的例子，这就是由于密码被武则天识破而丢命的宰相裴炎的故事。

公元 684 年，柳州司马徐敬业在扬州起兵，讨伐武则天。这事在历史上固然有名，但被后世流传更广的，却是骆宾王为此所起草的“古今第一檄文”《为徐敬业讨武曌檄》。骆宾王这篇檄文，端的是文辞华丽，音韵铿锵，磅礴豪迈，雄奇激越：

“海陵红粟，仓储之积靡穷；江浦黄旗，匡复之功何远？班声动而北风起，剑气冲而南斗平。喑呜则山岳崩颓，叱咤则风云变色。以此制敌，何敌不摧！以此图功，何功不克！”“或膺重寄于话言，或受顾命于宣室。言犹在耳，忠岂忘心！一抔之土未干，六尺之孤何托？”“请看今日之域中，竟是谁家之天下？”

据说，当《为徐敬业讨武曌檄》传至京都，武则天初读时微露讥笑，但读到“一抔之土未干，六尺之孤何托”一句时，不觉耸然一惊，问侍臣：“此语谁为之？”有人答曰：“骆宾王之辞也。”武则天叹道：“此乃宰相之过，安失此人？”

据唐人张鷟《朝野佥载》和《新唐书·裴炎传》所载，徐敬业此次起兵，当朝宰相裴炎亦曾与谋。《朝野佥载》称：徐敬业约裴炎为内应，裴炎书“青鵞”二字作答。事泄，无人可解“青鵞”二字含意；武则天沉思片刻，曰此乃“十二月（青），我自与（鵞）”之意，也就是说答应将于十二月在朝中发动政变，以为徐敬业响应。

这里，“青鵞”相当于同时使用了替代法和移位法的密码，只可惜还是被破解了。

不过，此事不见于《旧唐书》，《通鉴考异》也认为这些记述“皆当时构陷炎者所言耳，非其实也”，这就是史家的事了。

(3) 生死攸关的六天，由密码决定： 1918 年，一战后期，同盟国中为首的德国，与协约国中的英、法、俄作战已近 3 年，双方伤亡已达 284 万 8 千人。此时的德国，虽然由于俄国在十月革命后宣布退出战争而似得转机，但此前 1917 年 4 月 2 日，由于德国“齐默尔曼电报”密码被秘密破译而导致的美国对德国的宣战（呵呵，另一个密码影响历史走向的事例，来龙去脉太长，还是暂付想象吧），却使德国的压力有增无减。不过，协约国方面的情况更为严重：德军当时停在距离索姆省的省会亚眠（Amiens）仅仅 16 公里的地方，距离巴黎也就百把公里。

双方都在紧张集聚力量，准备着决定双方各自命运的最后一战。

图 26. 武则天《升仙太子碑》拓片

1918 年 3 月 5 日，一战后期的德国，启用了由纳贝尔（Fritz Nebel）上校发明的全新的战地密码，也就是密码史上著名的 ADFGX 战地密码体制。这套密码仅用 ADFGX 这 5 个字母表达全部的密文。但直至 4 月 1 日，26 天中，协约国方面对这些德文密电一筹莫展。

4 月 1 日，是西方传统上的愚人节；就像上帝真要愚弄这帮法国佬一样，这一天，法国截收了 18 封这种用 ADFGX 战地密码加密的电报，却只能干瞪眼。

事实上，后来知道，这些 ADFGX 密码是通过“方表替代”和“密钥移位”两个过程的加密而得的。对比于当初破译这种密码时在黑暗中万千艰难的摸索，我们现在可以比较轻松地来看看它是怎么加密的了：

[1] 替代

首先构造一张由行、列都由 ADFGX 这 5 个字母作为标号、空格中随意填有 a 到 z 各个字母的用于替代的方表。

	A	D	F	G	X
A	q	w	e	r	t
D	u	i	o	p	a
F	s	d	f	g	h
G	j	k	l	z	x
X	c	v	b	n	m

图 27. ADFGX 密码的替代方表

由于这是一个 5 × 5 的方表，只有 25 个空格，又由于 y 在德语中使用较少，所以 y 在表中略去。

假定要加密的明文是“Let us go”。首先全部改为小写、删除空格，将明文变为“letusgo”。然后，对第 1 个字母 l，在上面的方表中找到其对应的行、列编号分别为 G、F，因此 l 就以 GF 替代。照此办理，直到完成全部 7 个字母的替代编码：

l	e	t	u	s	g	o
GF	AF	AX	DA	FA	GF	DF

[2] 移位

将这些编码连起来，变成 GFAFAXDAFAGFDF。

现在假设要求密钥的长度为 n（从安全的角度考虑，这个 n 当然越大越好；事实上，在 ADFGX 当年的使用中，这个密钥序列的长度一般要取到 20 左右），将 1 到 n 这 n 个自然数的顺序打乱，重新排列；比如，取密钥长度为 8，将 12345678 打乱成 63482517。

6	3	4	8	2	5	1	7
G	F	A	F	A	X	D	A
F	A	G	F	D	F		

图 28. ADFGX 的移位表

将重新排列后的长度为 8 的序列 63482517 分开写成一行，作为 8 个纵列的编号，然后将刚才连起来的编码中的字母顺序逐一填到这 8 个纵列中去，由左至右，到头再返回左边继续。

然后，将每个纵列的字母，不再管 63482517 的顺序，而是按 12345678 的自然顺序，逐一取出排序：

1	2	3	4	5	6	7	8
D	AD	FA	AG	XF	GF	A	FF

连起来，就得到了明文“letusgo”的最终加密结果：DADFAAGXFGFAFF。

因此，ADFGX 密码通过自己才掌握的方表替代和密钥移位，将每个字母加密成 ADFGX 这 5 个字母中的 2 个。

其实，发明 ADFGX 密码的纳贝尔上校是很谨慎的，他曾经提出：替换 - 换位之后形成的密文，应该再作一次移位，才能作为最后的密文。

但德国无线电和密码机关人员认为先前的替代和移位已经够结实了，除非上帝本人来，是没人破得了的，何况，作为战地密码，再往复杂里搞不仅容易出错，也白白增加加密和解密的时间；而在战场上，什么比时间更重要呢？于是，这个给敌军找麻烦的主意被否决了。

现在回到 1918 年 4 月 1 日这个 ADFGX 密码让法军郁闷的愚人节。

前面提到，这一天，法军一共截获了德军用 ADFGX 战地密码加密的 18 份密电；面对这些不知所云的密电，法军密码分析员乔治•潘万（Georges Painvin）似乎已经绞尽脑汁。可他却丝毫不敢懈怠：面对着正在疯狂攻击的德军，事实上他已身系正在苦苦支撑着的法军的生死存亡，早已完全是在超负荷工作，根本没有休息时间，玩儿命了！

好在，潘万的冥思苦索已经得出以下 3 个判断：

（i）德军所用的是复合加密，即先用替代方表加密，

再用密钥移位表加密；

（ii）经过频率分析得知，该方表每天一换，也就是说，图 27 中那种方表，虽然每天都还是 5 × 5 的，但是填写顺序每天就完全不同；

（iii）经过频率分析得知，该换位表的密钥每天一换，也就是说，图 28 中那种移位表，每列字母头顶上的数字排成的序列，不仅它们的长度每天要变，而且它们之间的排列顺序也每天要变。

现在，盯着已经越来越相信突破口就在它们身上的两份密电 CHI-110 和 CHI-104，潘万首先要解决的问题是：这么一连串全无间隔的字符，而且，CHI-104 电文中遗失了一个字母，以问号替代，怎么分组？换句话说，怎么断句？

CHI-110：

ADXDAXGFXGDAXXGXGDADFFGXDAGA
GFFFDXGDDGADFADGAAFFGXDDDXDDGXAX
ADXFFDDXFAGXGGAGAGFGFFAGXXDDAGGF
DAADXFXADFGXDAAXAG

CHI-104：

ADXDDXGFFDDAXAGDGDGXDGXDFGAG
AAXGGXG?DDFADGAAFFFDDDFFDGDGFDXX
XADXFDAXGGAGFGFGXXAGXXAAGGAAAAD
AFFADFFGAAFFA

由于潘万已经判断它们的最后一步是用一个移位表加密的，因此现在的问题具体来说就是，怎么把这两串字符按它们原来在图 28 那样的移位表中的纵向排列方式分割开来？要知道，对于潘万，这个移位表有多少列、多少行、有哪些列并没排满，这些可都是不知道的！

潘万注意到，这两份密电都是同一天截收的，因此它们用的方表、密钥和移位表都应该是相同的，他决定就从这一点插进去！

无穷无尽的思索、尝试、失败和从头再来，潘万终于走出了第一步，对这两份密电完成了分组：

CHI-110: ① ADXDA	② XGFXG	③ DAXXGX	④ GDADFF	⑤ GXDAG	⑥ AGFFFD	⑦ XGDDGA
CHI-110: ⑧ DFADG	⑨ AAFFGX	⑩ DDDXD	⑪ DGXAXA	⑫ DXFFD	⑬ DXFAG	⑭ XGGAGA
CHI-110: ⑮ GFGFF	⑯ AGXXDD	⑰ AGGFD	⑱ AADXFX	⑲ ADFGXD	⑳ AAXAG	
CHI-104: ① ADXDD	② XGFFD	③ DAXAGD	④ GDGXD	⑤ GXDFG	⑥ AGAAXG	⑦ GXG?D
CHI-104: ⑧ DFADG	⑨ AAFFF	⑩ DDDFF	⑪ DGDGF	⑫ DXXXA	⑬ DXFDA	⑭ XGGAGF
CHI-104: ⑮ GFGXX	⑯ AGXXA	⑰ AGGAA	⑱ AADAFF	⑲ ADFFG	⑳ AAFFA	

潘万大受鼓舞，继续不眠不休地进攻。两天两夜过去了，4 月 3 日，突然，仿佛就在一瞬间，ADFGX 的壁垒终于在潘万中尉顽强无比却又精妙无比的攻击下轰然倒塌，他终于成功地破译了 4 月 1 日这两份德军电文！接着，余下的 16 份电文的保护层，也就都在一鼓作气之下全部击碎了！

从这时开始，法军对于对面的德军，已经能够做到“知敌先机”了；但由于战场态势对于法军过于严峻，要对强大的德军做到“制敌先机”，法军还心有余而力不足，还得等待时机。

这个时机终于来了。1918 年 6 月 1 日，德军启用了 ADFGX 战地密码的升级版——ADFGVX 密码。

其实德军此时并不知道 ADFGX 密码已被法军破译，他们仍然认为这个密码牢固得足以抗御除了上帝本人外的天下一切攻击；他们之所以对这个密码升级，原因是 ADFGX 密码不能直接对阿拉伯数字编码、加密。

从图 27 的替代方表可以看出，25 格的表中，连 26 个拉丁字母都没法装完，更没有 0 ～ 9 这 10 个阿拉伯数字的空余位置。然而，战场信息显然又不可能离开大量的数字，这样一来，就必须将所有数字都以德文来表达；这种用某一种民族语言来表达数字的麻烦，在瞬息万变的战场上，特别是在战场上操作本来就非常复杂的加密、解密（脱密）过程中，有时足以令人疯掉。例如，365872，用中文表示是“三十六万五千八百七十二”，用英文表示就得是“three and sixty-five thousand and eight hundred and seventy-two”。

为此，发明 ADFGX 密码的纳贝尔上校在 ADFGX 中增加了一个字母 V，变成 ADFGVX，这样，图 27 的替代方表就变成了 6 × 6 = 36 个空格了，不仅可以将先前略去的 y 放入，而且还余下 10 个空格，刚好可以放置 0 ～ 9 这 10 个数字。

图 29. 法军密码分析员乔治·潘万中尉

而且，由于增加了方表格数，也就增加了方表中字符排列顺序的变化种类，同时也就增加了破译难度。

更而且，现在包含 0 ～ 9 这 10 个数字的方表将这些数字与字母一视同仁都编码为 ADFGVX 中的两个字母，再通过移位表移位，那么，有着诸如“the”、“any”、“back”之类固定搭配的语言单词，就和没有这类固定搭配的数字一起，被混合打乱、搅成一锅浆糊了，让敌人更加难以从词频、字频的角度发现蛛丝马迹。

至于为什么增加的字母是 V 而不是另外什么字母，原因是字母 V 的摩尔斯电码为“...-”，易于拍发也易于分辨和抄收。

在战场上，选用一些无论在拍发还是在抄收时都不容易出错的字母作为密码字符，这一点非常重要：枪林弹雨中，密码操作员精神高度紧张，如果事先设计密码时对此考虑不周，这时出错的概率必然大大增加。

很完美，是不是？可惜，他们遇上的是一个天才级的对手，乔治 • 潘万！

在法国这边，结合战场形势，已经基本可以肯定德国人即将发动一场对于双方都是决定性的强大攻势；再从德国人并不知道 ADFGX 密码已被破译的情况下，却“悍然”启用强度更高的 ADFGVX 密码来看，德国人对这一攻势的期望之高可见一斑！因此，这一攻势之于法国命运的重要性，可想而知。

而且，关键是德国人要的只是协约国这边在战役结束之前不能破译即可，而协约国特别是法国这边，却必须在德国发起攻势之前——还不能是已经临近敌人进攻开始的“之前”，还必须得让自己有起码的反应、调动、准备的时间——破译这个密码，否则在此之后，败局已定，无论多么完美的破译也都没用了。这一点，德国人很清楚，法国人很清楚，潘万中尉也很清楚。

图 30. 联军统帅福煦元帅

在对截获的密电进行仔细端详以后，潘万的注意力很快集中到其中三份电文上。这三份电文有个共同特点：都是 GCI 电台发出的，电文的时间组都是 00 : 05。

基于此前他对 ADFGX 密码的成功破译，终于，他在第二天下午七时前，也就是 6 月 2 日 19 时前，完全还原了德军 6 月 1 日使用的 ADFGVX 的移位表和方表！

剩下的事情就没什么可说的了，他很快得出了这两份密电的明文：

“第 14 步兵师：司令部要求电告前线（情况）。第 7（军）司令部。”

“第 216 步兵师：司令部要求电告前线（情况）。第 7（军）司令部。”

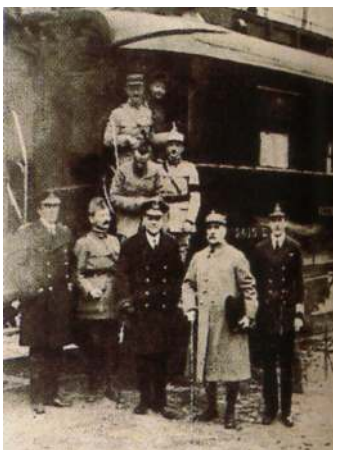

图 31. 贡比涅森林：福煦与德国签订停战协定后在福煦车厢前留影

但这对于法国来说，还没解决问题的全部，他们还必须尽早知道，德国将在何时、何地发起这场对于法国生死攸关的战役？

要知道，此时不仅德军前锋距巴黎已不足 70 公里，德军还占据了巴黎以北亚眠和蒂耶里堡两大突出部，对巴黎已形成了钳形进攻的态势！

这样的情况下，作为协约国联军统帅的法国福煦元帅，怎能不为猜测对面的德军统帅鲁登道夫元帅的想法而犯愁呢：他手里没有那么多预备队兵力，能让他布置到所有可能的德军进攻方向上，他必须知道鲁登道夫到底想在哪里动手。

好在，上帝此时对法国的心情似乎不错，让法国人的好运气再一次延续：6 月 2 日了，德军居然还在使用 6 月 1 日的替代方表和移位表！这已经够出奇的了，可到了 6 月 3 日，这种情况居然还在延续！真能让人晕倒！

这可犯的是密码学的大忌：“一次一密”做不到也就算了，但若连“一天一密”都不做到，这个战地密码最最起码的底线也就丢掉了！

6 月 3 日清晨，潘万的下级吉塔尔，面对着新截获的德军密电，不知德军今天的密钥又会把密文的分组搞成什么样；抱着死马当作活马医的态度，先用前天的分组方式试试，居然成功了！再用前天的替代表和移位表一试，让他都不敢相信自己的眼睛 : 居然都对了！这不是见鬼了么？

看看电文：“赶运弹药，不被发现（的话）白天也运。

就这么简单的十二个字，成为了协约国军队战场态势的一道分水岭！ 由此，赶紧辅以其他来源的情报和分析，法国