弗兰克·穆尔曼领导的无线电情报科，在一九一七年秋始见雏型，当时只有很少几个人，这些人在美国远征军扩充到最大时期，成为这个有七十二人的单位的核心力量。除了这些人员之外，每个集团军司令部还配有六个密码分析员，用总部所给的密钥，将从前线截收来的报文脱密。

无线电情报科的工作分成密码分析和其它四个次要方面——报务分析、截收敌军电话、跟踪敌军炮兵弹着观察机和监听美军通信以杜绝违反保密的现象。无线电情报科在截收战中第一个真正的胜利是随着德军"密钥本"的启用而获得的。这事发生在一九一八年三月十一日。

那是在德军启用一种新密本的当天，午夜零时四十分，苏伊的美军截收站截收到一份用新体制加密的电报。从 X2 台发给AN台：

00:25 CHI-13 845 422 373 792 240 245 068 652 781 245 659 659 504

十二时五十二分，AN 台回电：CHI-13 OS RGV KZD。五分钟后，X2 台向 AN 台发第二份电报：

00:25 CHI-14 UYC REM KUL RHI KWZ RLF RNQ KRD RVJ UOB KUU UQX UFQ RQK

当这些报文出现在密本破译负责人伯索尔德的办公桌上时，他立刻猜出所发生的事情：X2 台用一种新体制发出一份十三组的密报(CHI-13)。AN 台回电 OS，这是表示 Ohne Sinn(报文读不通)的电台公报缩语，内容是有关 CHI-13 的，接着是老的KRU密本的两组密码。于是X2 台发出第二份电报，这次用的是KRU密本，但仍用原来的时间组（00:25)。这种老的 KRU 密本已经部分被破开，因此伯索尔德知道 AN 台这份短报中的 RGV 意思为"老的"。他不知道 KZD 的意义，但是从所发生的情况来看，很可能表示"用密本加密发送"，从而构成"用老密本加密发送"这个完整的片语。难道德国人竟可能愚蠢到用新老两种体制发同一份报

文，而使它们的新密本在启用后一小时内就遭破译吗？

当伯索尔德用还原出来的KRU密本填入X2台的第二份电报时，这份电报读为：

UYC REM KUL RHI KWZ RLF RNQ KRD RVJ UOB
An 〔?〕 Bn. 2 h i r sch

KUU UQX UFQ RQK
w i tt e

KWZ和UOB可能是虚码，作为字间隔符号——这肯定是违反规定的，而REM可能表示Kommandant（司令官）。当伯索尔德用第二份报检验第一份报时，他立刻发现第一份报有同样的明文。用KRU密本的多名码和编字码隐蔽起来的明文中i和t的重码，在这份三码数字电报中显然是以重码245和659的形式出现。以这四点为基础，伯索尔德可得出下述对应关系：

845 422 373 792 240 245 068 652 781 245 659 659 504
An 〔?〕 Bn. 2 h i r sch w i t t e

一架参谋部联络机迅速将他的破译结果送往英国密码分析部门，而伯索尔德本人用破译人员专用密本加密，将破译结果电告法国人。三个单位紧密合作，在两天之内就剥开密钥本的加表，推出许多编字码，读通所有“密钥本”电报。

德军的ADFGVX体制在整个密码学中大概是最著名的战地密码。所以这样命名，是由于在这种密报中只出现这六个字母。*这种体制在一九一八年三月五日开始使用时只用其中的五个字母（未用V）。

当时西线战争已经成为消耗战的僵持局面。冬季，德国认识到要想获得全胜就必须在春天取得胜利。潜水艇未能迫使英国挨饿而投降，而美国已经加入反对她的战争。虽然俄国的崩溃使德军腾出几十个师用于西线，从而使德国在西线第一次在数量上占

* 选择这六个字母显然是由于这六个字母的国际莫尔斯电码的区别非常清楚，可以减少差错：A ·— D—·· F··—· G——· V···— X—··—

优势。但这只是在美国能够横渡大西洋运来强大的有生部队之前的优势。这是一去不再来的时机，于是帝国政府就驱使它的疲劳的部队和饥民来作获取最后胜利的最大努力。

对协约国来说，德军准备发动一场春季攻势那也是很清楚的。很多迹象说明这个问题，而采用新密码本身就是其中一个征兆。问题是真正的打击在何时何地发生？德军统帅部认识到突然袭击具有无限的军事价值，因此对作战计划绝对保密。据说经过一次德国密码专家会议从很多种体制中挑选出来的 ADFGVX 密码，构成这一全面保密措施中的一个要素。

当第一批 ADFGX 密报交给法军密码局最优秀的密码分析家乔治·潘万时，他眼巴巴地看着这些报文，露出一副窘态。然而测向表明，这种密码用于德军高级司令部之间的来往电报，通过对它的破译，就会取得战略情报。他假设这种密码是在棋盘代替的基础上再作一次移位作业，但什么结果也没有得出来。

三月二十一日晨四时三十分，六千门大炮用这次战争中最猛烈的炮火突然向松姆地区协约国军战线开火。五小时之后，六十二个德军师在一条四十哩宽的战线上压过来。这次袭击完全是突然的，它的成功是巨大的。法军和英军连日狼狈后撤，顿时被打得一片混乱。一星期之内，德军在协约国军战线上打开一个纵深三十八哩的缺口，直到法军和英军退却至亚眠重新集结部队，才阻止了德军的前进。

这种猛烈的推进，使无线电的报量剧增。第一次试破结果是令人失望的。潘万的频率统计表明棋盘密钥每天更换；移位密钥大概也每天一换。因此破译要求一天内有颇大数量的报文，但是在四月一日前截收报量太少。四月一日那天，法军截收到十八份ADFGX密报，总计五百十二个五码文字组。其中两份密报分成长度不同的三部分发送：德军在战争初期吃过复合猜字的亏，从中接受了教训。

在研究这两份报的过程中，潘万在四月四日发现这两份密报

的第一部分在密文相同位置上夹有一些相同的单码和多码。这种奇特的现象，很可能是由于这两份密报的报头部分相同，又用相同的移位密钥而产生的，那么报文的相同部分就表示移位表的纵行有相同的顶部。将密文分段，使每个相同的部分成为新的一段报文的起头部分，这样就可按照报文的抄写次序得出移位表的纵行。潘万对CHI-110和 CHI-104 两份密报进行了这种分析。CHI-110是一份 VI 台发往B8台的密报中由一百一十个码子组成的第一部分；CHI-104 是在十三分钟后 VI 台发往 BF 台的一份密报中由一百零四个码子组成的第一部分（CHI-104 报第十三组可能多一个码子——译注）：

CHI－110：（1)ADXDA(2)XGFXG(3)DAXXGX(4)GDADFF
CHI－104：（1)ADXDD(2)XGFFD(3)DAXAGD(4)GDGXD

CHI－110：（5)GXDAG(6)AGFFFD(7)XGDDGA(8)DFADG
CHI－104：（5)GXDFG(6)AGAAXG(7)GXG?D （8)DFADG

CHI－110：（9)AAFFGX(10)DDDXD(11)DGXAXA(12)DXFFD
CHI－104：（9)AAFFF （10)DDDFF(11)DGDGF (12)DXXXA

CHI－110：（13)DXFAG （14)XGGAGA(15)GFGFF
CHI－104：（13)DXFDAF(14)XGGAGF(15)GFGXX

CHI－110：（16)AGXXDD(17)AGGFD(18)AADXFX
CHI－104：（16)AGXXA (17)AGGAA(18)AADAFF

CHI－110：（19)ADFGXD(20)AAXAG
CHI－104：（19)ADFFG （20)AAFFA

现在的问题是找出移位密钥，或者换一种说法，还原移位表。开始可按照长纵行位于左侧的原则进行。潘万发现，在这两份密报中，第三、六、十四和十八纵行（3、6、14 和1 8 就是这些纵行

的密钥数字）比其它纵行长。他把这几个纵行移至移位表的最左侧。第四、七、九、十一、十六和十九纵行在 CH I-104 密报中为短纵行，而在 CHI-110 密报中为长纵行，因此，把它们集中在前四个纵行右侧和其余十个纵行左侧的区域内。其余十个纵行在两份密报中都为短纵行，所以都移至右侧。这三个区域标志着向密钥逼近了第一步。

潘万不能从这两份密报的第一部分获得更多的材料，于是就转向第三部分，希望从中找出相同的报尾。相同的重码形式表明这两份密报确实有相同的报尾，这就使潘万又能象第一部分那样适当地把报文分成纵行。根据长短纵行，在报文中初步分成三个区域，从而使潘万向密钥逼近了第二步。这种分析结果表明，第五、第八纵行在移位表中间区域是彼此相邻的两行，第十二、第二十纵行在最右侧，虽然潘万还不知道它们之间的次序是 5—8 还是 8—5，是 12—20 还是 20—12。

他又回过头来研究这一天截收的十八份密报的原报，把这些密报报文分成二十段，并将其中所有的第五和第八段进行配对。配对结果得出六十对字母，潘万对这些字母进行频率统计。统计结果表现出单表代替的所有特点。它表明这两个纵行在移位表中确实是相邻的。

他对 12—20 这组进行类似的试验，同样得出单表代替的频率表现。最高频率的双码是 DG，频率为 8，它大概表示明文 e。但是 DG 在 5—8 组合中频率为 0，所以不可能代表德文的 e。另一方面，GD 的频率为 8，由于潘万不知道每对纵行中的次序，所以在频率统计中他任意选择的次序 5—8，对于 12—20 纵行组合来说很可能把次序颠倒了。为调整两纵行组合的关系，潘万将 5—8 颠倒成 8—5，使 GD 转换成 DG。DG 的频率为 8，是 e 的更适合的可能双码。原来的 DG成为 GD，频率为 0。现在潘万可以构成一个棋盘的轮廓。按先纵行后横行的次序取座标码，并将还原的明文值填入表中：

	A D F G X
A	
D	e
F	
G	
X	

移位表的其余部分如何还原呢？由于坐标码是反复按纵行-横行次序取出，而移位表又有二十个纵行，因此，在加密时所有纵行坐标码都处于第一、三、五……十九的位置上，而所有横行坐标码全在偶数位置上，因此：

位置编号	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
位置奇(o)偶(e)	o	e	o	e	o	e	o	e	o	e	o	e	o	e	o	e	o	e	o	e
移位纵行密钥数字											8	5							12	20
纵行(s)或横行(t)坐标码	S	T	S	T	S	T	S	T	S	T	S	T	S	T	S	T	S	T	S	T
	S	T	S	T	S	T	S	T	S	T	S	T	S	T	S	T	S	T	S	T

潘万认为，如果纵行坐标码同横行坐标码分开，这就把奇数位置同偶数位置分开了。坐标码可以根据频率的特性分开。纵行坐标码D的频率不同于横行坐标码D的频率，因为D横行五个字母的总频率不同于D纵行五个字母的总频率。其它各个坐标码的情况亦相同。因此，横行坐标码应该呈现一条和纵行坐标码不同的频率曲线。

频率统计表明密报各纵行确实分成两群：一群以D为其最大值，以G为其最小值；另一群以G为其最大值，以F为其最小值。包括第十二纵行在内的第一群证实是处于奇数位置。潘万通过配对来确定相邻的奇偶纵行，只有正确的配对才呈现出单表代替的频率分布。同时他开始猜出明文并还原棋盘，通过四十八小时惊人的劳动，潘万终于破开用这种当时世界上最难破的战地密码加密的第一批电报。

这种密码将一个明文字母的对应密文分成双码，然后，移位以一种特别有效的形式将双码特性分散开来，而分散的特性又遮

住一些通常有助于还原移位的线索。因此，协约国从未研究出一种ADFGVX 体制的通用破译方法是不足为奇的。密码分析几乎总是依赖于找出具有相同的报头部分或报尾部分，或者有其它一些漏洞的两份密报。破译在顺利地进行，速度越来越快。从德军的观点看，这种体制迅速方便，只包括两步简单的作业。报文长度虽然增加一倍，但由于这种密报只有六个不同的字母，密报可以发得更快更准确，使这种缺点得到一定的弥补。

到六月一日，法军已遭到两次不愉快的打击——一次军事上的打击，一次编码技术上的打击。鲁登道夫又设法隐蔽一次大规模进攻的时间和地点。他的十五个师突然在七时发起进攻。德军灰色人流淹没了塞明德达梅斯高地的法军阵地，不可阻挡地挺进到离巴黎只有三十哩的马恩河畔。几乎使协约国的事业全遭覆没。与此同时，潘万突然发现在六月一日 ADFGX 密报因增加第六个字母 V 而更加复杂了。大概是德国人把他们的棋盘密扩大为 6×6 。

他在下午五时开始攻击六月一日的密报。这一天的三份密报都有相同的时间组(00:05)，而且都是由 GCI 台发出。潘万比较其中两份密报：一份发给 DAX 台，另一份发给 DAK 台，这两份密报报文大体相同，每份均为一百零六个字母。但是除表明密钥长度为二十一之外，其他就什么也得不到；这两份报太相似了。于是他把 DAX 台这份报同 GCI 台发出的第三份报进行比较，这是一份发往 DTD 台的一百零八个字母的密报，和其它两份密报十分相似。他象处理四月一日密报那样，把这几份密报分成各纵行段，得出两个大体上的移位表，但移位表的密钥序他还不知道。

潘万假定，这两份密报的明文全部相同，只是在那份 DTD台密报报内收报单位增加了一个明码。这就使得相同部分在 DTD 台报文的移位表中，比在DAX台报文的移位表内要后退两个字母的位置。他只好去排列能产生这种结果的纵行次序。一小时内，他找出了这种次序：

6 16 7 5 17 2 14 10 15 9 13 1 21 12 4 8 19 3 11 20 18

很快就得出这种棋盘密的破译结果：

	A	D	F	G	V	X
A	c	o	8	x	f	4
D	m	k	3	a	z	9
F	n	w	l	0	j	d
G	5	s	i	y	h	u
V	p	l	v	b	6	r
X	e	q	7	t	2	g

DAX台密报的明文为：14 ID XX Gen Kdo ersucht vordere Linie sofort drahten XX Gen Kdo 7〔第十四步兵师：司令部要求电告前线(情况)。第七(军)司令部〕。DTD台密报报文全部相同，仅收报单位是第二一六步兵师。

潘万在六月二日下午七时完成他的破译工作，并立刻将破译结果上送总司令部。此时法军正在设法阻止鲁登道夫的推进，但他们处境濒危，立足不稳。德军从六十哩外用远射程大炮轰击巴黎。德军三月和五月的巨大胜利已经把两大突出阵地推入协约国境内。这两大突出阵地就象匕首一样直指巴黎。那个重大问题又重新出现在面前：鲁登道夫下一次将在什么地方发起攻击？薄弱的协约国防线再也承受不起集中在一点上的象打桩机般的巨大打击。如果鲁登道夫象前几次攻势那样，成功地赢得这种突然性，他就可突破协约国防线，占领巴黎，甚至结束这场战争。协约国阻止鲁登道夫推进的唯一希望，是用后备队兵力顶住鲁登道夫的正面攻击。但是要达到这个目的，就必须知道应该将后备队开往何处。

法军讨论了各种可能性。是鲁登道夫会不顾两翼安危而从其中一个突出阵地的前沿直取巴黎？还是鲁登道夫会首先推平两大突出阵地之间的大马鞍形地段，然后从一个巩固的阵地向前推进？

如果是后一种情况，那么他将在这个大口袋的哪个地方下手？谁也不知道。

六月三日晨，法军密码局的吉塔尔突然出现在这种阴郁的气氛中，激动地挥动着一份截收到的电报。总司令部的一位密码分析家利用潘万送来的密钥恰好译通一份上午四时三十分，也就是仅仅在几小时前截收到的一份密报：

CHI-126 FGAXA XAXFF FAFFA AVDFA GAXFX
FAAAG DXGGX AGXFD XGAGX GAXGX AGXVF
VXXAG XFDAX GDAAF DGGAF FXGGX XDFAX
GXAXV AGXGG DFAGD GXVAX XFXGV FFGGA
XDGAX ADVGG A

测向机报告说这份密报系德军统帅部发出，收方是DIC台，根据报务分析和测向结果，是位于雷马奇的十八集团军参谋部，雷马奇是德军防线马鞍形地段上方的一个城镇。密报的明文是：Munitionierung beschleunigen Punkt Soweit nicut〔nicht之误〕eingeschen auch bei Tag(着赶运军需弹药。如不被发现日间也运)。

吉塔尔和情报军官们马上认识到，电报中提到的弹药就是德军通常在进攻前炮轰中使用的炮弹，电报收报单位所在位置向他们说明德军的进攻地点。他们喜气洋洋地把这个情报通知作战部的军官们：鲁登道夫将打平马鞍形地段，德军的重锤将打在蒙迪迪埃和贡比涅之间的法军防线上，这是一段位于巴黎以北约五十哩的扇形地区。

空中侦察证实德军在日间运送弹药。逃兵报告进攻将在六月七日开始。最高统帅福煦调动他的后备队进入阵地，疏散炮击主攻方向的防线，而加强第二道防御工事。六日，军官们接到通知说“进攻迫在眉睫。”空气紧张。七日敌军并无行动就过去了，而八日：鲁登道夫推迟进攻两天以便集中更多的大炮和弹药，他说：“充分准备乃是成功之本。”法军紧张而有信心地等待着。六月九日

午夜，蒙迪迪埃至贡比涅的战线上爆发一阵急风暴雨般地倾泻下来的高爆榴霰弹和毒气弹。前沿阵地平均不到十码有一门炮的德军，集中炮火连续轰击法军阵地三个小时——鲁登道夫紧急命令运送弹药的目的已经完全清楚了。但是这一次是鲁登道夫自从取得一连串惊人的胜利以来，头一次没有出奇制胜。潘万的甘露拯救了法国。

拂晓前不久，德军十五个师发起冲击。法军严阵以待。战斗来回拉锯五天。最初，德军占领梅里和库克勒小村庄，但是在六月十一日，夏尔·芒让将军以五个师的兵力和法军可以鼓起的全部锐气发起反攻。他阻止住德军的推进，然后肃清这两个村庄里的灰色的德军。德军再次大力进攻。德军失利，损失惨重。这是鲁登道夫在这个春天第一次在战役目的未达到前就中止战役行动。福煦认识到德军的其他猛攻就要到来，他必须抵御德军，但他知道最后他总有一天要发动攻势。这时他知道这场战争并未打输，而最终会取得胜利。在几个星期内，德军的最后几次攻击到来了，但德军大势已去，法军把德军挡了回去。不久在美军的支持下，主动权很快转到协约国方面，协约国发动的强大反攻赶得德军连连后退，直至德国皇帝在他的军国主义美梦破灭的情况下退位出走，他的将军们在贡比涅签署休战条约。这次世界大战至此结束。

第一次世界大战是密码史上一个伟大的转折点。在大战前，密码学还只是一个小的领域；在大战后，它成了一个大的领域。在大战前，密码学还只是一门年青的科学；在大战后它已经成熟。这种发展的直接原因是无线电通信大量增加。

随着密码分析一再显示出它的能力和价值，密码分析由一个辅助的敌方情报来源上升为一个主要的来源。密码分析作为一种持久的主要情报手段出现，是密码学成熟的最显著标志。

另一个标志是密码分析学本身的变化。这门科学最终摆脱了那种盛行四百年的关在黑屋内分析的工作方式，即一个人在房间

里独自钻研一份密报。在这次大战初期，黑屋式的分析使密码分析家感到不能满足需要。德国人的二次移位至少需要两份等长的密报才能破译，但是在获得这两份密报之前，必须截收大量密报。随着密码体制越来越复杂，密码分析也越来越依靠这类特殊的破译条件。因此，为了破译成功，就需要比那些戴着假发的黑屋分析行家认为必需的多得多的密报。他们也更多地依靠报务分析和了解外围情况这类辅助手段，因为对发报的前后情况知道得越多，根据特定情况进行破译就越容易。因此，密码分析人员和现实世界的联系也远比过去密切得多。

新的成熟的第三个标志是密码分析向专业化方面发展。秘密通信的体制不再是那样少而单纯，以至一个专家就能完全解决问题。秘密通信体制类型多样，特点各异，加上每种类型的报量，哺育出密码分析的各行专家。在所有的专家中，最令人感兴趣的大概是密码分析机构的主任。主任不再是一群密码分析人员的台柱人物，而是一个从不拿起颜色铅笔或橡皮从事实际破译的纯行政官员，他只能集中精力在向其他部门了解最需要什么情报，部署他的破译队伍来获取这种情报。

另一个成熟的标志，是对不熟练的、偷懒的、无知的密码员的过错所起作用的深切认识。专家们认识到，要消除这些问题，加强密码使用的保密要比采用最巧妙的密码有效得多。第一次世界大战中，密码学取得最大的实际教训，就是必须向密码使用人员灌输铁的纪律。吉维埃格宣布一个必须使密码人员牢记的原则："要么很好加密，要么完全不加密。以明文发报，你只是给敌军一份情报，而你知道这是哪份情报；但加密得不好，你就会使敌军读通你的全部电报以及你友军的电报。"

但是，所有这些发展主要来自密码学和外部世界的相互影响；这些发展的方向是由外界决定的。第一次世界大战中，并没有引起由内因决定的发展，例如，战地密码的出现。相反，实际的手工加密作业和呆板的频率分析的破译技术，这两个最主要活动的

效用已经达到了尽头。

手工体制承受不起这些体制从未设想到的报量。不少密码员梦想用机器从他们的肩上移去这种沉重的负担。在某种意义上，广泛使用的密本可以看成一种为加密者工作的机械器件的原始形式。但是，战壕密本和后来的印字密码机相比，就象马恩地区的士兵队列和装甲纵队的装甲军车相比一样。

同时，频率分析的古典原则也已施展至最大限度。这些原则应用得很巧妙，如潘万用比较频率分布的方法来确定 ADFGVX 密码移位表的奇偶纵行。但是没有出现新的原则。

在这两个密码学内在的核心问题上，第一次世界大战标志着的不是开端，而是结尾；不是成果累累，而是毫无成就。然而，这一门科学能这样生存下来，那末，这一门科学的真空就会得到填补，这一门科学的需要就会得到满足。

第十二章　两个美国人

赫伯特·奥斯本·亚德利(1889—1958)生于印第安纳州沃信顿，二十二岁时进入国务院当密码员。亚德利在国务院担任密码员期间，密码学点燃起他的想象力，他曾破开一份美国政府内部密码电报，破译的成功使他更沉醉在密码分析中。一九一七年四月，美国宣战后不久，他向陆军部提出建立一个密码部门的想法。他的想法得到采纳，并被任命为军事情报处新组成的密码科(代号为 MI-8)科长。在密码科下，相继设立教导股、密码编制股、通信股、速记股、密写墨水股。军事情报处密码科破译阿根廷、巴西、智利、哥斯达黎加、古巴、德国、墨西哥、西班牙和巴拿马等国外交电报。西班牙文报文构成该科密码分析工作的主体。

第一次世界大战结束后，亚德利在一九一九年五月十六日向陆军参谋总长提出一个建议成立“密码研究和破译的永久性机构”的计划。三天后，陆军参谋总长批准这项计划。这项计划由陆军部和国务院每年共同拨款约十万美元支持，但是实际支出从未达到过这个数额。国务院从一九一九年七月十五日开始拨款四万美元。十月一日，这个后来以美国黑屋闻名的机构就在纽约隐藏下来。虽然这个部门是军事情报处的分支机构，但是陆军部在一九二一年六月三十日才开始拨款。

这个机构的首批任务中有一项是破译日本密本，当时同日本的摩擦已日益加剧。亚德利把第一个破开的密本命名为“Ja”密，“J”代表日本，“a”代表一系列破译中的第一个破译结果。一九一九年至一九二〇年春，日本人由于聘请到波兰专家科瓦列夫斯基上尉修改他们的密码体制，先后启用十一种不同的密本。科瓦列夫斯基教会日本人如何将报文分成两个、三个或四个部分，并把各