公元 1040 年左右，北宋仁宗时期兵书《武经总要》中，讲述了三种军队中秘密通信的方法：符契、信牌和字验。

符契是《六韬》中阴符的改进。其中的“符”是皇帝派人向军队调兵的凭证，共有 5 种符，各种符的组合表示调用兵力的多少，每符分左右两段，右段留京师，左段由各路军队的主将收掌。使者将带着皇帝的命令和由枢密院封印的相应的右符，前往军队调兵；主将听完使者宣读皇帝的命令后，须启封使者带来的右符，并与所藏的左符验合，才能接受命令；然后用本将军的印重封右符，交由使者带回京师。“契”是主将派人向镇守各方的下属调兵的凭证，共有三种契，每契都是鱼形，可分为上下两段。上段留主将收掌，下段交各处下属收掌，使用方法类似于符。

信牌是两军阵前交战时，派人传送紧急命令的信物和文件。北宋初期使用的信物是一分两半的铜钱，后来改用木牌，上面可以写字。

字验则是秘密传送军情的一套方法。先约定 40 种不同的军情，然后用一首含有 40 个不同字的诗，令其中每一个字对应一种军情。传送军情时，写一封普通的书信或文件，在其中的关键字旁加印记。军使在送信途中，不怕被敌方截获并破解信中内容。将军们收到信后，找出其中加印记的关键字，然后根据约定的 40 字诗来查出该字所告知的情况，还可以在这些字上再加印记，以表示对有关情况的处理，并令军使带回。

1.1.1.3　矾书

矾书是用明矾水写的书信。当水干后，纸上毫无字迹，把纸弄湿后，字迹重新显现。

据记载，矾书是中国古代军事和政治斗争中常用的秘密通信方法。南宋李心传（1166—1243）所撰《建炎以来繫年要录・建炎元年正月》、元代《金史・宣宗纪上》中均记录有用明矾写的机密信。清康熙五十四年（1715 年）发生过“矾书事件”。

1.1.2　传统密码学与古代西方保密通信方法

1.1.2.1　传统密码学

西方国家大都使用拼音文字，只有二十几个字母和几个标点符号，文字符号较少，所以很适合对文字内容进行各种变换以实现保密通信。同时，由于西方世界率先进行了工业革命，发明了机器和电报等先进技术，所以，西方一直在引领着密码学的发展，尤其是近代以来。因此，逐步形成了以西方拼音文字为主要研究和操作对象的传统密码学理论和方法，这些理论和方法并不完全适用于中国的象形表意文字。

传统密码学主要分为两大类：换位加密法和替换加密法。

1．换位加密法

换位加密法是指在加密过程中不改变字或字母本身，只改变它们的排列顺序，以达到加密的目的。古希腊军队使用的 Scytale 棒就是一种简单的换位加密法。

另一种常用且较复杂的换位加密方法是按一种特定的路径，把信文写在一张信纸上，然后在信纸的其他空白处写上无关紧要的文字，信件按正常顺序读起来就是一封普通的信。收信者只需按照规定好的路径去读，就能获取真正的信文。中国古代的字验就采用这种换位加密方法。

中国古代的“藏头诗”也是一种换位加密方法：将每句诗的第一个字连起来读，就会表达另一种含义。如《水浒传》中梁山为了拉卢俊义入伙，智多星吴用在玉麒麟卢俊义家中的墙上写下一首藏头诗：“芦花滩上有扁舟，俊杰黄昏独自游。义到尽头原是命，反躬逃难必无忧。”该诗巧妙地把“卢俊义反”四个字暗藏于四句之首，而一心躲避“血光之灾”的卢俊义并没有细察这其中的隐秘。果然，这四句诗写出后，被官府拿到了证据，大兴问罪之师，到处捉拿卢俊义，终于把他逼上梁山。

意大利文艺复兴时期的名人达芬奇，总是用“镜像法”记笔记，据说是为了防止别人偷窥他的秘密。也就是说，他的笔记本只有通过镜子才能被正常阅读。因此，“镜像法”也是一种换位加密法。

2．替换加密法

替换加密法是指不改变信文中字或字母的顺序，而是用其他的符号来替换它们，以达到加密的目的。根据信文中每个字（字母）使用一个或多个字（字母）替换，又分为单表替换和多表替换。

古罗马军队的凯撒（Caesar）加密就属于单表替换加密，此类替换加密很容易被破解。

维吉尼亚（Vigenere）密码和杰弗逊（Jefferson）加密器属于多表替换加密，其破解难度要比单表替换加密大得多。近代以来，西方主要使用的是各种多表替换加密方法，甚至在第二次世界大战中使用的那些极其复杂的机器密码，本质上也是多表替换加密。

1.1.2.2 古希腊军队的 Scytale 棒

大约公元前 700 年，古希腊军队使用 Scytale 棒的加密方法是一种简单的换位加密法。其使用方法是：把长带子状羊皮纸缠绕在圆木棍上，然后在上面写字；解下羊皮纸后，上面只有杂乱无章的字符，只有再次以同样的方式缠绕到同样粗细的棍子上，才能看出所写的内容。例如，在缠绕于木棍上的纸带上写下英文字：tommorrow midnight attack，表示开始军事进攻的时间；然后把纸带从木棍上解下来，英文字将变成：tmaoitmdtmnaoicrgkrhow。

这种 Scytale 圆木棍也许是人类最早使用的文字加密解密工具，据说主要是古希腊城邦中的斯巴达人（Sparta）在使用它，所以又被称作“斯巴达棒”。

1.1.2.3 古罗马军队的凯撒（Caesar）加密

公元前 100 年前，古罗马军队统帅凯撒设计了一种军事信息加密方法，用于同手下的将军们进行保密通信。所有字母用字母表中顺序循环移位后的字母替换。当规定字母表顺序移动 3 位时，则 a 替换为 d，b 替换为 e，c 替换为 f，……，x 替换为 a，y 替换为 b，z 替换为 c，军事信息 tommorrow midnight attack 就变成 wrppruurz plgqljkw dwwdfn。如果不知道加密方法，就无法知道该信息的实际意义；解密时，只需把所有字母逆序移动 3 位，就能获得军事信息明文。

凯撒密码属于单表替换法，而且替换的规则很简单。

1.1.2.4 中世纪后保密通信方法

13 世纪开始，欧洲经历了一场提倡人文精神和思想解放的影响深远的文艺复兴运动，这一时期，欧洲诸国开始进行现代意义上的外交活动，纷纷在别国建立大使馆并互派大使。

身处异国的大使要向自己的政府汇报高度机密的信息，却只能通过两国之间的公共邮政系统来传递，为此外交官们不得不绞尽脑汁使用各种复杂的加密方法来写信。另外，情报机关也在费尽心机破解这些信。各方斗智的结果便促使了密码技术的迅速发展。

16 世纪开始，欧洲又掀起了一场范围广泛的基督教改革运动，因为涉及敏感的教义等问题，极其活跃的宗教界人士都在用五花八门的加密方法写信交流。

欧洲诸国的皇宫内也布满了各种阴谋诡计，密码当然成为不可缺少的酝酿阴谋的工具，同时，破解密码也成为揭露阴谋的最有效手段。种种因素导致密码在欧洲的外交界、宗教界和政界大肆流行，传统密码学迎来了它的繁荣时期。

1．维吉尼亚（Vigenere）密码

由于单表替换加密很容易被频率分析法破解，15 世纪中叶开始，欧洲人开始研究各种“多表替换加密”方法，即信文中同一个字母在不同的位置会有不同的替换符号，其中最有名的是“维吉尼亚密码”。

维吉尼亚密码因为其原理简单、使用方便而广受欢迎，它使用一张字母表矩阵：第一行是任意给定的字母替换表，第二行是第一行表顺移一位而形成的字母替换表，第三行表又是第二行表的顺移一位，以下各行以此类推。加密时，对于信文中的同一个字母，当其第一次出现时使用表的第一行替换，第二次出现时使用第二行替换，以此类推。如果该字母出现次数已超过矩阵的行数，则回到第一行继续。解密同加密一样，也是从上到下逐行进行。

显然，多表加密比单表加密复杂许多，因此其破解难度也加大许多。自从维吉尼亚密码出现以后，多表加密成为欧洲人主要使用的加密方法。

2．欧洲的黑室

到了 18 世纪，欧洲各国相继成立了专门截获和破解外交邮件中机密信息的机构，这些机构被称为“黑室”，其存在及所作所为在当时是各国之间心照不宣的秘密。黑室中的密码专家经常因破译重要的机密信而获得皇室的嘉奖。

3．杰弗逊（Jefferson）加密器

美国第三任总统托马斯·杰弗逊于 1795 年发明了一种加密装置叫杰弗逊转轮加密器。该装置有 36 片同样大小的木制转轮，套在一根铁杆上。每片转轮的圆周边缘上刻有乱序的 26 个英文字母。其使用方法是：进行秘密通信的双方必须各自拥有完全一样的转轮加密器，当一方要把一段文字（不超过 36 字）秘密通知身处异地的对方时，只需转动加密器上的各片转轮，使这段文字正好出现在同一行上，这时转轮上排列的其他 25 行都是无意义的乱码；再把其中任意一行的乱码抄下来交给信使。信使并不知道这段乱码文字的意义，只负责把它送交对方。对方收到乱码信后，只需拿出自己的转轮加密器，转动上面各片转轮，让其中一行的排列和这段乱码同处在一行上，然后再查看其他 25 行上的内容，其中必然有一行显示出加密者要传达的信息，而其他行显示的都是乱码。

杰弗逊加密器属于多表替换加密（每一个转轮相当于一张替换字母表），它很难被破解，除非得到通信双方所使用的加密装置。据称，美国军队到了 20 世纪 60 年代仍在使用它。轮转式加密器在第二次世界大战时很流行，不过都是机械电子式的，并且与打字机等设备结合使用，比杰弗逊的最初原始装置高级很多。

1.1.2.5 古代阿拉伯人开创密码分析学

公元 9 世纪，阿拉伯数学家、哲学家肯迪所著《解码手册》是历史上最早研究用频率分析法破解密码的文献。英文文章中每个字母出现的频率是不同的，如图 1-1 所示。由于 E 频率最高，如果一份密文中 R 出现的最多，则 R 可能就是 E；即使不是 E，也应是明文中出现频率较高的字母。按照这种频率分析方法，密码就容易破解。

字母	频率	字母	频率
a	0.08167	n	0.06749
b	0.01492	o	0.07507
c	0.02782	p	0.01929
d	0.04253	q	0.000009
e	0.12702	r	0.05981
f	0.02228	s	0.06327
g	0.02015	t	0.09056
⋮	⋮	⋮	⋮

图 1-1 英文字母频率表

基于字母和单词统计学特征的频率分析方法一直是破解密码最基本和最常用的方法。两次世界大战中的密码战，是当时敌对双方最优秀的科学大脑和最先进的科技之间的生死较量，但究其所依据的加密和破解原理，仍然是基于字母和单词的频率分析，只是复杂程度更高而已。

1.1.3 两次世界大战的密码斗法

1.1.3.1 第一次世界大战

1837 年，美国人发明了电报，1896 年前后，意大利人和俄罗斯人分别发明了无线电报，从此人类进入了电子通信时代。有线和无线电报能快速方便地进行远距离收发，因此很快成为军事上的主要通信手段。但是，有线电报需经过电缆传送，而设在海底和野外的电缆很容易被破坏或窃听；而无线电报是一种广播式通信，包括敌人在内的任何人都能够接收到发射在空中的电报信号。因此，为了防止机密泄露，电文的加密变得至关重要。

1914 年 6 月 28 日，塞尔维亚一位 19 岁青年人在其首都萨拉热窝，刺杀主张吞并塞尔维亚的奥匈帝国王储夫妇，由此引发了第一次世界大战，以英、俄、法为首的协约国对抗以德、奥匈帝国、奥斯曼土耳其为首的同盟国。

交战各方相继成立了专门的密码机构，密码专家们开始斗法。争斗中，大家互有胜负：德军截获到俄军的无线电通信，洞悉了其军事部署，结果把拥有优势兵力的俄国人打得大败；不久，战败的俄国在国内爆发了十月革命；法国人则数次破译了德军的密码，成功粉碎了德军攻占巴黎的阴谋。

然而，这场密码战中最大的赢家似乎是英国。1914 年 8 月 4 日，英国向德国宣战，当天就割断了德国的所有海底电缆，迫使德军只能严重依赖无线电报和国外电缆进行通信联系，使得英国海军部很容易地截获了大量的德国电报情报信号。为破解这些加密情报，英国海军部于 1914 年 10 月成立了一个代号为“40 号房间”的密码破译小组，在第一次世界大战期间，该小组成功破译了约 15 000 份德国密电，使得英国海军在与德国海军的交战中屡次占得先机，并最终帮助协约国赢得了战争。

1917 年 4 月 6 日，美国终于向德国宣战。美国陆军部于 1917 年 6 月成立军事情报处第八科，也被称为“美国黑室”。该机构成立时只有 3 人，一年后就发展成近 200 人的庞大组织，下设 5 个部门：密码编写组、通信组、速记组、密写组和密码破译组。该机构破译了德国和日本的大量密码，帮助美国赢得了军事和政治上的胜利。1929 年 10 月，“美国黑室”被新任美国国务卿下令关闭。自 1917 年成立到 1929 年关闭，该机构解读了 45 000 多份密码电

报，破解了包括中国、德国、英国、法国、俄国、日本等在内的 20 多个国家的密码。

1918 年 11 月 11 日，协约国和同盟国宣布停火，并经长达 6 个月的谈判后，于 1919 年 6 月 28 日在巴黎凡尔赛宫签署条约，标志第一次世界大战正式结束。

虽然密码的应用在第一次世界大战中大显身手，但密码学作为一门学科，在此期间并没有突破性的发展，使用的加密方法与古代相比并没有什么创新，只是增加了一些难度。

1.1.3.2　第二次世界大战

第二次世界大战中密码学的发展远远超过了以往任何时代，无论是在密码学的技术、理论还是应用方面，在此期间都发生了革命性变化。

从密码学的技术方面来看，基于机械和电气原理的加密/解密装置全面取代了以往的手工密码，不仅大大提高了加密/解密的速度，也使密码的复杂度大大提高，用传统的手工方式已不可能破解这些机器密码。另外，“矛”的进化也促进了“盾”的发展。破解密码也实现了机械化和电气化，甚至开始使用电子计算机，使得破解密码的效率大大提高。人类从此进入了机器密码时代。

从密码学的理论方面来看，大量的数学和统计学知识被应用于密码分析和破解，并大获成功。于是，越来越多的数学家不断加入密码队伍，他们开始取代语言学专家、象棋冠军和猜谜高手，成为密码战场上的主力军。

从密码学的应用方面来看，参战各国都已认识到密码决定着战争胜负的关键。于是，各国都纷纷研制和采用最先进的密码设备，建立最严格的密码安全体系。如德国军队全面使用“隐谜”密码打字机，德军最高司令部使用“洛伦兹”密码电传机，日本外交官使用“紫色”密码打字机，日本海军使用 JN 系列密码等。

另外，各国都投入大量的人力和物力，集中最优秀的密码专家们想方设法破解敌国的密码。如英国和美国都拥有上万人的密码队伍，专门从事破解德国和日本的军事和外交密码的工作。

英美政府和军队把通过破解密码所获得的情报称为“超级情报”，其重要性甚至超过传统的“顶级密码”。他们竭力保护“超级情报”的来源，不允许它们有任何泄露。正是依赖这些“超级密码”，才使得他们能扭转战争中的被动局面，在战场上取得一系列重要的胜利，最终大败了法西斯强敌。

在中国的抗日战场上，国民党政府建立的“军委技术研究室”也成功破解了日本空军的密码及日本外务省的部分密码，并且与美英两国的密码专家和情报机构建立了合作关系。

1.1.4　现代密码学与信息时代

第二次世界大战时期的密码学经历了历史上前所未有的一场革命，这场革命几乎颠覆了传统密码学中所有的理论和方法，从而迎来了机器密码的时代。这个时代的一个典型代表就是德国的“隐谜”密码机与波兰、英国和美国的“炸弹”破译机这两种机械密码装置之间惊心动魄的较量。

然而谁会想到，曾经如此辉煌的机器密码时代，竟然在第二次世界大战结束后不久，就很快终结了。因为从 20 世纪 50 年代开始，计算机技术突飞猛进，在具有超强计算能力的计算机面前，所有的机器密码都显得不堪一击。