密码技术发展史

密码学是一个即古老又新兴的学科。密码学(Cryptology)一字源自希腊文"krypto's"及"logos"两字，直译即为"隐藏"及"讯息"之意。密码学有一个奇妙的发展历程，当然，密而不宣总是扮演主要角色。所以有人把密码学的发展划分为三个阶段：

第一阶段为从古代到 1949 年。这一时期可以看作是科学密码学的前夜时期，这阶段的密码技术可以说是一种艺术，而不是一种科学，密码学专家常常是凭知觉和信念来进行密码设计和分析，而不是推理和证明。

早在古埃及就已经开始使用密码技术，但是用于军事目的，不公开。

1844 年，萨米尔·莫尔斯发明了莫尔斯电码：用一系列的电子点划来进行电报通讯。电报的出现第一次使远距离快速传递信息成为可能，事实上，它增强了西方各国的通讯能力。

20 世纪初，意大利物理学家奎里亚摩·马可尼发明了无线电报，让无线电波成为新的通讯手段，它实现了远距离通讯的即时传输。马可尼的发明永远地改变了密码世界。由于通过无线电波送出的每条信息不仅传给了己方，也传送给了敌方，这就意味着必须给每条信息加密。

随着第一次世界大战的爆发，对密码和解码人员的需求急剧上升，一场秘密通讯的全球战役打响了。

在第一次世界大战之初，隐文术与密码术同时在发挥着作用。在索姆河前线德法交界处，尽管法军哨 兵林立，对过往行人严加盘查，德军还是对协约国的驻防情况了如指掌，并不断发动攻势使其陷入被动，法国情报人员都感到莫名其妙。一天，有位提篮子的德国农 妇在过边界时受到了盘查。哨兵打开农妇提着

的篮子，见里头都是煮熟的鸡蛋，毫无可疑之处，便无意识地拿起一个抛向空中，农妇慌忙把它接住。哨兵们觉得这很 可疑，他们将鸡蛋剥开，发现蛋白上布满了字迹，都是英军的详细布防图，还有各师旅的番号。原来，这种传递情报的方法是德国一位化学家提供的，其作法并不复 杂：用醋酸在蛋壳上写字，等醋酸干了后，再将鸡蛋煮熟，字迹便透过蛋壳印在蛋白上，外面却没有任何痕迹。

1914 年 8 月 5 日，英国“泰尔哥尼亚”号船上的潜水员割断了德国在北大西洋海下的电缆。他们 的目的很简单，就是想让德国的日子更难过，没想到这却使德方大量的通讯从电缆转向了无线电。结果，英方截取了大量原本无法得到的情报。情报一旦截获，就被 送往 40 号房间——英国海军部的密件分析部门。40 号房间可以说是现代密件分析组织的原型，这里聚集了数学家、语言学家、棋类大师等任何善于解谜的人。

1914 年 9 月，英国人收到了一份“珍贵”的礼物：同盟者俄国人在波罗的海截获了一艘德国 巡洋舰“玛格德伯格”号，得到一本德国海军的密码本。他们立即将密码本送至 40 号房间，允许英国破译德国海军的密件，并在战争期间围困德军战船。能够如此 直接、顺利且经常差不多是同时读取德国海军情报的情况，在以往的战事中几乎从未发生过。

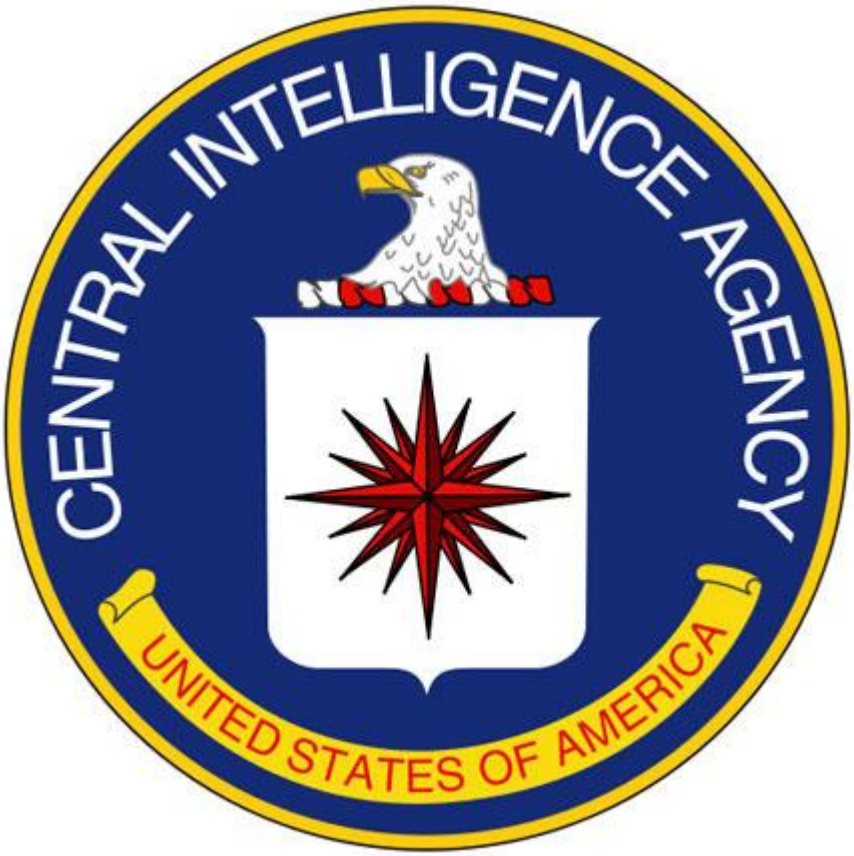
密码学历史上最伟大的密码破译事件开始于 1917 年 1 月 17 日。当时英军截获了一份以德国最高 外交密码 0075 加密的电报，这个令人无法想象的系统由一万个词和词组组成，与一千个数字码群对应。密电来自德国外交部长阿瑟·齐麦曼，传送给他的驻华盛 顿大使约翰·冯·贝伦朵尔夫，然后继续传给德国驻墨西哥大使亨尼希·冯·艾克哈尔特，电文将在那里解密，然后交给墨西哥总统瓦律斯提阿诺·加汉扎。

密件从柏林经美国海底电缆送到了华盛顿，英军在那里将其截获并意识到了它的重要性。但是， 同样接到密件的约翰·冯·贝伦朵尔夫却在他的华盛顿办公室里犯了个致命的错误：他们将电报用新的 0075 密件本译出，然后又用老的密件本加密后用电报传送 到墨西哥城。大使先生没有意识到，他已经犯下了一个密码使用者所能犯的最愚蠢的、最可悲的错误。

此时，已经破译了老密码的英方正对着这个未曾破译的新外交密码系统一筹莫展，不过没过多久，他们便从大使先生的糊涂操作中获得了新旧密码的比较版本。随着齐麦曼的密件逐渐清晰起来，其重要性令人吃惊。

尽管 1915 年美国的远洋客轮“露斯塔尼亚”号被德军击沉，但只要德国对其潜艇的行动加以 限制，美国仍将一直保持中立。齐麦曼的电文概括了德国要在 1917 年 2 月 1 日重新开始无限制海战以抑制英国的企图。为了让美国原地不动，齐麦曼建议墨西哥 入侵美国，重新宣布得克萨斯州、新墨西哥州和亚里桑纳州归其所有。德国还要墨西哥说服日本进攻美国，德国将提供军事和资金援助。

英国海军部急于将破译的情报通知美国而又不能让德国知道他们的密码已被破译。于是，英国的一个特工成功地渗入了墨西哥电报局，得到了送往墨西哥总统的解了密的文件拷贝。这样，秘密就可能是由墨西哥方泄露的，他们以此为掩护将情报透露给了美国。



美国愤怒了。每个人都被激怒了，原先只是东海岸的人在关心，现在，整个中西部都担心墨西哥的举动。电文破译后六个星期，美国对德国宣战。当总统伍德罗·威尔逊要求对德宣战时，站在他背后的，是一个团结起来的愤怒的国家，它时刻准备对德作战。

这可能是密码破译史上，当然也是情报史上最著名的事件。齐麦曼的电文使整个美国相信德国是国家的敌人。德国利用密码破译击败了俄军，反过来又因自己的密码被破译而加速走向了灭亡。

第一次世界大战前，重要的密码学进展很少出现在公开文献中。直到 1918 年，二十世纪最有影响 的密码分析文章之一¾¾William F. Friedman 的专题论文《重合指数及其在密码学中的应用》作为私立的“河岸（Riverbank）实验室”的一份研究报告问世了，其实，这篇著作涉及 的工作是在战时完成的。一战后，

完全处于秘密工作状态的美国陆军和海军的机要部门开始在密码学方面取得根本性的进展。但是公开的文献几乎没有。

然而技术却在飞速的发展，简单的明文字母替换法已经被频率分析法毫无难度地破解了，曾经认为是 完美的维吉耐尔(Vigenere)密码和它的变种也被英国人 Charles Babbage 破解了。顺便说一句，这个 Charles Babbage 可不是凡人，他设计了差分机 Difference Engine 和分析机 Analytical Engine，而这东西就是现在计算机的先驱。这个事实给了人们两个启示：第一，没有哪种“绝对安全”的密码是不会被攻破的，这只是个时间问题；第二，破 译密码看来只要够聪明就成。在二次大战中，密码更是扮演一个举足轻重的角色，许多人认为同盟国之所以能打赢这场战争完全归功於二次大战时所发明的破译密文 数位式计算机破解德日密码。

1918 年，加州奥克兰的 Edward H.Hebern 申请了第一个转轮机专利，这种装置在差不多 50 年里被指定为美军的主要密码设备，它依靠转轮不断改变明文和密文的字母映射关系。由于有了 转轮的存在，每转动一格就相当于给明文加密一次，并且每次的密钥不同，而密钥的数量就是全部字母的个数—26 个。

同年，密码学界的一件大事“终于”发生了：在德国人 Arthur Scherbius 天才的努力下，第一台非手工编码的密码机—ENIGMA 密码机横空出世了。密碼機是德軍在二戰期間最重要的通訊利器，也是密碼學發展 史上的一則傳奇。當時盟軍借重英國首都倫敦北方布萊奇利公園的「政府電碼與密碼學院」，全力破譯德軍之「謎」。雙方隔著英吉利海峽鬥智，寫下一頁精彩無比 的戰史，後來成為無數電影與影集的主要情節，「獵殺 U571」也是其中之一。

随着高速、大容量和自动化保密通信的要求，机械与电路相结合的转轮加密设备的出现，使古典密码体制也就退出了历史舞台。

第二阶段为从 1949 年到 1975 年。

1949 年仙农(Claude Shannon)《保密系统的通信理论》，为近代密码学建立了理论基础。从 1949 年到 1967 年，密码学文献近乎空白。许多年，密码学是军队独家专有的 领域。美国国家安全局以及前苏联、英国、法国、以色列及其它国家的安全机构已将大量的财力投入到加密自己的通信，同时又千方百计地去破译别人的通信的残酷游戏之中，面对这些政府，个人既无专门知识又无足够财力保护自己的秘密。

1967 年，David Kahn《破译者》(The CodeBreaker)的出现，对以往的密码学历史作了相当完整的记述。《破译者》的意义不仅在于涉及到相当广泛的领域，它使成千上万的人了解了密码 学。此后，密码学文章开始大量涌现。大约在同一时期，早期为空军研制敌我识别装置的 Horst Feistel 在位于纽约约克镇高地的 IBM Watson 实验室里花费了毕生精力致力于密码学的研究。在那里他开始着手美国数据加密标准（DES）的研究，到 70 年代初期，IBM 发表了 Feistel 和他的同事在这个课题方面的几篇技术报告。

第三阶段为从 1976 年至今。1976 年 diffie 和 hellman 发表的文章“密码学的新动向”一文导致了密码学上的一场革命。他们首先证明了在发送端和接受端无密钥传输的保密通讯是可能的，从而开创了公钥密码学的新纪元。

1978 年，R.L.Rivest，A.Shamir 和 L.Adleman 实现了 RSA 公钥密码体制。

1969 年，哥伦比亚大学的 Stephen Wiesner 首次提出“共轭编码”(Conjugate coding)的概念。1984 年，H. Bennett 和 G. Brassard 在次思想启发下，提出量

子理论 BB84 协议，从此量子密码理论宣告诞生。其安全性在于：1、可以发现窃听行为；2、可以抗击无限能力计算 行为。

1985 年，Miller 和 Koblitz 首次将有限域上的椭圆曲线用到了公钥密码系统中,其安全性是基于椭圆曲线上的离散对数问题。

1989 年 R.Mathews, D.Wheeler, L.M.Pecora 和 Carroll 等人首次把混沌理论使用到序列密码及保密通信理论，为序列密码研究开辟了新途径。

2000 年，欧盟启动了新欧洲数据加密、数字签名、数据完整性计划 NESSIE，究适应于 21 世纪信息安全发展全面需求的序列密码、分组密码、公开密钥密码、hash 函数以及随机噪声发生器等技术。