戏说“密码学”简史

杨义先 钮心忻

北京邮电大学信息安全中心

摘要与邀擂：霍金写了《时间简史》，布莱森写了《万物简史》，格雷克写了《信息简史》…。**这些简史真的好精彩哟！不但出神入化，而且还能改变读者的世界观！唉～，咱安全界，谁能出面也**写部“外行不觉深，内行不觉浅”的《安全简史》来“为百姓明心，为专家见性；为安全写简史，为学科开通论”呀！可惜，论“文”，咱比不过“旅游文学作家”布莱森和“科普畅销书作家”格雷克；论“武”，更不敢比世界顶级科学家霍金。可是，真的又需要有本《安全简史》！怎么办呢？老朽不才，想到了“众筹”和“迭代”，即，为了引出玉，先由我们抛出砖（α-测试版本的初稿），然后，由广大读者来进行全方位的修改、批评和版本更新，包括但不限于写作内容、素材、架构安排、等任何建议。希望“三个臭皮匠”真的能够“赛过诸葛亮”。当然，我们不可能全身心投入《安全简史》，因为，建立旨在统一安全各分支学科的基础理论，《安全通论》，才是我们的主业。但愿有朝一日，咱安全界既有《安全简史》来“立地”，又有《安全通论》来“顶天”。**本章是第五块“砖”，主题是密电码。**谢谢大家！

信息时代的关键是安全，安全的核心是密码学，密码学的“代言人”是一对金童玉女。可惜，这对金童玉女的名字，常被人们搞混淆！

金童的学名叫“密码”，主要是对信息进行加密和解密，可老百姓们更愿意称它为“密电码”，虽然，早在富兰克林玩风筝取“电”之前，金童就已诞生了。既然是科普，咱就得尊重大众意见吧，所以，本章名称，还是讨好读者，取名为“密电码”。据考证，“密电码”这个名字，之所以家喻户晓，完全是因为在“样版戏年代”，全国人民都已被《红灯记》中的“密电码”，打上了深深的烙印。当然，在本章主体内容中，我们仍然正本清源，叫它为“密码”。

玉女的学名叫“认证”，笔名之一也叫“口令”，主要包括信息认证、身份认证和行为认证等，或者说是对消息、行为和身份进行验明正身；可老百姓又调皮了，非要叫“口令”为“密码”。其实，玉女“认证”（后面章节内容）与金童“密码”可谓是天壤之别：一个是阆苑仙葩，一个是美玉无瑕。

一说起“密码”或“密电码”，人们马上想到的就是战争！确实，古今中外，人类历史上的每一场战争，无论大小或长短，几乎都与密码脱不了干系，甚至，可以说：战争的胜负，在很大程度上，直接取决于敌对双方“密码对抗”的胜负。因为，密码对抗的胜者，要么能把机密指令传给友军，以便同心协力，打败敌方；要么能够破译敌方“密电码”，从而掌握敌方的情况，始终把握主动权。这就像是明眼人打瞎子一样，密码失败者只有挨打的份，没有还手之力。

密码对战争走向的颠覆性影响，到底有多大呢？还是让实例说话吧。

在第二次世界大战中，日本这个军国主义的，穷兵黩武的，名符其实的“武大郎之国”，把亚太地区祸害惨了；同时，它自己也被密码给收拾惨了。

在日本的众多武大郎中，有一位其父56岁才生他的家伙，名叫五十六；后随母姓，改为“山本五十六”。他家的祖传基因就是冷血武士道，早在10岁时，“武老郎”就用武士刀，在儿子腿上狠划了12刀（幸好不是56刀），代表正式的“入道洗礼”。后来，这位武大郎果然如父所愿，成了凶残的战争机器。17岁上军校，20岁参加日俄战争。40岁时，竟然还从头学飞行，而且一飞成名，超过了大部分年轻的“武小郎们”。然后，他就武运亨通了：先是担任航空母舰舰长，接着晋升为少将，再调任航空舰队司令长官，然后提拔为中将，紧随着就登上了航空本部部长的宝座，最终，还成了海军大将。

在其被密码搞死的短命一生中，山本所获得的各种战争勋章简直不计其数，像什么大勋位菊花章呀，阿猫奖章呀，阿狗奖章呀，毒蜥奖章呀，蜈蚣奖章呀等等，估计这些破玩艺放一起，能别满整整一屁帘。要知道，每一枚奖章背后，都连着数不清的冤魂野鬼啊！特别是这王八蛋，在淞沪会战期间，曾派遣航母舰载机，疯狂轰炸了上海、杭州、广德等城市，欠我中华无数命债。

要不是用密码，还真难灭掉这位五毒俱全的杀人狂呢！在介绍他的密码沉浮人生之前，先看看山本到底有多变态。他在日本妓女界，可谓是如雷贯耳；当时，妓女在给客人染指甲时，是按每个指头一毛钱收费的，所以，一般嫖客都收一元。但是，由于山本只有八个指头，她们便撒娇地称他为“八毛”。这位“武大郎”，一生与无数“潘金莲”纠缠不清：所写情书多如牛毛，特别是给河合千代子等狐狸精的情书更是肉麻，还经常把内心的秘密及苦闷，毫无保留地端给她们；还有，为了另一位名叫正子的40岁老女人，这位日本联合舰队司令长官、海军大将，竟然像小丑那样模仿卓别林走路，来博取“徐娘”一笑。山本也是一个十足的冒险家，对赌博尤为着迷。嗜赌如命的他，不但与同僚赌，还与部属赌，甚至还与妓女们赌。据说，他出使欧洲时，由于赌技超群，赢钱太多，摩纳哥的赌场甚至都禁止他入场。其实，战争就是他的最大赌博！

算了，这家伙的龌龊事太多，简直罄竹难书，咱们还是回到密码正题吧。山本一生的成败，与其说是与战争密切相关，还不如说是与密码密切相关。

他的最大“功绩”就是策划并实施了“偷袭美军珍珠港”。其如意算盘是：“一开战就猛力击破敌军舰队，置美国海军及国民于无可挽救之地，使其士气沮丧……”；反正，其大意就是：先给美国佬来顿杀威棒，打它一个皮开肉裂，让其老老实实地俯首称臣，然后，再来收拾其它喽啰，并最终建立“大东亚共荣圈”。其实，本来这次偷袭是会失败的，因为，中国密码学家池步洲，破译了一份日本驻美大使的特级密电，得知大使先生被要求“立即烧毁一切机密文件；尽可能通知有关存款人，将存款转移到中立国家银行；帝国政府决定采取断然行动”等。据此，池步洲判断，这是“东风，雨”（即日美开战）的先兆。然后，结合“日本正在大量搜集美国檀香山海军基地”等密码破译结果，池步洲掐指一算，抛出两卦：1）开战时间在星期天；2）地点在檀香山珍珠港海军基地。可惜，当这么重要的破译

结果，通过“亚洲战区总司令”，报告给时任美国总统富兰克林·罗斯福时，由于当时美国的旁观情绪正浓，不想介入战争，所以，罗大总统竟然不信这两卦，甚至还一点也未防备！结果，血光之灾果然应验，美国珍珠港海军几乎全军覆没：8 艘战列舰中，4 艘被击沉，一艘搁浅，其余都受重创；6 艘巡洋舰和 3 艘驱逐舰被击伤，188 架飞机被击毁，数千官兵伤亡。欲知这次美国被炸得有多惨，建议你下载电影“虎，虎，虎”自己找答案。而日本却只损失了区区 29 架飞机和 55 名飞行员以及 2 艘潜艇，当然，也许还有几张“炊饼”。日本大胜，山本五十六从此更加飞黄腾达。

你看，由于日本密码的“胜利”（因为，罗总统不信嘛），山本也就胜利了。但是，幸好“武大郎”的密码噩运，马上就要来了！

借助偷袭珍珠港的余威，日本急于一鼓作气，再给美军来个雪上加霜；于是，便精心策划了中途岛战役。与刚受重创的山姆大叔相比，日军可谓计划周详，组织严密，时机掌握得当，而且还兵多将广，比如，其可投入决战的战舰，更是多达四艘舰队航母、二艘轻型航母、十一艘战列舰、十六艘巡洋舰和四十六艘驱逐舰等等。而美军却捉襟见肘，那怕翻箱倒柜，也只能拿得出可怜巴巴的三艘航母、八艘巡洋舰和十五艘驱逐舰；因为其它舰船，刚被日本沉入海底，养珍珠去了。日美双方兵力悬殊，看上去，山本几乎必胜无疑，美国佬你就等着投降吧。天皇升任地球“球长”，几成定局。

可是，结果却完全相反！日军大败，山本这位赌场高手，甚至连老本都赔光了：不得不放弃中途岛，并全军撤退。小日本的扩张也到此为止，美军开始转入战略反攻，星条旗终于飘起来了。为什么会如此意外呢？最根本的原因就是：美军对日本的作战计划了如指掌，因为，美国破译了日本海军的 D 号密码（美军称为 JN-25 密码），而日本却被完全蒙在鼓里！比如，美国太平洋舰队司令，通过密码破译，早就知道了山本设下的陷阱，于是，将美方仅有的部队，配置在最适合的位置，来伏击日军航母。相反，日本还得意洋洋，按既定计划对美佯攻，试图诱其上当；但是，美军航母早已成竹在胸，只是专心设伏，关门打狗。于是，就在战役开始当天，1942 年 6 月 4 日，美军抓住最佳时机，一举击沉了日本的全部四艘舰队航母，顺便也把“炊饼旗”送了王八。

密码破译给山本的苦头，还没完呢！

1943 年 4 月 14 日，又是那位中国密码学家，池步洲，截获并破译了一份日本密电，得知“武大郎”要出宫了：他将于 1943 年 4 月 18 日早上，从拉包尔起飞，前往所罗门群岛布干维尔岛附近的野战机场；甚至还知道他搭乘的飞机型号和护航阵容等。这次，当“亚洲战区总司令”将破译结果交给罗斯福时，这位美国老大终于相信了，而且马上下令：“干掉山本！”

于是，一个中队的闪电式战斗机，受命拦截一名“重要的高级军官”。精选的 18 位飞行员，经过 430 英里无线电静默超低空飞行，虽然只有 16 架飞机到达目标空域，但是，仍然在东京时间 9 点 43 分，与山本的 6 架零式护航战斗机短兵相接，并在三十秒之内，把舷号为 T1-323 的山本座机打成了筛子。电光火石之

间，日本海军部最高统帅，就这样去了阎王殿。事后，据日军搜救小队回忆，山本的尸体压在飞机残骸之外的一棵树下，仍然僵硬地坐在座椅上，白手套魔掌仍拄着日本军刀。解剖报告显示，山本共吃了两粒枪子儿：一粒自身后穿透左肩；另一粒从下颌左后方射入，从右眼上方穿出。当然，为防止日军得知自己的密码已被破译，美军愣是没有公开其大部分刺杀行动。

山本之死，对开战以来，自以为不可一世的小日本，可以说是沉重打击。日本朝野震惊，当局一再隐瞒，直到一个多月后的 1943 年 5 月 21 日，才公布了“阎王爷在阴间亲切接见了山本”的死讯。虽然，一百多万个“武大郎”，在东京给山本举行了所谓的国葬；“潘金莲”们也背着枕头，趴在榻榻米上，嚎叫着为他哭丧；“炊饼老板”更是追授他什么大勋位呀、功一级呀、天篷元帅呀等称号。但是，“纸船明烛照天烧”，生死簿上一旦被除名，无论你还多么想继续“恶贯”，也都只能“满盈”了。

密码不但将山本送上了黄泉路，而且，也把小日本赶进了十八层地狱。实事上，据战后评估，正是因为盟军在密码破译方面的绝对优势，使得法西斯们节节败退，终于，二战被提前至少两年结束！

当然，密码也绝不是战争的专利。后面我们将会看到，密码及其衍生品，在人类历史上，一直就扮演着不可替代的重要角色；甚至，日常生活的许多细节都已完全融入到密码之中，就像空气和阳光那样，以至于根本感觉不到它的存在了。比如，你身边的几乎所有 IT 及周边产品（电脑、手机、电视、饭卡、身份证、汽车、银行卡等）中，最核心的部分都是密码；你每天的网上活动（购物、支付、收发信件等）的安全保障，也离不开密码；而且，人类对密码的依赖程度，还将越来越高。

那么，密码到底是什么呢？所谓的加密和解密又是怎么实现的呢？

单单从名词解释角度来看，答案其实很清楚：加密嘛，就是把明白的东西（称为“明文”）变糊涂，当然是让非法人员糊涂，而合法人员仍然保持清晰；加密后的东西叫“密文”。解密嘛，也叫“破译”（仅对非法解密者而言），就是把糊涂的东西搞明白；或者说，把“密文”变成“明文”。对合法人员来说，解密易如反掌，因为，他事先已经知道了“解除魔法的咒语”；但是，对非法人员来说，解密却异常困难，所以，又称为“破译”，他要么得想法搞到咒语，要么另辟奇径，把魔法打回原形。而“密码”就是“加密”和“解密”两件事情的统称。比如，山本的故事中，日军将机要的军事命令，变换成乱七八糟的密文，一般人根本就读不懂；而当这些乱码被传到日军自己的相关部门后，由于他们事先已有一些称为“密钥”的约定，所以，便能很快恢复出原来的机要信息，这个过程就是“解密”。但是，“一般人根本就读不懂”并不意味着“所有人都读不懂”，而有时还真会碰巧出现几位能够读懂这些乱码的神人，比如，前面的池步洲；于是，这份密电码就被破译了。

但是，要想从技术上来具体说明“加密和解密到底是怎么实现的”，这可不是一件容易的事情！因为，历史事实表明，在加密和解密方面，根本就没有规矩可言；只有你想不到，没有密码学家们做不到！既然说不清楚，那怎么办呢？想来

起去，只好玩趟穿越，到遥远的古代去重新进化一次，随便请教几位最著名的密码专家，看看他们是如何加密、解密和使用密码的。

各位旅客请注意，穿越马上就要开始啦！

到古代了~，到中古了~，到远古了~，到伊甸园门外了。好了，现在可以睁眼了！

大家请看，那个门内就是伊甸园。据说，里面特舒服：学生不考试，老师不考核，工人不上班，农民不下田；而且，人人都土豪，喝酸奶都不舔盖，手机也不贴膜……，反正，想吃啥肉吃啥肉，想炖粉条炖粉条。什么？那位游客说，想进伊甸园去看看？！抱歉，咱没资格，因为，人类就是从那里被赶出来的。

谁赶的？请看，就是墙上画的这位。别看他长得和你我一样，其实，我们只不过是他的泥土仿制品。他就是有文字记载的第一位，也是最著名的一位密码学家，名字叫“上帝”！

上帝教授，也许已是院士了，真可谓著作等身，他最有影响的代表作就是《圣经》，密码只不过是其中一小节而已。那他为什么要发明密码呢？唉，说来话长呀！

当年，亚当和夏娃同学偷吃禁果后，人类就被赶出了伊甸园，并受到了滔天洪水的惩罚，几乎绝种。幸好诺亚造船厂厂长，诺亚先生，躲过一劫。俗话说“大难不死，必有后福”，果然，诺厂长又多活了 350 年。他的三个儿子繁衍了人类的三大支系，居住在世界各地。那时候人类的语言、口音都没有分别。后来，他们开始东迁，并在示拿平原汇合，于是，就在那里住下，发明了制砖，并建造了繁华的巴比伦城。这时，人类开始膨胀了，忘乎所以了，打算在巴比伦修一座通天高塔，一来传颂威名，二来方便集合天下兄弟，以免分散。因为大家语言相通，同心协力，所以，通天塔的修建相当顺利，很快就高耸入云了，严重干扰了上帝教授的工作和生活。

教授很仁慈，不想再用洪水来袭击人类，但又必须阻止人类的狂妄。于是，上帝就连夜连晚，设计了若干套名叫“语言”的密码，并亲自离开天国来到人间，让不同的族人讲不同的语言。终于，人们各自操起不同的语言，感情无法交流，思想很难统一。互相猜疑就出现了，开始各执己见了，甚至争吵斗殴了，当然，通天塔工程，也终于因语言纷争而停止了。人类分裂了，按照不同的语言，形成许多部族，又散落到世界各地去了

旅客同志们，你们也许不全信《圣经》，甚至可能怀疑上帝的知识产权，不过，这丝毫不影响一个铁的事实：语言确实是一种密码！因为，甚至 N 年后，当日历翻到 1942 至 1945 年的太平洋战争时，人类都还在使用语言密码。

具体地说，美国真的征召了 420 名印第安纳瓦霍族人，让他们用自己的土著语言来传递密码。由于纳瓦霍语没有文字，语法和发音又极其复杂，所以，日军一直无法破译，并称这种密码为“不可破译的密码”。又过了约半个世纪，2001

年 7 月 16 日，时任美国总统布什先生，还隆重地向 4 名仅存健在的、白发苍苍的土著密码员颁发了“国会金质奖章”呢！

如果非要找出语言这种密码，与其它密码有什么区别的话；那么，只不过这时加密者和合法的解密者，不再是少数人，而是一族人，甚至是一国人而已。

好了，请大家与上帝说再见，咱们继续拜访第二位密码专家。

如果说上帝是加密专家的话，那么，这第二位就是解密专家。他的名字叫莱桑德，与上帝相比，这个名字几乎可以忽略不计；但是，他所破解的密码却是人类历史上最重要的两种密码之一，称为“滚筒密码”。

注意，此时咱们已进入公元前 405 年了。确实跑得快了点，但是，时间紧呀，咱还得赶路呀，不然就来不及了！

话说，雅典和斯巴达之间的战争已进尾声，虽然双方都精疲力竭了，但是，斯巴达好像逐渐占了上风。就在擂主斯巴达准备给挑战者雅典，最后一记连环拳，要结束其性命时，突然，裁判员波斯帝国翻脸了。要知道，本来斯巴达已经买通裁判为盟友的，现在关键时刻，他却不帮斯巴达吹黑哨了。莫非裁判想让雅典和斯巴达两败俱伤，以便从中渔利？但是，仅仅猜想而已，没有证据呀！怎么才能摸清波斯帝国的底牌呢？

幸运的密码之神降临了！斯巴达军队碰巧捕获了一名信使，他正从波斯帝国回雅典送密码信件呢。仔细搜查俘虏后，发现了“一条布满杂乱无章的希腊字母的普通腰带”。情报肯定就藏在腰带上，躲在这些杂乱的字母之中；但是，谁能读懂这些乱码呢？严刑拷问信使，也一无所获，因为，他真的什么也不知道，只知道系了一条别致的腰带而已。

怎么办呀，怎么办？！正当大家抓耳挠腮，无计可施时，咱们的第二位密码专家出现了！他就是斯巴达军队的统帅，莱桑德讲师（肯定不能是教授，否则就是对上帝的不尊）。只见他面对这些天书似的文字，反复琢磨、研究，用各种方法进行重新排列组合，看看能否排出有含义的文字来。时间一分一秒地过去了，太阳升起来又落下去了；胡子长了，头发乱了，能用的办法都想尽了，可还是解不出秘密来。

最后，莱桑德几乎失望了，他一边摆弄着那条腰带，一边思考着其他可能的破解途径。无意中，他把腰带，呈螺旋形无缝缠绕在手中的剑鞘上；这时，奇迹出现了：腰带上那些杂乱无章的字母，竟然组成了一段文字！原来是一份惊天情报：波斯准备在斯巴达消灭雅典的那一瞬间，突袭斯巴达。于是，斯巴达转手就是一拳，向波斯发动了闪电战，一举将裁判打倒在地，解除了后顾之忧。随后，斯巴达顺便收拾了雅典，终于再一次捍卫了自己的擂主地位，取得了最后胜利。

腰带上的这种密码，为什么要叫“滚筒密码”呢？其实，它是世界上有文字记载的最早的密码，采用的加密解密规则是：加密方，先将腰带（或羊皮纸带）呈螺旋形地、无缝地缠绕在约定直径的圆筒上，然后，将情报按正常顺序直接书写在圆筒上，再取下腰带就行了。而合法的解密方在收到腰带后，他只需要仍然将

它呈螺旋形地、无缝地缠绕在约定直径的圆筒上，便可直接读出情报原文。但是，对破译方来说，由于他不知圆筒的直径，所以，就总也读不懂密文，除非像莱桑德讲师那样，刚好“瞎猫碰到死耗子”。

旅客朋友们，现在咱们又穿越了400年，可以考察第三位密码专家了。

他既不是加密专家，也不是解密专家，但是，却是千真万确的密码使用专家，估计已达到副教授水平。他使用密码的本领，已经炉火纯青了。他的一生，既是战斗的一生，也是使用密码的一生。作为著名的军事家、政治家和罗马帝国的奠基者，他不但在战争中经常使用密码，而且，还在给朋友写信的时候，也要使用密码；好像离开了密码就不会写字似的。由于他擅长使用某种密码，以至于现在这类密码就干脆以他的名字命名了。而且，该密码还不是一般的密码，它与前面的那个“滚筒密码”一起，构成了所有算法密码的两个重要基石。换句话说，到目前为止，包括最先进的现代密码在内的一切算法密码，其实都可以最终分解为这两类“基石密码”的某种融合。至于到底如何融合，咱这篇科普就够不着了。

由于这第三位密码专家的名字太牛，直接说出来怕吓着你，所以，我先介绍一下他的简历，就算是打个预防针吧。他，公元前58年，被任命为高卢总督。仰仗高超的密码使用技巧，刚上任的他，就发动了高卢战争；并经过9年的血雨腥风，夺取了整个高卢地区，并将比利牛斯山、阿尔卑斯山、塞文山、莱茵河和罗纳河等围成的，周长超过3000英里的地区变成了高卢省，并强征了大量的税赋。接着，他跨过莱茵河，征讨西班牙、希腊，并在公元前48年，彻底击败其女婿，将他追杀到埃及。他还干涉埃及内政，不但与艳后“插了一腿”，而且还反客为主，宣布由他的情人和正宗的托勒密十三世，一起共享埃及王位；后来，干脆杀了正宗王，让艳后独占王位。再后来，他又找了个借口，征讨潘特斯王国，说别人“破坏罗马协约”。公元前46年，他又杀到北非，把女婿的余党赶尽杀绝。之后，回到罗马，举行了长达十天的凯旋仪式，然后，开始改革：将“罗马公民权”赐给了北意大利和西西里岛人民，制作了新的历法（儒略历），建立了和平广场等。公元前45年，他再次远征西班牙，干掉了两个外孙；最后，于公元前44年回国，宣布自己成为终生独裁官。

伙计，通过这个简历，也许你已隐约猜到他是谁了。但是，我敢打赌，你绝对不知道他的全名，因为，这位副教授有好几个全名，而且读起来都像密码：盖厄斯·儒略·凯撒、葛约斯·尤利乌斯·凯撒、盖乌斯·尤利乌斯·凯撒、朱利叶斯·凯撒！

算了，别兜圈子玩密码了！干脆用他名字中最后两个字来称呼他吧，那就是：凯撒！对，就是那位，史称“凯撒大帝”的凯撒。以他名字命名的密码，就叫“凯撒密码”。

凯撒密码虽不是凯撒设计的，但是，根据《高卢战记》的描述，确实是由他将该密码的作用，发挥到了极致；并因此使其军事生涯从一个辉煌，走向另一个更大的辉煌。

对凯撒密码原理感兴趣的读者，可顺序阅读此段；只想看热闹的朋友，建议直接跳入下一段。凯撒密码的加解密其实很简单：通过把字母移动一定的位数来实现加密和解密，即，明文中的所有字母都在字母表上向后（或向前），按照一个固定数目进行偏移后，被替换成密文。这里的“位数”，就是凯撒密码加密和解密的密钥。例如，当偏移量是 3 的时候，所有的字母 A 将被替换成 D，B 变成 E；以此类推，X 将变成 A，Y 变成 B，Z 变成 C。于是，明文句子“A boy”便被加密为“D erb”，这对破译者来说显然是天书，而对合法的解密者来说，他只需要将每个字母换成标准字母表中其前面第 3 个字母就行了（比如，d 变回成 a，e 变回成 b，r 变回成 o，b 变回成 y；于是“D erb”就变回成了“A boy”，解密完成）。

伙计，别告诉我说凯撒密码太简单，你都能破译。的确，我信你的话，但是，如果把你送回到两千多年前，你还能吹此大牛吗？冒冒失失地去揭榜，小心掉脑袋哟，况且凯撒在真正使用时，还添了油，加了醋呢，比如，把 A 国文字换成 B 国字母等！

各位旅友，到此我们已考察过三位顶级密码专家了。但是，由于时间太紧，后面我们只能将单独考察，换为群体考察；而且，穿越的年代也将更长。干脆，我们下一步，直接穿越 2000 年，跨入到电子时代吧……。

乘客朋友们，电子时代到了，大家可以下车了。请看，这是电报，那是电话，旁边是无线通信设备！注意啦，现在传送密电码，已经不用快马，而是改用远程电波传递了；破译者也不用逮俘虏，而是直接从空中截获密文信号了；当然，“抓舌头”还是有必要的，万一他知道某些密码细节呢。

这一阶段的加密和解密工作，都主要依靠机械方式来完成。所以，像什么高大上的“群环域”呀、数论呀等复杂运算，根本就无法进行，只能弃之不用。设计加密算法的手段也相当有限，仅能采用一些“用转盘和齿轮等就能实现的简单替换和置换”。

特别提醒一下：现在人类正进行第二次世界大战，所以，请旅客们注意安全。不要打扰各方密码专家，静静旁观，看看他们是如何斗智斗勇就行了。

首先，请大家往这边看，这台机器就是“恩尼格码密码”机，它是纳粹德国的主战密码；于 1918 年，由德国发明家发明。它是人类第一款自动编码机，首次利用电气技术，来取代手工编码加密。

该密码的破译过程，也算惊心动魄。话说，1928 年，波兰情报部门，从海关扣押了一个邮包，一个寄往德国驻波兰使馆的邮包，并从中偶然发现了一台“恩尼格玛商用机”，这算是天上掉馅饼吧。接着，1931 年，出了一个德奸（德国国防部密码局的提罗·施密特同学），他将恩尼格玛密码机的详细情报，泄露给了法国情报人员，这算是送货上门吧。法国当然将这些资料，转给了波兰盟友。但是，即使有了这些情报和样机，要想破译恩尼格玛也还早着呢，因为，如果采用常规的穷举法，盟军就还得测试数以亿亿计的组合，这在当时，显然是不可能的。终于，名字最后都带一个“基”字的，三位“基字辈”天才数学家登场了。他们是亨里克·佐加尔斯基、杰尔兹·罗佐基和马里安·雷杰夫斯基。这三位可了不得呀，是

波兰密码界的“三杰”。只见他们站如松，座如钟；眼观鼻，鼻观心；气沉丹田，双手合十；嘴里叽里呱啦，念念有词；接着，突然一睁眼，大吼一声：开！只听得晴天霹雳，恰似原子弹爆炸；然后，你再看那恩尼格玛密码，早已被打回了原形，德军密码就这样神奇般地破译了！

德军不服，于1938年12月，又对该密码进行了改进，使得原来波兰的“原子弹破译法”完全失效。于是，英国只好在伦敦远郊的布莱切利庄园，开设了一期“太极神功班”，集中招募了多位顶级数学家和语言学家，让他们全职进行密码破译，这便引出了图灵大战恩尼格玛密码的传奇故事。

对，就是图灵；伙计，你没听错！他就是你所熟悉的那位“计算机之父”和“人工智能之父”：艾伦·图灵。现在“计算机界的诺贝尔奖”，就是以他的名字命名为“图灵奖”。这位神人，不但是著名的数学家，而且还是逻辑学家。由于我们将专门有一章为他立传，所以，这里就不多说了。只是想指出：正是因为图灵“发现了一种不依赖重复密钥的破解方法”---这绝对是太极高手的“四两拨千斤法”---才最终将恩尼格玛家族，永远、彻底赶出了密码领域！

看过纳粹密码后，请大家往那边看：那台像“王八盖”样的密码机，叫“九七式密码”，它是日本的主战密码。其名字听起来很怪，“武大郎”家的事都怪，主要源于它的诞生日期：“炊饼纪元”二五九七年。盟军称它为“紫密”。

它与纳粹的“恩尼格玛密码”大不相同，更加先进：它不用机械转盘，而是使用电话交换开关，所以更难破译。

1938年山姆大叔发誓，那怕是长征，也要攻破紫密。经过20个月的围追堵截，终于在1940年秋，迈出了长征的第一步，即，仿制出了一台“九七式”密码打字机，这也算是建起了“长征宣传队”吧。1941年初春，美军特工设圈套迈出了第二步：他们以检查毒品为名，在旧金山，强行拦截了一艘开往德国的日本油船，并从船长室的保险柜中，抢走了一套日本《船舶密码本》。于是，美国便获得日本的密码本，这也算是发布了“长征宣言书”吧。由于日本商船是海上兵力的重要组成部分，因此，《船舶密码本》当然也是日本海军的密码核心。最后，又是两位天才的密码学家，威廉·弗里德曼和弗兰克·罗莱特，依靠其绝世神功，完成了“长征播种机”，最终将“紫密”全面破译，完成了长征的“宣传队、宣言书和播种机”！于是，美军就像长了一双透视眼，把日军的五脏六腑看得清清楚楚。果然，小日本腹中好恶心：心已黑，肝如墨，肺全烂，屎乱蹿；那肠子，细得如麻线；那胆之大，都快撑破了；胃也奇大无比，好像要生吞全世界。只可惜，“武大郎”心比南天高，命比黄连苦。

好了，请大家赶紧上车，继续密码考察。现在是咱们的最后一站：计算机时代！

计算机，又称电脑，可不得了啦，啥事都能干。更有好事者，将电脑连成了一张网，称为互联网。于是，通信方便了，加密方便了，解密也方便了，普通老百姓也开始频繁使用密码了。由于这时加密和解密算法都必须公开，唯一保密的

只是“密钥”而已，所以，对加密算法的设计要求就相当高，挑战也极其严厉。怎么应对这些挑战呢？老办法，一个字：打！两个字：摆擂！三个字：淘汰赛！

于是，1976 年，山姆大叔搭起了高高的擂台，“DES”三个血盆大字格外醒目。

规则很简单，无论是教授，还是老板，还是官员，甚至叫花子，只要你愿意都可以拿着你设计的密码算法，前来叫阵；无论是大公司，还是小企业，还是科学院，甚至智障高校，都可以对公布的密码进行破译，而且还不算违法；无论你是亚洲，还是美洲，还是非洲，甚至南极洲，都可以既攻击别人的密码，又公布并捍卫自己的密码。

一时间，全世界密码界沸腾啦，大家奔走相告！江湖上，更是人人跃跃欲试，个个摩拳擦掌。少林派来了，武当派到了；峨眉派早已按捺不住，跳上擂台与南拳派干上了。天罗拳、地煞拳、哪吒拳，拳拳飞舞；金刚锤、观音锤、罗汉锤，锤锤致命；夜叉掌、铁沙掌、空门掌，掌掌生风；莫家腿、薛家腿、岳家腿，腿腿不让。但见，天昏地暗，日月倒转；喊声杀声哭笑声，掀起阵阵惊雷。刚躲过连环鸳鸯步，又迎面闪现鹿步梅花桩；你来一招孔明拜灯，他回敬一式达摩点穴。燕青十八翻开路，七十二插手断后；盖手六合拳攻左，九宫擒跌脚击右……。

最后，经过历时三年多的入围赛、初赛和决赛，终于，只独独剩下蓝色巨人，IBM 公司，趴地上喘粗气了。它竟然用名不见经传的“揉面功”，也就是你我做馒头“和面”的功夫，打败了所有对手。这时，裁判入场，宣布：首个面向全社会公开的数据加密标准算法（DES）诞生啦！

当然，约三十年后，美国佬又故伎重演，同样用这种擂台法，淘汰了第一代拳王（DES）；选出了第二代拳王（AES），这回笑到最后的，是比利时的两位密码学家：Joan Daemen 和 Vincent Rijmen。

无论是第一代拳王（DES）还是第二代拳王（AES），它们都有一个共同的学名，叫“对称密码”。形象地说，此时加密者将机要信息锁进了一个“结实的箱子”，而开锁的钥匙只有两个，一个留给加密者，另一个通过安全方式，事先发给合法的解密者。如果破译者没能截获这个“箱子”，那自然就不存在被破译的问题；当破译者获得这个“箱子”后，他要么想办法配出一个钥匙来开锁，要么，干脆直接砸坏“箱子”取出秘密。当合法解密者收到箱子后，他只需要用事先获得的钥匙，打开此箱子就行了。至于破译者们如何配钥匙、偷钥匙、抢钥匙、骗钥匙，以及如何砸箱子，在许多电影和电视中都已经演绎得出神入化了，比如，大家所熟悉的《红灯记》，其主要情节就是加密者如何“事先将钥匙传递给合法的解密者”。

如果你还没明白“对称密码”是怎么回事的话，那么，请假想一下这样的场景：把你和破译者扔进某个巨大的迷宫中，这时你与破译者的地位是相同的，即“对称的”；但事先却悄悄告诉了你“迷宫地图”，这相当于你知道了“打开箱子的密钥”；而破译者却什么都不知道。于是，比赛开始后，你很快就能走出迷宫；而破译者则只能像无头苍蝇那样，永远陷在迷宫的密码中，扮演一只“热锅上的蚂蚁”。那

么，实际中是如何来设置这种“迷宫”的呢？办法其实很原始，那就是前面已经描述过的方法：打擂！

如果说 DES 和 AES 是官方擂台拳王的话，那么，接下来，就请大家看看民间擂台的拳王：RSA。它的发明者是三位教授，至于打擂的过程，咱们就别浪费时间了，还是直奔加密主题吧。

在计算机时代，无论是加密还是解密，都离不开计算机的看家本领：快！那么，如何才能使加密者，在这场“以快治快”的竞争中，略占优势呢？唯一的思路就是“用足加密者的主动性优势”，毕竟是先加密，后解密嘛。为解释清楚 RSA 的做法，我们先介绍一点数学中的，称为“单向函数”的，奇怪东西：

伙计，你会乘法和除法吧！你肯定知道乘法比除法容易，比如，给你两个比“天文级”还大的大素数 p 和 q，那么，你便可以轻松求出它们的乘积 n=p.q；但是，如果你把这个已经乘好的数 n 交给全世界最伟大的数学家，并让他求出原来的 p 和 q，那么，非常不好意思的是，他只能交白卷！你也许以为，多给他们一点时间就可以了，但是，数学家们早在三百多年前就进考场了，至今仍在那里发呆呢！如果以为数学家不够聪明的话，那你进去试试，肯定更尴尬。

其实数学和日常生活中，像这样“从起点到终点”非常容易，但是“从终点返回起点”却非常困难的问题还有很多；加密者们正是充分利用了这种“不对称性”，来把简单的事情留给自己，并以此来加密；而把困难的事情推给敌人，让他去破译。比如，自己加密，就只需要做“乘法”就行了；而破译者解密，则必须翻过“除法”这座大山。于是，虽然加密者和破译者都有极大的计算资源，甚至破译者的计算能力更强些，但是，由于他们所需的计算量完全不在一个档次，加密者几秒钟就能完成的加密运算，破译者为进行其逆运算，则需要几千年甚至几亿年。这就有点像两只青蛙玩游戏，一只在井底，另一只在井台，双方约定：谁先到达对方的地点，谁就获胜。但是，由于加密青蛙占主动，它肯定先选井台，破译青蛙就只剩井底了。于是，口哨一响，加密青蛙只需轻轻一跳，就锁定了胜局；如果井底足够深，井壁足够陡的话，那么，井底的破译青蛙可能永远也上不了井台！

细心的你也许会问，那么，合法的解密者怎么办呢，他们不会也花费成百上千年才能读懂加密信息吧？嘿嘿~，问得好，当然不需要！因为，他们已经事先知道了一些“破译者不知道的关键”。比如，仍然是从前面那个“从 n=p.q 中，求出 p”的问题。对破译者来说，他不会强过那些，至今还关在考场中的，数学家们；而对合法解密者来说，因为，它事先已经知道了 q，于是，从 n 中求 p 就是小菜一碟了！又比如说，那只加密青蛙，因为它事先已经知道了井底中的某个暗道，所以，即使是它跳入井底后，也能够通过暗道，轻松重上井台，虽然花费的时间会长过跳水时间，但是，这已经足够满意了。当然，要设置这种“暗道”，是相当困难的；技巧很多，水也很深；如果你非要自虐一把的话，那么，请在网上搜索“公钥密码”或“非对称密码”等关键词吧。

好了，各位旅客朋友，穿越结束了。如果大家还没考察够的话，且听本导游再多啰嗦几句：

其实，从古至今，人类在任何时期的所有重要发现，都会首先被或多或少地应用到加密和解密当中。比如，量子纠缠才刚刚发芽，人们就已经迫不及待地要用它设计出“牢不可破的量子密码”之盾了；量子计算还没实现，人们却已在磨刀霍霍，要用量子计算机这支矛，去戳穿所有现行的密码之盾了！又比如，人类发明电子计算机的直接动因，其实就是密码破译，希望借助其神奇的快速计算能力，来破尽天下密码，永远称霸密码擂台，因为，唯快不破嘛；而事实却是，电脑一诞生，加密专家们便迅速跳上新擂台，手持刚刚设计出的另类密码（也就是前面刚刚说过的“公钥密码”等）之盾，就完全挡住了任何计算机的强攻！在密码江湖上，类似的恩怨情仇数不胜数，反正加密专家和解密专家们，永远都在路上：今天你刚炼就屠龙刀，明天他就掌握了金钟罩；这边刚学会遁地法，那边的火眼金睛却早又明察秋毫了……。

既然是科普，本章就没有必要详细介绍加密专家和解密专家们的“武林秘笈”了。其实，即使是密码专家，往往也只有几招杀手锏，也不可能掌握所有的加解密技术，因为，这些技术几乎遍布了计算机、电子工程、信息与通信等各个学科，涉及到数学、物理等绝大部分基础科学，而且还都是尖端部分。总之，既不可能，也无必要在这里晒出加密和解密的全部具体内容。

一个秘密（无论它是无形的信息，还是有形的实物）怎么才能让友人知悉，而同时又对敌人保密呢？！从逻辑上看，无非两招：其一，让敌人不知道“秘密”的存在，这不是本章所要研究的场景，因为它不算密码，后面“信息隐藏”一章将对它进行详述；其二，即使敌人知道“秘密就在这里”，但是，他却得不到它，只能“望密兴叹”！

又怎么让敌人明明知道“秘密就在这里”，却眼巴巴地得不到呢？相应的办法，也只有两类：其一，让敌人近不了身，比如，在古代，镖局押镖时，情况就是这样：劫匪明知宝贝就在车上，可是，却无能为力，除非先取镖师性命；就在几年前，光纤保密通信也是这样，因为那时人们还无法对光纤进行搭线窃听，所以，黑客只能眼看着秘密信息在光纤中飞速传播，却根本近不了身，当然，现在光纤保密的神话已被打破了；据说，今后量子专家也仍然会这样，他们会充分利用“测不准原理”，把窃听者挡在门外干着急。不过，密码学要真正研究的内容绝不是“让解密者近不了身”，而是，其二，敌人虽然能够获取加密信息，但是，却无法读懂它！

那么，又怎么才能让敌人无法读懂“就在手边的加密信息”呢？这可就是一个与时俱进的问题了，而且，从哲学本质上说，这根本就是一个悖论！因为，既然任何加密都需要友人能（轻松）读懂，那么，也就可能会被敌人偶然读懂，毕竟友人和敌人是不可能被彻底分割清楚的。事实也是如此，在人类历史上，从来就没有哪个实用的密码是绝对安全的，虽然密码破译确实非常困难。

抱歉，都快要分别了，还给大家说这么多专业的东西，好像故意卖弄水平一样。作为补偿，最后再让大家轻松一下，看看上帝创造人类之前的密码场景。

当人类还是猴子的时候，其实就在使用密码了。如果再说远一点，自打动物出现以后，就有密码了，而且这些密码一直沿用至今。不但动物有密码，而且，不同的动物还使用了不同的密码呢！比如，猫和狗为啥很难成朋友呢？因为，它们使用了不同的密码，解密后经常会出现歧义：

狗狗“摇尾巴”的密文，正确解密后，应该是：主人好，你吃了吗！

而同样是“摇尾巴”的这个密文，由猫咪来解密时，结果却是：别动，老子开枪了！

于是，当狗狗好心好意摇着尾巴去讨好猫咪时，换来的却是一顿爆打。唉~，译错密码害死人啊！

如果再往前推，即使是动物还没进化出来的时候，也已有密码了！这个密码，就隐藏在植物基因中。君不见，现在全世界的生物学家们，都在忙忙叨叨地破译这些密码吗！当然，动物中也有这些基因密码。

那么，生物出现前有密码吗？还是有密码！其实，宇宙大爆炸就已经完成了这个密码的加密。如今，物理学家、天文学家等，不是都在努力破译这个密码吗！前段时间人类还因为“发现了宇宙大爆炸时，留下的背景辐射”而狂欢了好一阵子呢！

如果你还要追着问：宇宙诞生前，有密码吗？！嘿嘿，伙计，别再执着了。告诉你吧：仍然有密码！因为，“宇宙诞生前到底是什么情形”这个问题本身，就是人类想要破译的最终密码。

好了，伙计，别再一根筋了。咱们还是按惯例，用宋朝诗人苏东坡的《江城子.密州出猎》，从加密和解密两个方面，来归纳并结束本章吧。

老夫聊发少年狂。

巧加密，赛铜墙。

秘钥不知，穷举也白忙。

倾巢进攻一夫守，轻戏虎，笑看狼。

酒酣胸胆尚开张。

妙破密，又何妨。

持矛云中，铜墙变朽框。

手挽雕弓如满月，西北望，盾难挡。