

战争史上有哪些不起眼的小发明改变了战争形态？

图灵和他发明设计的炸弹机。他的发明不是用来打仗的，而是用来破译密码的。

图灵这个人一生当中曾经改变人类文明的走向。

有些历史学家就做出论断，说图灵以其一人之力，至少让第二次世界大战提前两年结束，他至少救了上千万人的命。

图灵作为第二次世界大战期间，英国人的首席密码破译专家所做出的贡献。当然他的这段经历直到今天仍然扑朔迷离，因为英国人觉得这是绝密，直到今天大量的档案文件仍然没有解密，历史学家只能透过当时一些信息的一鳞片爪，去判断图灵到底干了些什么。

有些历史学家就做出论断，说图灵以其一人之力，至少让第二次世界大战提前两年结束，他至少救了上千万人的命。当然这种文科教授做出来的计算结果信不信您自己看着办，但是我读完了《图灵传》之后，至少觉得图灵的功劳是怎么评价都不过分的。

那密码学到底是干吗用的？当然就是破译情报了。两国对战，在现代化的战争条件下，我干什么你完全不知道，而你干什么我就像看着澡盆里的鱼一样清楚，那这个仗还怎么打？希特勒输得一点也不冤。当然不是说第二次世界大战只有图灵这一个原因，但他确实是非常重要的一个因素。

在西方的文明当中，密码是一个非常简单的东西，就是把字母顺序打乱。比如说最早发明密码的恺撒，他发明的就叫恺撒密码，如果我跟前线的将领要传达信息，那我们约定另外一套字母系统。比如说 A 在我写的里面，它就变成了 K，J 就变成了 Z，我们俩互相约定好，那我就用约定的那一套密码，用正常的字母来书写，那敌人拿到肯定就看不懂了。

可是这种密码有一个问题，就是它架不住大数据，因为大家知道，任何语言一个字母，在一个单词当中，它出现的频率是可以统计出来的。只要资料足够多，马上就可以知道你是用哪个字母代替了哪个字母，稍微做一点功课，这种密码就能被破译。

但是到第二次世界大战之前，德国人发明了一套密码系统，这真叫成也萧何，败也萧何。这套密码系统是落实在一架机器上的，就是所谓的恩格码机，「恩格码」这个词是音译，原文就是「谜」的意思，又称之为谜机。因为德国人当年造的这种密码机特别多，现在市场上还有人专门收藏。

这个机器有什么好处？大家知道，直到今天我们人类都面对一种两难，就是如果你要更多的安全，对不起，你就必须承担和面对更多的麻烦。就像我们现在电脑系统里、网络上，越是追求安全，设置的密码就要越长，那你用起来肯定就不方便。但

是恩格码机或者说谜机，恰恰解决了这个问题，它是又安全，同时又方便，德国人多聪明。

那恩格码机的具体原理是什么？因为太复杂，我只能简单给大家介绍。它同样是用恺撒密码的原理，但是一个字母输进去，它通过一些转盘的转化，每一个字母最后输出出来的结果，会有150万亿种可能，德国人就通过一个机器把它做到这么牛。

150万亿是什么概念？就是15后面写18个0。你可以慢慢地试，你可以试着去破译，但是可能一个很大的团队要干几千年，你才能将它破译，它非常安全。

与此同时，它还特别方便，因为那个谜机的形象，有点像打字机，只要你把这封密码文件按照打字机上的键盘输进去，按一个字母，它的屏幕上就有另外一个字母灯亮。只要一个密码抄写员把那个亮的字母给抄下来，就能够还原成平时我们要传达的那个正常的信息。这个操作真的是用一分钟就可以教得会的操作。

德国人在发明这套系统之后觉得特别自信，谜机或者说恩格码机在第二次世界大战中，是德国人普遍运用的一种密码机器。那个时代的密码破译，就是数学家对决的战场，像图灵这样的人就有了用武之地。当然我们顺便说一下，第二次世界大战之后，人类的密码系统其实有一个小小的转向。

比如说这本书的序言是马慧元老师写的，她就讲到，她上大学的时候老师就跟她讲，说现在的密码不能再靠小轨迹了，就是数学轨迹，也就是我的算法你不知道。那万一对方知道了，你

这套密码系统不就变得极其脆弱吗？二战之后，人类倾向于用一种什么密码系统？就是膀大腰圆、傻大黑粗。

说白了，我即使把密码告诉你，把破解程序也告诉你，你找来世界上最快的计算机算。你算完了，结果可能是一年后，因为运算量实在太大，而一年后我这套密码已经过期了，这才是最安全的密码。当然现在我看到有人说，随着量子计算机的计算速度进一步提升，这种密码可能也不保险了。那是以后的话了。

总而言之，我们回到二战的时候。德国人觉得自信心爆棚，这套恩格码机是没有人能破解的。当然也有人距离成功只差一步之遥，这就是波兰人。

波兰人为什么要破译密码？因为这个民族在历史上三次被瓜分，到第二次世界大战之前，他们心知肚明，这边一个德国，那边一个苏联，肯定是要对我下手。什么时候下手，怎么下手，打又打不过，天天就琢磨这双方都在嘀咕点什么，天天就用电台去截获对方的电报，然后试图破译。

波兰还真就搞出了一批密码学家，然后距离破译谜机已经很近了，但是没有最终成功，因为德国人也不断地在换。1939年9月1号，德国人冲过了波兰和德国的边境，发动了第二次世界大战。在8月的时候，波兰人已经把这套系统交给了英国人，英国人对波兰人竖大拇指，说他们就好像一个骑士在倒下之前，把手里的剑交给了战友。

于是这个球就到了英国人的脚下，你大英帝国不是人才济济吗？你行你上，你能不能破译这套密码？英国人刚开始也是一

头雾水，完全找不着北。但是英国人有一个长项，就是在二战期间，体现出一种非常难得的坚持和隐忍，愿意吃苦，投入精力。

他们在伦敦以北 100 公里的布莱切利公园，设立了一个破译大本营，最多的时候在那儿投入了上万人，坚决要破掉希特勒的密码。每天大量截获德国人的电报，这些电报都是用密码写成的天书，什么时候能将这些电报破译出来？哪怕只是一张纸。没有人知道，大家都在外面等。

这里面当然就包括图灵，图灵脑袋里想什么，当时很多人其实是不知道的，连图灵在那儿干什么，很多守卫也不知道，因为他整天破衣褴褛，一副邋遢的样子，很多人觉得这家伙是间谍吧？在布莱切利公园里经常有人拦住他盘问。其实很少有人知道他们到底在干什么，只知道他们是在做一件很重要的事情。因为数学家脑子里想的东西，直到今天我们都不能用很方便的语言把它说出来，更何况当时的人？

那现在回头看，其实我们已经搞不清楚，哪些是波兰人奠定的基础，哪些是图灵自己搞的创新。但是我们可以清晰地看到两点，就是图灵坚信两种力量。

第一种，就是坚信机器对机器，因为恩格码谜机是一种机器，如果我用人力来对抗你，那就天然落了下风。图灵坚持要制造一个机器，这个机器现在就称为炸弹机，这是《图灵传》这本书的翻译；我还看到另外一种翻译法，叫小甜点。

我们在电影《模仿游戏》里看到过那个机器，就是一面墙那么大，上面全是小圆块，那就是炸弹机。后来英国人就是靠这种

机器对机器的方法，生生破译了德国人的密码。

当然，图灵还坚信第二种力量，就是人性的欠缺。因为密码是个数学现象，它是个死的；机器是个物理现象，它也是个死的。如果你要想把它破译，你就得坚信使用机器和数学的这个人是有缺陷的，因为对方德国人也是人，德国人的人格缺陷就是有点死板。

图灵就用到一系列的方法，他发现德国人经常会用密钥，它往往是相邻的两个字母，比如说 AB，或者 CD，这是德国人的一个习惯。这就缓解了一大部分计算量。

再比如说，他发现德国人发出来的电报，前面经常会有一些固定的语句，譬如说今天是星期几，今天天气如何。更重要的还有一句词，叫「希特勒万岁（Hail Hitler）」，这句词往往就成为他捕捉对方密码的一个很重要的线索。

此外，图灵还会诱使对方发一些固定的信息，然后通过一套数学算法，来判断对方这个密码到底是什么，这当中的原理当然极其杂乱，这里就不赘述。

总而言之，在 1941 年和 1942 年期间，图灵居然就把这个谜机给破译了。破译密码的结果就是英国人全都知道希特勒的一举一动，但是英国人的麻烦在于，我虽然全知道还得假装不知道，因为我不能让德国人知道了我破译了密码。

因为德国人并不傻，万一发现最近英国人怎么揍我揍得那么准？是不是密码被破译了？如果德国人意识到这一点，只要在恩格码机上改几个设置，那图灵此前所做的工作可就付诸东流

了。如果重算一遍，得花多少时间？这期间又得多死多少人？英国人这时候不得不开始装傻充愣表演。

举个例子说，德国舰队来了，你明明知道它就在这儿，你还真就不能直接派轰炸机去炸，得先派侦察机去，假装偶遇，「发现」你在这里，然后再回去叫轰炸机，这个表演也很辛苦。

其中最危险的一次，是德国的九条油轮的行踪被英国人发现了。德国到后来能源已经很紧张，如果炸掉九条油轮，这对德国的战斗力打击是很大的。英国人心痒，这口大肥肉真想给它吃下来，但是又不敢，这样吧，九条炸它七条，留两条逃生去吧，以便让德国人不猜疑到密码被破译。

但是德国人是挺倒霉，英国人也太阴险，最后这两条油轮逃出生天后，居然又遇到了英国的舰队，被炸沉了。这其实是德国人非常有机会发现密码被破译的一次，但德国人生生就没发现，为什么？因为他们对恩格码机器太自信了，觉得这套东西根本不可能被破译。

后来在二战期间，虽然德国人也升级了这套系统，但是没有彻底地毁掉或者说将恩格码机器弃之不用，给英国人留下了大量的空间。英国人在第二次世界大战期间，从敦刻尔克大撤退一直到诺曼底登陆期间，在欧洲大陆是没有什么作为的。它跟德国人打仗主要是在两个战场，一个是海上，还有一个就是北非。

1941 年英国海军打了一个大胜仗，围歼了德国海军引以为豪的那个大战列舰俾斯麦号。1942 年，蒙哥马利元帅带领英国的坦克部队，在北非消灭了德国号称沙漠之狐的隆美尔元帅的坦克

部队。这两场胜仗的背后，都是因为英国人掌握了德国人的情报。

当然还有一点，就是英国的地理位置是一个海岛，它的很多粮食都得从盟国运输回来，尤其是从美国。可是德国人当时搞出了一个 U 型潜艇战术，就是群狼战术，动不动就击沉它的商船。英国的物资供应一度紧张到整个英伦三岛的粮食供应只剩下一周，境况非常危险，眼看就要全民饿肚子。但是图灵因为破译了这套密码系统，英国商船的损失就迅速下降了。

我曾经见过本书的译者孙天齐先生，他给我看了一张图，自打图灵破译之后，可以明显看到英国商船的损失下降，下降多少？75%。后来德国人又把恩格码机器升级了，而且立竿见影，这边一升级，英国商船的损失马上就飙升。但紧接着，图灵和他的团队又破解了德国人的新机器，损失又下来了，在这根曲线里看得非常清楚。

战争哪里是我们平常想象的那样，仅仅是战场上士兵和将军的事？这背后有多少数学家和密码学家的努力，他们是实质性地影响着战争的进程。后来丘吉尔讲过一句话，说我们打这场战争，其实是捏着敌人的脉搏在打，他们干什么我们全知道。那这份功劳是属于谁的？当然就是属于伦敦以北 100 公里的布莱切利公园里面的那些学者们，其中就包括图灵。

但是这帮人可没有享受到战争胜利带来的红利，为什么？不能说。英国人先是打二战，二战一结束就开始跟苏联人死磕，这冷战就开始了。布莱切利公园里面发生了什么事情，一直是国家的机密。

这就发生了很多悲剧，比如说图灵身边的一个工作人员，他的老师就给他写信，说你年纪轻轻的，看着别的青年人都在为国家抛头颅洒热血，你小子在战争期间躲哪儿去了？把他一顿臭骂。这个人还不能说，百口莫辩。

图灵其实也是一样，在 1945 年战争接近胜利的时候，他身边一个人陪着他在布莱切利公园的树林里散步，就跟他说战争马上胜利了，你这期间的研究成果终于可以大白于天下了。图灵说，你怎么能这么幼稚？这怎么可能。

果然，后来丘吉尔下令，说战争期间你们搞的那个破解德国人机器的炸弹机，一共 210 多台，全部给我销毁，包括设计它的那些图文资料，全部销毁，一点都不能留。为什么？因为英国人一直不想让苏联人知道，英国其实捏着德国人的脉搏。

图灵这个人到底在二战期间做了多大的贡献，我们只能看一个大概，未知其究竟。这要是一般人，不得冤死。但是图灵有后手，为什么？他对人类还做了一项贡献，就是发明图灵机。

我们今天所有的计算机都是在那个原型上发展出来的，今天无论是在键盘上「啪啪啪」，还是在手机上「滑滑滑」，都是在一台图灵机上进行工作。

当然你别误解，图灵机可不是一台已经造出来的机器，它仅仅是一个提出来的理论模型构想。而且图灵提出来时是在 1936 年，那年他只有 24 岁。

而且还有一点，这可不是一个什么大规模、高成本、长时间的科研项目的结果，它仅仅是 24 岁的图灵整天胡思乱想的思绪当

中，飘出来的一个片断。何以见得？因为最早完整地提出图灵机那个构想，是在他论文的一则脚注里面，你说这个人是不是一个大神？要不怎么 20 世纪 60 年代，美国计算机学会把他们的大奖命名为「图灵奖」？

要知道图灵可是英国人，真正发明计算机的冯·诺依曼是美国人，美国人居然不用冯·诺依曼来命名它，而是用图灵来命名这个奖项，这个奖现在就是计算机界的诺贝尔奖，我们中国人还得过一次，2000 年清华大学一个教授得了「图灵奖」。图灵机，现在我们公认的计算机的发明者是美国科学家冯·诺依曼，但是冯·诺依曼自己都承认，说所有的思想来源都是图灵的，我最多算是计算机的助产士，我是帮它生下来而已。

为什么图灵这么牛？首先我们简单说一下什么是图灵机。图灵机就是想象中有一根无限长的纸带子，上面有一个一个格，有的格是黑色的，有的格是白色的，那黑色就代表 1，白色就代表 0。

图灵就想象，如果有一根打印头，它既能读取这个格当中的状态，它到底是 1 还是 0，又能进行擦写，那这个格不断地在探头面前移动，我就可以对这个探头的走向进行编程，从而影响计算结果。这说得再详细就没法说了，总而言之，我只要用这种方法给这个探头进行编程，我就可以得出一个计算结果，就是这么一个假想中的机器。

你说这很伟大吗？这当然很伟大。首先，24 岁的图灵就已经想到，让人类摆脱自己熟悉的十进制，转而用机器更容易识别和读写的二进制进行机器运算，这本身就需要想象力吧？更何况，图灵的思维境界是超越当时人一筹的。

在他之前，人类已经有了很多机器吧，这些机器也很强大，从最早的蒸汽机到后来的飞机、大炮、汽车，这些机器的本质都是一个，就是人的肢体力量的延伸和替代。只不过是利用了当时的新能源，什么煤炭、电能，这些机器也很强大，它替代人腿能跑得那么快，甚至能飞上天，但是这些机器都是在人的操控下才能够运转的。

可是图灵机的本质就不一样，它可不是人的肢体的简单延伸和替代，它是对人的思考过程的复制和再现。这才是图灵机的野心。人类的思考过程跟图灵机的本质是一样的，都是先输入一个信息，然后进行编程、处理，得出一个结果，再把这个结果输入回来，我们再进行处理，再得出结果。如此循环往复，往前一步一步地进行思考，图灵机要再现的就是这么一个过程。

图灵的野心不仅仅是帮当时的人类卸下沉重的计算担子，用机器来代替计算这么一个浅层的技术目标，他其实思考的一直是一个哲学问题。整个第二次世界大战之后，图灵的那一段生涯都在思考一些什么样的问题？比如说机器可不可能有智能？人是不是就是个机器？蚂蚁如果作为神经元，它们之间互相进行交流，拼接出一个巨大的蚁巢，那这个蚁巢是不是就是个大脑？那如果我用晶体管来替代一个单个的蚂蚁，让晶体管之间也形成神经元之间的互动，我是不是就可以再造一个人类的大脑？那这个大脑如果出来，它会不会是个智能？如果它有智能，它会不会跟人一样，会犯错误？它有没有情绪？会不会沮丧？会不会得意？图灵思考的全是这个问题。这些问题是近些年才在中国内地的科技界兴盛起来，因为现在人工智能的话题很热。其实几十年前的图灵，他的思考的起点就是这些问题。图灵哪里仅仅是什么计算机科学之父，他还是人工智能之父。

直到今天，我们判定一个机器是不是具有了人工智能，用的还是图灵当年发明的一套测试方法，这就是著名的「图灵测试」。图灵哪里仅仅是一个科学家？他之所以是一个大神，是因为他是个哲学家。

刚才我们介绍了那么多事儿，为大家塑造出一个大神级的图灵的形象，人又聪明，功劳又大，我们普通人是望尘莫及。可是如果把他从神坛请回到人间，从日常生活中你再看一眼这家伙，他是个什么德行？这本《图灵传》里面有大量的细节描写。

简单给大家归纳，他就是我们今天在中国很多互联网公司里见到的码农形象，是个典型的理工男。平时不修边幅，有时候跟他说话，你会觉得他神情恍惚，不知道在想什么，他沉浸在自己的世界里面。

图灵二战的时候在哪儿工作？布莱切利公园，那里是国家一级保密单位，那些警察又不是吃素的，一旦看这个人神情恍惚、晃来晃去，想干什么？肯定是个间谍，把他抓了好几回。

而且这个人还有一点神经质，是数学家式的神经质，经常要在心里数数。他有一辆破自行车，破到什么程度？就是每蹬 12 下，车一定掉链子。一般人肯定就送去修了，图灵不，数学家，一旦掌握这个规律，他就用数学方法来解决。在心里默数 12 下，就捯一下，确保不掉链子。

后来捯烦了，说这样，我亲手做一个手工的计数器安在这个自行车上，就盯着这数，一旦到 12 就捯一下，图灵就是这么个

人。虽然在日常生活当中，很多朋友都说他很好打交道，但是他缺乏处理自己社会事务的能力，在这方面很低能。

举一个例子，他那个时候非常苦恼一件事，就是花粉过敏。他拼命给领导打报告，说我需要一个防毒面具。领导觉得很为难，首先战争期间物资都很紧张，而且在工作场合，你天天戴着个那么丑的防毒面具，大家怎么跟你一同工作？就不给他。

他居然为了这么一件事，给英国首相丘吉尔写信。后来丘吉尔也真是够意思，居然批示了，说图灵博士需要这防毒面具是事关我国战略成败的大事，你们赶紧办，办完之后还要亲口跟我汇报。这算是领导亲自督办的工程，他才算戴上了这防毒面具。

你脑补一下那个场景，一个人蹬着破自行车，戴着一个防毒面具转来转去，太奇葩了吧。

而且图灵在二战期间还干了一件荒唐事，他并不认为英国一定能够战胜，老担心希特勒要是能打过来怎么办。我替英国政府做这么多事，家产肯定得没收。他就想出一个招，变卖了很多家产，买了两锭大银块。有人就建议他，让他存到英格兰银行，可他不相信，觉得英格兰银行迟早会倒闭，会归希特勒。

那这两锭银子怎么办？他就找了一片树林，埋下了一块银锭。又找了河床旁边的一座桥，把另一块银锭埋在这河床里，而且还做了大量的地图、标记，心想一旦战争结束，我再来挖。

后来战争结束了，英国给炸烂了，一塌糊涂，什么参照物都没有了。图灵就傻眼了，再也找不着这银锭了。这家伙后来居然

自己做了一个金属探测器，在树林里、河道里到处找，最后也没找着，非常沮丧。

二战期间图灵还老犯愁，万一我将来没饭吃怎么办？他居然用自己的收入囤了好多箱刮胡刀的刀片，说一旦没饭吃，就卖这个过活。

当然，我们今天谈图灵，前面这些全是小事，我们唯一不能回避的是他的性取向问题，他是一个同性恋。当时人们对于同性恋的观感和今天不一样，当时觉得这就是道德败坏。

无论是在那部电影里，还是在这本书里，关于图灵这个人前半生的同性恋的痕迹，其实很少提及，因为他确实也做得非常隐秘。

但是在 1951 年的 12 月，他因为同性恋，终于遇到了命中的克星。这个小男孩 19 岁，叫莫瑞，是一个无业游民，而且平时还有一点小偷小摸的坏习惯，属于典型的底层青年，但是因为人长得俊俏，图灵就跟他相处了。

处了一段时间之后图灵就发现，你怎么还偷东西？居然一次性从我家偷走了价值 50 英镑的东西。要说起来，这些东西也不值钱，无非是一件衬衫、一条裤子、一把刮胡刀之类的破玩意儿，但是图灵居然就没忍得下这口气，跑到警察局把莫瑞给告发了。这一天还挺有纪念意义的，因为就在前一天，是英女王伊丽莎白登基的日子，第二天就发生了这么个事。

警察很负责任地做笔录，你们俩怎么相识，他是怎么偷的你东西？一来二去，居然把图灵是同性恋这件事情给供出来了，而

且图灵大言不惭，他不觉得自己是犯罪，国家没有权力干涉我的私生活。这种话你穿越到今天讲可以，在当时，英国法律明文规定，同性恋是犯法，是要判刑坐牢的，但是图灵觉得没事。

那警察能咋办？法律面前人人平等，对不起，把你送到法庭去。英国的知识界，甚至包括美国的知识界都轰动了，都去拯救图灵，宣称他对国家非常有用，不能让他去坐牢，耽误研究。但是法律哪管这些，尤其图灵在法庭上态度又不好，他就觉得我无罪，我就是同性恋，你能拿老爷怎么样？一下子就把法官和陪审团全给激怒了。

他的位置那么高，岁数那么大，对方是一个 19 岁的小孩，大家自然有那个反应，是你勾引和玩弄人家。而且图灵在法庭上还大包大揽，没有他什么事，都是我，都冲老爷我来。那大家自然要判你刑，最后就顶格给他判了两年徒刑。

当时的英国法律有一个选项，就是如果你不想去坐牢也可以，必须接受治疗。当时人的医学观念，觉得同性恋是一种病，是病就得治疗，但所谓的治疗，就是注射大量的雌激素，其实就是化学阉割了。

图灵觉得可以接受这个方案，愿意接受治疗，不去坐牢。但是如果你问他，为什么会接受如此屈辱的一个方案？图灵的回答很简单，我不能去坐两年的牢，这会让我当下的研究中断。

可是你有没有想到，在长达两年的时间里，不断地往身体里注射雌激素，这会对身体造成什么样的伤害？除了性功能丧失，全身的其他功能也都会紊乱。后来图灵居然发育出了一对乳

房，可想而知，在这两年，他从精神到肉体，承受了什么样的苦难。

后来果然就发生了众所周知的那件事情，1954 年的 6 月，有一天他的女管家早上推开他的房门，发现他已经死在了床上，床头搁了一个被咬了一口的苹果，而且化验出了氰化钾。当时人都判断，图灵是自杀身亡，还不到 42 岁。

从 1861 年开始，英国人就废除了同性恋者要判死刑的法律，但是活罪还是难免。从那一天起，一直到 1967 年的一百多年间，对同性恋行为还是要判刑，只不过比较轻，两年的监禁或者是苦役。一共判了五万多人，其中既包括图灵，还包括那个著名的英伦才子王尔德，他是 1895 年到 1897 年，坐了两年的苦役牢。

1967 年的时候，英国人觉得这事就是私事，国家管个什么劲？就把同性恋从刑事犯的序列当中拿出来了，交给民间的道德法庭吧。到了 2009 年，英国首相布朗第一次在公众场合下承认，对不起图灵，当年搞错了。

到了 2013 年的时候，英女王就正式赦免了图灵，这说明在法律上，是撤销了那个时候的判决，然后对图灵进行致敬；到 2015 年的时候，美国法律居然允许同性恋的婚姻。这一百多年的历史，是逐步放开的历史。