微博上的数学漫游（连载三）

歌之忆 http://weibo.com/wildmath

当一部数学史摆在我们面前的时候，我们总会津津乐道于那些创造了伟大的数学理论或者证明了著名的数学猜想的数学家们。可是，真切的数学却同这个世界经历着同样的历程——战争与和平、繁华与凋零。我们不该忘却那些隐秘的数学英雄，他们以数学为武器来捍卫着我们安宁的生活，他们以卓绝的才华印证了数学在华美的外衣下，蕴含的是能将智慧发挥到极致的伟大力量。正是这强悍的力量，在守卫着我们的世界，构建着我们的心灵。

波兰三杰

波兰的密码三杰：雷耶夫斯基（1905-1980, 右）、罗佐基（1909-1942, 中）和佐加尔斯基（1907-1978, 左）

今年是计算机科学伟大的先驱者阿兰·图灵诞辰一百周年，在无数有关图灵的故事中，流传甚广而且特具魅力的就是他破译德国英格玛（Enigma）密码系统的传奇。可波兰数学家和密码学家雷耶夫斯基（Marian Rejewski）、罗佐基（ Jerzy Różyck）和佐加尔斯基（Henryk Zygalski）对破译英格玛所做出的居功至伟的贡献，却并不广为人知。

围绕密码的传奇故事可谓汗牛充栋。古罗马的凯撒征战高卢（今法国）时，就用加密的方式向其副帅、政治家西塞罗的弟弟传递情报。凯撒的加密不过是把字母替换成字母表中后移三位的字母。如果借英语想象一下，埃及艳后收到凯撒的一行字“ehdxwb”，她将会心一笑：夸我是美人儿（beauty）！

向美人儿表白心迹自然无需加密，可国与国

电影《凯撒与克丽奥佩拉》剧照

之间，难免许多秘密。一战结束后，德国的保密通信成为各国的研究热门，不过大多无功而返。法国间谍还算不错，搞到了商用英格玛加密机，多少了解到一点加密原理。可是破译密码还需要找到密钥。估算一下可能的密钥数量，1 亿亿，这可是个天文数字。

擅长解读爱情密码的法国人，在英格玛面前却一筹莫展，只好把这台加密机送给波兰。这是三十年代初的事情，当时全世界恐怕都没有想象到，波兰人早在二十年代就探索用数学来解读密码。就在这台英格玛面前，波兰数学家雷耶夫斯基开启了波兰数学的另一段传奇。不过，这台好戏需要对手的配合。

对手戏的好看，在于双方旗鼓相当。德国人向来以严谨著称。二战时，盟军派出许多间谍去打探德国到底有多少坦克，而统计学家发现德国人严谨得过了头，居然给其出厂的坦克连续编号，于是要求盟军：别只顾清点战场上干掉了多少辆，把干下来的最大编号告诉我们！由此直接估算出了坦克总量。

波兰华沙博物馆的英格玛加密机

德国人在使用貌似天衣无缝的英格玛加密机时，照样秉承了德国无与伦比的严谨，也同样严谨得过了头。德国人为了防止通信中的错误或干扰，每发送一条信息时，都在前端把三个字母的密钥重复发送两次。看似很保险的这一细微的步骤，却被曾在德国哥廷根学过保险精算的雷耶夫斯基抓住了漏洞。

雷耶夫斯基从截获的德国密文中，判读出德国人把三字母密钥连发了两次，这个发现非同小可。更令人叫绝的是，他针对这种密钥重复，运用排列群来分析英格玛机的加密过程。由此，他把密钥搜索范围从原先的 1 亿亿降低到了 10 万。德国人重复了密钥的三个字母，送给了波兰数学家一份真正的厚礼。

二战之前，英格玛让英法情报机构摇头叹息，因为谁都无法从 1 亿亿个候选中及时找到密钥。英格玛却让波兰情报机构大放异彩，因为他们只需在 10 万个候选中去找密钥。虽然德国每天都改变密钥，但只要截获到 80 条信息，就能确定密钥的位置，再用两小时即可破解。这就是波兰数学家创造的奇迹。

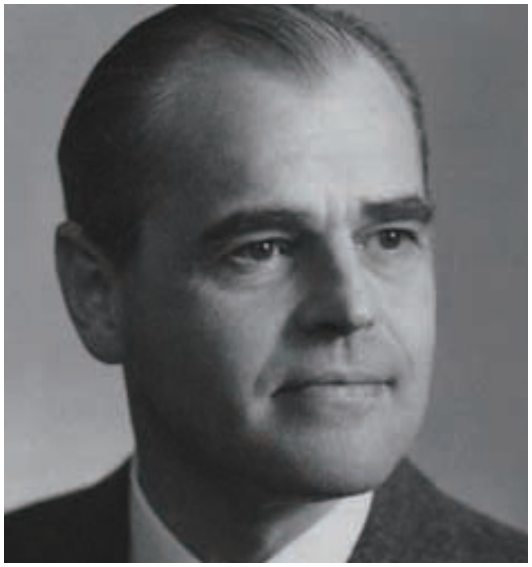
图灵雕像

雷耶夫斯基雕像

今天人们习惯于把破译英格玛的功劳记在图灵身上，但那样一个横空出世的图灵反而是没有质感的。图灵破译英格玛的成就是在 40 年代，而在这之前的 1932-1938 年，波兰率先破译英格玛，令他国望尘莫及。甚至有数学家评价：雷耶夫斯基解密英格玛所创造的，是一条赢得第二次世界大战的数学定理。

二战后返回波兰的雷耶夫斯基，遭到安全机构反复调查。守口如瓶的他艰难地以记账员的身份生活着，直至退休多年才向世人告白真相。波兰三杰，从此成为波兰民族的骄傲。然而，波兰数学家创造的奇迹，却并非二战中的唯一。二战结束半个世纪后，又一位成就斐然的数学家以绝世高手的形象走出密码战的历史尘封。

玻尔林 Beurling



瑞典数学家玻尔林（1905-1986）

德国在二战的战略通信中使用的是比 Enigma 远为复杂的 G-Schreiber 密码。但依旧是栽倒了，栽倒在更厉害的数学家手下。解码的巨牛甚至连样机都没见过，全靠手工演算两个星期，直接将密码攻克！后来，他到美国普林斯顿高等研究所，继承了爱因斯坦的办公室。此人就是瑞典数学天才玻尔林（Arne Beurling）。

破译德军战略通信密码的玻尔林，极富原创思想。虽破译密码只是其专业外的客串，但希特勒进攻苏联的巴巴罗萨行动就此被瑞典破译。多年来，人们百思不得其解："只靠笔和纸在两个星期破解 G-Schreiber 密码，您到底怎么玩的？"他对此避而不答，却反问：哪有魔术师会揭秘自己玩的魔术？

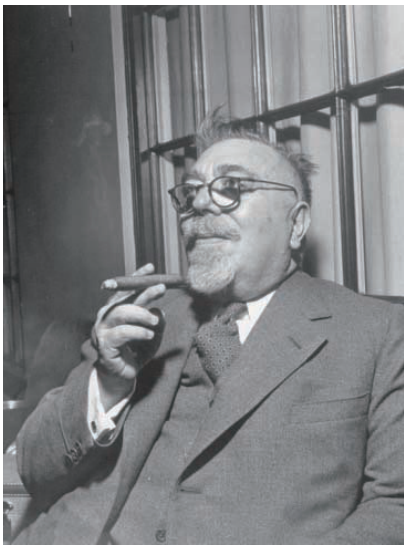
美国数学家道格拉斯（1897-1965）

也许玻尔林对自己破译 G-Schreiber 密码还有许多意犹未尽的思考。此君总是在深思熟虑之后才发表自己的作品。有次听 Peter Duren 做报告，玻尔林当即告知：数年前他就得到了同样结论，只不过没去发表。Duren 迎头痛击，申明自己要去发表。于是上演了一出玻尔林四处追打 Duren 的喜剧！

追猎可是玻尔林擅长的。 在此君做博士论文的 1929 年，就已经证明了复分析中著名的 Denjoy 猜想。证明刚一完毕，玻尔林便拉着他老爹跑到巴拿马去捕猎鳄鱼。鳄鱼倒是逮到了，可这次度假却让他错失了一份巨大的荣耀——芬兰数学家阿尔福斯（Lars Ahlfors）率先发表了证明，并借此拿下 1936 年菲尔兹奖。

不知道玻尔林猎杀的鳄鱼是否吃掉了一枚菲尔兹奖章，不过玻尔林倒没有因为这事和阿尔福斯闹过不愉快。两位杰出的数学家岂止是惺惺相惜，他们常聚在一块儿痛饮美酒，甚至跑到阿尔福斯家里一醉方休。末了，玻尔林和阿尔福斯再加上阿尔福斯太太，三个人一齐和衣醉卧在同一张床上！

假如时光能穿越，放在今天这样一个物欲横流的社会，那个曾经醉心于捕猎鳄鱼、二战时玩残了德军战略情报的瑞典天才玻尔林，会不会依然不去计较落在芬兰同行阿尔福斯手里的菲尔兹奖？虽然 1936 年在挪威奥斯陆颁发的第一届菲尔兹奖，名头远非今天这般如日中天，却也吸引了无数眼球。



美国数学家维纳（1894-1964 ）

与阿尔福斯同时获菲尔兹奖的是美国数学家道格拉斯（Jesse Douglas）。然而此君无法出席会议，只得请维纳（Norbert Wiener ）登场帮忙。求名心切的维纳毫不推辞、光鲜登场，对着记者一顿神侃。啥也没整明白的挪威记者，无比兴奋地拍了一通新闻照片，却没去理会个中曲直。最终报纸上名为道格拉斯的获奖者，却是维纳的尊容！

出了风头的维纳，内心很是烦恼。维纳一生多次在优先权上与其他名流纠缠不清。他曾要求把巴拿赫空间命名为“巴拿赫 - 维纳空间”，无奈无人理睬。人性的弱点，早被莎士比亚一眼看穿。看看《亨利四世》就明白：惟友谊能超越荣誉，成就人生。而阿尔福斯和玻尔林，拥有了几乎完美的真正友谊。