图灵—密码破译者

曹箭 (编)

阿兰·麦席森·图灵出生于 1912 年 6 月 23 日，是一位伟大的英国数学家、密码学家，被誉为计算机之父。图灵的一生很短暂，但是却十分精彩。图灵是一位真正的天才数学家，年仅 23 岁的图灵就被选为剑桥大学国王学院院士，一年后他向伦敦权威的数学杂志投了一篇论文，题为“论可计算数及其在判定问题中的应用”主要对哥德尔 1931 年在证明和计算的限制的结果作了重新论述，重新定义计算，把计算归结为最简单、最基本、最确定的操作动作，与自动机相联系，并与人的计算过程类比，提出包含存储器、运算语言、扫描、下一步计算的计划与执行等过程的计算机概念模型，即图灵机。“图灵机”与“冯·诺伊曼机”齐名，被永远载入计算机的发展史中。

在密码领域，图灵的贡献也毫不逊色，曾有人说如果没有图灵的贡献，二战至少多打十年。

图灵的密码故事要从一个“谜”开始，ENIGMA (谜) 源自于希腊文，既是战争时期所用的密码（在所有用于军事和外交的密码里，最著名的恐怕应属第二次世界大战中德国使用的 ENIGMA），而破解这个密码的正是阿兰·麦席森·图灵。二战期间，德国发明了一种看似不可破译的密码“ENIGMA”，这是一种用于 ENIGMA 加密和解密的机器，这种密码被德军广泛使用，包括定位出没于大西洋运输线上的潜艇，这些潜艇以令人心惊胆战的速度击沉英军的船只，被丘吉尔称为“大西洋海战”。丘吉尔担心英军会因补给短缺而战败，而解决的唯一办法便是阻止德军的潜艇战术，破解 ENIGMA 就是阻止德军的方式之一。如果英军能破译这些情报，他们就可以确定位置并击毁潜艇。

但在整整 13 年里，英国人和法国人都认为 ENIGMA 是不可破译的。针对这一情况，政府成立了一个新的机构——英国政府密码学校（Government Code and Cipher School, GCCS），总部坐落在白金汉郡的布莱切利庄园。这个难题也交到了图灵手中，从 1938 年 9 月开始，图灵一直专门负责 ENIGMA 的密码分析。他率领着大约 200 多名精干人员进行密码分析，其中甚至还包括象棋冠军亚历山大。分析和计算的工作非常复杂，26 个字母在“ENIGMA”机中能替代 8 万亿个谜文字母。如果改动接线，变化会超过

2.5 千万亿亿。图灵凭借着他的天才设想设计出一种破译机。这台机器主要由继电器构成，还用了 80 个电子管，由光电阅读器直接读入密码，每秒可读字符 2000 个，被称为“图灵炸弹（Bombes）”

图灵对 ENIGMA 的破译方法完全是纯数学和理论性的，据他的同事们回忆，他在破译密码的工作中，曾创造好几种新的统计理论，但都未形成论文发表，后来又重新为他人所创建，由 A．瓦尔德(Wald)重新发现并提出的“序贯分析”就是其中之一。序贯分析是数理统计学的重要分支之一，其特点是，在研究决策问题时，不是预先固定样本量，而是逐次取样，直到样本提供足够的信息，能恰当做出决策为止。其中“序贯概率比检验（Sequential Probability Ratio Test, SPRT）”在密码分析中的应用，可以明显约减相关攻击所需的密钥量。

由于这个组的努力，特别是图灵的出色工作，他们掌握了破译该密码的一整套方法，从而了解了德军的动向，掌握了战争的主动权，为英美联军击败德国做出了突出贡献。

1941 年 5 月 21 日，破译小组第一次立了大功，因为截获了希特勒给海军上将雷德尔的一封密电，将当时号称世界上最厉害的一艘德国战列舰“俾斯麦”号击沉。

1943 年 4 月，日本联合舰队总司令长官山本五十六，在 4 月 18 日将飞抵卡西里湾，这份情报被破译小组破译，于是，这位战功卓著的日本司令的飞机，在距离卡西里只有几英里被拦截并击落。

图灵的许多思想和预见都在他死后不断得到验证，也始终引导、推动着计算机科学的发展。国际计算机协会于 1966 年设立“图灵奖”，以专门奖励对计算机科学研究与推动计算机技术发展有卓越贡献的杰出科学家。