信息战——密码的核心机密

复旦大学计算机科学与技术 16307130335 方煊杰

摘要: 虽说密码学是信息时代新兴学科，但事实上密码学贯穿人类整个历史以及各个领域，尤其在战争中得到广泛应用。魔高一尺，道高一丈，加密与解密的破译跨越千年，在智慧与科技的竞争中，从密码战中我们可以窥见信息背后的秘密，以及密码学的核心机密。

1.古代战争中的密码应用

密码因战争而生。

1.1 密码的诞生

”密码和文字的历史一样长。“

在密码诞生之前，中国古代便有蜡丸藏于口舌的保密传信方法，而正如“点子硬，并肩上”一类的我们耳熟能详的黑话一般，人们逐渐把隐藏信息藏匿在公开明文中，也就是密码。

公元前400年是历史学家公认的密码学诞生时期，当时在雅典与斯巴达战争后期，间谍通过将写有字符的纸张缠绕到不同尺寸的木棍而获得有用信息，而这便是世界上最早的密码情报。后来，这种密码通信方式在希腊广为流传。现代的密码电报，据说就是受了它的启发而发明的。

1.2 古代密码应用

除了早期希腊罗马时期的密码传承，古代中国也有其自己的密码斗争历史。

在各个电视剧里经常出现的虎符实际上就是最简单的一种：使用时各执一半，已验真假。这正对应着当今秘钥密码。除此之外，阴书也是常用的传递密报方法，将一段内容分为三份分别传递，只有完整拿到三份内容才能拼凑出对应消息，由此也可以想到现在很多在线文档题库系统也采取这种方式分段传输，当然这更多地作为反爬虫而并非密码的体现，但古代密码思想从中也可见一斑。

而对于拉丁文系语言，也有其特有的简便加密方式，比如换位密码：将26个字母打乱顺序，重新对应，如每个字母向后移3位；或者可以更难一些全部随机打乱，通信双方留有母本查看。或者是用数字来代表字母，对应编码。

可以看出，古代虽然没有明确成熟的密码概念，但是军事领域中逐渐用“密文”代替”明文“的方式，也证明了密码思想是战争中不可或缺的一部分。

2 近现代密码发展

到了近现代，随着计算机技术的飞速发展，密码学也迎来了它的辉煌时期。

2.1 二战下的密码

恩尼格玛密码机是二战时期纳粹德国使用的一系列相似的转子机械加解密机器的统称。

这种加密方式在密码学上被称为“复式替换密码”，三个转子的初始方向、转子之间的相互位置以及连接板的连线状况就组成了“恩尼格玛”三道牢不可破的保密防线，其中连接板是一个简单替换密码系统，而不停转动的转子，虽然数量不多，但却是点睛之笔，使整个系统变成了复式替换系统。连接板虽然只是简单替换却能使可能性数目大大增加，在转子的复式作用下进一步加强了保密性。恩尼格码密码机大约有一亿种可能性，这样庞大的可能性，换言之，即便能动员大量的人力物力，要想靠“暴力破解法”来逐一试验可能性，那几乎是不可能的。

同样在动荡时期的中国，也根据汉字特有的特征，创造了很多新的加密方式。

比如跨越地区几乎无法相互听懂的方言系统为密码传递提供了很好的载体。通过普通加密方式翻译出的明文可以是方言的谐音，正如视频中所看到的”嘎嘎“代表外婆家，只有真正的接头人才能明白其含义，日军对此确实一筹莫展。这里想到初中时有老师提过，当初家乡方言中“玉米”的发音是“八路”，于是我放军队就以玉米来称呼部队，从而达到了保密的效果。

最终反法西斯联盟的胜利，无论是欧洲战场或者中国战场，我想取得胜利的原因中对于敌方密码破译以及自身信息加密也占据了重要的一部分。

2.2 现代战争下的密码

计算机时代是继手工密码，机械密码以后，密码发展的第三个阶段，在这一阶段斗争就更复杂了。

而在当今世界的情报活动中，间谍也超过以往任何时候，手段高明，技术先进，今非昔比。苏联克格勃每年窃取的情报超乎人的想象。现在人的手机，电脑使用率大大上升，同时越来越多的信息存储在云端，电子侦察的手段也愈发复杂。简单如qq木马病毒，撞库密码攻击；复杂如窃听植入，超级计算机破译，密码学斗争的今天，形势更加难以预料，斗争也愈发激烈。现代加密算法虽然看似复杂完美，对称不对称轮番启用，但终究还是抵不过情报局日夜钻研，超级计算机不停演算。

挑战未来，信息安全不容小觑。

破谜与解密形影不离，相互纠缠，而在它们博弈的过程中，密码学愈发壮大，快速发展。尽管密码依附战争而生，其本质带有诡秘与不佳，但无论是什么时代都不会有人放过它。

在过去，它是能够扭转战争成败的关键；而在未来，它也会逐渐融入到平凡生活中，或许会给我们带来不一样的影响。只要我们有需要保密之处，密码学就将永不消亡。