“打死我也不说”——数据加密技术

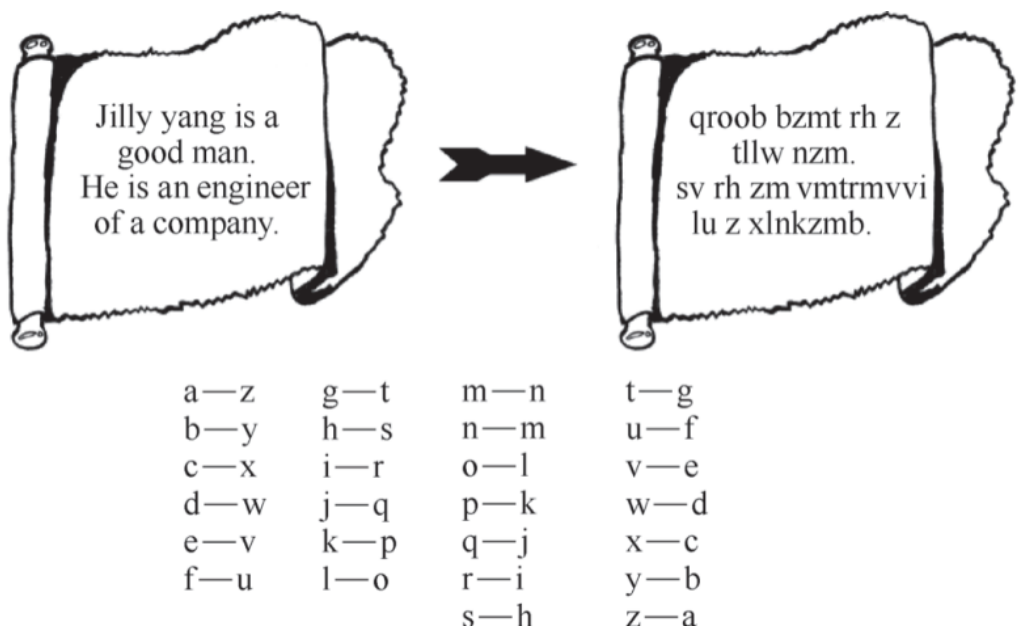
发布时间：2023年08月11日

人与人的交流，需要私密性。对于政府机构、金融机构、保密机构，大量的信息是对绝大多数人保密的；对于企业，也存在大量的商业机密，这些商业机密的价值就是交给最合适的人并把它利用起来；对于个人，任何人之间的通信都可能带有隐私成分，不希望被第三者听到。

当然，生活中的“保密”包含两方面的内容。一方面，你需要把保密的内容“藏”起来，“存储”到某个保密空间，防止让别人获取，类似于孩子玩的“捉迷藏”游戏。有专门的技术来保证你的保密内容不被偷窃，如最先进的密码锁、你的守口如瓶和最先进的文件存储技术。其中任何一个方面，都不属于我们本书讨论的范围。另一方面，当你需要把这些保密的内容通过特定通道传递出去时，需要保证内容不会外漏。这些方式包括雇用押运车、说悄悄话等。在通信中，则有专门的通信保密技术。当然，雇用押运车也不是我们目前讨论的范围，我们还是要将话题拉回到我们通信的保密技术上来。

最传统的通信保密技术叫作“密电码”技术。我们经常看到战争片有这样的情节：我情报员英勇无畏、智慧过人、战无不胜，成功破译了敌人的密电码，从而获取了敌人的重要情报，并一举粉碎了敌人的阴谋。在战争中，信息交互非常频繁，未经充分加密的信息被敌人获取或破译后，战争局势可能因此而彻底改变。

最简单的保密方式是通信双方拥有一样的明文和密文的对应方式，如下图所示。



比如英文里面 26 个字母，每个字母对应另外一个字母。比如 a 对应为 z、r 对应为 i、e 对应为 v、d 对应为 w。那么，read 就对应为 ivzw，dear 就对应为 wvzi，dare就对应为 wziv。如果你把 ivzw 通过某个渠道送达要获取信息的人，他也有一个同样的字母对应表，就很容易破译出 read 这个单词来。这种方式，便捷、容易理解和记忆，但是缺点也是明显的：如果你的敌人也获得了同样的字母对应表，加密就变得毫无价值。

即使敌人没有获取字母对应表，这种方式也非常容易被破解出来。专门研究密码的人会从人的使用习惯、经验规律、字母使用频率等角度来破解密码。比如在英文中应用最多的字母是 s、t，那么不管你的暗文多么晦涩，破译者也会根据使用频率最高的字母可能映射 s 或者 t 中的某个字母开始着手，很快就破译出所有密电码规则。

密电码技术在真正需要保密的机构，必须采取更先进的算法，而这些算法都是数学家发明的。自诞生之日起，密码技术就是一门高科技学科。研究加密和破解加密永远是此消彼长，既然都是人发明的方法，也一定有别人能破解，要做到百分百的“保密”，恐怕也会存在无人能读懂的风险。

--摘自《大话通信》

上一篇：贝尔实验室

下一篇：天冷掉电快？难道手机也怕冷？