保密系统的通信原理

C. E. Shannon

翻译：李晓峰 (cy_lxf@163.com)

译文来自于经典文献翻译项目 https://gitee.com/uisu/InfSecClaT

译者单位：北京联合大学智慧城市学院

2022 年 3 月 10 日

摘要

此文是对香农“Communication Theory of Secrecy Systems”文章的翻译。

1 引言和概述

密码学和保密系统的问题为通信理论提供了一个有趣的应用[1]。本文提出了一种保密系统理论, 该方法在理论层面上，旨在补充密码学以前工作的处理方法[2]。在那里，对许多标准类型的编码和密码以及破解它们的方法进行了详细的研究。我们将更加关注保密系统的一般数学结构和性质。

这个处理方法在某些方面受到限制。首先，一般有三种类型的保密系统：（1）隐蔽系统，包括隐形墨水、在文本中隐藏消息、或密码隐藏在假消息中，或对敌人隐藏消息存在的其他方法；（2）隐私系统，例如语音反转，其中需要特殊设备来恢复信息；（3）“真实”保密系统，其中信息的含义被密码、代码等隐藏，虽然它的存在并不隐蔽，而且假定敌人拥有拦截和记录传输信号所需的任何特殊设备。我们认为只有第三种类型的隐匿系统是心理上可以接受的技术型的隐私系统。

[1] Shannon, C. E., “A Mathematical Theory of Communication , ” Bell System Technical Journal, July 1948 , p. 379 ; Oct. 1948 , p.623 .

[2] See , for example , H . F . Gaines , “Elementary Cryptanalysis , ” or M . Giviergc , “Cours de Cryptographic .”

其次，处理仅限于离散信息的情况，其中要加密的消息由一系列离散符号组成，每个符号从有限的集合中选择。这些符号可以是一种语言中的字母、一种语言中的单词、“量化”语音或视频信号的振幅等，但是主要关注与字母有关的情况。

本文分为三个部分。现在将简要总结主要结果。第一部分论述保密系统的基本数学结构。正如在通信理论中一样，一种语言被认为是由一个随机过程来表示的，这个随机过程根据某种概率系统产生一个离散的符号序列。与语言相关联的是一个特定的参数 D，我们称之为语言的冗余。从某种意义上说，D 衡量的是语言中的文本在不丢失任何信息的情况下可以缩短多少长度。举个简单的例子，因为在英语单词中 u 总是跟在 q 后面，所以 u 可以省略而不会丢失含义。由于语言的统计结构、某些字母或单词的高频率等原因，英语中可能会有相当多的冗余，冗余在保密系统的研究中至关重要。

保密系统被抽象地定义为一个空间（可能的消息集）到第二个空间（可能的密码集）的一组转换。集合的每个特定变换对应于使用特定密钥进行加密。这些变换被认为是可逆的（非奇异的），因此当密钥已知时，可以进行唯一的解密。

在每个转换下，每个密码都有一个与选择此密码概率相关的先验概率。类似地，假设每个可能的消息都有一个相关的先验概率，由潜在的随机过程决定。这些不同密钥和消息的概率实际上是敌方密码分析员对相关选择的先验概率，代表了他对情况的先验知识。

要使用保密系统，首先选择一个密钥并将其发送到接收点。密钥的选择决定了构成系统的设备中的特定转换。然后选择一条消息，并将与所选密钥对应的特定转换应用于该消息以生成密文。该密文通过信道传输到接收点，并可能被“敌人”截获，在接收端，将特定转换的逆运算应用于密文，以恢复原始消息。

如果敌人截获了密文（cryptogram），他可以从中计算出可能产生该密文的各种可能消息和密钥的后验概率。这组后验概率构成了他在拦截后对密钥和消息的知识。因此，“知识”被认为是一组与概率相关的命题。后验概率的计算是密码分析的通常解决的问题。