第 1 章：密码学简介

1.3 发展历史

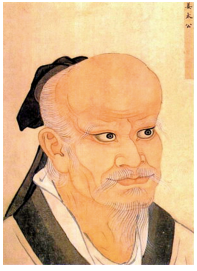
赵俊舟

junzhou.zhao@xjtu.edu.cn

2025 年 2 月 20 日

中国古代加密技术：姜子牙阴符

太公曰：主与将，有阴符，凡八等。有大胜克敌之符，长一尺。破军擒将之符，长九寸。降城得邑之符，长八寸。却敌报远之符，长七寸。警众坚守之符，长六寸。请粮益兵之符，长五寸。败军亡将之符，长四寸。失利亡士之符，长三寸。诸奉使行符，稽留，若符事闻，泄告者，皆诛之。八符者，主将秘闻，所以阴通言语，不泄中外相知之术。敌虽圣智，莫之能识。



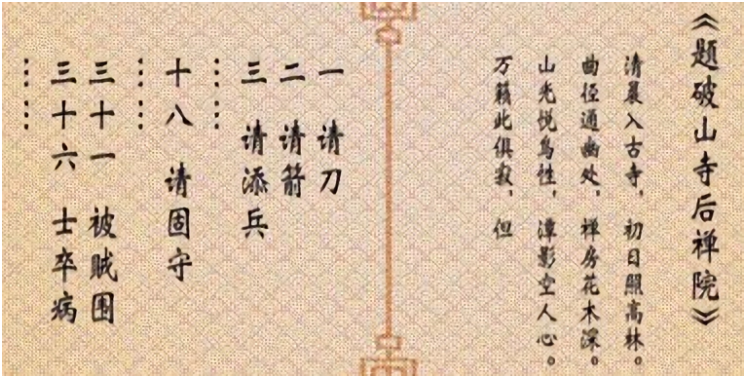
(? – 1015BC 或 1036BC)

中国古代加密技术：牙璋、虎符

一份在君王手里，一份在将领手里，两两相对才能调动军队。

中国古代加密技术：五言律诗秘钥加密法

- 约定一首 40 字的五言律诗保密，文字不得重复；
- 如果需要补充兵力，前方将领从密码本中查出“请添兵”的编号，是第三，则将律诗中第三个字写到文书中，发给后方；
- 后方从律诗中找到该字的位置，从而得到编号，得知情报。



中国古代加密技术：戚继光声韵加密法，反切法

柳边求气低，波他争日时。莺蒙语出喜，打掌与君知。

春花香，秋山开，嘉宾欢歌须金杯，孤灯光辉烧银缸。之东郊，过西桥，鸡声催初天，奇梅歪遮沟。

- 加密：前一首诗歌的前 15 个字作为声母，依次编号为 $1-15$；后一首诗歌的 36 字为韵母，按顺序编号为 $1-36$；然后再将当时字音的八种声调，也按顺序编号为 $1-8$，就编写出完整的“反切码”体系。
- 解密：如果密码的编号是“5-25-2”，5 是声母“低”字，25 是韵母“西”字，2 是声调的二声。据此，“5-25-2”就可以读为“敌”字。

Auguste Kerckhoffs 与柯克霍夫准则

- 奥古斯特 · 柯克霍夫 (Auguste Kerckhoffs, 1835 – 1903)，荷兰语言学家与密码学家。
- 人们尝试发送加密信息已有 2000 多年历史，但是在 1900 年以前，只有两个想法对现代密码学产生了重大影响，其一为**柯克霍夫准则**。
- 柯克霍夫准则体现在所有现代密码学中。
- 香农后来提出了类似观点："The enemy knows the system"，称为**香农准则**。

柯克霍夫

柯克霍夫准则

A cryptographic system should be secure even if everything about the system, except the key, is public knowledge.

William Friedman

- 威廉 · 弗里德曼（William Friedman, 1891 – 1969），美国陆军密码专家。
- 1918 年发表著作《The Index of Coincidence and its Applications in Cryptography》，被认为是现代密码学最重要的著作之一。
- 1930 年代，他领导了陆军的一个研究部门 Signals Intelligence Service (SIS)，其中一部分服务一直延续到五十年代。
- 三十年代晚期，在他的指导下，Frank Rowlett 破解了日本人的 PURPLE 加密机（紫密），截获了日本的大量外交和军事的秘密。

弗里德曼

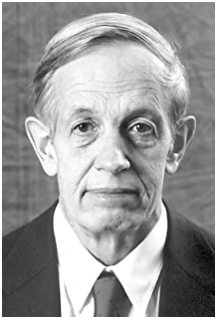
Claude Shannon 与分组密码设计的准则

- 克劳德 · 香农（Claude Shannon, 1916 – 2001），美国数学家、信息论创始人。
- 1948 年，香农发表《The Communication Theory of Secrecy System》，成为现代密码学理论基础。
- 1949 年，香农发表论文《保密系统的通信理论》，首次将密码学研究置于坚实的数学基础上。
- 证明了一次一密（one-time pad）的理论安全。
- 提出分组密码设计应遵循的准则：扩散和混淆。
- 证明了消息冗余使得破译者统计分析成功的理论值（唯一解距离）。

香农

John Nash 与密码学安全性的一般性准则

- 约翰 · 纳什（John Nash, 1928 – 2015），美国数学家，博弈论创建者。
- 1955 年，纳什在一封给 NSA 的信中提出了计算安全的思想。
- 遗憾的是，纳什的信一直处于机密状态，直到 2012 年才公开。如果纳什的想法能提早公开，那么势必会加速现代密码学的发展。

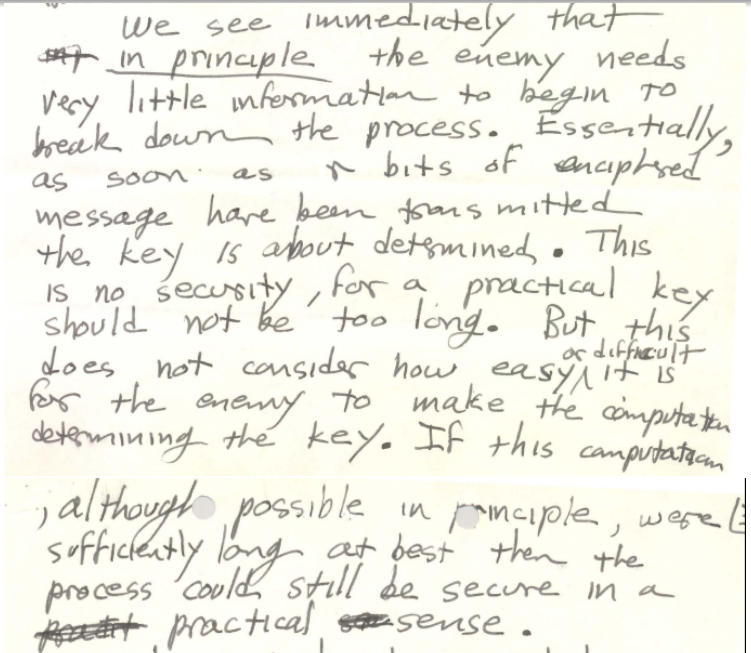


约翰 · 纳什

计算安全的思想

It doesn't really matter whether attacks are impossible, only whether attacks are computational infeasible.

纳什的信件



We see immediately that ~~in~~ in principle the enemy needs very little information to begin to break down the process. Essentially, as soon as r bits of enciphered message have been transmitted the key is about determined. This is no security, for a practical key should not be too long. But this does not consider how easy or difficult it is for the enemy to make the computation determining the key. If this computation

, although possible in principle, were sufficiently long at best then the process could still be secure in a ~~practical~~ practical ~~sense~~ sense.

沉寂期

1949 – 1967，**密码学研究处于沉寂时期**。

Horst Feistel 与数据加密标准 DES

- Horst Feistel（1915 – 1990），德裔美国密码学家。
- Horst Feistel 在 IBM 工作期间于 1971 年发明分组加密算法 Luciffer 密码，提出 Feistel 密码结构。
- Feistel 密码结构激发了 70 年代对数据加密标准 DES 的研发高潮。
- 1976 年 – 1977 年，美国国家标准局正式公布实施数据加密标准 DES。

Horst Feistel

Whitfield Diffie, Matin Hellman 与公钥密码学

- 1975 年，W. Diffie 和 M. Hellman 发表论文《New Directions in Cryptography》，提出公开密钥思想，揭开现代密码学研究的序幕。
- 该开创性研究获得 2015 年图灵奖。

W. Diffie

M. Hellman

Stanford | News

Home Find Stories For Journalists Contact

Stanford Report, March 1, 2016

Stanford cryptography pioneers Whitfield Diffie and Martin Hellman win ACM 2015 A.M. Turing Award

The groundbreaking algorithm from Whitfield Diffie and Martin Hellman enabled a secure Internet and sparked a clash with the NSA that foreshadowed current privacy battles between government agencies and Silicon Valley companies.

Whitfield Diffie, Matin Hellman 与公钥密码学

New Directions in Cryptography

Invited Paper

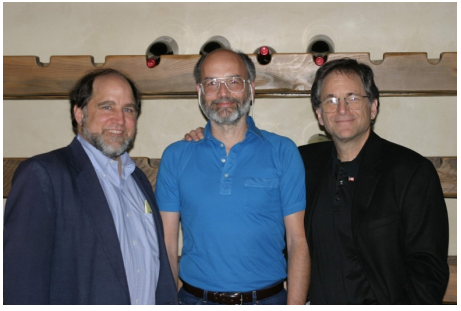
WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

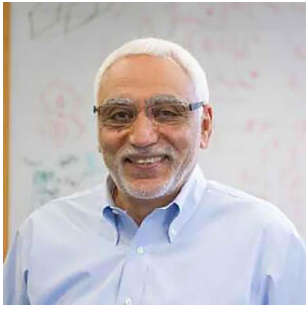
***Abstract*—Two kinds of contemporary developments in cryptography are examined. Widening applications of teleprocessing have given rise to a need for new types of cryptographic systems, which minimize the need for secure key distribution channels and supply the equivalent of a written signature. This paper suggests ways to solve these currently open problems. It also discusses how the theories of communication and computation are beginning to provide the tools to solve cryptographic problems of long standing.**

The best known cryptographic problem is that of privacy: preventing the unauthorized extraction of information from communications over an insecure channel. In order to use cryptography to insure privacy, however, it is currently necessary for the communicating parties to share a key which is known to no one else. This is done by sending the key in advance over some secure channel such as private courier or registered mail. A private conversation

R. Rivest, A. Shamir, L. Adleman 及 A. El Gamal

- 1977–1978，Ronald Rivest, Adi Shamir, Len Adleman **第一次提出公开密钥密码系统的实现方法** RSA。
- 1981，**成立** International Association for Cryptology Research。
- 1985，Abbas El Gamal **提出概率密码系统** ElGamal **方法**。
- 2000，Advanced Encryption Standard（AES）





姚期智

- 1946 年 12 月 24 日出生于中国上海，祖籍湖北孝感，幼年随父母移居中国台湾，中科院院士。
- 2000 年图灵奖获得者，是唯一获得该奖的华人学者（截至 2023 年）。
- 贡献 1: 建立理论计算机科学的重要次领域：通讯复杂性和伪随机数生成计算理论；
- 贡献 2: 奠定现代密码学基础，在基于复杂性的密码学和安全形式化方法方面有根本性贡献；
- 贡献 3: 解决线路复杂性、计算几何、数据结构及量子计算等领域的开放性问题并建立全新典范。

姚期智