第 1 章：密码学简介

赵俊舟

西安交通大学网安学院

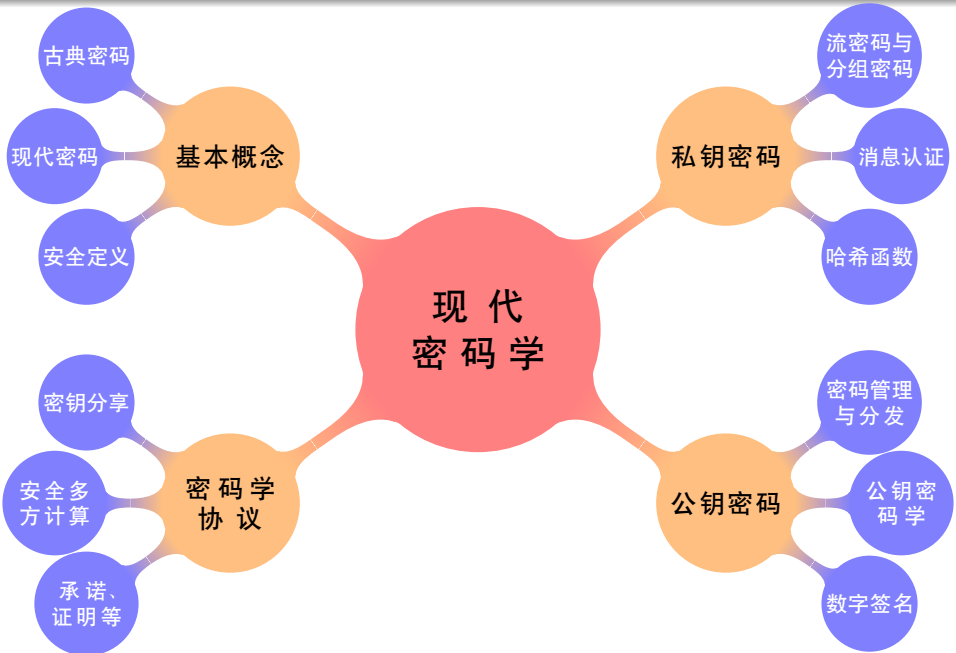
junzhou.zhao@xjtu.edu.cn

2025 年 12 月 20 日

目录

目录

课程内容


现代密码学
基本概念
古典密码
现代密码
安全定义
私钥密码
流密码与分组密码
消息认证
哈希函数
密码学协议
密钥分享
安全多方计算
承诺、证明等
公钥密码
密码管理与分发
公钥密码学
数字签名

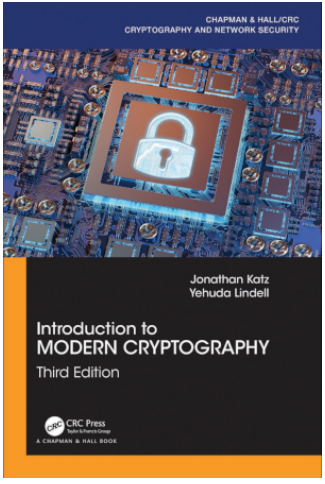
教材及参考书

教材：

- Introduction to Modern Cryptography, 3rd ed., Jonathan Katz and Yehuda Lindell, 2021.

参考书：

- 《密码编码学与网络安全：原理与实践》，电子工业出版社
- The Joy of Cryptography, Mike Rosulek, 2022.
- Foundations of Cryptography, Oded Goldreich, 2004.



课程简介

- 学时：32 学时，9–16 周
- 成绩：作业（50%）+ 闭卷考试（50%）（注：博士生不必参加考试，但要交作业）

作业：二选一

作业一

设计并实现一个与密码学相关的简单系统，例如加密聊天、可搜索加密、隐匿查询、隐私计算等，要求：

- 源码：github 或 gitee 上创建一个代码库，readme 中有项目简介。
- 演示：录一个简单的演示视频，上传到 B 站（视频最后给出学号）。
- 成绩：70 – 100

作业二

选择本课程的一个知识点，录个短视频进行讲述，要求：

- 形式：通过动画的形式介绍（例如使用 Manim 库），有配音。
- 时长：不短于 3 分钟，上传到 B 站（视频最后给出学号）。
- 成绩：60 – 90

- 作业提交：思源学堂 https://lms.xjtu.edu.cn/user/courses
- 提交时间：下学期开学前

目录

中国古代加密技术：姜子牙阴符

(? – 1015BC 或 1036BC)

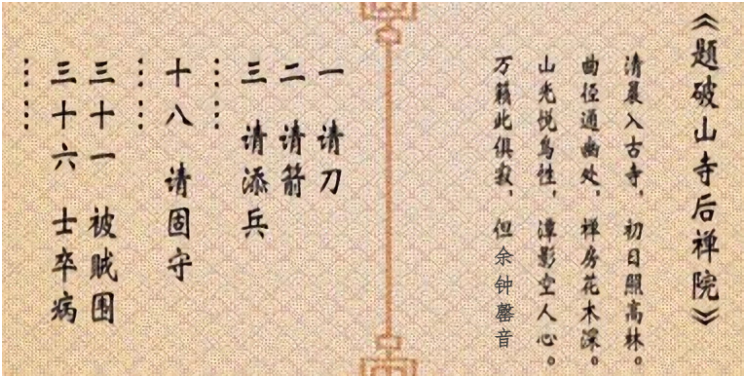
太公曰：主与将，有阴符，凡八等。有大胜克敌之符，长一尺。破军擒将之符，长九寸。降城得邑之符，长八寸。却敌报远之符，长七寸。警众坚守之符，长六寸。请粮益兵之符，长五寸。败军亡将之符，长四寸。失利亡士之符，长三寸。诸奉使行符，稽留，若符事闻，泄告者，皆诛之。八符者，主将秘闻，所以阴通言语，不泄中外相知之术。敌虽圣智，莫之能识。

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**。

奥古斯特 · 柯克霍夫

柯克霍夫准则

一个加密系统是安全的，即便关于该系统除密钥之外的所有算法都公开。A cryptographic system should be secure even if everything about the system, except the key, is public knowledge.

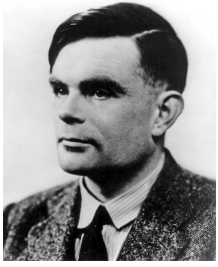
William Friedman

- 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。

威廉 · 弗里德曼

Alan Turing 与 Enigma 密码机的破译

- 阿兰 · 图灵（Alan Turing，1912–1954），英国数学家、逻辑学家，被视为计算机之父。
- 1931 年图灵进入剑桥大学国王学院，毕业后到美国普林斯顿大学攻读博士学位。二战爆发后回到剑桥，协助军方破解德国的著名密码系统 Enigma，帮助盟军取得二战的胜利。
- 1936 年，图灵在论文“论数字计算在决断难题中的应用”中给“可计算性”下了一个严格的数学定义，并提出著名的“图灵机”设想。

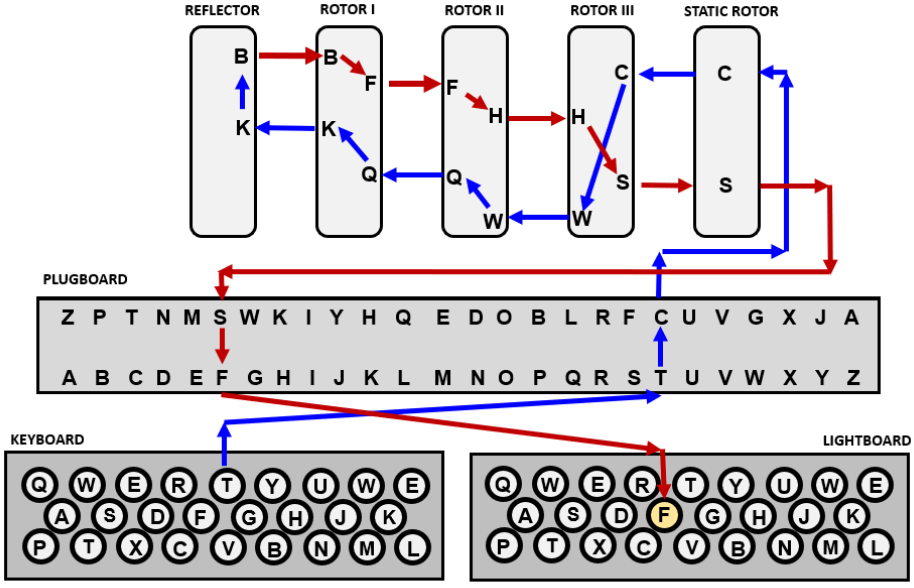


阿兰 · 图灵

- 1952 年图灵因同性恋被判重罪；1954 年死于氰化物中毒。
- 2009 年时任英国首相戈登 · 布朗发布致歉声明；2013 年英国女王伊丽莎白二世签署了图灵的赦免令。

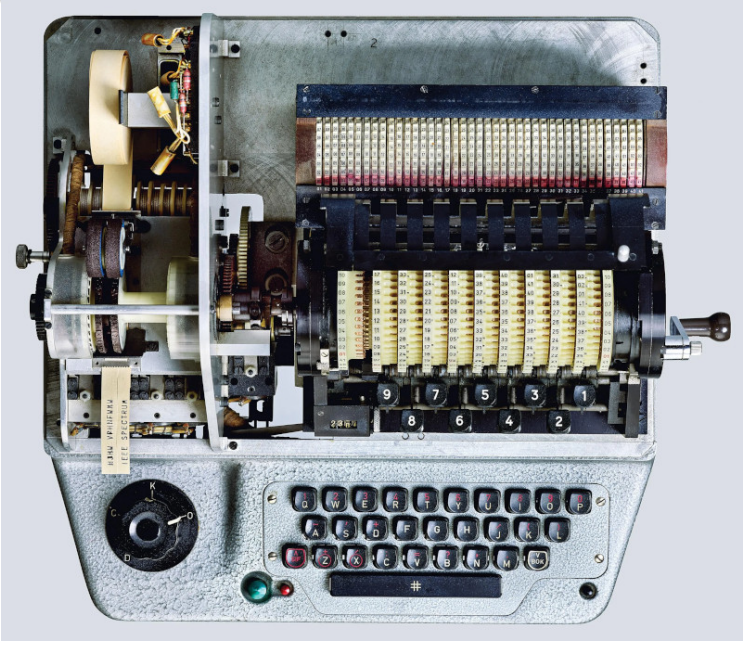
Enigma 密码机与古德里安的“闪电战”

Enigma 密码机原理



The path taken by a letter through an Enigma machine as it is encrypted

Enigma 密码机其他型号（HX-63）



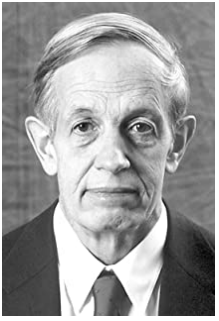
Claude Shannon 与分组密码设计的准则

- 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）的绝对安全。
- 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）。

克劳德 · 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

真正重要的是攻击是否在计算上不可行，而不是攻击是否完全不可能。It doesn't really matter whether attacks are impossible, only whether attacks are computational infeasible.

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 Networks。
- Feistel 网络激发了 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

644 IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

New Directions in Cryptography

Invited Paper

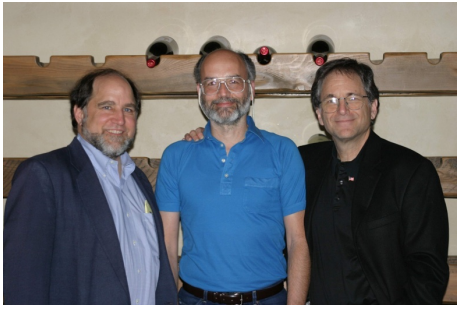
WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

***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，是目前唯一获得该奖的华人学者。
- 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。

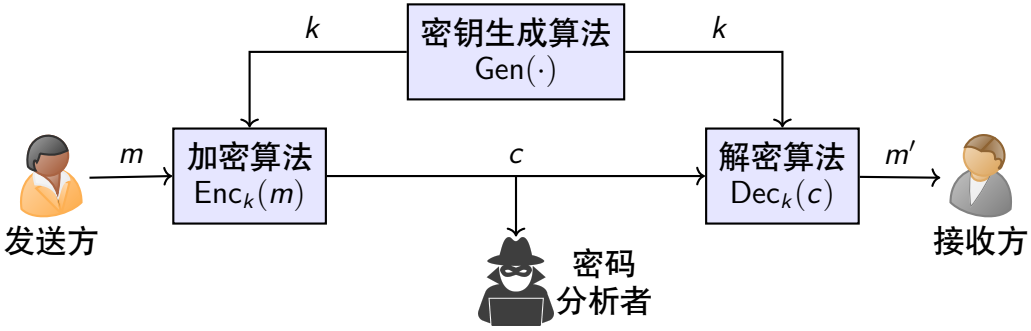
姚期智

目录

密码学基本术语

- Cryptology：保密学，源自希腊语；
- Cryptography：密码编码学，研究如何将明文转换为密文；
- Cryptanalysis：密码分析学，研究如何破译密文得到明文或获得密钥；
- Cipher：加密方法；
- Encipher, encryption：将明文转换成密文的过程；
- Decipher, decryption：将密文还原成明文的过程；
- Plaintext (cleartext)：原始的可读数据，称为消息或明文；
- Ciphertext (cryptogram)：加密后得到的密文；
- Key：密钥，对加密与解密过程进行控制的参数

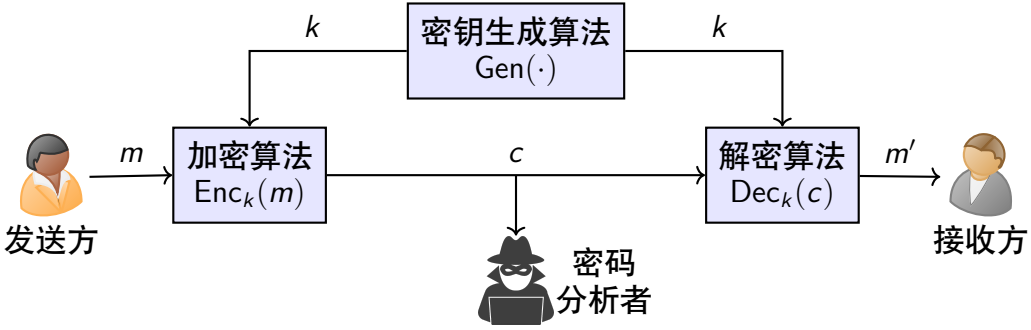
私钥密码（Private-Key Encryption）



由定义在空间 $(\mathcal{K}, \mathcal{M}, \mathcal{C})$ 上的运算 $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ 构成

- $\mathcal{K}$ 为密钥空间，$\mathcal{M}$ 为明文空间，$\mathcal{C}$ 为密文空间
- $\mathsf{Gen}\colon \{0,1\}^* \mapsto \mathcal{K}$ 为密钥生成函数
- $\mathsf{Enc}\colon \mathcal{K} \times \mathcal{M} \mapsto \mathcal{C}$ 为加密运算，并且 $c = \mathsf{Enc}_k(m)$
- $\mathsf{Dec}\colon \mathcal{K} \times \mathcal{C} \mapsto \mathcal{M}$ 为解密运算，并且 $m = \mathsf{Dec}_k(c)$

私钥密码的要求



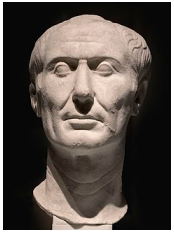
- **正确性**：$\mathrm{Dec}_k(\mathrm{Enc}_k(m)) = m$
- **保密性**：由密文或明密文推测密钥和明文，在计算上不可行。
- **计算效率**：加解密算法的计算效率应足够高，便于系统实现。
- **Kerckhoffs 准则**：系统的安全性不依赖于对加解密算法的保密，而是密钥。

目录

目录

凯撒密码（Caesar Cipher）

- 已知最早的代换密码是由古罗马时期的 Julius Caesar 发明的凯撒密码 (Caesar Cipher)，用于加密作战命令。

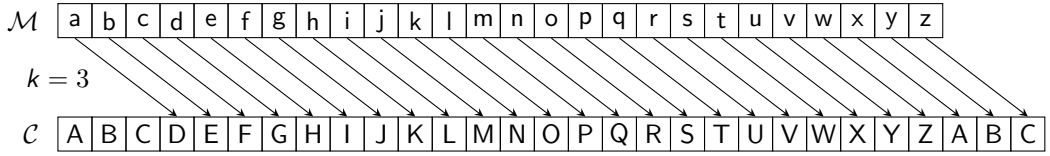


(公元前 100 年 – 公元前 44 年)

There are also letters of his to Cicero, as well as to his intimates on private affairs, and in the latter, if he had anything confidential to say, he wrote it in cipher, that is, by so changing the order of the letters of the alphabet, that not a word could be made out...

The Lives of the Caesars, the Deified Julius (110CE)

凯撒密码



- **加密**：将每个明文字母向右循环移 3 位

$$c = \mathsf{Enc}_k(m) \triangleq (m + 3) \bmod 26$$

- **解密**：对密文进行相反操作

$$m = \mathsf{Dec}_k(c) \triangleq (c - 3) \bmod 26$$

例 (凯撒密码加密)

利用凯撒密码加密 “begin the attack now”，忽略空格，得到密文

EHJLQWKHDWWDFNQRZ

目录

移位密码（Shift Cipher）

- 凯撒密码其实不存在密钥，任何知道凯撒密码算法的人都可以轻易破解密码。
- 移位密码对凯撒密码进行改进，引入密钥 $k \in \{0, \ldots, 25\}$，表示循环移位的位数。

$$\text{加密：}\ c = \mathsf{Enc}_k(m) \triangleq (m + k) \bmod 26$$

$$\text{解密：}\ m = \mathsf{Dec}_k(c) \triangleq (c - k) \bmod 26$$

- 移位密码的安全性如何？

例（破解移位密码）

尝试破解密文 EHJLQWKHDWWDFNQRZ

移位密码的安全性

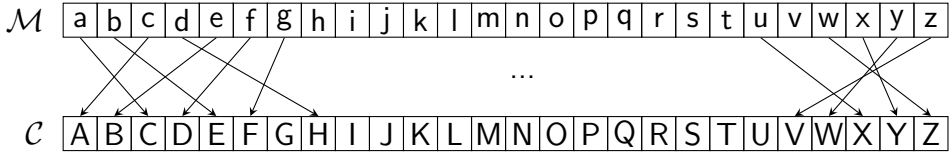
- 移位密码的密钥空间大小为 26。
- 容易对密钥空间进行穷举攻击（brute-force attack）。
- 一个密码体制安全的必要条件是密钥空间要足够大。

k	尝试解密后
0	ehjlqwkhdwwdfnqrz
1	dgikpvjgcvvcempqy
2	cfhjouifbuubdlopx
3	begintheattacknow
4	adfhmsgdzsszbjmnv
5	zceglrfcyrryailmu
	...

目录

单表代换密码 (The Mono-Alphabeta Substitution Cipher)

- 为增强移位密码的安全性，设计代换表时可以不仅仅是依次替换，而是允许任意替换，称为单表代换密码。
- 单表代换中每个明文字母可以映射到任意一个密文字母，密钥是 26 个字母的任意置换。
- 密钥空间大小为 $|\mathcal{K}| = 26! > 4 \times 10^{26}$。



单表代换密码举例

例

使用代换表：

```
plaintext:  abcdefghijklmnopqrstuvwxyz
ciphertext: DKVQFIBJWPESCXHTMYAUOLRGZN
```

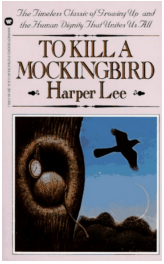
对消息 “if we wish to replace letters” 进行加密：

```
plaintext:  ifwewishtoreplaceletters
ciphertext: WIRFRWAJUHYFTSDVFSFUUFYA
```

问题

? 单表代换密码的密钥空间大小为 $|\mathcal{K}| = 26! > 4 \times 10^{26}$，似乎已经足够大了，单表代换密码是否真的安全？

《杀死一只知更鸟》：哈珀 · 李著长篇小说

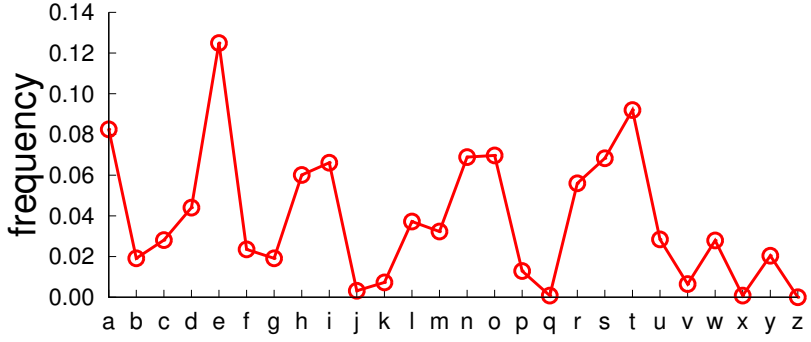


When he was nearly thirteen, my brother Jem got his arm badly broken at the elbow. When it healed, and Jem's fears of never being able to play football were assuaged, he was seldom self-conscious about his injury. His left arm was somewhat shorter than his right; when he stood or walked, the back of his hand was at right angles to his body, his thumb parallel to his thigh. He couldn't have cared less, so long as he could pass and punt.

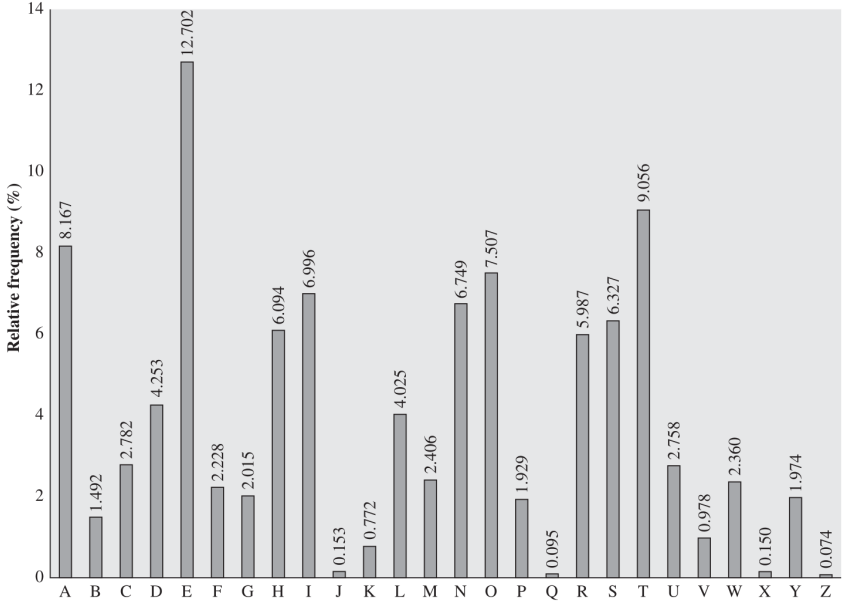
When enough years had gone by to enable us to look back on them, we sometimes discussed the events leading to his accident. I maintain that the Ewells started it all, but Jem, who was four years my senior, said it started long before that. He said it began the summer Dill came to us, when Dill first gave us the idea of making Boo Radley come out.

I said if he wanted to take a broad view of the thing, it really began with Andrew Jackson. If General Jackson hadn't run the Creeks up the creek, Simon Finch would never have paddled up the Alabama, and where would we be if he hadn't? We were far too old to settle an argument with a fist-fight, so we consulted Atticus. Our father said we were both right.

Maycomb was an old town, but it was a tired old town when I first knew it. In rainy weather the streets turned to red slop; grass grew on the sidewalks, the courthouse sagged in the square. Somehow, it was hotter then: a black dog suffered on a summer's day; bony mules hitched to Hoover carts flicked flies in the sweltering shade of the live oaks on the square. Men's stiff collars wilted by nine in the morning. Ladies bathed before noon, after their three-o'clock naps, and by nightfall were like soft teacakes with frostings of sweat and sweet talcum.



英文字母的相对使用频率



利用语言的统计特性进行密码分析

- 单表代换密码的密钥空间看似足够大，可以抵御穷举攻击，其实不然，这是因为语言往往具有统计特性。
- 人类的语言是有冗余性的，字母使用的频率并不一样：英文字母 E 是使用最频繁，然后是 T, R, N, I, O, A, S 等；有些字母使用得很少，如 Z, J, K, Q, X；双字母也有统计特性，例如 TH 等。
- 这样可以得到英文字母使用频率分布表，最早由阿拉伯科学家在公元九世纪发现。
- 单表代换不能掩盖字母出现的频率，只要统计密文中字母出现的频率，与已知的统计值做比较就可以分析出明密文字母的对应关系。

单表代换密码攻击举例

例

- 给定密文：

  UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSX
  AIZVUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
  EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

- 统计相关字母出现的次数，可以猜测 P 和 Z 是 e 和 t，ZW 是 th，这样 ZWP 就是 the。

- 这样反复试验并不断修正错误，最后可得：

  it was disclosed yesterday that several informal but direct contacts have been made with political representatives of the viet cong in moscow

目录

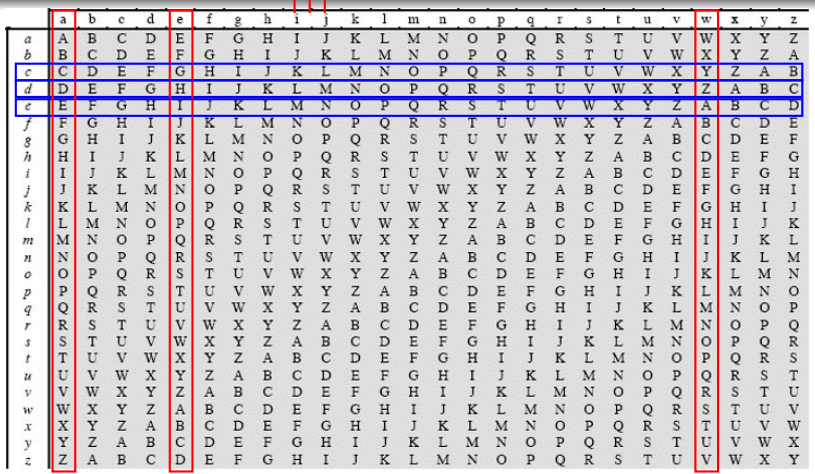
Vigenère 密码

- 多表代换密码：使用多个代换表对明文消息进行多重单表代换加密。
- Vigenère 密码的代换规则集由 26 个凯撒密码的代换表组成，每个代换表对明文字母移位 $0 \sim 25$ 次。
- 密钥词中的密钥字母用来代换明文字母 a，故移位 3 次的凯撒密码由密钥字母 d 代表。
- 加密一条消息需要与消息一样长的密钥，通过重复密钥实现。
- 加密：给定密钥字母 x 和明文字母 y，密文字母是位于 x 行和 y 列的那个字母。
- 解密：密钥字母决定行，行里密文字母所在列的顶部字母就是明文字母。

Vigenère 密码举例

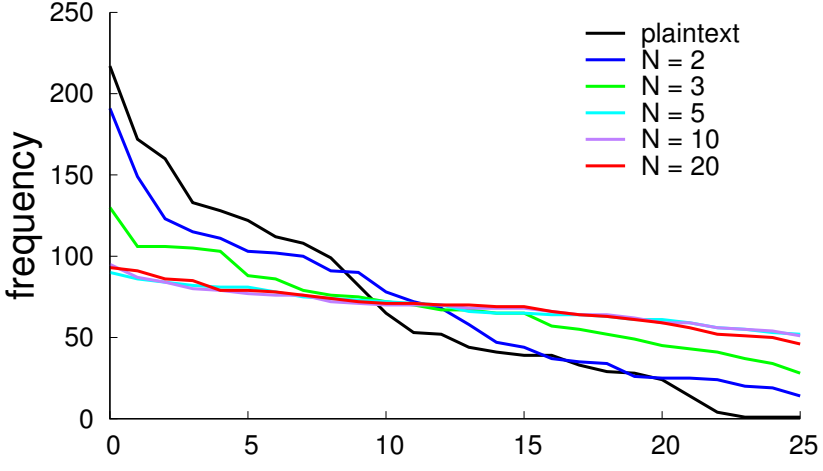
例 (使用密钥词 deceptive)

```
key:        deceptivedeceptivedeceptive
plaintext:  wearediscoveredsaveyourself
ciphertext: ZICVTWQNGRZGVTWAVZHCQYGLMGJ
```



Vigenère 密码的安全性

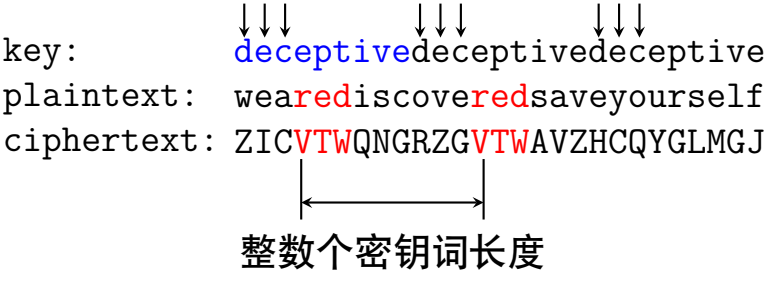
- 每一个明文字母可以有多个密文字母对应，这样字母使用的频率特性减弱了，但是没有完全消失。



横轴为 26 个字母，N 为密钥词长度

Vigenère 密码的安全性

- 如果知道密钥词长度，那么对 Vigenère 密码的攻击可以转化为对多个单表代换密码的攻击。
- 破译的关键是确定密钥词的长度，可以通过发现密文重复序列来判断。
- 重复的密文片段相距整数个密钥词长度。



最终措施是选择与明文毫无统计关系且和它一样长的密钥。

目录

一次一密（One-Time Pad）

- 一次一密（One-Time Pad，简称 OTP）：
  - 每个消息使用与之等长且随机的密钥来加密。
  - 一个密钥只对一个消息加解密，之后弃之不用。
- OTP 满足绝对安全，是不可攻破的。
- 1882 年 Frank Miller 首次描述了 OTP，之后又被其他人再次发明。Gilbert Vernam 在 1919 年申请了基于异或运算的 OTP 的专利。
- 在 1900 年以前的密码学研究中，只有两个想法对现代密码学有用，其中之一为柯克霍夫准则，另外一个则为一次一密。
- 古巴导弹危机之后，1963 年，美苏两国启用“红色电话”专线，使用一次一密进行通信加密。

一次一密（One-Time Pad）

- OTP 运算基于二进制数据而非字母。
- **密钥生成算法** Gen：$k \leftarrow \{0,1\}^{|m|}$
- **加密**：

$$\mathsf{Enc}_k(m) \triangleq m \oplus k$$

- **解密**：

$$\mathsf{Dec}_k(c) \triangleq c \oplus k$$

x	y	$x \oplus y$
0	0	0
0	1	1
1	0	1
1	1	0

- **正确性**：

$$\mathsf{Dec}_k(\mathsf{Enc}_k(m)) = \mathsf{Dec}_k(m \oplus k) = m \oplus k \oplus k = m$$

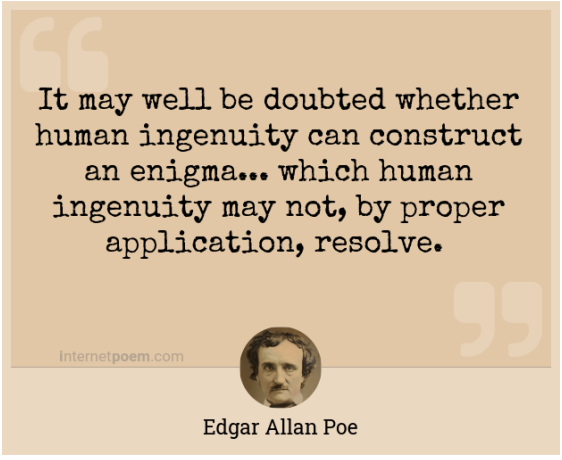
- **局限性**：
  - 产生大规模随机密钥有实际困难。
  - 密钥的分配和保护无法保证。

目录

目录

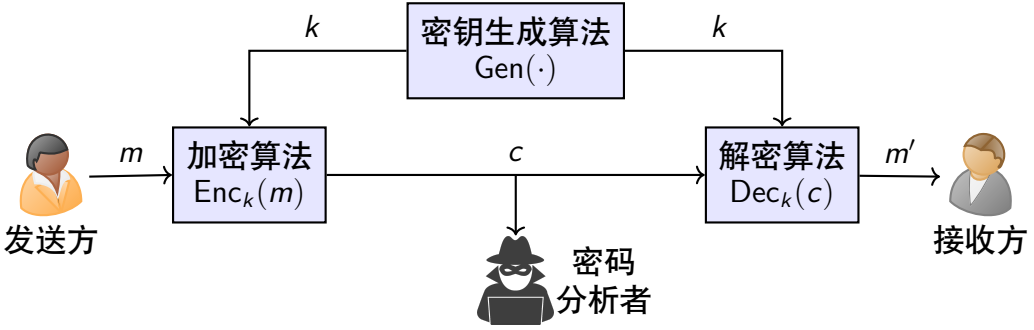
是否存在绝对安全的密码体制？

- 1841 年，悲观主义者认为：没有绝对安全的密码，人类无法构建一个无法攻破的密码。



- 需严格定义什么是安全，包括两部分：安全定义和威胁模型。

安全定义应该考虑什么？



- 敌手不能恢复加密体制所使用的密钥。
- 敌手不能由密文恢复关于明文的任何额外信息。

威胁模型：敌手具备什么能力？

对密码分析者攻击能力的假设：除了知道加解密算法，还知道下面信息：

- 唯密文攻击：知道密文；
- 已知明文攻击：知道密文，还知道一些明密文对；
- 选择明文攻击：知道密文，且可选择一些明密文对用于密码分析；
- 选择密文攻击：知道密文，且可选择一些密文及其对应明文用于密码分析；
- 选择文本攻击：同时可选择明文或选择密文。

从上往下，密码分析者的攻击能力逐渐增强。

目录

绝对安全（Perfect Security）

- 用随机变量 K, M, C 表示发送方可能使用的密钥、发送的消息以及对应的密文。
- 假设敌手事先知道

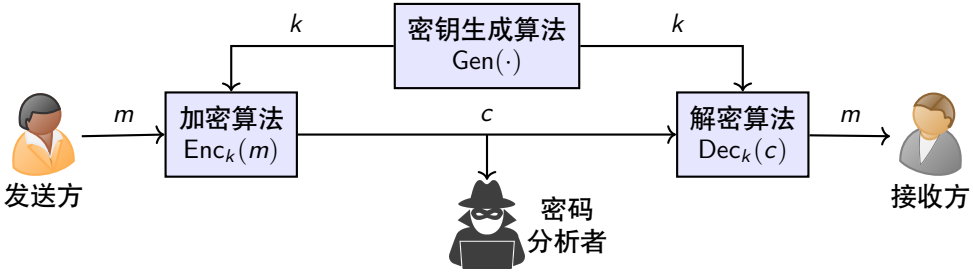
$$P(M = \text{“attack today”}) = 0.6$$
$$P(M = \text{“don't attack”}) = 0.4$$

- 敌手截获密文 $C = c$，经过分析，然后修正概率为

$$P(M = \text{“attack today”}) = 0.8$$
$$P(M = \text{“don't attack”}) = 0.2$$

- 能否说明发送方使用的密码体制是安全的？
- 不能！

绝对安全的定义



定义 (绝对安全、完美安全、理论安全、Perfect Security)

一个密码体制 $\Pi = (\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ 是绝对安全的，当且仅当对于任意密文 $c \in \mathcal{C}$ 且 $P(C = c) > 0$，有

$$P(M = m | C = c) = P(M = m)$$

- 敌手无法根据密文获知关于明文的任何额外信息。
- 敌手得到的关于明文的后验概率等于先验概率。

举例：移位密码是否绝对安全

例 (移位密码)

- 考虑一个特殊的移位密码，明文空间为 $\mathcal{M} = \{aa, ab\}$，发送方发送 aa 或 ab 的概率不为零。
- 假设敌手截获的密文为 $c = XX$，那么根据移位密码的特点，敌手得到
$$P(M = ab|C = XX) = 0$$
- 从而
$$P(M = ab|C = XX) \neq P(M = ab)$$
- 说明移位密码不满足绝对安全的定义。

绝对安全的一个等价定义

定理 (绝对安全的等价定义)

一个密码体制 $\Pi = (Gen, Enc, Dec)$ 是绝对安全的，当且仅当对于任意明文 $m, m' \in \mathcal{M}$，都有

$$P(Enc_K(m) = c) = P(Enc_K(m') = c)$$

证明.

对于任意 $m \in \mathcal{M}$ 且 $P(M = m) > 0$，对于任意 $c \in \mathcal{C}$，有

$$\begin{aligned} P(C = c|M = m) &= P(\mathrm{Enc}_K(M) = c|M = m) \\ &= P(\mathrm{Enc}_K(m) = c|M = m) \\ &= P(\mathrm{Enc}_K(m) = c) \end{aligned} \tag{1}$$

对于任意 $c \in \mathcal{C}$ 且 $P(C = c) > 0$，有

$$P(M = m|C = c)P(C = c) = P(C = c|M = m)P(M = m) \tag{2}$$

绝对安全的一个等价定义

$\Rightarrow$ (必要性)：如果 Π 绝对安全，那么 $P(M = m|C = c) = P(M = m)$，由式 (2) 得

$$P(C = c|M = m) = P(C = c)$$

由式 (1) 得

$$\begin{aligned} P(\mathrm{Enc}_K(m) = c) &= P(C = c|M = m) \\ &= P(C = c) \\ &= P(C = c|M = m') \\ &= P(\mathrm{Enc}_K(m') = c) \end{aligned}$$

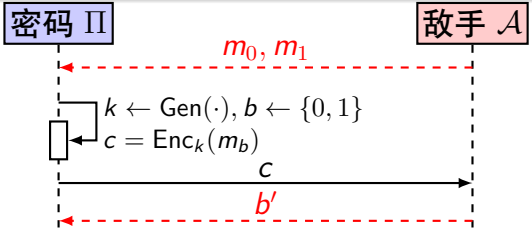
绝对安全的一个等价定义

$\Leftarrow$ (**充分性**): 令 $p_c \triangleq P(\mathrm{Enc}_K(m) = c)$, 式 (1) 表明 $P(C = c|M = m') = p_c$。

$$\begin{aligned} P(C = c) &= \sum_{m' \in \mathcal{M}} P(C = c|M = m')P(M = m') \\ &= \sum_{m' \in \mathcal{M}} p_c P(M = m') \\ &= p_c \\ &= P(C = c|M = m) \end{aligned}$$

再由式 (2) 得 $P(M = m|C = c) = P(M = m)$。

绝对安全的博弈描述



当 $b' = b$ 时，敌手成功，记为 $\mathrm{PrivK}^{eav}_{\mathcal{A},\Pi} = 1$。

定义 (绝对不可区分，Perfect Indistinguish)

一个密码体制 $\Pi = (\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ 满足绝对不可区分，当且仅当对于任意敌手 $\mathcal{A}$，有

$$P(\mathrm{PrivK}^{eav}_{\mathcal{A},\Pi} = 1) = \frac{1}{2}$$

定理

一个密码体制 Π 是绝对安全的当且仅当 Π 是绝对不可区分的。

一次一密（OTP）满足绝对安全

定理

一次一密是绝对安全的。

证明.

用 ℓ 表示明文、密文和密钥的二进制串比特数。对于任意 $m \in \mathcal{M}$ 且 $P(M = m) > 0$，有

$$\begin{aligned} P(\mathsf{Enc}_K(m) = c) &= P(C = c | M = m) \\ &= P(K \oplus m = c | M = m) \\ &= P(K = m \oplus c | M = m) \\ &= 2^{-\ell} \end{aligned}$$

说明对任意 $m, m' \in \mathcal{M}$，有 $P(\mathsf{Enc}_K(m) = c) = P(\mathsf{Enc}_K(m') = c)$，所以绝对安全。

一次一密（OTP）满足绝对安全

- 1917 年 Vernam 申请了 OTP 的专利。25 年后，香农给出了绝对安全的定义，并证明 OTP 满足绝对安全。
- OTP 被用于古巴导弹危机之后美苏两国之间的加密通信——红色电话。
- OTP 的局限性在于要求密钥长度必须和消息长度相等。有时通信双方并不知道发送的消息的长度，因此难以事先准备足够长的密钥。
- OTP 的另一个缺点是密钥只能使用一次，否则会导致不安全：假如两个消息 m 和 m' 都使用相同密钥 k 加密，得到密文 c 和 c'，那么

$$c \oplus c' = (m \oplus k) \oplus (m' \oplus k) = m \oplus m'$$

因此会泄露两个消息之间的关系。

绝对安全的局限性

定理 (香农定理)

如果密码体制 $\Pi = (Gen, Enc, Dec)$ 绝对安全，则 $|\mathcal{K}| \geq |\mathcal{M}|$。

证明.

- 只需证明当 $|\mathcal{K}| < |\mathcal{M}|$ 时，密码体制 Π 不是绝对安全的。
- 令 $\mathcal{M}(c) \triangleq \{m | m = \mathrm{Dec}_k(c), k \in \mathcal{K}\}$，显然 $|\mathcal{M}(c)| \leq |\mathcal{K}|$。
- 如果 $|\mathcal{K}| < |\mathcal{M}|$，则存在 $m' \in \mathcal{M} \backslash \mathcal{M}(c)$，满足
$$P(M = m' | C = c) = 0 \neq P(M = m')$$
因此 Π 不是绝对安全的。

- 要达到绝对安全，密钥长度不能小于明文长度。
- 不可能用短密钥实现绝对安全，导致绝对安全的密码不实用。

小结

1. 课程简介
2. 发展历史
3. 基本概念
4. 古典密码
5. 安全性定义