密码学发展简史及其数学原理

彭煜 数学与统计学院 2021302011116 15327763310

June 2023

目录

1 内容摘要 **3**

2 关键词 **3**

3 密码学历史简述 **3**

3.1 古典密码学 3

3.2 近代密码学 4

3.3 现代密码学 4

4 密码学历史上的数学家 **5**

4.1 肯迪 5

4.1.1 凯撒密码 5

4.1.2 肯迪频度分析 6

4.2 香农 7

4.2.1 香农信息论 7

4.2.2 信息论发展 8

4.3 狄菲赫尔曼 9

4.3.1 RSA 方法 9

4.3.2 狄菲-赫尔曼理论意义 10

5 密码学与现代社会 **10**

5.1 密码学与现代社会发展 10

5.2 密码学发展趋势 11

5.3 密码学是一把双刃剑 11

6 参考文献 **11**

1 内容摘要

本文先简要介绍了一下密码学的发展历史的三个阶段；接下来阐释一些密码学历史上出现的数学家所提出的理念或做出的重大贡献，解释其中密码学的数学原理；最后分析了密码学在目前的发展态势以及对人类社会产生的影响。

2 关键词

密码学历史、数学语言、信息、加密。

3 密码学历史简述

密码学离人类生活并不遥远，其实早在古埃及时代人类就开始使用密码了，人类掌握密码的历史几乎同文字一样长久。

密码学的发展变迁大致可以分为 3 个阶段:1949 年以前称为古典密码学阶段; 1949 年至 1975 年密码学成为科学的分支，称为近代密码学阶段;1976 年以后对称密钥密码算法得到进一步发展，产生了密码学的新方向—公钥密码学，称为现代密码学阶段。

3.1 古典密码学

古典密码学是一种传统的密码学方法，它涉及使用各种技术和工具来加密和解密信息。在古典密码学中，主要使用了替换和重排字母的方法来隐藏原始信息。

古典密码学的其中一种形式是凯撒密码，它是一种移位密码。凯撒密码通过将字母按照指定的位数向右或向左移动来加密消息。例如，如果将字母按照位数 3 向右移动，那么字母 A 将被替换为 D，B 将被替换为 E，以此类推。

古典密码学还包括一种称为换位密码的方法。在换位密码中，字母的顺序被重新排列，而不是进行替换。其中一个著名的换位密码是栅栏密码，它将消息按照一定规则放置在栅栏上，然后按照特定的顺序逐个读取。

这一时期的密码学更像是一门艺术，其核心手段是代换和置换。代换是指明文中的每一个字符被替换成密文中的另一个字符，接收者对密文做反向替换便可恢复出明文；置换是密文和明文字母保持相同，但顺序被打乱。

3.2 近代密码学

近代密码学是指在 20 世纪出现的一种密码学方法，相较于古典密码学更加复杂和安全。近代密码学主要包括对称加密和公钥密码学两种主要方法。

对称加密是一种使用同一个密钥进行加密与解密的方法。发送方使用该密钥对消息进行加密，然后接收方使用相同的密钥对密文进行解密。常见的对称加密算法有 DES AES 和 $RC4$ 等。对称加密具有高效性和速度优势，但需要在发送和接收方之间安全地共享密钥。

公钥密码学使用了一对密钥，其中一个是公钥，用于加密消息；另一个是私钥（也称为密钥），用于解密消息。发送方使用接收方的公钥来加密消息，只有接收方才能使用其私钥来解密。常见的公钥密码学算法有 RSA DSA 和 ECC 等。

近代密码学还涉及到消息认证码（MAC）和数字签名等技术来确保消息的完整性和真实性。MAC 是一种通过对消息应用密钥相关的函数生成的固定长度代码，用于验证消息是否被篡改。数字签名通过使用发送方的私钥对消息进行加密来确保消息的真实性和不可否认性。

近代密码学的方法基于复杂的数学和计算机科学原理，通过更强大的算法和密钥管理技术来提供更高的安全性。这些方法广泛应用于网络通信、电子支付、数据存储和保护个人隐私等领域。

3.3 现代密码学

现代密码学是指在当今时代使用的密码学方法，它是基于复杂的数学和计算机科学原理发展起来的。现代密码学采用了更强大和安全的算法，并使用更复杂的密钥管理技术来确保信息的保密性和完整性。

现代密码学主要包括对称加密和公钥密码学两种主要方法。

在对称加密中，发送方和接收方使用相同的密钥进行加密和解密。常见的对称加密算法有高级加密标准（AES）和数据加密标准（DES），它们被广泛应用于保护数据的机密性。

公钥密码学使用一对密钥，其中一个是公钥，另一个是私钥。发送方使用接收方的公钥进行加密，而接收方使用自己的私钥进行解密。公钥密码学提供了更强大的安全性和更好的密钥管理，常见的公钥密码学算法有 RSA 和椭圆曲线密码学（ECC）。

现代密码学还涉及到数字签名、消息认证码（MAC）和哈希函数等重要技术。数字签名用于验证消息的真实性和不可否认性，消息认证码用于验证消息的完整性，而哈希函数用于将任意长度的消息转换为固定长度的编码，以便进行校验和比较。

现代密码学在保护网络通信、电子支付、数据存储和隐私保护等领域起着重要作用。它不断演进和发展，以应对日益复杂的安全威胁和攻击技术。

4 密码学历史上的数学家

4.1 肯迪

4.1.1 凯撒密码

尤利乌斯 · 凯撒在秘密信函里使用过一种简单的密码，被用于传递军事机密。他生活的那个时代，字母表里没有字母 J、U 和 W，我们仍使用现代字母表来解释一下背后的数学原理。其思路是，先按常规顺序把字母表写下来，然后在它下面写一个移位的字母表，例如：

$$A\ B\ C\ D\ E\ F\ G\ H\ I\ J\ K\ L\ M\ N\ O\ P\ Q\ R\ S\ T\ U\ V\ W\ X\ Y\ Z$$

$$F\ G\ H\ I\ J\ K\ L\ M\ N\ O\ P\ Q\ R\ S\ T\ U\ V\ W\ X\ Y\ Z\ A\ B\ C\ D\ E$$

也就是说，$A \to F$,$B \to G$ 以此类推 $\cdots$ 为了破译密码，则需要得到逆关系。为了制作一种将字母绕在环上的实用机械装置，我们可以把字母放置在一个圆环或圆筒上。

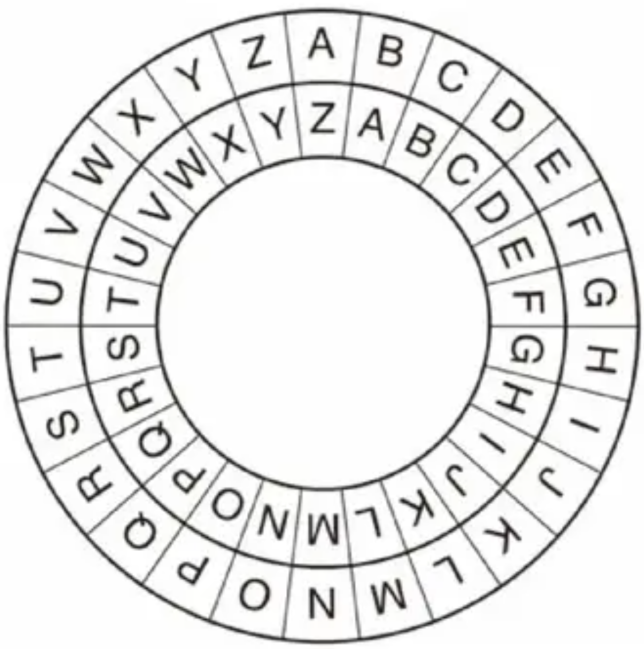

图 1: 字母环

利用模运算，我们可以将凯撒密码完全转化为数学语言。这种情形下模数等于 26，即字母表上字母的个数。用数字 $0 \to 25$ 代表字母 $A \to Z$，即 $A = 0$、$B = 1$、$C = 2$，以此类推 $\cdots$ 直至 $Z = 25$。把 A（位置 0）移动到 F（位置 5）的加密过程就是数学规则

$$n \to n + 5 \ mod \ 26$$

解密过程也有类似的规则：

$$n \to n - 5 \ mod \ 26$$

这是因为 $n + 5 - 5 = nmod26$，所以解密把加密还原了。一般来说，当密钥为 k 时，意味着“向右移动 k 步”，于是加密过程的规则成了：

$$n \to n + k \ mod \ 26$$

而解密的规则是：

$$n \to n - k \ mod \ 26$$

把密码转换成数学语言的优点在于，我们可以用一种精确的方式来描述密码，并分析它们的性质，同时还不必考虑字母本身。与此同时，我们也可以考虑其他符号，如小写字母 $a\ b\ c \cdots$，以及标点符号，还有数字。只要把 26 换成特定数字即可，再确定如何分配这些数。

4.1.2 肯迪频度分析

肯迪完成了对凯撒密码的破解。在英语里，最常见的字母是 E，它大约占全部出现频率的 13%；接下来是 T，大约是 9%；再往下是 A，大约是 8%，等等。如果你截取了一段很长的密文，并猜测它是通过打乱字母表的方法生成的，那么就能计算所有字母的频率。由于文本各式各样，因此它们或许并不能和理论值精确地吻合。但是，比方说，如果在密文里的字母 Q 出现得比其他字母更频繁，那么你可以试着用 E 代替 Q。如果接下来最常见的字母是 M，那么试试看用 T 代替 M 结果会怎样，以此类推。当然，你还可以微调它们的顺序。即便如此，你需要尝试的可能性也会少很多。

这种方式被称为频度分析，它的出现对凯撒密码的安全性是非常大的打击。肯迪于 9 世纪的“破译加密信息手稿”（$Manuscript\ on\ Deciphering\ Cryptographic\ Messages$），其包含利用统计数据与频率分析的详细讨论，这可以视为统计学与密码分析学科的诞生。

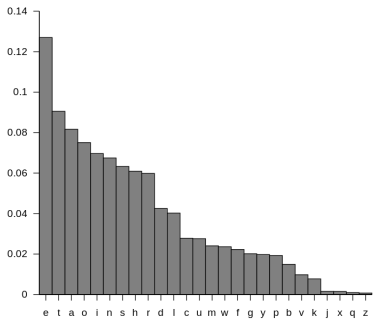

图 2: 英文明文字母出现频率

4.2 香农

4.2.1 香农信息论

在第二次世界大战期间，香农对密码术产生了极大的兴趣，他意识到对密码术根本性问题的研究与他当时正在研究的通信理论的思想密切相关。他的许多成果在语音加密装备中有着重要的应用，而该装备是罗斯福和丘吉尔在战争期间使用的主要通信工具。1945 年，香农向贝尔实验室提交了一份机密文件，题目是《$A\ Mathematical\ Theory\ of\ Cryptography$》，这一成果在第二次世界大战结束后的 1949 年以《$Communication\ Theory\ of\ Secrecy\ Systems$》为题目正式发表，这一篇论文为对称密码系统的研究建立了一套数学理论——香农信息论，从此密码术成为了密码学，由一门艺术成为一门真正的科学。

香农信息论主要研究信息传输和通信系统的基本原理。香农信息论的内容包括信息的度量、信道容量、编码理论和误差校正等方面。

香农提出了度量信息量的概念，使用信息熵（$Entropy$）来衡量信息的不确定性和随机性。信息熵越高，表示信息越无序和随机，反之，信息熵越低，表示信息越有序和确定。这一概念对于理解信息的传输和压缩具有重要意义。

香农还提出了信道容量的概念，表示在给定的传输信道条件下，能够传输的最大信息速率。信道容量与信噪比、带宽等信道特性密切相关，对于设计和优化通信系统具有重要指导意义。

编码理论是香农信息论的另一个关键内容，它研究如何将信息进行编码以实现高效的传输和存储。通过使用适当的编码技术，如霍夫曼编码、香农-费诺编码等，可以达到信息压缩和纠错的目的。

香农信息论对通信、数据压缩和存储、语言处理等领域产生了深远的影响。它提供了一种定量的方式来理解和分析信息的特性，为现代通信系统的设计和优化提供了理论基础。此外，香农信息论的概念和方法也被广泛应用于计算机科学、统计学和人工智能等领域。

4.2.2 信息论发展

在香农发表这篇论文后，信息论迅速成为了一个独立的数学领域。在接下来的几十年中，许多学者在这个领域中做出了重要的贡献，推动了信息论的发展。信息论的发展随着科学技术的进步而不断演进。在香农之后，人们进一步研究了通过引入纠错码、调制技术和多用户通信等方法来提高信息传输的效率和可靠性。同时，量子信息论的发展使得信息论的范围扩展到了量子通信和量子计算等领域。信息论的发展为人们更好地理解和应用信息提供了理论基础，它在现代科学和技术发展中发挥着重要的作用。

1. 噪声信道编码定理:

在香农的论文中，他提出了一个基本的通信模型，即发送方将信息编码为信号，然后将信号传输到接收方，接收方将信号解码回原始信息。然而，在实际通信中，信号往往受到噪声的干扰，这使得信号的解码变得非常困难。为了解决这个问题，$R.Gallager$ 在 1963 年提出了噪声信道编码定理。这个定理表明，只要编码长度足够长，就可以通过编码来最小化噪声对信号的影响。

2. 压缩理论:

在信息论中，压缩理论涉及到如何将信息编码为更紧凑的格式，以便更有效地存储和传输。$D.Huffman$ 在 1952 年提出了一种将信息压缩为最小长度的方法，这个方法被称为霍夫曼编码。霍夫曼编码是一种基于信息的概率分布来进行编码的方法，它可以用于压缩各种类型的数据，如文本、图像、音频等。

3. 通信复杂度

在信息论中，通信复杂度是指在通信过程中所需的最小通信成本。$A.Wyner$ 在 1975 年提出了一种新的方法来计算通信复杂度，这个方法被称为 $Wyner-Ziv$ 定理。$Wyner-Ziv$ 定理表明，如果发送方和接收方都知道一些关于信息的概率分布的信息，那么在某些情况下，可以使用一种称为“分布式压缩”的方法来降低通信成本。

4. 信息论在计算机科学中的应用

信息论在计算机科学中的应用非常广泛，例如，数据压缩、加密、错误检测和校正等。其中，最著名的应用之一是在计算机网络中使用的 TCP/IP 协议。TCP/IP 协议是 $Internet$ 中最常用的网络协议，它是基于信息论的思想来设计的。通过使用序列号和确认号来跟踪数据包的传输，以及使用冗余校验和来检测和校正错误，TCP/IP 协议可以保证数据传输的可靠性和完整性。

4.3 狄菲赫尔曼

4.3.1 RSA 方法

在密码学发展的历史上，1976 年是一个值得纪念的年份. 这一年，美国斯坦福大学年轻的数学家狄菲 ($Diffie$) 和计算机专家赫尔曼 ($Hellman$) 联名发表了《密码学的新方向》一文，开创了现代密码学的新领域——公开密钥体制 (简称公钥体制)。30 年来，公钥体制获得了巨大的发展，它不仅消解了传统的秘密密钥体制存在的一些困难，而且解决了信息安全的一些问题，推动了包括电子商务在内的一大批网络应用的深入和发展。

这种开创性的思想引进了密码学中的全新方法——RSA 方法。非对称加密算法中，有两个密钥：公钥和私钥。它们是一对，如果用公钥进行加密，只有用对应的私钥才能解密；如果用私钥进行加密，只有用对应的公钥才能解密。

非对称加密算法实现机密信息的交换过程为：甲方生成一对密钥并将其中一个作为公钥向其他方公开；得到该公钥的乙方使用该密钥对机密信息进行加密后发送给甲方；甲方再用自己的另一个专用密钥对加密后的信息进行解密。最有名的非对称加密算法当属 RSA 了。

RSA 定理与数论息息相关，定理内容为：p,q 是不同的素数，$n=pq$，$\varphi(n)=(p-1)(q-1)$，如果 e,d 是与 $\varphi(n)$ 互素的两个正整数，并满足 $ed\equiv 1(mod\ \varphi(n))$，则对于每个整数 x，都有 $x^{ed}\equiv x(mod\ n)$。

现在我们简述 RSA 公钥体制的原理:

(1) 取两个超过 100 位的大整数 p 和 q，求出 $n=pq$ 和 $\varphi(n)=(p-1)(q-1)$ 的值。

(2) 选一个与 $\varphi(n)$ 互素的正整数 e，解同余方程 $ed\equiv 1(mod\ \varphi(n))$，得到解 d，则 $\{e\ d\}$ 是可供一个用户使用的密钥对. 其中 e 为公钥，d 为私钥。

(3) 构造两个定义域为 $(0,1,2\cdots,n-1)$ 的函数：$E(x)=x^e(mod\ n)$ 为加密函数，$D(x)=x^d(mod\ n)$ 为解密函数。

(4) 根据 RSA 定理，$D(E(x))=D(x^e)=(x^e)^d=x^{ed}\equiv x(mod\ n)$，即在 $D(x)$ 和 $E(x)$ 的作用下，经加密和解密后，明文信息 x 变换为密文 y 后又恢复为明文 x. 所以 $E(x)$ 和 $D(x)$ 是互逆的。

(5) 把供某用户使用的私钥 d 交该用户，并将其公钥 e 和 n 公开，$\varphi(n)$ 则由密钥制作者

秘密保管。

(6) 别的用户要与该用户秘密通信时，先将明文信息 x 用该用户的公钥 e 建立的加密函数 $E(x)$ 加密，得密文 $y = E(x) \equiv x^e (mod\ n)$，该用户收到密文 y 后，用自己的私钥 d 建立解密函数 $D(x)$ 解密，得明文 $x = D(y) \equiv y^d (mod\ n) \equiv (x^e)^d \equiv x^{ed} \equiv x (mod\ n)$。

4.3.2 狄菲-赫尔曼理论意义

在《密码学的新方向》一文中，狄菲和和赫尔曼提出了一个算法，揭示了非对称或公共密钥加密存在的可能性。在这一理论中，一个公钥，不用再进行保密，加密后可自由分配，而一个私人密钥，不能离开接收设备，以此用于解密。在这个非对称的密码系统中，私钥虽然也来自公共密钥，但是难以通过计算得到。而解密过程需要提供一个电子签名（或数字签名）。消息发送器可使用私钥签署消息，而接收者使用发送器的公钥来验证它。这样的数字签名比书面签名更安全，因为即使是改变一个词的信息，也是无效签名。相比之下，一个人的 10 美元支票的书面签名同他的 100 万美元支票签名看起来很像。

事实上，互联网中的任何用户对这种通过公开密钥加密建立的安全连接并不陌生。一个典型的安全 URL 始于“$https$”, 其中的“s”意味着安全传输层协议（$Secure\ Transport\ Layer\ Protocol$）将用于加密通信。安全连接通过使用一个公开密钥加密组合来传输一个对称加密且随后通信的密钥。狄菲和赫尔曼的工作，除了为当前的网络通信安全行业打下了基础，以及为计算机科学建立密码学外，它还使得加密技术走入个人和商业公司的日常世界。

5 密码学与现代社会

5.1 密码学与现代社会发展

密码学在现代社会的发展起到了至关重要的作用。随着信息技术的迅猛发展，人们越来越依赖于数字通信和电子数据存储。密码学通过提供保密性、完整性和认证等安全保障，帮助我们在网络通信、电子支付、数据存储和隐私保护等方面进行安全操作。

密码学与现代社会的发展密切相关。随着互联网的普及和数字化的加速，许多关键领域的安全性成为重要问题，例如网络安全、电子商务和个人隐私。密码学提供了一种保护信息和数据安全的手段，帮助社会在数字化时代保持稳定和安全。

5.2 密码学发展趋势

密码学在现代社会的发展趋势是朝着更强大和更高效的算法以及更安全的密钥管理技术方向前进。近年来，量子密码学成为密码学领域的新兴研究方向，旨在应对未来可能出现的量子计算攻击。量子密码学利用量子力学原理来实现更高级别的保密性和安全性。

然而，密码学发展也面临一些局限性。其中一个是算法的安全性问题。随着计算技术的不断进步，某些算法的安全性可能受到威胁。因此，密码学需要不断更新和改进算法，以应对新的安全挑战。

5.3 密码学是一把双刃剑

密码学的发展既有利又有弊。优点是它提供了保护个人和组织机密信息的方法，确保数据的完整性和真实性。它为企业和个人提供了一种安全通信和信息交换的方式，为经济和社会发展提供支持。然而，密码学的弊端在于，一些恶意人士可能滥用密码学技术来进行非法活动，例如网络攻击和勒索软件。因此，密码学需要在保护安全的前提下进行合理使用和监管，以维护社会秩序和个人权益。

6 参考文献

[1] 密码学发展简史——$https://link.zhihu.com/target = https\%3A//github.com/guoshijiang/cryptography/blob/master/history/README.md$.

[2] 舒昌勇.RSA 公开密钥体制及其主要数学基础. 数学通报.2008 年. 第 47 卷. 第 6 期.

[3] 最新图灵奖宣布：得主贡献在于互联网加密 - 饶毅的文章 - 知乎 https://zhuanlan.zhihu.com/p/20616996

[4] 信息的奥秘：从香农到信息论的发展历程 - 知乎用户 qFA1DD 的文章 - 知乎 https://zhuanlan.zhihu.com/p/619703613

[5] 伊恩 · 斯图尔特（Ian Stewart）.Professor Stewart's Incredible Numbers. 图灵新知