密码学理论发展与进步

古代加密方式

在这个阶段算法和密钥都是保密的，但是密钥空间较小。[1]信息传递过程的安全性主要依赖于加密和解密的 算法保密。古典密码加密阶段经历漫长的发展历史，最大的特点就是依靠算法进行手工加密和解密。因此，这一阶段也称之为手工加密时代。比较为我们熟知的便是凯撒密码和斯巴达手杖。

凯撒密码：运用数学方法进行信息替换。C=f(m,k)=m+k mod26，它利用单表替换的思想，即即将一个信息符号通过单射函数替换为另一个符号。不过，由于单表替换不够安全，只要能够收集到足够多的密文，通过统计学方法就能够很容易地进行密码的破译。因此，也有科学家提出了更复杂的多表替代密码，如维吉尼亚密码。

维吉尼亚密码技术使用一个词组作为密钥,词组中的每一个字母都作为移位替换密码的密钥并确定一个替换表,然后循环地使用每一个替换表完成明文字母到密文字母的转换。

加密函数：Ci=Pi+Ki(mod 26)

解密函数：Pi=Ci-Ki(mod 26)

古代加密方式大多基于替换和置换的思想，虽然能有针对性设计算法，但是安全性有所提高。

近代密码

近代密码指的是20世纪初到1949年的加密方式，其主要标志是机械密码/机电密码，用机电代替手工，最著名的就是转轮机（RotorMachine）。

转轮密码机ENIGMA[2]，由ArthurScherbius于1919年发明，4轮PNIGMA在1944年装备德国海军。使得英国从1942年2月到12月都没能解读德国潜艇的信号。



图一：ENIGMA

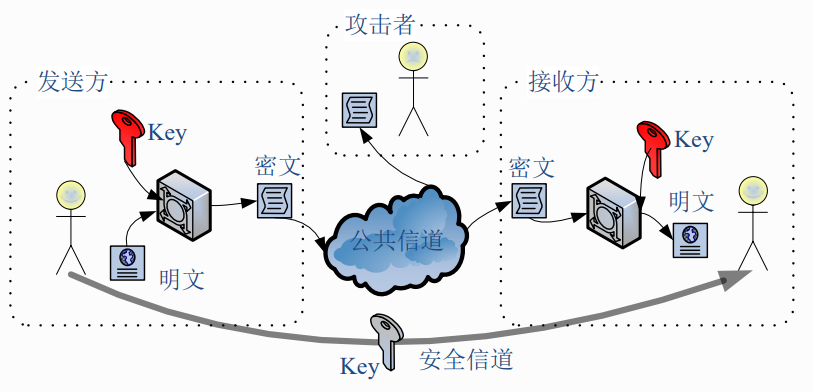
ENIGMA相较于普通的代替密码复杂性更强，随机性更高，效率更高。

现代密码

现代密码学主要分为对称加密阶段和公钥加密阶段。这一时期不仅依赖于数学和密钥，更加复杂的加密方式被引入了密码学中，极大提高了密码学的丰富度。

对称加密

对称加密方式中，信息的安全性主要依赖于对密钥的保密。对称加密指加密和解密使用相同密钥的算法。一方面，加密密钥可以从解密密钥中计算出来，同时解密密钥也可以从加密密钥中推演出来。由此，加密密钥和解密密钥是相同的，称之为“对称密码阶段”或者“单钥密码阶段”。信息的发送与接收双方应该协商好密钥，如果双方任何一方保存密钥不谨慎（或者故意泄露），那么传递信息将存在不安全性。



图二：对称加密

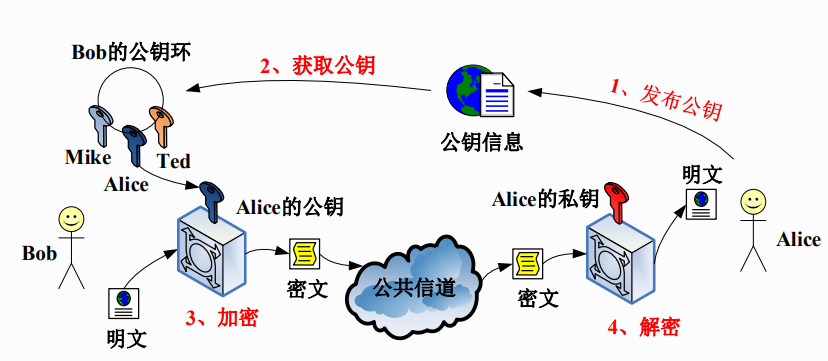
对称加密虽然相比较非对称加密存在劣势，但是依旧广泛的应用的电脑与信息技术中。目前主要的对称加密的算法有：DES、3DES、AES、IDEA等。

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 算法名称 | 特征 | 实用性 |
| 1 | DES | 最传统的对称加密 | 安全性低，基本不用 |
| 2 | 3DES | 安全性较DES高，效率低 | 很少使用 |
| 3 | AES | 密钥建立时间短，灵敏性高，内存占用少，安全性高 | 利用频率高 |
| 4 | IDEA | 加密速度更快，安全性更好 | 用于电子邮件加密 |

表一：对称加密体制下算法分析表

公钥加密

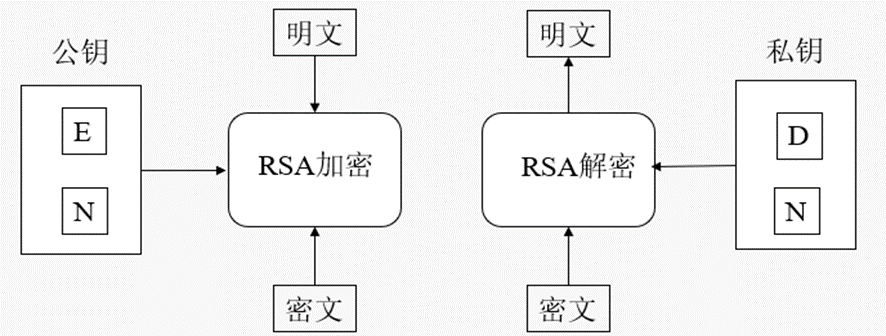
在公钥密码阶段，加密密钥（公钥）可以公开，仅对解密密钥（私钥）保密，基于一些数学难题保证很难通过公钥推出私钥。因此，公钥密码也被称为非对称加密。与对称加密体制下的算法不同，非对称加密算法在信息传递的过程中，需要两个密钥：一个是公开密钥(Public Key)；；另一个是私有密钥（Private Key）。如果用公开密钥对需要传递的信息与数据进行加密，只有用对应的私有密钥才能解密；相反，如果用私有密钥对需要传递的信息与数据进行加密，那么信息的接收方必须用对应的公开密钥进行解密。



图三：公钥加密

常见的公钥加密算法有RSA,DSA,ECC等。

1. RSA[3]是目前最具影响力的公钥加密方法，该算法基于将两大素数相乘，但是对其乘积所得进行因式分解很复杂。由此可见，通过两个素数乘积公开作为加密密钥操作简单，即公钥，两大素数的组合称之为私钥。但是不可否认的是，在同样安全级别条件下，RSA相对于对称加密算法速度慢很多，相当于1/1000左右。



图四：RSA加密

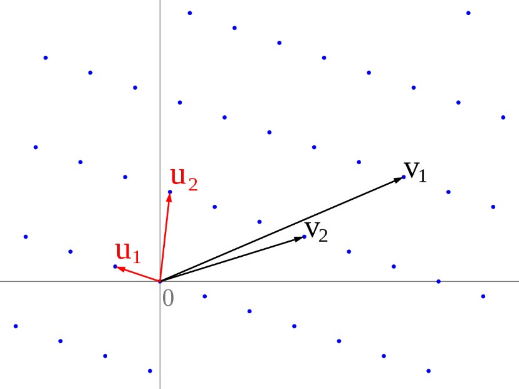
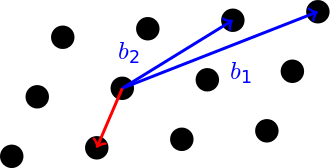
1. DSA（全称Digital Signature Algorithm）, 是一种更加高级的验证方式，其主要特点是不单单有公钥、私钥，还有数字签名。私钥加密生成数字签名，公钥需要同时验证数据与签名，如果数据或者签名与私钥不匹配，被认为验证失败。
2. ECC（称之为椭圆加密算法），是一种公钥加密算法，采用的数学基础理论是利用椭圆曲线上的有理点构成Abel加法群上椭圆离散对数的计算困难性。其主要优势是使用更小的密钥，提供更高级别的安全性。 例如，160位的椭圆密钥与1024位的RSA密钥安全性相同。此外，ECC的处理速度要比RSA更快，存储空间更小。

后量子密码

后量子密码学（Post-quantum cryptography，缩写：PQC）[4]，又称抗量子计算密码学，是密码学的一个研究领域，专门研究能够抵抗量子计算机的加密算法，特别是公钥加密（非对称加密）算法。不同于量子密码学，后量子密码学使用现有的电子计算机，不依靠量子力学，它依靠的是密码学家认为无法被量子计算机有效解决的计算难题。

后量子密码学的研究方向包括了格密码学（Lattice-based cryptography）、容错学习问题（LWE）、多变量密码学（Multivariate cryptography）等，密码学家认为，基于这些计算难题有望构建出不受量子计算机的威胁的公钥加密系统，替代现有的方案。

格密码学是在算法构造本身或其安全性证明中应用到格的密码学。格（lattice (group)）（lattice），又称点阵，是群论中的数学对象，可以直观地理解为空间中的点以固定间隔组成的排列，它具有周期性的结构。更准确地说，是在n维空间Rn中加法群的离散子群，这一数学对象有许多应用，其中存在几个称为“格问题（Lattice problems）”的难题，如最短向量问题（Shortest Vector Problem）和最近向量问题（Closest Vector Problem）。



图五：格密码

容错学习问题在密码学上的应用[5]：

A是一个m x n矩阵，s是一个n维向量，e是一个m维向量。我们定义LWE(s,e) = b = As + e。由此可以构造一个对称加密算法。

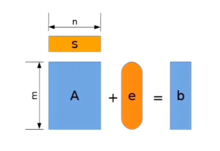
加密算法定义如下:

s作为密钥k使用；

(A,e)这一组数据在加密时随机生成；

由s, A, e所求得的值b作为一次性密码本的密钥使用，同密文m进行异或操作。

这一算法和传统对称密钥加密算法的区别的关键在于，加密方不将误差数据e传送给解密方，导致解密方所解得明文存在一个小的误差。

图六：容错学习的密码学应用

[1]王伟然,刘志波.密码学与加密技术的发展历程及提升路径[J].数字技术与应用,2022,40(01):237-239.DOI:10.19695/j.cnki.cn12-1369.2022.01.76.

[2] Smart N P. The enigma machine[M]//Cryptography Made Simple. Springer, Cham, 2016: 133-161.

[3] Boneh D. Twenty years of attacks on the RSA cryptosystem[J]. Notices of the AMS, 1999, 46(2): 203-213.

[4] Bernstein D J, Lange T. Post-quantum cryptography[J]. Nature, 2017, 549(7671): 188-194.

[5] Regev O. The learning with errors problem[J]. Invited survey in CCC, 2010, 7(30): 11.