中图分类号:TN918.1 文献标识码:A 文章编号:1007-9416(2022)01-0237-03
DOI:10.19695/j.cnki.cn12-1369.2022.01.76

密码学与加密技术的发展历程及提升路径

武警河北省总队综合信息保障中心 王伟然 刘志波

本研究通过文献分析法，从历史的角度将密码学归纳为三个阶段：古典密码学阶段、现代密码学的对称密码阶段、现代密码学的公钥密码阶段。文章分别阐述了不同发展阶段的“加解密”算法，以及各类算法的优缺点。我们认为密码学的可持续发展，离不开数学以及通讯信息技术的基础性支持，从而针对不同领域的密码技术需求，做出不同的发展战略。

1 密码学发展历程

密码学（源于希腊语krypt ó s“隐藏的”），主要是研究如何隐密地传递信息的学科。著名密码学家Ron Rivest曾经直白、生动的将密码学归纳定义为“如何实现在敌人存在的环境中通讯”。这一定义显然是旨在军事领域的信息传递，避免被敌方截获与破解。但是，在互联网与大数据时代，密码学不仅仅应用于军事领域，同时强有力地渗透到人们生活的方方面面，如商业领域与政府治理领域。密码学的发展与计算机科学技术的发展相辅相成，彼此促进，大数据背景下，公民、法人及组织的各方面公共事务与私人事务，均需要网络安全技术，这对密码学的发展提出了更高的要求。

严格意义上讲，密码学包括两个部分：一是编码学，即致力于编制密码，从而达到保密的效果；二是破译学，主要是通过破译密码的手段与技术，截获通信情报。随着科学技术的不断突破与发展，密码学中的加密算法与密钥性能也在不断提升，从而大大地增加了信息传递的安全与保密程度。大体上，密码学的发展经历了以下三个阶段[1]如图1所示。

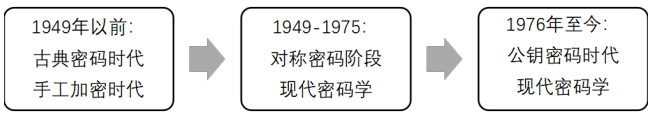

图1 密码学的发展历程

Fig.1 The history of cryptography

第一阶段：古典密码阶段（1949年前）。

在这个阶段算法和密钥都是保密的，但是密钥空间较小。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。

第二阶段：对称密码阶段（1949—1975年）。

这段时间，也称之为现代密码学的阶段，和古典密码阶段的主要区别在于这个阶段的加密和解密算法无需保密，但信息的安全性主要依赖于对密钥的保密。这一阶段，也称之为现代密码学的传统密码算法。对称加密指加密和解密使用相同密钥的加密算法。即一方面，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。

第三阶段：公钥密码阶段（1976年—至今）。

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。1976年，美国学者Dime和Heman提出发送信息与接收信息双方在交换信息，可以在不安全环境下的媒体上进行，这种方法为 “非对称加密算法”。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）。公私两个密钥之间的关系可以简单的总结为“一对”。公私两种密钥之间的具体的关系可以解释为：一是，如果用公开密钥对需要传递的信息与数据进

收稿日期:2021-11-06

作者简介:王伟然(1985—),男,河北廊坊人,本科,助理工程师,研究方向:网络信息安全。

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。由此可见，在这一阶段，加密和解密需要使用的是两个不同的密钥，由此称之为非对称加密算法。

在此阶段，非对称加密安全性更好，非对称在加密与解密的过程中使用的是“一对密钥”，一个用来信息传递方对数据进行加密，另一个信息接收方对数据进行解密。此外，非对称加密的另一个优势是：公钥是公开的，私钥是自己保存的，不需要像对称加密那样在通信之前要先同步密钥。在对称密钥时代，由于双方共享使用的是相同的密钥，如果一方泄露，信息将存在被盗取、泄密的风险[2]。非对称密钥大大地规避了这种风险的存在。

2 对称加密体制下算法的应用

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[3]。对称加密体制下算法分析表如表1所示。

（1）DES算法，是最传统的对称加密体制下的算法，奠定了对称加密算法的基础。但是目前为止，DES算法已经被全面破解，由此该算法不再安全，甚至已经基本放弃使用。例如，在企业商务领域，基本上没有企业应用了。

（2）3DES(3重DES，Triple DES,DEsede),在DES被破解之后，DEsede用于代替DES的使用。对一块数据用三个不同的密钥进行三次加密，相比较DES强度更高。该加密技术计算密钥时间长、加密效率低下，随着计算机科学技术的发展，直至今日也基本上被弃用了。

（3）AES，也是在对称加密体制下被利用的频率最高的算法。这种算法密钥建立时间短、灵敏性高、内存占用少、安全性高。在实际使用中，工作模式通常是CTR，引用16个字节数组的IV参数，密钥长度128/192/256。

（4）IDEA,相比较DES与3DES，加密速度更快，安全性更好，常用于电子邮件的加密。IDEA密钥长度为128位，数据块大小为64bit,是一种“轮次加密”技术，密钥经过多轮扩展参加“加解密”流程。从理论上讲，IDEA属于“强”加密算法，具有较高的安全性。

3 非对称加密体制下算法的应用

非对称加密技术相比较对称加密具有很大的优势，保密效果好，算法相对复杂[4]。目前为止，主要的算法有RSA、DSA、ECC等[5]。非对称加密体制下算法列表如表2所示。

（1）RSA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

表1 对称加密体制下算法分析表

Tab.1 Algorithm analysis table under symmetric encryption system

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，基本弃用
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2 非对称加密体制下算法列表

Tab.2 List of algorithms under asymmetric encryption

序号	算法名称	特征	实用性
1	RSA	最具影响力，操作简单，加密速度慢	适用各种安全或认证领域
2	DSA	更高级，但速度慢；需要“公钥+私钥+数字签名”	适用于数字签名于认证
3	ECC	更小密钥，更高级别安全性；存储空间小	适用于互联网领域

左右。

（2）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。

（3）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。

4 密码学的发展展望

纵观密码学的发展，我们发现：(1)密码算法得到了快速发展，提升了信息传递的安全性。(2)我们应该看到不同的密码体制，以及不同密码加密解密算法，在不同领域得到了应用。我们应该继续深入基础性研究，如密码学算法的数学基础，发展数学等基础性学科，扎实投入，从而为密码学算法的可持续发展提供理论与学科基础。(3)不同领域，如军事领域、企业商务领域、政府行政管理领域、个人信息传递领域，对密码学中加密解密技术的需求不同，由此密码学的各种算法，应该针对不同领域需求的差异性，并找寻不同的发展方向、制定不同的发展策略。

引用

[1] 王宝仓,贾文娟,陈艳格.密码学现状、应用及发展趋势[J].无线电通信技术,2019,45(1):1-8.

[2] 谢宗晓,董坤祥,甄杰.国产商用对称密码算法及其相关标准介绍[J]. 中国质量与标准导报,2021(4):14-16.

[3] 李青,陈靓,冯梅,等.浅析几种典型数据加密算法[J].中信息系统工程,2017(11):148-149.

[4] 杨帅航,何进荣.数据加技术在计算机网络数据安全中的应用[J].延安大学学报（自然科学版）,2021,40(3):78-82.

[5] 杨波.现代密码学[M].北京:清华大学出版社,2017.

……上接第206页

3 集成平台面临的问题

3.1 异构数据整合

由于医院信息系统在建设初期并未考虑后期的系统集成，所以不同系统多由不同的厂商开发，使用的数据标准也不一致，这就导致医院信息系统集成平台建设难度大，协调成本高。所以医院在建设信息系统集成平台时应重视顶层设计，定义好平台主数据，以患者为中心，以流程优化为导向，建设一种标准化、语义化的信息处理平台，为临床诊疗提供重要的技术支撑。

3.2 安全问题

医院信息系统集成平台在各系统互联互通、数据共享和调用的过程中，如未对数据进行严格的加密处理就会发生信息泄漏的风险，所以在集成平台建设的过程中要重视数据安全的问题，采取多种加密措施，防止患者信息泄露。

3.3 不易扩展

集成平台建设之前，某系统功能扩展只需要在本系统内考虑如何实现，集成平台建设后，若想扩展某一系统的某一功能需综合考虑各个系统，扩展成本高、难度大。

4 结语

医院信息平台既是实现院内各信息系统间互联互通的基础设施，也是实现区域内各级医院间信息共享与业务系统的前提条件[3]。在大数据时代，我们要充分利用信息系统集成平台收集到的海量医疗数据，利用数据挖掘技术，挖掘数据背后的潜在价值，为临床诊疗提供强大的支持。

引用

[1] 黄跃,魏岚,张蕾,等.基于大数据的医院信息集成平台建设与应用[J].中国医学装备,2019,16(4):103-105.

[2] 王文成.集成平台在医院信息系统集成中的应用[J].中国信息界,2020(5):86-89.

[3] 李伟,张麟,王爱娥,等.国内医院信息平台现状及解决方案分析[J].医疗卫生装备,2018,39(2):96-102.