**密码学发展简史**

金洋

（云南大学 数学与统计学院 信息与计算科学，学号20131910023）

**摘 要** 密码学是研究如何隐密、安全地传递信息的学科。本文对密码学的发展历史做了简单的介绍，密码学的发展大致经历了对通信本身保密、对密码算法和密钥保密、对密钥保密、对解密密钥保密四个阶段，可以看出密码系统的特点是趋向简单化、公开化。

**关键词** 密码学； 算法； 密钥； 对称密码体制； 非对称密码体制

**1 引言**

自从有了人类社会就有了信息交流，远距离的信息交流称为通信。通信的内容对国家安全、经济发展、军事行动都有非常重要的意义，所以人们需要进行保密通信，即采取某些技术使用公开的通信工具传递秘密的消息，以确保通信双方传递的消息只有通信双方知道，第三方无法知晓。

密码学的发展史可谓源远流长。但在1949年以前，密码的研究与应用没有形成一门科学，仅是一门文字变换艺术。1949年，Shannon发表了“保密系统的通信理论(Communication Theory of Secrecy Systems)”一文[1]，为密码学的发展奠定了坚定的数学理论基础，因此，此后的密码研究才真正称得上是密码学。

密码系统的特点是趋向简单化、公开化，密码系统的发展大致经历了如下过程：

①对通信本身保密；

②对密码算法和密钥保密；

③对密钥保密；

④对解密密钥保密[2]；

本文对密码学发展的介绍也将按照这个顺序展开。

**2 对通信本身保密**

从古代到19世纪末，通信的方式多种多样，为了传递一则消息，常使用不同的载体记载密文进行传送。例如将密文隐藏于食物中。还有使用“矾书”这种隐写术来隐藏消息的办法：矾书就是用明矾水写的书信，当水干后，纸上毫无字迹，把纸弄湿后，字迹即可重新显现。这样直接对通信本身保密，可以使第三方难以察觉两方之间发生了通信从而起到保密效果。

然而，可以用来藏匿密文的载体、手段必定有限，一旦时间一长令第三方生疑，第三方只需对有可能藏匿消息的地方进行一一排查即可窃取通信内容。

**3对密码算法和密钥保密**

对通信本身保密的办法不再安全后，人们开始希望设计出一种密码体制——即使通信内容被第三方窃取，但第三方却无法知晓通信内容。

公元前约50年，罗马皇帝Julius Caesar发明了一种用于战时秘密通信的方法——凯撒密码。他将字母表按顺序构成环，加密将明文中的每个字母用其后的第5个字母代替，解密时只需把密文中每个字母用其前的第5个字母代替即得明文[3]。

这样一来，只需通信双方事先知道这种替换算法和密钥5就可以实现保密通信。即使这封信被送信的人看了，或者被敌军截获，那么他们也很难弄懂信的内容到底是什么，因为密码算法和密钥是保密的。

**4对密钥保密**

**4.1 从古典密码到现代密码**

一个密码体制如果需要同时依赖于密码算法和密钥的保密，那么这将带来如下两点不便：

①加密算法/解密算法的长度比密钥长得多，维护算法的保密性很难；

②当密码算法不公开，那么只能由发行者将算法定制成一种硬件或软件，秘密制造，然后在不公开其构造的情况下统一分发给使用者。但是密码分析者可以用反汇编代码或逆向设计工程的方法得到密码算法的实现过程。

因此，如果密码系统的安全强度依赖于攻击者不知晓的密码算法，那么这个密码系统最终注定失败。荷兰密码学家Auguste Kerckhoffs于1883年曾阐明了关于密码分析的一个基本假设——秘密必须完全寓于密钥中，即加密和解密算法的安全性取决于密钥的安全性，而加密/解密的过程和细节（算法的实现过程）是公开的，只要密钥是安全的，那么攻击者就无法推导明文[4]。密码算法是否公开，这也是现代密码体制和古典密码的根本区别。

“如果许多聪明人都不能解决的问题，那么它可能不会很快得到解决”，这是密码学界普遍承认的一个事实，它说明了目前许多密码算法的安全性并没有在理论上得到严格的证明，但是该算法经过许多人若干年的攻击并没有发现目前科技水平下的弱点或漏洞，没有找到攻击它的有效方法，从而被认为是安全的。

**4.2** **对称密码体制**

对称密码体制要求通信双方拥有相同且对第三方保密的密钥。Whitefield与Martin Hellman在1976年提出了一个奇妙的密钥交换协议，称为Diffie-Hellman密钥交换协议。这个机制的巧妙在于需要安全通信的双方可以用这个方法确定对称密钥，然后可以用这个密钥进行加密和解密。其安全性基于求有限域上离散对数的难度。

由于受历史的限制，上世纪70年代中期以前的密码学都是在军事、政府等重要部门秘密进行。密码学的真正蓬勃发展和广泛应用是从70年代中期开始的。1973年，美国国家安全局认识到建立数据加密标准的迫切性，开始征集联邦数据加密标准。最后IBM的Lucifer加密系统获得了征用。经过两年多的公开讨论，1977年1月15日美国国家安全局决定使用该算法，并将其改名为数据加密标准（DES），不久其他组织也认可并采用DES作为加密算法供商业和非国防性政府部门使用。1997年开始征集高级加密标准AES，2000年选定由比利时计算机科学家Vincent Rijmen和Joan Daemen开发设计的Rijndael算法作为新标准。数据加密标准完全公开了加密、解密算法，使得密码学得以在商业等民用领域广泛应用，从而给这门学科带来了巨大的生命力，得到了迅速发展。

**5对解密密钥保密**

**5.1 非对称密码体制**

对称密码体制的缺点在于密钥分发和管理困难。在1976年，Diffie和Hellman发表了《密码学的新方向》，提出了一个崭新的思想，不仅密码算法可以公开，而且加密密钥也可以公开，这就是非对称密码体制的思想。这篇论文为现代密码学的发展开辟了一个新的思路，标志着非对称密码体制的诞生。

非对称密码体制的安全强度取决于它所依据的问题的计算复杂度。目前比较流行的非对称密钥加密算法主要有两类：一类是基于大整数因子分解问题的，其中最典型的代表是RSA算法；另一类是基于离散对数问题的，如Elgamal加密算法等。

**5.2 RSA密码体制**

在非对称密码思想提出后的1978年，美国麻省理工学院的Ron Rivest, Adi Shamir, Leonard Adleman提出了RSA公钥密码体制。RSA是第一个比较完善的非对称密码算法，它既能用于加密，也能用于数字签名。这个算法经受住了多年深入的密码分析，虽然密码分析者既不能证明也不能否定RSA的安全性，但这恰恰说明该算法有一定的可信性，目前它已经成为最流行的公开密钥算法。  
　　RSA的安全基于大数分解的难度。其公钥和私钥是一对大素数的函数。从一个公钥和密文恢复出明文的难度，等价于分解两个大素数之积的难度（这是公认的数学难题）。

**5.3 ElGamal密码体制**

自1976年Diffie和Hellman阐述了[非对称密码体制](http://baike.baidu.com/view/696428.htm" \t "http://baike.baidu.com/_blank)的思想后，人们希望设计出一些基于困难问题且实用的密码体制。1985年T.ElGamal[5]提出了ElGamal密码体制，这是继RSA以后的又一突破性算法。与RSA不同的是，ElGamal体制借鉴了1976年Diffie和Hellman论文中的成果，与Diffie-Hellman密钥交换协议类似，ElGamal体制的安全性是基于有限域上的离散对数问题的难解性。

和RSA相比，ElGamal的运算速度、安全性有了一定提升，美国数字签名标准（DSS）便是ElGamal签名方案的一种变形。

**5.4 ECC密码体制**

自非对称密码产生以来，人们基于各种数学难题提出了大量的密码方案，但能经受时间考验而广泛为人们所接受的只有基于大整数分解及离散对数问题的方案，但就如此狭窄的数学背景来说，这两个困难问题的方案还是引起了人们的担忧。另一方面，随着计算机信息处理能力的不断提高，对RSA、ElGamal的密钥长度的要求也越来越高，这个问题对某些计算能力没有很好支持的系统来说显得更加突出。因此，寻找一种基于新的数学难题、有效率的密码体制是人们努力的方向。

椭圆曲线密码体制（ECC）的提出改变了这种状况，实现了密钥效率的重大突破，大有取代RSA之势，它也成为迄今被实践证明安全、有效、应用较广公钥密码体制之一，以高效著称。

椭圆曲线在代数学和几何学上已被广泛研究近160年，有丰富而深厚的理论积累。1985年Neal Koblit和Victor Miller首先将椭圆曲线引入密码学，提出了基于有限域GF(p)的椭圆曲线上的点集构成群，在这个群上定义离散对数系统并构造出基于离散对数的一类公钥密码体制——椭圆曲线密码体制，其安全性基于椭圆曲线上离散对数问题的安全性。

基于椭圆曲线上的离散对数问题要比大整数分解问题、有限域上乘法群离散对数问题难解得多，因此ECC仅需较小的密钥长度就可以提供与RSA、ELGamal相当的安全性。另一方面椭圆曲线具有丰富的群结构和多选择性，因而，ECC在密码学领域有着广阔的应用前景。

**6小结**

非对称密码的高效性仍然是目前的一个研究热点。同时，由于近年来相关学科的进步和发展，出现了一些新的密码技术，如DNA密码、量子密码[4]。

从密码学的发展史可以看出，密码学的发展过程是从不完善到完善、理论上从简单到复杂的过程，这符合人类认识客观事物的认识规律。数学、计算机科学对密码学的发展起到了极大的促进作用，这说明在科学的发展中各个学科相互推进、互相联系和渗透，从而使人类对事物有更深的认识。

**参考文献**

[1] 毛明. 大众密码学[M]. 北京：高等教育出版社, 2005.

[2] 金德纯. 国外密码学的现状与发展[J]. 信息安全与通信保密, 1985.

[3] Silverman J H, Pipher J, Hoffstein J. An Introduction to Mathematical Cryptography[M]. Springer, 2008: 1-9.

[4] 谷利泽, 郑世慧, 杨义先. 现代密码学教程[M]. 北京邮电大学出版社, 2015.

[5] Elgamal T. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms[M]. Advances in Cryptology. Springer Berlin Heidelberg, 1985:469-472.