现代密码学的起源及其发展

保密一直是密码学的核心。然而，在早期的密码学中，关于什么是保密令人困惑。经典的密码系统如凯撒密码（其中每个字母被进一步替换为一个三个位置，所以a被带到d，b到e等）等依赖于保持整个加密过程秘密的安全性。在电报发明之后，通用系统和特定密钥之间的区别允许通用系统被损害，例如通过盗窃加密设备，而不会损害在新密钥中加密的未来消息。这一原理由Kerchoffs提出，他在1881年写道，加密系统的受损不应对通信者带来不方便。①

大约1960年，密码系统被投入使用，被认为足以抵抗已知的明文密码攻击，从而消除了保持旧消息秘密的负担。这些发展中的每一个都减少了系统必须免受公共知识的保护的部分，免除了对外发送前对加密方式的冗余的解释。因此，公钥系统是对减少秘密这一趋势的自然延续。

在20世纪七八十年代，廉价的数字硬件的开发从机械计算的设计限制中释放出来，使高档加密设备的成本降低到可在这些商业应用中作为远程现金分配器和计算机终端使用的地方。反过来，这种应用程序需要新型的加密系统，这最小化了安全密钥分发信道的必要性，并提供相当于书面签名。与此同时，信息理论与计算机科学的理论发展展示了提供可怕的安全密码系统，将这座古老的艺术改为科学。

密码学的两个发展方向开始引人关注，一个是公钥密码系统，一个是单向密码系统。但在这之前，密码学是否能成为一门科学，而非“设计艺术”，是一个值得探讨的问题，这就取决于是否有研究的公理以及范式。现代密码学在20世纪80年代，通过强调定义，精确的假设和严格的安全证明，与古典密码学区分开。

- 定义的核心作用：现代密码学的一个关键智力贡献一直是认可，安全性的正式定义是任何加密原语或协议设计的重要一步。原因

是，如果你不知道你在想实现什么，你怎么能知道你何时达到呢？密码学的定义非常强，而且可能似乎无法实现。但是密码学的最惊人的方面之一就是，可以证明出满足这样强定义的有效结构（基于一些被认可的的假设）。

- 正式和精确假设的重要性：我们目前无法在无条件的意义上证明许多加密结构。安全经常依赖于一些广泛认可（尽管未经证实的）假设。现代加密方法决定了任何此类假设必须清楚和明确地定义。这不仅需要对假设的客观评估，而且更重要的是，严格的证明了安全性。②

清楚了现代密码学与古典密码学的区别后，我们再来审视其发展的两大方向。

公钥分发系统提供了不同的方法来消除对安全密钥分发渠道的需求。在这样的系统中，希望交换密钥的两个用户来回通信，直到它们拿到共同的钥匙。

加密算法包括两个密钥：一个公开（公钥）；一个保密（私钥）。所以在公钥密码体制中，每个用户拥有两个密钥，公钥用于公开，私钥用于本地保存。

在公钥密码体制中，其加密与解密由不同的密钥完成的。如果使用公钥进行加密，就可以使用私钥进行解密，同理使用私钥进行加密，就可以通过公钥进行解密。尽管知道加密算法，但是从加密密钥得到解密密钥在计算上是不可行的 。

另一个方向是单向加密，又称为不可逆加密算法，在加密过程中不使用密钥，明文由系统加密处理成密文，密文无法解密。一般适合于验证，在验证过程中，重新输入明文，并经过同样的加密算法处理，得到相同的密文并被系统重新认证。①

该算法有如下特点：

1. 对同一消息反复执行加密得到相同的密文。

2. 加密算法生成的密文不可预见，根明文没任何关系。
3. 明文的任何微小的变化都会对密文产生很大影响。
4. 不可逆，即不能通过密文获取明文。

随着现代密码学的发展以及保密意识的加强，这两个重要的发展方向在实际生活中的应用愈发广泛。

非对称加密算法在，例如**HTTPS**，S端使用自己的私钥解密对称加密随机密钥，双方握手完毕。后续的所有数据都会使用这个密钥进行对称加密/解密。又比如近些年相当火爆的比特币，比特币的钱包系统使用的就是非对称加密技术，通过公私钥对及零知识证明，比特币可以做到在区块链上广播属于自己的一笔交易且其他中间人无法伪造这一结果。

单向加密算法则广泛用于提取数据，验证数据的完整性，防止篡改和校验数据。现在许多系统的账户密码就是以SHA加密后储存的。

①: Whitefield Diffle and Martine E. Hellman "New Directions in Cryptography" vol IT-22, No.6, November, 1976

②: Jonathan Katz and Yehuda Lindell "Introduction to Modern Cryptography"