第 4 章 数据加密

沙之洲 2020012408

1 公钥密码的出现解决了对称加密算法的什么问题？但对称加密至今仍被广泛使用，请至少从一个角度简述对称加密算法未被淘汰的原因？

公钥密码解决了对称加密算法的密钥分发问题。在对称加密算法中，加密和解密使用的是同一个密钥，这就导致密钥分发的过程中可能会被窃听和篡改。而在公钥密码体系中，加密和解密所需要的密钥不同，因此密钥分发的问题得以解决。

对称加密算法没有被淘汰得益于它的计算效率很高。虽然公钥密码能够避免密钥分发的问题，但是公钥密码算法往往涉及到复杂的数学运算，这就导致公钥密码无法快速加解密大批量的数据。而对于对称加密算法而言，它比公钥密码的速度快很多，而且在保证密钥分发是安全的前提下，对称加密算法是安全的，因此对称加密算法没有被淘汰。

2 请分别简述五种密码分析技术的大致流程。

2.1 唯密文攻击

分析者已知用统一密钥加密出的多个消息的密文，其目标是尽可能恢复出足够多的明文或者推算出加密消息的密钥

2.2 已知明文攻击

分析者已知部分明文及其对应的密文，其目标是推算出加密消息的密钥或者某种能够对使用该密钥加密的任意消息进行解密的算法

2.3 选择明文攻击

分析者已知部分明文和对应的密文，还可以选择一个或者多个明文，得到其加密后的密文。其目标是推算出加密消息的密钥或者某种能够对使用该密钥加密的任意消息进行解密的算法

2.4 选择密文攻击

分析者可以选择一个或者多个密文，得到其对应的明文。其目标是推算出加密消息的密钥

2.5 选择文本攻击

是选择明文攻击和选择密文攻击的结合。分析者可以选择一个或者多个明文，得到其加密后的密文，也可以选择一个或者多个密文，得到其对应的明文。