第 4 章 数据加密

赵晨阳 2020012363

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，可以只向外公开公钥而保留秘钥，因此密钥分发的问题得以解决。

对称加密算法未被淘汰的原因至少有如下两点：

1. 计算效率高：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。对于许多场景（甚至包括部分网络银行），对称加密算法已经足够安全，并且可以满足快速处理大量数据的需求，因此被广泛使用。
2. 支持设备广泛：对称加密算法对称加密算法不需要太多的计算资源就能够处理大量数据，可以在各种设备上高效地运行。同时，由于对称加密算法具有高效的硬件实现方式，因此在某些应用场景中，对称加密算法的计算效率可以比公钥密码高出几个数量级，这是公钥密码算法无法比拟的优势。

2 请分别简述五种密码分析技术的大致流程

密码分析技术是破解密码的方法和手段，主要分为以下五种：

2.1 唯密文攻击

分析者通过同一密钥加密出的多个密文，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，推算出加密消息的密钥或者破解该密钥加密消息的算法。

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。分析者的目标是推算出加密消息的密钥或者破解该密钥加密消息的算法。

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。这类攻击主要针对公钥密码算法。

2.5 选择文本攻击

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。