网络空间安全导论 · Ch4

计01　容逸朗　2020010869

Q1.

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？

- 公钥密码的出现解决了对称加密算法中密钥分发的问题。
- 对称加密算法至今仍被广泛使用，主要原因包括：
  - 与公钥密码相比，对称加密算法有更快的加密速度；
  - 对称加密算法的实现通常比公钥密码简单得多。这使得对称加密算法在一些计算资源较少的设备上也可以使用。

Q2.

请分别简述五种密码分析技术的大致流程。

- **唯密文攻击：**已知密文，尽量恢复明文或者推算出密钥。
  - 收集密文：首先，攻击者需要收集尽量多的密文；
  - 选择攻击方式：根据加密算法、密钥长度以及其他相关因素来确定合适的攻击方式：
  - 分析密文：使用选定的攻击方式来分析密文，以获取有关加密算法、密钥以及加密过程的信息；
  - 推断密钥：分析密文和加密算法的特征，尝试推断出密钥。
  - 解密消息：一旦成功破解了密钥，就可以使用该密钥来解密被加密的消息。
- **已知明文攻击：**已知密文及对应明文，找回加密的密钥或者一个可解密上述方式加密密码的算法。
  - 数据收集：收集一些已知明文和对应的密文，这些明文和密文必须由相同的密钥和加密算法生成。
  - 推断密钥：使用数学算法和技巧分析密文和加密算法的特征，尝试使用不同的密钥来加密已知的明文，然后比较生成的密文和已知的密文结果来判断密钥是否正确。
  - 解密消息：一旦成功破解了密钥，就可以使用该密钥来解密被加密的消息。
- **选择明文攻击：**攻击者不仅知道一些消息的明文和密文，而且可以选择被加密的明文。
  - 收集明文：攻击者需要从通信渠道中收集一些明文，或是自己设计明文。
  - 选择攻击方式：根据加密算法、密钥长度以及其他相关因素来确定合适的攻击方式：
  - 加密明文：使用选定的攻击方式加密明文，以获取有关加密算法、密钥以及加密过程的信息。
  - 推断密钥：使用数学算法和技巧分析密文和加密算法的特征，尝试推断出密钥。
  - 解密消息：一旦成功破解了密钥，就可以使用该密钥来解密被加密的消息。
- **选择密文攻击：**分析者能选择不同的被加密的密文，并可以得到对应的解密的明文，任务是找回密钥。
  - 收集密文：攻击者需要从通信渠道中收集一些密文，或是自己设计密文。
  - 选择攻击方式：根据加密算法、密钥长度以及其他相关因素来确定合适的攻击方式：
  - 解密密文：使用选定的攻击方式解密明文，从中得到有关加密算法、密钥以及解密过程的信息。
  - 推断密钥：使用数学算法和技巧分析密文和加密算法的特征，尝试推断出密钥。

  - 解密消息：一旦成功破解了密钥，就可以使用该密钥来解密被加密的消息。
- **选择密钥攻击：**密码分析者具有不同密钥之间关系的有关知识
  - 收集密文：攻击者需要从通信渠道中收集一些密文，或是自己设计密文。
  - 选择攻击方式：根据加密算法、密钥长度以及其他相关因素来确定合适的攻击方式：
  - 选择密钥：需要选择特定的密钥来加密明文。这些密钥通常是与弱加密算法或错误实现有关的。
  - 加密明文：使用选定的攻击方式加密明文，以获取有关加密算法、密钥以及加密过程的信息。
  - 推断密钥：分析加密过的明文和选定的密钥，尝试推断出加密算法中使用的密钥。
  - 解密消息：一旦攻击者成功破解了密钥，他们就可以使用该密钥来解密被加密的消息。