计算机网络 第八章 读书笔记

8.1 什么是网络安全

- 安全通信具有下列所需要的特性：
  - 机密性。
  - 报文完整性。
  - 端点鉴别。
  - 运行安全性。

8.2 密码学的原则

- 发送者报文的最初形式被称为明文。发送者使用加密算法加密其明文报文，生成的加密报文被称为密文，该密文对任何入侵者看起来是不可懂的。发送方提供了一个密钥 KA，它是一串数字或字符，作为加密算法的输入。加密算法以密钥和明文报文 m 为输入，生成的密文作为输出。用符号 KA(m)表示使用密钥 KA 加密的明文报文 m 的密文形式。类似地，接收方将为解密算法提供密钥 KB，将密文和接收方的密钥作为输入，输出初始明文。也就是说，如果接收方接收到一个加密的报文 KA(m)，他可通过计算 KB(KA(m)) = m 进行解密。在对称密钥系统中，发送方和接收方的密钥是相同并且是秘密的。在公开密钥系统中，使用一对密钥：一个密钥为发送方和接收方两人所知，另一个密钥只有发送方或接收方知道。

- 当考虑入侵者破解加密方案的难易程度时，可以根据入侵者所拥有的信息分为三种不同的情况：
  - 唯密文攻击
  - 已知明文攻击
  - 选择明文攻击

- 多码代替密码是对单码代替密码的改进。

- 在块密码中，要加密的报文被处理为 k 比特的块。

- RSA 算法
  - 选择两个大素数 p 和 q。该值越大，破解 RSA 越困难，而执行加密和解密所用的时间也越长。
  - 计算 n = pq 和 z = (p – 1)(q – 1)。
  - 选择小于 n 的一个数 e，且使 e 和 z 互素。
  - 求一个数 d，使得 ed – 1 可以被 z 整除。即给定 e，求 d，使得 ed mod z = 1。
  - 接收方使外界可用的公钥 是一对数(n, e)，其私钥是 是一对数(n, d)。

- 在实际应用中，RSA 通常与对称密钥密码结合起来使用。

8.3 报文完整性和数字签名

- 报文完整性是指，接收方为了鉴别收到的报文，需要证实：
    - 该报文确实源自希望的发送方。
    - 该报文在到达的途中没有被篡改。

- 散列函数以 m 为输入，并计算得到一个称为散列的固定长度的字符串 H(m)。密码散列函数要求具有下列附加的性质：找到任意两个不同的报文 x 和 y 使得 H(x) = H(y)，在计算上是不可能的。这种性质就意味着入侵者在计算上不可能用其他报文替换由散列函数保护的报文。这就是说，如果(m, H(m))是报文和由发送方生成的报文散列的话，则入侵者不可能伪造另一个报文 y 的内容，使得该报文具有与原报文相同的散列值。

- 为了鉴别报文完整性，除了使用密码散列函数外，发送方和接收方需要共享秘密 s。这个共享的秘密只不过是一个比特串，它被称为鉴别密钥。

- 数字签名是一种在数字领域实现的密码技术。使用数字签名的发送方的步骤：发送方让他的初始长报文通过一个散列函数。然后他用自己的私钥对得到的散列进行数字签名。明文形式的初始报文连同已经数字签名的报文摘要一道被发送给接收方。

8.4 端点鉴别

- 端点鉴别就是一个实体经过计算机网络向另一个实体证明其身份的过程。

- 端点鉴别的步骤：
    - 发送方向接收方发送报文“我是 xxx”。
    - 接收方选择一个不重数 R，然后把这个值发给发送方。
    - 发送方使用他与接收方共享的对称秘密密钥 K 来加密这个不重数，然后把加密的不重数 K 发回给接收方。由于发送方知道 K 并用它加密一个值，就使得接收方知道收到的报文是由希望的发送方产生的。这个不重数用于确定希望的发送方是活跃的。
    - 接收方解密收到的报文，如果解密得到的不重数等于他发送给发送方的那个不重数，则可鉴别发送方的身份。