Chap4

对称密码

- 对称密码算法的两条基本设计原则 (P.35)
  - 1. **扩散（Diffusion）**：重新排列消息中的每一个比特，使明文中的冗余度能够扩散到整个密文，将每一个比特明文的影响尽可能作用到较多的输出密文位中。
  - 2. **扰乱（Confusion）**：密文和密钥之间的统计特性关系尽可能复杂化。如果密钥的一位发生变化，密文的绝大多数位也发生变化。这两种设计原则是由信息论的创始人克劳德·艾尔伍德·香农提出的。
- 分组密码 (P.37)
  - ECB模式 (P.38)
  - CBC模式 (P.40)
  - CFB模式 (P.41)
  - OFB模式 (P.42)

DES(年年讲年年烂，建议看课件）

公钥密码

- **事先共享密钥**：在加密通信之前，以安全的方式将密钥交给接收方。
- **通过密钥分配中心（Key Distribution Center，KDC）**：当参与加密通信的人过多时，可以使用KDC。当需要进行加密通信时，KDC会生成一个通信密钥，每个人只需和KDC事先共享密钥即可。
- **通过Diffie-Hellman密钥交换**：进行加密通信的双方仅需要交换一些信息，即使这些信息被窃听，也无法对算法进行解密，而通信双方则可以通过这些信息各自生成相同的密钥。
- **通过公钥密码**：由于加解密使用不同的密钥，所以无需进行密钥分发。
- 公钥密码系统的加密原理 (P.64-65)
- 公钥密码系统的签名原理 (P.66)
- 公钥密码算法的表示 (P.67)
  - **对称密钥密码**
    - 密钥：会话密钥(Ks)
    - 加密函数：EKs[P]
    - 对密文C，解密函数：P=DKs[C]
  - **公开密钥**
    - (KUa，KRa)
    - 加密/签名：C= EKUb[P]，EKRa[P]
    - 解密/验证：P= DKRb[C]，DKUa[C]
- 对公开密钥密码算法的要求 (P.68-69)
  - 参与方B能容易地生成密钥对(KUb, KRb)。
  - 已知KUb，A的加密操作应该是容易的：C= EKUb[P]。
  - 已知KRb，B的解密操作应该是容易的：P= DKRb (C) =DKRb (EKUb (P))。
  - 已知KUb，求KRb应该是在计算上不可行的。
  - 已知KUb和C，欲恢复P应该是在计算上不可行的。
- 公钥密码算法的误解 (P.603)
  - 1. 公开密钥算法比对称密钥密码算法更安全：事实上，任何一种算法的安全性都依赖于密钥长度和破译密码的工作量。从抗分析的角度来看，没有哪一种算法是绝对优越的。
  - 2. 公开密钥算法使对称密钥成为过时的技术：事实上，公开密钥算法运行速度较慢，只能用在密钥管理和数字签名上。因此，对称密钥密码算法仍将长期存在。
  - 3. 使用公开密钥加密，密钥分配非常简单：事实上，密钥分配既不简单也不有效。

摘要与签名

- 散列函数 (P.80)
- 散列函数的性质 (P.82)
  - 1. 可以根据任意长度的消息计算出固定长度的散列值。
  - 2. 能够快速计算出散列值。
- 散列函数的安全性：HASH 碰撞 (P.84)
- 哈希算法实例 (P.87)
  - **MD5**: 生成128位的哈希值，广泛用于确保信息传输的完整无误。
  - **SHA-1**: 安全哈希算法，主要用于各种安全认证中，生成160位的哈希值。
  - **SHA-256**: 属于SHA-2标准下的哈希算法，生成256位的哈希值，被广泛用于比特币中。
- 散列函数的应用: 比特币 (P.88)
- SHA256算法 (P.89)
- 消息认证码 (MAC) (P.97)
- HMAC (P.97)
- 公钥密码与数字签名 (P.98)
  - 数字签名方法 (P.100)
  - 数字签名的分类 (P.101)
  - 数字签名的应用 (P.102)
  - 密码分析技术 (P.105)
  - 唯密文攻击(Ciphertext only) (P.106)
  - 已知明文攻击(Known Plaintext) (P.106)
  - 选择明文攻击(Chosen Plaintext) (P.106)
  - 选择密文攻击(Chosen Ciphertext) (P.106)
  - 相关密钥攻击(Related Key) (P.106)
  - 密码分析技术 (P.107)

密码学简史

- **古典密码**：主要是通过替换和移位等简单手段来加密信息。
- **近代密码**：包括复杂的机械或电子密码机，如二战期间的德国恩尼格玛密码机。
- **现代密码**：主要指的是计算机时代的密码技术，比如公钥密码和哈希函数等。
- 隐写术与密码学
  - **隐写术**：源自希腊语，意为"隐秘书写"。它是一门关于信息隐藏的技巧和科学，主要是将信息隐藏在其他无害的信息中，以达到传递秘密信息的目的。
  - **密码学**：源自希腊语，意为"隐藏的书写"。它是一门研究如何隐密地传递信息的学科。密码学的目的不仅仅是隐藏信息，而是确保信息的安全性，包括保密性、完整性和可用性等。
  - 密码学的基本概念
    - **密码编码**：通过信息编码使信息保密。
    - **密码分析**：用分析方法解密信息。
    - **基本术语**：
      - 明文(plain text)：原始要加密的信息。
      - 密文(cipher text)：经过加密的信息。
      - 加密(encrypt, encryption)：将明文转化为密文的过程。
      - 解密(decrypt, decryption)：将密文转化为明文的过程。
      - 密码算法(Algorithm)、密码(Cipher)：用来加密和解密的数学函数。
      - 密钥(Key)：密码算法中的一个变量。
    - **代替**：每个明文元素映射为另一个元素。
    - **换位**：明文中的元素重新排列。
    - **对称加密**：同一个密钥既用于加密又用于解密。
    - **非对称加密**：使用一对密钥，一个用于加密，另一个用于解密。
    - **块加密**：一次处理一个数据块进行加密。
    - **流加密**：一次处理一个数据单元进行加密。
  - 密码技术的主要用途
    - **数据保密**：通过数据加密和解密保护数据的私密性。
    - **认证技术**：实体身份认证和数据源发认证。
    - **信息完整性保护**：保证信息在传输过程中没有被插入、篡改、重发。
    - **数字签名和抗抵赖**：源发抗抵赖和交付抗抵赖。
- 古典密码
  - **代替密码 (Substitution Cipher)**
  - **换位密码 (Transposition Cipher)**
  - **代替密码与换位密码的组合**
  - 受限算法的缺陷
  - 不适合大规模使用
  - 不适合人员变动较大的组织
  - 用户无法了解算法的安全性
  - 例子：凯撒密码（PPT第17页）
  - 例子：猪圈密码（PPT第18页）
  - 例子：纵行换位密码（PPT第19页）
- 1949年~1975年：戚继光反切码（PPT第20-21页）
- 近代密码 (P.22)
  - ENIGMA机 (P.23-P.26)
    - **工作原理** (P.24-P.26): 它的工作方式基于三个核心要素：转子的初始设置，转子之间的相互位置，以及连接板连线的状况，这三者组合构成了所有可能的密钥。此外，由于每个转子的旋转，使得可能的加密变化在每次输入时都会变化。
    - **工作过程** (P.27): ·根据密码本取得当日密钥·首先发送一个新的密钥·随机地选择三个字母，比如说PGH·把PGH在键盘上连打两遍，加密为比如说KIVBJE（注意两次PGH被加密为不同的形式）·把KIVBJE放在在电文的最前面·重新调整三个转子的初始方向到PGH·正式对明文加密
  - 对称密钥密码系统的缺陷 (P.31)
    - 1. 密钥必须经过安全的信道分配。
    - 2. 无法用于数字签名。
    - 3. 密钥管理复杂，随着用户数量的增加，密钥的数量将呈指数级增长，这是因为每个用户都需要与每个其他用户有一个唯一的密钥。
  - 现代密码 (P.31)
  - 量子密码 (P.32-P.33)
    - **工作原理**：量子密码利用光的偏振状态来编码信息。例如，"水平垂直方向"偏振和"对角方向"偏振可以被用来代表二进制的0和1。
    - **量子密钥生成方法**：在量子密码中，发送方生成并发送偏振，接收方则进行测量。由于量子力学的原理，任何未经授权的测量都会改变量子态，从而被检测到。

RSA算法简介 (P.70)

- RSA算法的诞生 (P.71)
- RSA算法的性能表现 (P.73, 74)
- RSA算法的操作过程 (P.604-608)
- 公钥密码系统的应用 (P.77)