Chapter 4 Digital signature, One-way hash & MAC

2017年3月20日 10:39

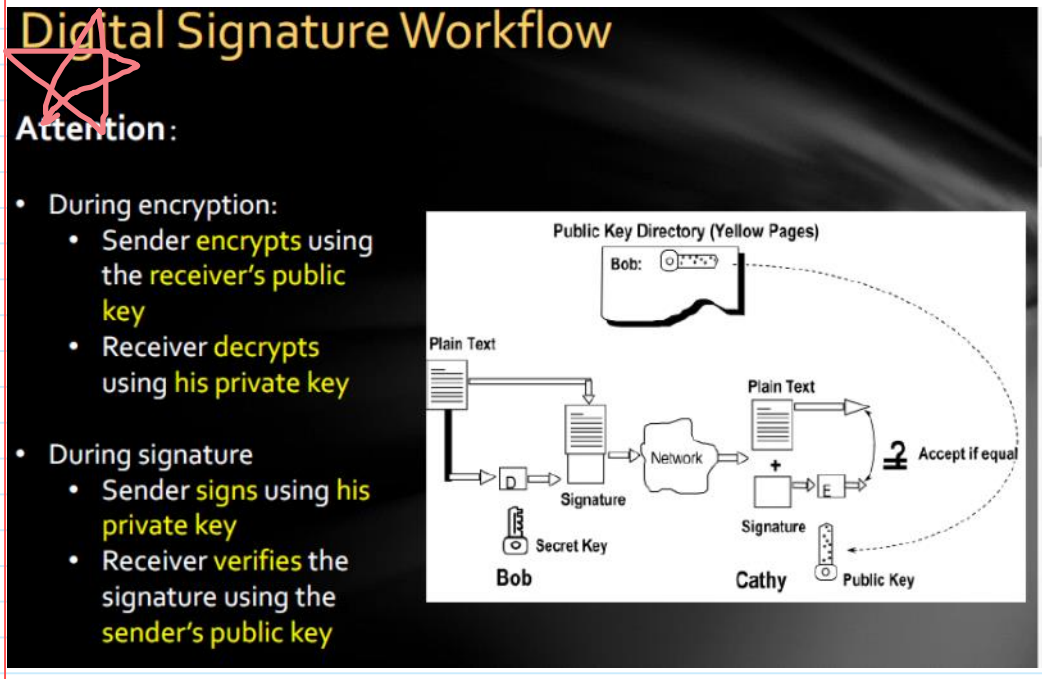
BY LSY

Outlines:

- Digital Signature
- One-way hash function
- Message Authentication Code, MAC
- PGP

1. the Signature

- 特点
  - Signature is credible, the recipient believe that the signer signed the document carefully
  - 很难被伪造
  - 签名不能被重用
  - 被签名的文件不能被更改
  - 签名不能杯否认
  - 和时间一起绑定
  - Signature can be legal evidence , and can be proved
- 数字签名的要求
  - 数字签名和文档进行绑定
  - 其他人不可以进行伪造
  - 不能否认自己的签名
  - 第三方可以来验证签名
  - 需要和其它的一些信息绑定，比如时间之类的
- 数字签名的需求
  - .....
- 算法
  - DSS/DSA

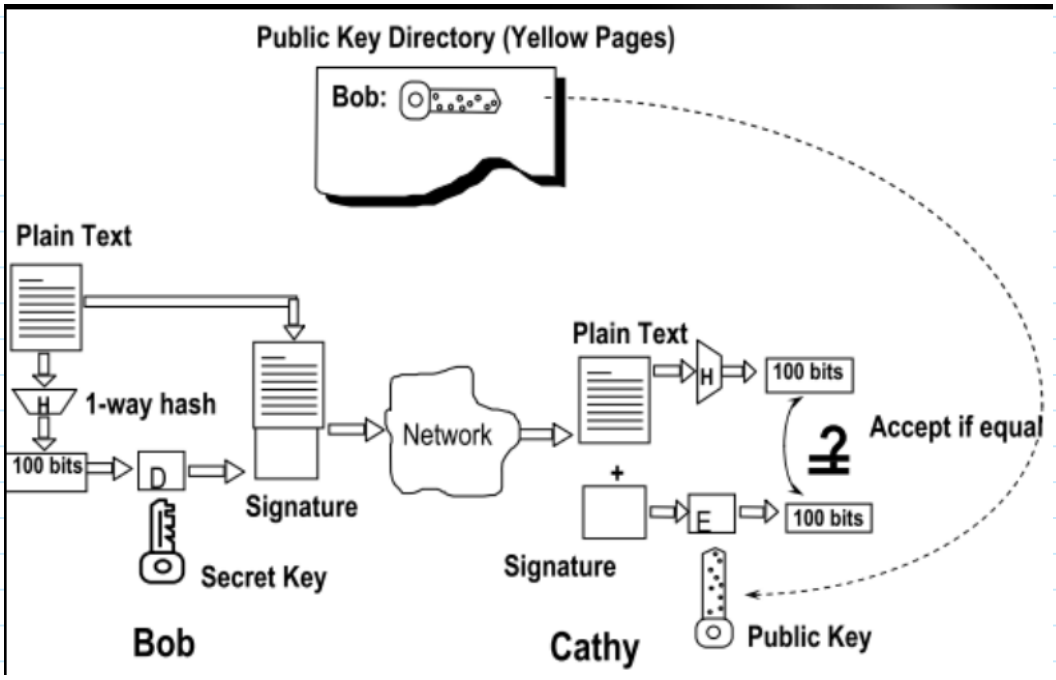


pp

2. one-way hash algorithm
- 特征：
  - easy to compute
  - difficult to reverse computing
  - difficult to find collision
- MD5 Algorithm
  - 和加密的区别：
    - 加密必须是可逆的，因此信息量是不可以损失的
    - 单向函数是不可逆的，信息是可以损失的
  - 算法
    - padding
    - hashing
  - 攻击
    - 知道哈希值，得到一个明文

- 没有给定对应的明文
- 给出明

2017/3/22 8:09
1. the procedure of signature for long plain text
- Hash值可以完全代表明文
- 一旦明文发生改变，Hash值会发生改变



2. MAC(message authentication code)
- 消息完整性服务，确保中间没有被篡改
- 基于类似对称密钥的特性
- 存在key

3.HMAC (hash-based message authentication code)

4.CBC_MAC

5.Difference of MAC & Digital Signature
- MAC:
  - 只有特定的接收方才可以验证密钥，

- 不提供“不可否认行”服务，不具备私钥功能，每一个能验证的人必有密钥，也可以构造出
- Digital Signature:
  - 只要有发送者公钥就可以进行验证
  - 提供“不可否认性”服务，因为只有私钥的拥有者才可以进行签名

6. introduction of PGP
   - history
   - gnupg