简答题可能的范围

往年出现过（cut）

对称密码与非对称密码的定义和区别

- 对称密码是指双方共享一个密钥，并使用相同的加密方法和解密方法。
- 非对称密码是指双方使用不同的密钥：一个公钥和一个私钥。
- 对称加密算法
  - 优点：加密安全快速，密钥短。
  - 缺点：无法解决密钥分配问题，密钥个数多，对对方的欺骗没有防御机制。
- 非对称密码
  - 优点：可以解决密钥分配问题，能够提供消息验证，完整性和不可否认等安全性
  - 缺点：加密速度慢，密钥长
- 联系：在安全系统中，常常同时需要对称密码和非对称密码算法，两者相结合使用， 可以有效的解决安全问题。

简述哈希函数的属性以及作用

- 属性
  - 任意的消息大小： 对任意大小的消息适用
  - 固定的输出长度：生成的哈希值的长度是固定的
  - 有效性：计算相对简单有效
  - 抗第一原像性：给定一个输出 z，找到满足 h(x)=z 的输入 x 是不可能的
  - 抗第二原像性：给定一个 x1 和 h(x1)，找到满足 h(x1)= h(x2)的 x2 在计算上不可能的
  - 抗冲突性：找到满足 h(x1)= h(x2)的一对 x1和 x2且不等，在计算上不可行的
- 作用
  - 应用于数字签名，解决高计算负载，消息开销和安全性限制等问题
  - 还可与 对称密钥相结合，产生消息验证码，验证消息的完整性和消息源认证

简述序列密码与分组密码之间的联系与区别

- 两者之间的联系
  - .....
- 区别：

课上提及较多

单向陷门函数

- 单向性：单向性，也称不可逆性，即对于一个函数 $y = f(x)$，若已知 x 要计算出 y 很容易，但是已知 y 要计算出 $x = f^{-1}(y)$ 则很困难。

- 陷门：对于单向函数 $f(x)$,若给出 $f(x)$ 和一些秘密信息 z ，则很容易就计算出 x ,则 z 称为陷门。
- 在公开密钥密码中，计算 $f(x)$ 相当于加密，陷门 z 相当于私有密钥，而利用陷门 z 求 $f(x)$ 中的 x 则相当于解密。
- 举个例子(上面三点分数不够): 以RSA为例.....

分组密码相关

- 分组密码的操作模式
  - ECB：电子密码本模式
  - CBC：密码分组链接模式
  - CFB：密码反馈模式
- 分组原则
  - 分组长度足够大
  - 密钥足够长，密钥量足够大
  - 密码变换足够复杂

一些概念

两大认证技术

- 认证函数
  - 哈希函数
- 数字签名

哈希函数

- $H(M)$：只保证完整性，并不保密
- $H(M,K_{AB}$：$MAC($消息认证码$)$ //----K_{AB} 是密钥
- $H(pwd,salt)$：基于口令加密

认证

- 身份认证：对通讯双方的身份加以鉴别
- 消息认证：对接收到的消息的完整性加以鉴别

$$H\{0,1\}^* \rightarrow \{0,1\}^k$$

- 单向性：已知 H 和 x ,求出 $H(x)$ 容易；反之，已知 H 和 $H(x)$ ，求出 x 难
- 抗碰撞性：若 $x_1 \neq x_2$,则 $H(x_1) \neq H(x_2)$

按密钥使用方法

- 对称密码
  - 分组密码
  - 序列密码
- 非对称密码：(公钥密码，双钥密码)