No.: Date:

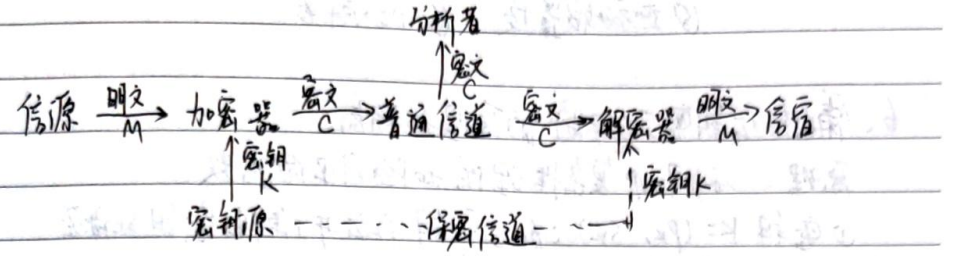
1、简述密码学的基本功能和保密通信的基本模型

①保密性，非授权者无法知道消息的内容

②完整性，消息的接收者应该能够验证消息在传输过程中没有被改变

③鉴别，消息的接收者应该能够确认消息的来源

④不可否认性，发送方不能否认已经发送的消息



2、简述对称密钥体制和非对称密钥体制的区别

对称密钥密码体制中的加密密钥和解密密钥完全相同，彼此之间很容易相互确定，密钥需经过安全通道进行传送，这种密码体制的安全性等价于密钥的安全性

而在非对称密钥体制中，比如在公钥密码体制，加密密钥和解密密钥不同，不需要专门传送密码的安全通道。

3、密码分析有哪几种方法和哪几种类型

方法：①穷举攻击法　　类型：①仅密文攻击　②已知明文攻击

②统计分析法　　③选择明文攻击　④选择密文攻击

③解密变换法

4、简述分组密码和流密码的区别

流密码按照位进行加解密，密码序列的长度与被加密消息长度相等

分组密码则将明文按照一定长度，以组为单位进行加解密，并且不同组采用相同的密钥。

NOTEBOOK

No: Date:

5、阐述DES密码体制的基本流程和关键步骤.

关键步骤：① 两次初始置换 ② 子密钥控制下的16轮迭代加密
③ 十六轮子密钥生成

基本流程：① 初始置换IP ② 子密钥生成
③ 轮函数 ④ F函数：位选择函数，S盒代换，P盒代换.
⑤ 逆初始置换 ⑥ DES解密.

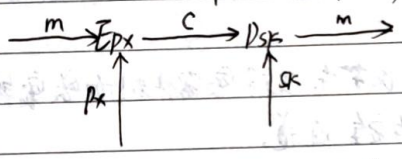
6、简述公钥密码体制的原理和特点。

原理：利用NP复杂性理论和陷门单向函数

① 密钥 K=(PK, SK)：加密密钥 PK公开；解密密钥 SK保密
在计算上由 PK推出 SK是困难的.

② 加密算法 EPK：C=EPK(m)

③ 解密算法 DSK：满足：m=DSK(C)
即：DSK(EPK(X))=X



特点：① 产生密钥对K=(PK, SK)在计算上是可行
② 两个密钥中的任何一个都可以用来加密，另一个则用来解密.
③ 已知公钥与明文，产生密文是容易.
④ 利用私钥解密密文在计算上是可行.
⑤ 利用公钥求解私钥在计算上是不可行。
⑥ 利用密码算法和公钥求解私钥在计算上不可行
⑦ 已知公钥与密文，不知私钥时，恢复明文在计算上是不可行
⑧ 用私钥加密，公钥解密，则可获得一个数字签名。在有数字签名的条件下，发送者无法否认是发送的信息，即不可否认性。

NOTEBOOK

No. Date:

7. 以明文1024为例说明RSA算法的密钥生成和加解密过程

密钥生成：(1) 选择素数 $p, q = 17, 11$

(2) 模数 $n = p \cdot q = 187$

$\phi(n) = (p-1)(q-1) = 16 \times 10 = 160$

(3) 随机地选择一个加密密钥 e　gcd为最大公约数运算

满足 $1 < e < \phi(n)$, $GCD(e, \phi(n)) = 1$, $e = 7$

(4) 求解下面的方程，以得到解密密钥 d

$e \cdot d = 1 \bmod \phi(n)$ and $0 \le d \le n$　$d = 23$

(5) 公钥：$PU = \{e, n\} = \{7, 187\}$

(6) 私钥：$PR = \{d, n\} = \{23, 187\}$

(1) 加密：$C = 1024^e \bmod n = 1024^7 \bmod 187 = [(1024 \bmod 187) \times (1024^6 \bmod 187)] \bmod 187$

(2) 解密：$C^d \bmod n = (1024^7 \bmod 187)^{23} \bmod 187 = 1024$

NOTEBOOK