清华大学本科生考试试题专用纸

考试课程　现代密码学　　2022 年 06 月 08 日

姓名：　　学号：

古典密码

1. 密码学上的柯克霍夫原则(Kerckhoffs's principle)是什么？(4 分)

2. 密码算法的分类？(按功能分类以及按照密钥使用方式不同分类) (6 分)

3. 已知用 Vigenere Cipher 加密的明文为 SBHOCQANUPEDTYXHSBHOCQAD
其对应的密文 SCJRCRCQUQGGTZZKSCJRCRCG
(1) 使用 Kasiski Test 计算可能的 m 值。(5 分)
(2) 使用重合指数法对密文分析 m=3 和 m=4 的重合指数。(6 分)

4. 对于 3 转子的 Enigma 密码机(转子是从 5 个中选择 3 个)
(1) 不考虑 Ring Setting，接线板交换 10 对字母，计算其总密钥空间。(写出计算式子，不需计算最终结果)。(6 分)
(2) 已知一段密文：...YBOIEAMIIA...，且知其中完整包含了明文 ENIGMA 对应的密文，找出其对应关系。(6 分)

对称密码

5. (1)简述密码 HASH 函数定义。(3 分)
(2)简述密码 HASH 函数满足的安全属性。(3 分)

6. 分别简述 ECB、CBC、CFB、OFB、CTR 加密模式中，若密文传输过程中出现 1 比特错误，错误如何传播(该错误会影响多少个消息分组或比特不能正确解密)。(5 分)

7. 如何针对如下 MAC 进行伪造攻击？需要多少次 MAC 询问？(10 分)

$$
\begin{aligned}
&M = x_1||x_2||\ldots||x_m \\
&|x_i| = n \\
&y_0 = 0 \\
&y_i = E_k(x_i \oplus y_{i-1}), 1 \le i \le m \\
&CBC_k(M) = (y_m + 0x1) \cdot y_m + 0x1
\end{aligned}
$$

8. **(证明题)** 证明 DES 具有对称互补性，即假定 y=DES(x, k)，y′=DES(c(x), c(k))，这里c(·)表示对自变量逐比特位取反。
试证明：y′=c(y) (即：DES 加密中若将明文消息 x 和加密密钥 k 都逐比特位取反，则加密的密文也是原密文逐比特位取反。)(10 分)

公钥密码

9.设 RSA 加密体制的公钥(e,n)=(77,221)。
(1) 重复平方加密明文 160，得中间结果为：

$160^2 \pmod{221} \equiv 185$
$160^4 \pmod{221} \equiv 191$
$160^8 \pmod{221} \equiv 16$
$160^{16} \pmod{221} \equiv 35$
$160^{32} \pmod{221} \equiv 120$
$160^{64} \pmod{221} \equiv 35$
$160^{72} \pmod{221} \equiv 118$
$160^{76} \pmod{221} \equiv 217$
$160^{77} \pmod{221} \equiv 23$

若敌手得到以上结果就很容易分解 n，问敌手如何分解 n？(6 分)
(2)求解私钥 d。(6 分)

10. 在 Diffie-Hellman 密钥交换过程中，设大素数 p=11，a=2 是 p 的本原根。
(1) 描述 Diffie-Hellman 密钥交换协议。(6 分)
(2) 设用户 A 选择一个私有的 X_A=6，用户 B 选择一个私有的 X_B=8，求 A 和 B 的共享密钥 K。(6 分)

11. 在 ElGamal 数字签名体制中，假设 p=19，g=13。
(1) 如果签名者选择的私钥为 x=10，试计算公钥 y。(6 分)
(2) 设用户 A 要对消息 M=15 签名，且选取随机数 k=11，求消息 M=15 的签名。并验证该数字签名的有效性。(6 分)