《网络安全技术》作业

第二章 第 1 部分作业（古典密码）

2-1. 已知使用 Vegenere 密码加密，明文是：we meet at river，密钥 Key: stream。求加密后的密文。

2-2. 已知置换密码，明文是：nice work，置换表如表 1 所示，

x	1	2	3	4
∏(x)	2	4	1	3

求：密文和逆置换

第二章 第 2 部分作业（对称密码体制）

2-3. 完成下列分组密码算法的比较

	DES	AES	3DES
明文分组长度			
密钥长度			
有效密钥长度			
迭代轮数			

2-4. 在 CBC 模式中，如果用户每次加密都使用同一个初始化向量 IV，在这种情况下，密码破译者能够从中得到怎样的线索？请尝试举一个这方面的例子进行说明。

第二章 第 3 部分作业（公钥密码体制）

2-5. 根据 Diffie-Hellman 计算密钥机制，假定素数 q=11，本原根 a=2，请完成下列计算。

（1）用户 A 的公钥 YA=9，计算私钥 XA

（2）用户 B 的公钥 YB=3，计算共享密钥 K

2-6. 基于 RAS 公钥密钥算法，请回答如下问题

（1）用户 A 基于如下参数计算密钥对：p=3，q=11，e=7，请问 A 的密钥是什么？

（2）用户 A 基于如下参数计算密钥对：p=5，q=23，e=3，请问 B 的密钥是什么？

（3）应用上述产生的密钥进行如下通信：

- 通过加密消息 m 产生密文 c(从 B 向 A 发送消息)；
- A 收到加密消息 c 后对其进行解密；
- A 向 B 发送一个消息 m，不仅需要确保 m 的机密性而且能够对消息源进行认证（即 B 收到消息后能够确认该消息是 A 发送的），请给出该通信中加解密的过程并说明是如何保证机密性和可认证的。