1.设加密变换为 (mod 26)，则明文m=8的密文为\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_；

2．分组密码一般采用 Feistel结构或SPN结构，DES采用的是\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_结构，AES采用的是\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_结构。

3．设杂凑函数h的杂凑值的长为n比特，则对任意消息和，

成立的概率为\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_；

4． DES的分组长度为\_\_\_\_\_\_\_\_\_\_\_\_比特，AES的分组长度为\_\_\_\_\_\_\_\_\_\_\_\_比特。

三、

（1）阐述对称密码和公钥密码体制的区别。

（2）阐述Feistel结构和SPN结构的区别

（3）简述杂凑函数应满足的三条安全属性。

（4）简述混乱和扩散。

四、（1）描述RSA加密算法。

（2）已知RSA算法参数：p=5，q=11，e=3，明文M=9。求私钥d及密文C。

（3）假定已知某用户的公钥e 和n ，以及若干用RSA算法加密的密文，且这些密文所对应的明文中有一个与n有公因子，如何恢复所有的明文？

（4）RSA算法中加密和解密运算分别可采用何种方法加快计算？

五、叙述零知识证明的基本思想。

七、 简述DES算法。

（2） DES算法的E扩展、P置换和S盒在保证密码算法的安全性方面分别起到什么作用（混淆和扩散）？

八、

（1）在一个通信网络中，服务器存储了所有的密钥，网络的每个节点都分配了一个唯一的密钥，用这个密钥来保证结点和可信任的服务器之间的通信安全。用户A想要发送明文*M*给用户B，使用以下协议：

1. A产生一个随机数*R*（不发送给服务器），并且将自己的名字，用户B的名字，及发送给服务器。
2. 服务器做出响应，发送给A。
3. A发送和给B。
4. B知道因此将解密，从而得到R，然后用R解密得到*M*。

请分析该协议的安全性。若一个敌手可访问该网络中的一个节点，并获取了该节点的密钥，在不知道（）的情况下，他能否恢复明文*M*。

（2）概述Diffie-Hellman密钥交换算法，并给出对该算法的中间人攻击。