1. 消息机密性和消息完整性有什么不同？可以只提供消息机密性而不提供消息完整性吗？可以只提供消息完整性而不提供消息机密性吗？请说明理由。

2. 凯撒密码非常简单，将字符射为字母表中偏移若干位置的字符即可，可以表示为 c= $E(b,p)=(p+b)\ mod\ N$，其中 p 为明文，c 为加密后的密文，密钥 b 为偏移量，N 为字母表的字符个数。凯撒密码的密钥空间的密钥个数总共为 N 个，分别为 0, 1, 2, …, N-1（尽管偏移量为 0 时，密文就是明文，我们也将 0 算作密钥空间的元素）。考虑凯撒密码的变种，密码为[a, b]，可以表示为 c= $E([a,b],p)=(ap+b)\ mod\ N$。假设字母表中允许的字母为英文字母，因此 N=26。对于不同的输入（明文，可取值 0，1，…, N-1），进行加密后的密文一定要求也不同, 因此对于某些 a 来说, 是无法作为密码的。比如 a=2, b=3，有 E([2, 3], 0) = 3，E([2, 3], 13) = 3，因此 a 不能取 2。
   （1） b 的取值有没有限制？
   （2） 在小于 26 的整数中，满足什么条件的值可以作为 a 的取值，具体是哪些？
   （3）该变种的密钥空间的大小是多少？

3. 在一个安全系统中总共有 N 个节点，这些节点之间都要进行通信，并且任何节点都可以看到其他节点传输的分组流，为此需要对通信进行加密，可以有两种选择，一种是采用对称密钥算法，另外一种是采用公开密钥算法，请问各需要多少个密钥对。

4. 采用 RSA 算法，设 p=5, q=11
   （1）求 n 和 z
   （2）若取 e=27，求出满足要求的最小的 d
   （3）对 m=11 进行加密得到密文，然后对该密文解密还原明文。请给出加密和解密的过程

5. 密码哈希函数有哪些基本特性？为什么 Internet 检验和算法不能作为密码哈希函数？

6. 在端点认证中引入了 Nonce，其目的是什么？

7. 考虑 Alice 和 Bob 采用 Diffie-Hellman 密钥交换算法协商共享密钥，假设 n=71， a=7，Alice 和 Bob 选择的私钥 x 和 y 分别为 5 和 12。请问 Alice 和 Bob 发给对方的公钥分别是多少？最后协商的共享密钥是什么？

8. 什么是证书链？

9. SSH 协议支持端口转发，什么是端口转发机制？

10. 在 IPsec 中，为什么 ESP 包含了填充字段，请简要说明采取这种设计的原因。

11. 在 TLS 协议和 IPsec 协议中都用到了顺序号，引入顺序号的目的是什么？两者采用的顺序号机制有什么不同？