1. 已知明文攻击是指密码分析者根据已知的某些明文-密文对来破译密码 （对）
2. DES 算法中 S 盒是该算法中唯一的一种非线性运算 （对）
3. 3 个密钥的 3DES，总的密钥长度达到 168 位 （对）
4. RIJNDAEL 算法不存在弱密钥和半若密钥，能有效抵抗目前已知的攻击 （对）
5. 传统密码既可提供保密性又可提供认证 （对）
6. “一次一密”密码在理论上是绝对不可破译的 （对）
7. 凡是能够确保数据的真实性的公开密钥密码都可以数字签名 （对）
8. 目前影响电子政务、电子商务、电子金融应用的主要技术障碍是网络安全和信息安全问题 （对）
9. 扩散指的是将每一位明文和密钥数字的影响扩散到尽可能多的密文数字中 （对）
10. 盲签名比普通的数字签名的安全性要高（错）
11. DES 算法存在弱密钥，但不存在半弱密钥（错）
12. 为了序列密码的安全，应使用尽可能长的密钥（对）
13. SKIPJACK 算法不是对合运算，所以加密和解密过程不一致（对）
14. 如果一个密码，无论密码分析者截获了多少密文和用什么技术方法进行攻击都不能被攻破，则

称为是绝对不可破译的（对）

1. 对于 CLIPPER 密码算法，如果需要，可经法律部门许可破译密码进行监听（对）
2. Vernam 密码不属于序列密码（错）
3. DES 算法是面向二进制的密码算法，所以可以加解密任何形式的计算机数据（对）
4. Hash 函数要能够用于报文认证，它必须可应用于任意大小的数据块并产生定长的输出（对）
5. M 序列的 0，1 分布及游程分组都是均匀的，而且周期达到最大（对）
6. RIJNDAEL 算法在整体结构上采用的是代替－置换网络构成圈函数，多圈迭代（对）
7. 有限状态自动机密码是我国学者陶仁骥提出的（对）
8. DES 算法中共有四个弱密钥（对）
9. 对于一个 n 级线性移位寄存器，至少有一种连接方式使其输出序列为 m 序列（对）
10. 根据密码分析者可以利用的资源来看，已知密文攻击是对密码分析者最不利的情况（对）
11. 如果一个密码，不能被密码分析者根据可利用的资源所破译，则称为是计算上不可破译的（对）
12. RC4 密码是一种基于非线性数据表变换的序列密码（对）
13. “一次一密”密码在实际应用中是行不通的，因为其密钥管理和密钥分配方面是非常困难的（对）
14. 如果采用相同长度的密钥，则椭圆曲线密码的安全性比 RSA 密码的安全性要高（对）
15. 如果用 AES 算法对 128 位的明文信息进行 10 轮加密，则圈密钥的总长为 1280 位（错）
16. 在公钥密码体制中，密钥的秘密性不需要保护（错）