1、香农建议密码设计的基本方法包括

A、对合运算 B、扩散 C、混淆 D、迭代

2、下列关于 IDEA 算法的描述中，正确的是

A、 IDEA 算法的加密过程由连续的 8 轮迭代和一个输出变换组成

B、 IDEA 算法的每一轮迭代中以 4 个 16 比特的子段作为输入，输出也是 4 个 16 比特的子段

C、 IDEA 算法的 9 轮迭代中，每一轮都需要 6 个 16 比特的子密钥

D、 IDEA 算法的明文、密文和密钥的长度都为 64 比特

3、盲签名与普通签名相比，其显著特点为

A、 签名者是用自己的公钥进行签名

B、 签名者不知道所签署的数据内容

C、 签名者先签名，然后再加密自己的签名，从而达到隐藏签名的目的

D、 在签名被接收者泄露后，签名者不能跟踪签名

4、一个好的口令应该满足

A、应使用多种字符 B、应有足够的长度 C、应尽量随机 D、应定期更换

5、由于传统的密码体制只有一个密钥，加密钥等于解密密钥，所以密钥分配过程中必须保证

A、秘密性 B、可用性 C、真实性 D、完整性

1. RIJNDAEL 算法中的轮函数由下面的那些运算部件组成 abcd

A、行移位 B、字节代换 C、列混合 D、密钥加

2、链接技术是一种掩盖明文数据模式的有效方法，下面关于链接技术正确的说法是 abd

A、 链接是算法的当前输出不仅与当前的输入和密钥有关，而且还与以前的输入与输出有关

B、 采用链接技术，即使明文和密钥相同，所产生的密文也可能不相同

C、 采用链接技术，如果明文和密钥相同，所产生的密文也一定不相同

D、 会产生错误传播

3、公钥密码体制的基本思想包括 acd

A、 将传统密码的密钥一分为二，分为加密密钥 e k 和解密密钥 d k

B、 e k 由加密方确定， d k 由解密方确定

C、 由加密密钥 e k 推出解密密钥 d k 在计算上是不可行的

D、 e k 公开， d k 保密

4、身份识别对确保系统的安全是极其重要的，下面那些方法可以用来进行用户身份认证 acd

A、 用户知道什么 B、用户能做什么 C、用户拥有什么 D、用户的生理特征

5、DES 算法的 S 盒满足下面的那些准则 abd

A、 输出不是输入的线性和仿射函数

B、 任意改变输入中的 1 位，输出中至少有 2 位发生变化

C、 任意改变输入中的 1 位，输出中至少有 3 位发生变化

D、 保持输入中的 1 位不变，其余 5 位变化，输出中的 0 和 1 的个数接近相等

1、分组密码的短块加密方法主要有

A、填充法 B、序列密码加密法 C、输出反馈模式 D、密文挪用技术

2、一种完善的签名应满足下面那些条件

A、签名者的签名应该被保密 B、签名者事后不能抵赖自己的签名

C、签名不能被伪造 D、签名可以通过仲裁机构来仲裁

3、下面那些方法可以用来产生报文认证码

A、序列号 B、报文加密 C、消息认证码 D、散列函数

4、DES 算法的主要缺点有

A、密钥比较短 B、存在弱密钥 C、算法为对合运算 D、存在互补对称性

5、KASUMI 算法设计的原则为

A、安全性要有足够的数学基础 B、算法的软件实现要足够快， C、算法的硬件实现要电路简单，功耗低 D、算法必须采用 Feistel 网络结构