1. 我国的密码分级：

①核心密码：

用于保护党、政、军的核心机密。

②普通密码：

用于保护国家和事企业单位的低于核心机密的机密信息。

③商用密码：

用于保护国家和事企业单位的非机密的敏感信息。

④个人密码：

用于保护个人的隐私信息。

前三种密码均由国家密码管理局统一管理！

2. 我国商用密码政策：

①统一领导：

国家密码管理局统一领导。

②集中管理：

国家密码管理局集中管理。

③定点研制：

只允许定点单位进行研制。

④专控经营：

经许可的单位才能经营。

⑤满足使用：

国内各单位都可申请使用。

3. 密码设计的基本方法

⑴ 公开设计原则

密码的安全应仅依赖于对密钥的保密，不依赖于对算法的保密。

⑵ 扩散和混淆

扩散(diffusion)：将明文和密钥的每一位的影响散布到尽量多的密文位中，理想情况下达到完备性。

混淆(confusion):使明文、密钥和密文之间的关系复杂化。

⑶ 迭代与乘积

迭代：设计一个轮函数，然后迭代。

乘积：将几种密码联合应用

4. S 盒其他准则

非线性度准则：S 盒必须有足够的非线性度，否则不能抵抗线性攻击；

差分均匀性准则： S 盒的差分性应均匀，否则不能抵抗差分攻击；

代数次数及项数分布准则 ：S 盒必须有足够的代线次数和项数，否则不能抵抗插值攻击和高阶差分攻击；

5. AES 的设计要求

①安全性：可以抵抗目前所有已知的攻击；

②实用性：适应各种应用环境，加解密速度快；

③扩展性：分组长度和密钥长度可扩展，可以适应

社会对保密性不断提高的需求。

6. AES 整体特点

①分组密码

明文和密文长度 128 位，密钥长度可变（128/192/256 等，现在选用 128 位）。

②面向二进制的密码算法

能够加解密任何形式的计算机数据。

③不是对合运算

加解密使用不同的算法。

④综合运用多种密码技术

置换、代替、代数

⑤整体结构

SP 结构，基本轮函数迭代，迭代轮数可变（≥10）

7. Hash 函数的作用

Hash 码也称为数据摘要、数据指纹。

具有极强的错误检测能力:

输入有很小的变化，输出将有很大的不同！

检测错误，检测篡改。

用 Hash 码作消息认证码（MAC），可用于认证。

用 Hash 码辅助数字签名：

缩短签名长度

增强签名安全

Hash 函数还可用于伪随机数产生。

8. 传统密码的优缺点：

①优点

- 理论与实践都很成熟。
- 安全容易把握。
- 加解密速度快。

②缺点

- 收发双方持有相同密钥， Ke ＝ Kd ，密钥分配困难，网络环境更突出。
- 不能方便地实现数字签名，商业等应用不方便。

9. SM2 与传统 ECC 比较

- 传统ECC：
  - 计算点X_2（x_2，y_2）=kQ。
  - 计算密文 $C = Mx_2 \bmod n$ 。
  - 最终密文是< X_1，C >
- SM2：
  - 计算点kP_B=(x_2，y_2)；
  - 计算t =KDF(x_2 ‖ y_2, $klen$) ；
  - 计算$C_2 = M \oplus t$；
  - 最终密文是< C_1， C_2， C_3 >
- 传统椭圆曲线密码
  - 利用分量x_2作密钥进行加密：$C = m\,x_2 \bmod n$，加密运算是乘法比较复杂。
  - 分量y_2没有利用。
  - （X_1，C）为密文。
- SM2
  - 利用分量x_2和y_2经过密钥派生函数产生中间密钥t，再用t进行加密：$C_2 = M \oplus t$，加密运算是模2加，因此效率更高，
  - 密钥派生函数提高了安全性，却增加了时间消耗。
  - $C = C_1 \| C_2 \| C_3$为密文，密文数据扩张较前者严重。
  - SM2 采取了许多检错措施，从而提高了密码系统的数据完整性和系统可靠性，进而提高了密码系统的安全性。

- 对于SM2所使用的椭圆曲线，h=1。因此，步骤③对于保密来说是非本质的。但是，如果h或P_B发生了错误或P_B选得不好，致使S=hP_B=O，则它可以把错误检查出来。
- 在解密算法中加入了更多的检错功能，这是因为解密的密文是经过信道传输过来的，由于信道干扰的影响和对手的篡改，在密文中含有错误或被篡改的可能性是存在的。采取措施把错误和篡改检测出来，对提高密码系统的数据完整性、系统可靠性和安全性是有益的。

- 解密算法中的检错
  - ①检查密文C_1是否是正确的。
  - ②进一步检查C_1的正确性，其作用与加密算法中的③类似。
  - ④检查t的正确性，其中包含着C_2的正确性。
  - ⑥检查C_3的正确性。
  - 这样，密文$C = C_1 \| C_2 \| C_3$的正确性都得到检查。

10. 对 RSA 数字签名的攻击

①一般攻击:

- 因为e和n是用户A的公开密钥，所以任何人都可以获得并使用e和n。攻击者可随意选择一个数据Y，并用A的公钥计算

  $X=(Y)^e \bmod n$

- 因为 $Y=(X)^d \bmod n$，于是可以用Y伪造A的签名。因为Y是A对X的一个有效签名。
- 注意：这样的 X 往往无正确语义！因此，这种攻击在实际上有效性不大！

②利用已有的签名进行攻击:

- 攻击者选择随机数据 M_3，且$M_3=M_1M_2 \bmod n$ 。
- 攻击者设法让A对M_1和M_2签名：

  $S_1=(M_1)^d \bmod n$， $S_2=(M_2)^d \bmod n$
- 于是可以由S_1和S_2计算出A对M_3的签名。因为

$S_1S_2=(M_1)^d(M_2)^d \bmod n=(M_3)^d \bmod n=S_3$

- 对策：A不直接对数据M 签名，而是对HASH(M)签名。

- 此时：

  $S_1=(\mathrm{HASH}(M_1))^d \bmod n$， $S_2=(\mathrm{HASH}(M_2))^d \bmod n$

而，

$(\mathrm{HASH}(M_1))^d(\mathrm{HASH}(M_2))^d \neq (\mathrm{HASH}(M_1M_2))^d \bmod n$

- 所以：$S_3 \neq S_1S_2$
- 于是不能由S_1和S_2计算出A对M_3的签名。

③攻击签名获得明文:

- 攻击者截获C，$C=(M)^e \bmod n$ 。
- 攻击者选择小的随机数r，计算：

  $x=r^e \bmod n$，$y=xC \bmod n$， $t=r^{-1} \bmod n$
- 攻击者让A对y签名，

  $S=y^d \bmod n$

  于是攻击者又可截获S
- 攻击者计算$tS=r^{-1}y^d=r^{-1}x^dC^d=C^d=M \bmod n$
- 对策：A不直接对数据M签名，而是对HASH(M)签名。

- 结论:
  - 不直接对数据M签名，而是对HASH(M)签名。
  - 使用时间戳
  - 对于同时确保秘密性和真实性的通信，应当先签名后加密。

11. 比较 SM2 签名算法与传统签名算法

① 传统椭圆曲线密码签名算法是原理性的算法，而SM2是实用性的标准算法

② 两者的基本思想一致：

- 都是以 r, s为签名
- 以 kG 产生r
- 以 d, r, k 产生s

③两者有许多不同

- 传统椭圆曲线签名直接使用m产生签名；
- 而SM2使用$M^* = Z_A \| M$， $e = \text{Hash}(M^*)$
- SM2使用了用户参数和系统参数，起到一定的认证作用，提高了安全性：
  - ID_A是A的标识。$ENTL_A$是ID_A的长度。基点是$G = (x_G, y_G)$
  - A的私钥是d_A，A的公钥是$P_A = d_A G = (x_A, y_A)$
  - $Z_A = \text{Hash}(ENTL_A \| ID_A \| a \| b \| x_G \| y_G \| x_A \| y_A)$
- 传统椭圆曲线签名算法计算：点$R(x_R, y_R) = kG$，并记$r = x_R$；
- SM2计算：点$G_1(x_1, y_1) = kG$，且计算$r = (e + x_1) \bmod n$；

- 传统椭圆曲线签名算法计算：
  $$s = (m - dr)k^{-1} \bmod n$$；
- SM2计算：$s = ((1 + d_A)^{-1} \cdot (k - r \cdot d_A)) \bmod n$。
  M 没有直接出现，而是通过r参与其中；私钥d_A作用了两次。
- SM2增加了合理性检查，确保签名正确，提高安全性。
- 例如第⑤中检查$r+k=n$是否等于n。

如果$r+k=n$，则$k = -r \bmod n$，会使$s = ((1 + d_A)^{-1} \cdot (k - r \cdot d_A)) \bmod n = ((1 + d_A)^{-1} \cdot (-r)(1 + d_A)) = -r \bmod n$。 $s = -r \bmod n$，显然是不合适的。

12. 协议与算法的比较

- 协议和算法都是一组有穷的运算或处理步骤。它们都要求具有有穷性、确定性和能行性。
- 协议强调至少要有两个参与者，而且双方之间还要进行通信。而算法却不要求这一点。
- 例如，计算N以内的自然数的和的方法，对一个合数进行因子分解的方法，都是算法，却都不是协议。因为它们都不要求至少要有两个参与者，一个人就可以计算完成。
- 协议强调完成某一特定任务，而算法强调问题求解。换句话说，协议强调处理，而算法强调计算。

- 协议的执行步骤在粒度上比较粗、比较宏，例如协议的一个步骤可以是执行一个算法。而算法的执行步骤在粒度上比较细，其步骤常常是一些基本运算和操作。
- 由于算法强调计算，所以输入和输出都是一些量。与算法类似，协议也有自己的输入和输出，输入通常是协议执行的一些条件，而输出则是协议执行的结果，结果通常表现为一种状态。
- 总而言之，算法和协议是两种不同层次上的概念。算法是低层次上的概念，而协议是高层次上的概念，协议建立在算法的基础之上。

13. SM2 安全性

中国商用密码SM2密钥分配协议

■ 安全性

- ◆ 由公钥$P = dG = (x, y)$求私钥d，要求解ECDLP问题。这是困难的。
- ◆ 计算共享密钥需要计算点U和V，其中要用私钥d，攻击者没有d，所以攻击是困难的。
- ◆ 在协商所得密钥中包含了用户A和B的身份标识信息、曲线参数信息。这对提高了安全性起到一定的作用。
- ◆ 与SM2的其他算法一样，密钥交换协议也采用了许多检错措施。这不仅提高了协议的数据完整性和系统可靠性，而且也提高了协议的安全性。
- ◆ 从应用看来，这一协议与DH协议相比，比较复杂。如果能够更加简明，则用户应用将会更方便。

	威胁模型	安全目标	
对称加密	唯密文攻击（攻击者弱） CPA 选择明文，同一密钥下 CCA 选择密文（攻击者强）	不可区分性（不泄露明文任何信息）	分组密码 序列密码 保证机密性 速度快，key分两已发生
消息认证码	CMA选择消息攻击	不可伪造性（完整性） （攻击者不能输出消息和标签	对称技术 无真实性 对称加密 Hash
哈希函数		抗弱/强碰撞性	SM3
公钥加密	CPA CCA 唯密文任何人都有	不可区分性	基于大整数分解RSA 基于离散对数ElGamal ECC
数字签名	选择消息攻击 CMA	不可伪造性，完整性，真实性 （抗抵赖，M_A一定是A生成，不能否认） （攻击者不能输出消息和标签） （可由第三方仲裁）	基于大整数分解RSA 基于离散对数ElGamal ECC 公钥技术
密钥协商	被动攻击：只能窃听	不可区分性（不能区分密钥真假） 机密性	diff Herman 协议