第四章

一、填空：

1. RSA 密码算法的安全性是基于_____困难性构建的

2. A 给 B 发送消息时用公钥加密算法进行加密，则加密时使用的密钥是公开钥还是秘密钥？_____该密钥由谁产生？_____

3. A 的密钥对为 PK_A,SK_A, B 的密钥对为 PK_B,SK_B，公钥密码算法记为 $f(\ )$，若 A 给 B 发送一个既加密又认证的消息 m，则密文 C 可表示为_____

4. 蒙哥马利模乘是为了避免求模运算中的_____运算而提出的

5. RSA 中最耗时运算是_____

6. 在 RSA 算法中为保证算法的安全性，对两个大素数 p，q 有什么要求_____和_____

7. 已知一超递增背包向量 A=(1, 3, 5, 11, 21, 44, 87, 175, 349, 701)，现在背包容积为 s＝452，试求该背包的解_____

8. ECC 算法的安全性是基于_____困难问题构建的。

9. 椭圆曲线 $y^2=x^3+x$-2 mod 5 的判别式是_____？

10. 160 比特的 ECC 的安全性相当于_____比特 RSA 算法的安全性；211 比特相当于_____比特 RSA 算法的安全性

二、选择：每一项有 1 个或多个选项是正确的

1. 用户 A 向 B 传输消息 m，采用公钥密码来实现 m 的保密性和认证性，则下列正确的是_____

A 先用 A 的私钥签名，再用 B 的公钥加密　　B 先用 B 的公钥签名，再用 A 的私钥加密

C. 先用 A 的私钥签名，再用 A 的公钥加密　　D 先用 A 的私钥加密，再用 B 的公钥签名

2. A 给 B 发送消息，并对消息进行认证，记 A 的密钥对为(PK_A, SK_A)，B 的密钥对为(PK_B, SK_B)，则 A 用密钥_____对消息加密，B 用密钥_____对消息解密，即可完成。

A. PK_B, SK_B　　B. PK_A, SK_A　　C. SK_B, PK_B　　D. SK_A, PK_A

3. 对公钥密码的可能字攻击属于_____

A 惟密文攻击　B 已知明文攻击　C 选择明文攻击　D 选择密文攻击

4. 基于有限域上离散对数困难性问题构建的体制有_____

A. RSA　B. Rabin　C. ECC　D. NTRU　E. 背包　F. ElGamal 体制

5. 椭圆曲线群 $E_3(1, 2)$上有多少个元素_____　A. 1 个　B. 2 个　C. 3 个　D. 4 个

6. 下列算法中可实现抗抵赖功能的是_____

A. AES　B. MD5　C. ElGamal 签名　D. DH 密钥交换协议

7. 用数字签名算法对所要传送的消息进行签名，并连同消息一起传送给接收方，这种做法可实现

——

A. 对消息来源的认证 B.消息完整性认证 C. 发方身份认证 D. 消息的保密性

8. 公钥密码算法的安全性最强的是下面哪一个

A. 适应性选择密文攻击下不可区分安全(IND-CCA2)

B. 非适应性选择密文攻击下不可区分安全(IND-CCA2)

C. 语义安全的

D. 单向性

三、判断：(正确的划"√"，错误的划"×"，以下同)

1. Millar-Rabin 素性检验算法是一种确定性检验算法 ( )

2. 公钥密码算法也是一种分组加密算法 ( )

3. 对于一个安全的公钥密码算法而言，已知公钥密码算法和加密密钥，求解密密钥在计算上是不可行的 ( )

4. 现有的典型公钥密码算法都是计算上安全的 ( )

5. 可以证明 Rabin 密码体制的安全性与大数分解困难问题等价 ( )

6. 椭圆曲线上的无穷远点为 O=(0,0)。 （ ）

四、简答与计算：

1. 试用扩展欧几里德算法求解 38 mod 103 的逆元

2. 利用蒙哥马利算法求 509 mod 101

3. 已知 RSA 的公钥为 n＝23×29，设加密指数 e＝13，试用扩展欧几里德算法求解私钥 d，并分别完成对消息 456 和 1000 的 RSA 加解密运算过程。

4. 试描述背包密码体制的密钥产生、加密和解密算法

5. 什么是陷门单向函数？

6. 试给出公钥加密体制同时提供加密和认证的过程。

7. 试述公钥密码的可能字攻击及对抗方法

8. 试描述 RSA 算法的密钥产生、加密、解密过程

9. 为了提高 RSA 算法解密速度，假设用户知道 $n=pq$ 的分解，则如何用中国剩余定理进行 RSA 解密，试给出其过程。

10. 试给出 a^{19} mod n 的快速指数算法的运算表达式

11. 已知一系统采用公共模进行公钥加密，攻击者截获了两个密文 c_1 和 c_2，公私钥对分别是（e_1,d_1）和（e_2,d_2）现在攻击者可以判断对应的明文相同，试问如何恢复明文 m

12. RSA 容易受到低指数攻击，试描述该类攻击。

13. 试述针对 RSA 的重复加密攻击。

14. 试述 Rabin 密码体制的密钥产生，加密，解密的过程；如何解决其解密不唯一的问题？

15. 已知一椭圆曲线 $E_7(1,1)$，则单位元是什么，该曲线上 P=(x,y)的逆元是什么，设该曲线上的两个点 P＝(2，2)，Q＝(0,6)，试计算 3P，P+Q

16. 试给出椭圆曲线群 $E_5(1,1)$上的所有点。

17. 如何将明文 m 转化为椭圆曲线上的一个点，如何再从该点中正确提取出 m？

18. 试述基于有限域 GF(p)上离散对数困难问题的 DH 密钥交换算法和 ElGaml 加密算法。

19. 试述基于椭圆曲线 $E_p(a,b)$的 DH 密钥交换算法和 ElGaml 加密算法。

20. 试给出 19P mod p 的快速倍点运算表达式，其中 P 是某椭圆曲线群 $E_p(a,b)$上的一个生成元。

21. 什么是基于身份的密码算法，用户的私钥由谁产生，有什么优点？

22. 试述双线性映射和 BDH 假设

五、证明题：

1. 证明. |p-q|的差值充分小时，n 能够被快速分解

2. 试证：RSA 中的解密算法能够正确恢复明文.

3. 对于 RSA 算法中两个大素数 p，q，试分析如果 2p 与 3q 的差值很小，也能被快速分解。

4. 试证，椭圆曲线群上的 DDH 问题是容易的

六、综合题

采用 KEM+DEM 的混合机制对消息 m 进行加密和认证，假设公钥密码算法是 RSA 算法，数字签名算法也采用 RSA 算法，H( )为 hash 函数，AES 为对称加密算法。请给出加密过程。