## 第七章 公钥密码体制

### 1．是非判断题

(1)公钥密码体制为密码学的发展提供了新的理论和技术基础，它的出现是迄今为止整个密码学发展史上最伟大的一次革命。（ V ）

(2)促使公钥密码体制的出现主要原因是密码专家的智慧。（ X ）

(3)成熟的公钥密码算法出现以后，对称密码算法在实际应用中已无太大价值了。（ X ）

(4)在实际应用中，尽量少用公钥密码技术进行加解密操作，对大量数据作加解密操作，往往结合对称密码技术来实现。（ V ）

(5)在公钥密码体中，用户的私钥和公钥是有关联的，为了保证用户私钥的安全性，用户的公钥是不能公开的。（ X ）

(6) 在 RSA 公钥密码体制中，素数 $p$ 和 $q$ 确定后，可生成多个公私钥对为用户使用。(X)
注：共模攻击

(7) 在 RSA 公钥密码体制中，素数 $p$ 和 $q$ 的选取很重要，影响了私钥的安全性。（ V ）

(8) ElGamal 密码体制是除了 RSA 之外最有代表性的公钥密码体制之一，有较好的安全性，且同一明文在不同的时间所生成的密文是不同的。 （ V ） 注：每次生成随机数不同

(9) 在**相同的安全强度**下，ElGamal 的安全密钥长度与 RSA 的安全密钥长度基本相同。（ V ）

(10) 在 ECC 公钥密码体制中，椭圆曲线确定后，可生成多个公私钥对为用户使用。（ V ）

### 2．选择题

(1) 下列哪个算法不具有雪崩效应。（ D ）

A.DES 加密 B.序列密码生成器 C.哈希函数 D.RSA 加密

(2)公钥密码体制的出现，解决了对称密码体制的密钥分发问题，那么，在公钥密码算法中，加密~~对称密钥~~所使用的密钥是( C )。

A.发送方的公钥 B.发送方的私钥 C.接受方的公钥 D.接受方的私钥

(3)第一个较完善、现使用最多的公钥密码算法是( C )。

A.背包算法 B.Elgamal C.RSA D.ECC

(4)在现有的计算能力条件下，非对称密码算法 RSA 被认为是安全的最小密钥长度是( C )。

A．256 位 B．512 位 C．1024 位 D．2048 位

(5) 在现有的计算能力条件下，非对称密码算法 Elgamal 被认为是安全的最小密钥长度是( C )。

A．256 位 B．512 位 C．1024 位 D．2048 位

(6) 在现有的计算能力条件下，非对称密码算法 ECC 被认为是安全的最小密钥长度是( B )。

A．128 位 B．160 位 C．512 位 D．1024 位

(7) 设在 RSA 的公钥密码体制中，公钥为（e,n）=（13，35），则私钥 d=（ B ）。

A.11 B.13 C.15 D.17

(8)二次筛因子分解法针是对下面那种密码算法的分析方法。( B )

A.背包密码体制 B.RSA C.ElGamal D.ECC

(9) 指数积分法（Index Calculus）针对下面那种密码算法的分析方法。( C )

A.背包密码体制 B.RSA C.ElGamal D.ECC

(10)下面那种公钥密码体制是利用 NP 完全问题来设计公钥密码算法的。( A )

A.背包密码体制　　B.Rabin　　C. Goldwasser-Micali　　D.NTRU

## 3．填空题

(1) 公钥密码体制的思想是基于_陷门单向_函数，公钥用于该函数的__正向__计算，私钥用于该函数的_逆向__计算。

(2) __1976__年，W.Diffie 和 M.Hellman 在_《密码学的新方向》_一文中提出了公钥密码的思想，从而开创了现代密码学的新领域。

(3) 公钥密码体制的出现，解决了对称密码体制很难解决的一些问题，主要体现以下三个方面：__密钥分发问题_、__密钥管理问题_和__数字签名问题__。

(4) 在公钥密码体制中，每用户拥有公钥和私钥，当用户 A 需要向用户 B 传送对称加密密钥时，用户 A 使用__B 的公钥_加密对称加密密钥；当用户 A 需要数字签名时，用户 A 使用__A 的私钥_对消息进行签名。

(5) 在目前计算能力条件下， RSA 被认为是安全的最短密钥长度是_1024_位，而 ECC 被认为是安全的最短密钥长度是_160_位。

(6) 公钥密码算法一般是建立在对一个特定的数学难题求解上，那么 RSA 算法是基于_大整数的素因子分解___的困难性、ElGamal 算法是基于_离散对数求解_的困难性。

*(7) Rabin 公钥密码体制是 1979 年 M.O.Rabin 在论文“Digital signature and Public-Key as Factorization”中提出了一种新的公钥密码体制，它是基于_合数模下求解平方根的困难性_（等价于分解大整数）构造的一种公钥密码体制。*

*(8)1984 年 S.Goldwasser 与 S.Micali 提出了概率公钥密码系统的概念，其安全性是基于_平方剩余问题_的难解性的假设，Goldwasser-Micali 概率公钥密码系统的主要特点是_由于加密过程中引入随机数，使得相同的明文和密钥两次加密的结果是不同的_，其缺点是_加密后数据扩展 $\log_2 n$ 倍_，使用于_比特级_加解密。*

*(9)NTRU 公开密码算法的安全性是基于_数论中在一个非常大的维数格中寻找最短向量的数学难题。*

## 4．术语解释

(1) 公钥密码体制

(2) 陷门单向函数

(3) 大整数因子分解问题

(4) 离散对数问题

(5) 背包问题

(6) *平方剩余问题*