自测练习二参考答案

选择题

① 如果p是素数，a是正整数，那么$a^p \equiv a \pmod p$是____D____定理的推广。

A. Rijndael’s
B. Vignere’s
C. Euler’s
D. Fermat’s

选择题

② 在____D_____中，攻击者为攻击者选择的特定消息伪造签名。

A. 强力攻击

B. 一般性伪造

C. 存在性伪造

D. 选择性伪造

选择题

③ 下列哪种算法____D_____是一种需要使用密钥的算法。

A. MD5

B. SHA-1

C. MD4

D. MAC

选择题

④ MAC函数是____B_____函数。

A. 一对多

B. 多对一

C. 一对一

D. 一对二

选择题

⑤ 发现通信双方之间的通信量模式，比如在面向连接的应用中，确定连接的频率和持续时间，确定消息的数量和长度，是____A_____攻击。

A. 通信流分析
B. 窃听
C. 伪造
D. 内容修改

选择题

⑥ 构造MAC的一种方法是使用对称分组密码，使其对任意长度的输入产生_____A_____输出。

A. 固定长度
B. 可变长度
C. 更长长度
D. 任意长度

选择题

⑦ 哈希函数的主要目的是____A_____。

A. 数据完整性
B. 压缩
C. 抗碰撞性
D. 映射消息

选择题

⑧ _____是一种算法，在计算上无法找到（a）映射到预先指定的散列结果的数据对象或（b）映射到相同散列结果中的两个数据对象。

A. 密码学的散列函数

B. 强抗碰撞能力

C. 单向散列函数

D. 压缩函数

选择题

⑨ 密码学的散列函数要求___D_____，该要求保证不可能找到与给定消息具有相同散列值的替代消息，这样可使用加密散列码防止伪造。

A. 抗碰撞

B. 伪随机性

C. 抗原像攻击

D. 抗第二原像攻击

选择题

⑩ ____A_____是用于验证消息完整性的机制或服务。

A. 消息鉴别

B. 数据压缩

C. 数据映射

D. 消息摘要

选择题

⑪SHA-1产生_____位的散列值。

A. 224

B. 160

C. 384

D. 256

选择题

⑫密码学散列函数的要求包括_____C____，这是单向属性。

A. 抗碰撞
B. 伪随机性
C. 抗原像攻击
D. 抗第二原像攻击

选择题

⑬ Alice 设计了一个密码系统，采用密钥长度为128位的AES算法加密消息，如果要采用RSA算法来加密AES算法的密钥，RSA算法的模n至少应该是多少位，才能保证信息系统的安全性？

A. 1024

B. 2048

C. 3072

D. 7068

判断正误题

⑭（对）消息鉴别可以保护通信双方进行信息交换，防止任何第三方的破坏，但是，它不能保护通信双方不受对方的伤害。

⑮（错）数字签名功能不包括鉴别功能。

⑯（对） DSA中使用散列函数。

⑰（对） Schnorr签名方案基于离散对数。

⑱（对）与RSA不同，DSS不能用于加密或密钥交换。

⑲（对）在数字签名算法DSA中，如果签名的生成过程导致值s＝0，则应生成新的k值。

判断正误题

⑳（错）拥有共享密钥的接收者无法生成验证消息完整性的鉴别码。

21（错）消息加密本身不能提供消息鉴别。

22（对） SH3-512生成的消息摘要长度为64字节。

23（错）如果消息仅被改写了1比特，则用SHA-1生成的消息摘要值也仅发生1比特的改变。

24（错）使用消息鉴别码能保证消息的机密性。

25（错）使用消息鉴别码能够防止否认。