第五章

一、填空：

1. 消息认证中认证符的产生有哪两大类_____和_____

2. 消息认证码和杂凑函数的算法都是公开的，其根本区别是_____

3. MAC 与加密算法的区别在于_____

4. 某 MAC 算法输出长度为 64bit，认证密钥为 160bit，则对 MAC 的穷搜索攻击至少需要____轮

5. 采用先 hash 再对称加密的方法对消息进行认证，设密钥为 k，hash 函数为 H，加密算法为 E，认证的消息为 M，则在考虑和不考虑消息保密性的条件下，认证消息分别可表示为_____

6. 杂凑函数的单向性是指_____ 强单向散列函数是指_____

7. 已知杂凑函数的数出值为 m 比特，则第 I 类生日攻击的复杂度为_____，第 II 类生日攻击的复杂度为____

8. MD5 算法的分组长度为_____输出长度为_____，轮数为_____所以用穷搜索攻击寻找具有给定消息摘要的消息的复杂度为_____以大于 0.5 的概率用穷搜索攻击找出具有相同消息摘要的两个不同消息的复杂度为_____

9. SHA 算法的分组长度为_____输出长度为_____，轮数为_____所以用穷搜索攻击寻找具有给定消息摘要的消息的复杂度为_____以大于 0.5 的概率用穷搜索攻击找出具有相同消息摘要的两个不同消息的复杂度为_____

10. 假设消息的长度为 x，则 MD5、SHA-1、SHA-3 对消息的填充算法分别是_____

11. MD5 以 little-endian 方式存储数据，那么十六进制数 20347AB1 的实际存储是_____

12. HMAC 需要调用_____次 hash 运算，其输出长度由_____决定。

13. 对于一个长度为 n 的 MAC 码算法 $C_K(M)$，随机选取两个消息 M、M'，当 $Pr[C_K(M)=C_K(M')]$=____时，$C_K(M)$是均匀分布的。

二、选择：每一项有 1 个或多个选项是正确的

1. 以下哪些属性是消息认证能够完成的(　).

A.真实性；B.完整性；C.时间性和顺序性；D 不可否认性；E 保密性

2. 设杂凑函数 H( )的输出长度为 m 比特，已知 H(x)，找到 y≠x 满足 H(y)=H(x)的复杂度_____，若找到 y≠x 满足 H(y)=H(x)的概率大于 0.5 则复杂度为_____

A. $O(2^m)$　B. $O(2^{m-1})$　C. $O(2^{m/2})$　D. $O(2^m-1)$

3. $E_K[M||H(M)]$提供了哪些安全服务_____

A. 保密性　B. 完整性　C. 认证性　D. 不可否认性

4. $M||SK(H(M))$提供了哪些安全服务_____，其中 SK 是签名私钥

A. 保密性　B. 完整性　C. 认证性　D. 不可否认性

5. $E_K(M||(H(M||S)))$的安全性和下列哪个相当

A. HMAC　　B. $E_K[M||H(M)]$　　C. $E_{K1}[M||C_{K2}(M)]$　　D. $M||SK(H(M))$

6. SHA-3 标准算法是_____. A. MD5　　B. Keccak　　C. HMAC　　D. Sponge

7. 杂凑函数的单向性是指_____

A. 已知 h，求使得 $H(x)=h$ 的 x 在计算上是不可行的

B. 已知 x，找出 $y(y\neq x)$使得 $H(y)=H(x)$在计算上是不可行的

C. 找出任意两个不同的输入 x、y，使得 $H(y)=H(x)$在计算上是不可行的

8. 下面哪种对消息的认证方式所能提供的安全服务最多_____

A. HMAC(M)　　B. $E_K[M||H(M)]$　　C. $E_{K1}[M||C_{K2}(M)]$　　D. $E_K[M||SK(H(M))]$

三、判断：(正确的划"√"，错误的划"×"，以下同)

1. 采用消息认证码 MAC 认证消息可以实现消息完整性认证和消息源认证　　(　　)

2. 杂凑码是消息中所有比特的函数，因此提供了一定的错误检测能力　　(　　)

3. 带密钥的杂凑函数可以作为一种消息认证码　　(　　)

4. 数据认证算法采用 DES-CBC 模式，所以算法是可逆的　　(　　)

5. MD5 算法已经被破译，因此用于构造 HMAC 时也是不安全的　　(　　)

四、简答与计算：

1. 什么是第 I 类生日攻击和第 II 类攻击

2. 采用数据认证算法对消息进行认证，如果消息为 100bit，则应该怎样对消息填充？

3. 数据认证算法和 DES 的 CBC 模式的区别是什么？

4. 对消息认证码的攻击和对对称密钥算法的攻击在难度上有什么区别？

5. 试分析先加密再认证的 MAC 认证方式是否有被替换的可能，为什么，对安全有危害吗？

（一般没有危害，因为消息源认证是在双方共享密钥的条件下进行的，如果替换为别的密钥，收方可以检测出来，这和先加密再签名的问题不同）

6. 简述用杂凑函数来实现消息认证的三大类基本方式

7. Alice 要给 Bob 发送消息 M，为同时提供对 M 的保密性和认证性保护，试分别给出用消息认证码的实现方法和使用先 hash 再对称加密的实现方法表达式，并比较这两种方法的优劣。

8. 试分析加密密钥和认证密钥分开在安全性上的不同

9. HMAC 算法如何进行预计算？

10. 试描述迭代型杂凑函数的一般结构以及 SHA-3 算法的 sponge 结构

五、证明题：

1. 试证：对于基于 DES-CBC 的数据认证算法，如果仅将第一个分组 D_1 取反，密钥 k 取反，则最后输出的 MAC 也取反。

六、综合题

1. A 要向 B 发送消息 M, 设共享密钥为 k，消息认证码算法记为 $C_k(\quad)$，试回答下列问题：
   (1) 若仅关心 M 的认证性，则 A 发送的消息可表示为？
   (2) 若同时关心保密性和认证性，该怎么办？
   (3) 如果采用的消息认证算法为数据认证算法标准，试述该算法的过程
2. 某用户 A 想要给用户 B 发送一个消息 m，如果要对消息 m 的保密性与认证性进行保护，有四种方法，采用数据认证算法、先 hash 再加密、先签名再加密、HMAC
   (1) 请分别给出这几种方法下认证消息 m 的表达式。所需符号和算法自行定义和选取。
   (2) 其中安全性最强的和最弱的分别是哪一种方法，为什么