《密码学》课程习题

执笔 张焕国

第七章习题

1. 什么是 Hash 函数？Hash 函数与一般的压缩函数有何区别？
2. 密码学 Hash 函数的安全性要求有哪些？
3. Hash 函数在密码学中有何作用？带密钥的 Hash 函数和不带密钥的 Hash 函数在应用方面有何不同？
4. 为什么 SHA-1 要求进行填充数据，使数据长度=448 mod 512？
5. 为什么 SHA-512 要求进行填充数据，使数据长度=896 mod 1024？
6. 在 SHA-1 和 SHA-2 的轮函数中使用参数 W_t 和 K_t 有何作用？
7. SHA-1 和 SHA-2 中使用的基本算术和逻辑函数各是什么？
8. 试计算 SHA-512 中 W_{16}，W_{17}，W_{18}，W_{19} 的值。
9. 编程实现 SHA-1 和 SHA-2 算法。
10. 举例介绍 Hash 函数的实际应用。