学号： 线 姓名： 封 院系： 密

东 南 大 学 考 试 卷

课程名称 移动通信和无线网络安全 **考试学期** 14-15-1 **得分**_____

适用专业 _____ **考试形式** 开卷 **考试时间长度** 120 分钟

一、 问答题 (本大题共 9 题，每题 ~~11.11111111111~~ 分)

1、 有些古典加密算法加密的内容到今天都无法被破解，为什么我们现在不再使用?

答 大部分古典加密算法都未遵守柯克霍夫原则 (Kerckhoffs's principle)，其系统的保密性基于算法的保密性。虽然部分古典算法的保密性能优秀，然而算法一旦泄露，算法加密的内容的安全性将无法保障。

相对地，现代密码学的保密性基于的是密钥的保密。密钥一旦丢失，可以使用新的密钥替代泄露的密钥，并不会妨碍算法和加密内容的安全性。

2、 随着处理器运算能力的增加，现有无法破解的算法是否有可能在未来被破解?

答 有的算法随着运算能力的增加将会被破解。也有的算法，如“一次一密”机制，与运算能力无关，不会随着计算能力的增加而降低安全性。

此外，现代密码学加密算法的安全性依赖的是密钥的长度。考虑到通常处理器运算能力的增加是线性的，而扩展密钥长度带来的密钥空间的增长是指数级的，因此通过不断扩展密钥长度也可以有效解决运算能力的增加带来的风险。

3、 为什么我们在 3 重 DES 算法中使用“加密-解密-加密”的过程，而不是直接加密三次?

答 设三组 DES 算法的密钥分别为 K_1, K_2 和 K_3。当 $K_1 = K_3$ 时，密钥长度被缩短到 112bit。相对于双重 DES 算法，该方法可以有效防止中间相遇攻击。第二步使用“解密”可以增强这种情况下的加密强度。

当 $K_1 = K_2 = K_3$ 时，该算法可以向后兼容 DES 算法，因为第一步和第二步互相抵消了。这种密钥分配方式可以允许 3DES 用户解密单 DES 加密的数据，因为:

$$C = E(K_1, D(K_1, E(K_1, P))) = E(K_1, P)$$
$$P = D(K_1, E(K_1, D(K_1, P))) = D(K_1, C)$$

4、 已知密钥的情况下，能不能通过 HMAC 码推导出对应的明文? 为什么?

答 视使用的 Hash 函数而定。

当已知密钥时，攻击者想要通过 HMAC 码推导出对应的明文，就需要找到 Hash 函数中的碰撞，即寻找到一条消息 M’，其哈希值 Hash(M’) 与需要破译的明文 M 的哈希值 Hash(M) 相等。可以证明，对于 n 位的 Hash 码，碰撞所需的代价是 $2^{\frac{n}{2}}$ 数量级的。根据现有的技术，若代价是 2^{64} 数量级的，则被认为可以通过暴力破解完成，因此 MD5 算法可能被破解。而分组更长的 SHA-1 和 SHA-256 则无法被暴力破解出明文。

5、 对于 Diffie-Hellman 密钥交换协议，攻击者生成两组公/私钥对能够形成中间人攻击。请问攻击者只生成一组公/私钥对能否实现 Diffie-Hellman 协议的中间人攻击? 如果能，请说明理由。

答 能实现 Diffie-Hellman 协议的中间人攻击。攻击过程如下:

(a) B 给 A 发送公钥 Y_B。

(b) 中间人 E 监听到该消息，将 B 的公钥 Y_B 保存下来，并向 A 以 B 的用户标志发送带有 E 的公钥 Y_E 的报文。A 接收了 E 的报文，并将 E 的公钥 Y_E 和 B 的用户标志一起存储。同样地，E 伪装成 A 向 B 发送了带有 Y_E 的报文。

(c) B 在 B 的私钥 Y_B 和 Y_E 的基础上计算会话秘钥 K_1，A 在 A 的私钥 Y_A 和 Y_E 的基础上计算会话秘钥 K_2。E 使用 E 的私钥 X_E，Y_B 与 Y_A 分别计算出 K_1 和 K_2。

(d) 之后，E 就可以转接 A 到 B 和 B 到 A 的消息来获得 A 与 B 的通信内容，而 A 与 B 无法得知他们在与 E 共享通信。

6、 用户 A 与用户 B 进行通信，已知用户 A 和用户 B 共享密钥 K，用户 A 为了验证用户 B 的身份采用了如下方法：

步骤 1：用户 A 产生一个随机数 N，用它和 K 异或，产生 C 值；

步骤 2：用户 A 将 C 值发给用户 B，用户 B 拿到 C 后，用 K 与之异或，得出 N；

步骤 3：用户 B 将 N 发送给 A，A 验证之。

问：这种验证方法是否存在安全漏洞？为什么？

答 这种验证方法存在安全漏洞。

假设攻击者 E 可以监听 A 与 B 的通信内容。在步骤 2 中，E 可以得到 A 向 B 发送的 C 值；在步骤 3 中，E 可以得到 B 向 A 发送的 N 值。在此基础上，将 C 和 N 异或，就可以计算出 A 与 B 通信的密钥 K。

7、 试讨论流加密算法的架构，及其使用时需要注意的问题。请描述无线局域网 WEP 机制中的设计，并解释其如何解决流加密算法中的问题。

答 流加密算法每次加密一个字节的明文。流加密算法将密钥输入到一个伪随机数发生器中，发生器输出一串伪随机的序列，成为密钥流。将密钥流和明文流的每个字节进行按位异或运算，得到密文序列。

使用流加密时需要注意的问题是：

(a) 加密序列的周期要长。伪随机数发生器使用的函数产生的是确定性的比特流，该比特流最终将出现重复。重复的周期越长，密码分析的难度就越大。

(b) 密钥流应该尽可能的接近于真正随机数流的特征。密钥流的随机特性越好，则密文越随机，密码分析就越难。

(c) 随机数发生器的输出受输入秘钥 K 的调节。为了防止穷举攻击，密钥也应该足够长。

WEP 机制中使用了 RC4 流加密算法。该算法是一个可变密钥长度、面向字节操作的流加密算法。RC4 的核心部分——S-box 的长度可以随意调整，且算法的运算速度可以达到 DES 的 10 倍左右。该算法包括密钥调度算法 (KSA, Key-Scheduling Algorithm) 和伪随机子密码生成算法 (PRGA, Pseudo-Random Generation Algorithm)，能够有效地扩展生成的加密序列的长度，增强加密算法的安全性。

8、 GSM 体系是如何提供匿名保护的？试分析 GSM 匿名保护的安全性能。

答 为保证用户身份的机密性，对用户的鉴权成功后，网络为用户分配临时移动用户标识符 TMSI 来代替国际移动用户标识符 IMSI，使第三方无法在无线信道上跟踪 GSM 用户。TMSI 在 GSM03.03 中定义，只有在某个 VLR 范围内有意义，必须和位置区域标识符 LAI 一起使用。VLR 负责管理合适的数据库来保存 TMSI 和 IMSI 之间的对应关系。

当 TMSI 认证失败或旧的 VLR 不可达时，网络请求 MS 发送 IMSI，利用 IMSI 重复认证步骤。这时 IMSI 以明文形式在空中传输，这是系统的一个漏洞。

9、 试说明如何破解 WEP 机制的完整性保护机制并分析其安全性能，并给出相应的改进建议。

答 WEP 采用 CRC 循环校验作为其完整性保护方法，CRC 是一种线性的校验算法，容易受到攻击。已知密钥 K 和明文 M，密文 C 可以由以下方法得到：

$$C = RC4(iv, K) \oplus \{M, crc32(M)\}$$

如果攻击者伪造明文 M'，使得 $M' = M + \Delta$，可以得到以下密文：

$$C' = C \oplus \{\Delta, crc32(\Delta)\}$$

显然，该密文也能够通过 CRC32 算法的完整性校验。

鉴于 CRC 循环校验算法的完整性保护性能较为简陋，可以考虑采用基于密码学的消息认证算法，如 MD5，SHA-1 或 RIPEMD-160 等 Hash 函数。

(答案仅供参考)