公钥密码学

C3.1. 在 Diffie-Hellman 密钥交换中，Alice 将 $g^x \mod p$ 发送给 Bob，Bob 将 $g^y \mod p$ 发送给 Alice。他们如何得到共同的秘密值？

C3.2. 在 Diffie-Hellman 密钥交换协议中，攻击者知道 g、p 和 $g^x \mod p$。为什么仍然无法由这些数据求出 x？

C3.3. 令 $n = 3 \times 11$、$e = 3$，求私有指数 d。

C3.4. 令 $n = 2419 = 41 \times 59$、$e = 7$。（1）求私钥指数 d；（2）加密消息 6；（3）对消息 10 签名。假设使用 RSA，只需给出计算式，无需算出后两问的最终数值。

C3.5. 我们选择 $p = 17$ 和 $q = 13$，我们可以选择 $e = 3$ 作为公共指数吗？

C3.6. Bob 刚刚发现了一种高效的大整数分解算法：对于任意给定的整数 n，他都能在 $O(\log(n))$ 时间内完成因数分解。请说明这一发现会对 RSA 算法产生什么影响。

C3.7. 在 RSA 中，为什么解密的计算开销通常高于加密？

C3.8. 为什么要使用混合加密？为什么不能只用公钥密码算法加密所有数据？

C3.9. 设 M 是一个 1000 字节的字符串。Bob 想直接使用 2048 位 RSA 密钥加密 M，即计算 $M^e \mod n$。这样做可行吗？

C3.10. 在 RSA 中，$(M^e)^d \mod n$ 与 $(M^d)^e \mod n$ 都得到 M。Bob 因此决定把 e 作为私钥用于解密，并公开 d 作为公钥用于加密。这种做法安全吗？

C3.11. 在 PKCS#1 v1.5 和 OAEP 填充方案中，填充结果的第一个字节总是 `00`。其主要目的是什么？

C3.12. 使用 PKCS#1 v1.5 对消息 M 填充，结果如下。哪一部分是原始消息 M？

```
0002 19ba 93fa 39af ... 039a 8818 1903 dfa0 3300 fa31 ff93 dd19
cad5 6356 fa30 f003
```

C3.13. 同一消息加密两次时应产生不同密文。请说明 AES-128-CBC 和 RSA 分别如何实现这一性质。

C3.14. AES-128-CBC 和 RSA 都使用填充，但目的不同。请说明二者的区别。

C3.15. ★

数字签名通常作用于消息的单向哈希值，而不是直接作用于消息本身。原因之一是计算开销：对较短的哈希值签名比对可能很长的消息签名更高效。Bob 表示他的消息总是很短，因此决定直接对消息签名，而不先计算哈希。(1) 在不知道 Bob 私钥的情况下，能否构造一对 (m, s)，使 s 是 Bob 对消息 m 的有效签名，而 m 的内容可以任意？(2) 如果 Bob 改为对消息的单向哈希值签名，还能构造出这样的一对吗？

C3.16. 与基于密码的方案相比，基于公钥的身份认证方案有哪些优点？

C3.17. Charlie 为同为密码学家的 Alice 和 Bob 安排了一次相亲，两人此前并不认识。Bob 想确认赴约者确实是 Alice。赴约前，Bob 从 Charlie 处获得了 Alice 的公钥。请说明 Bob 如何要求 Alice 证明自己的身份（请不要在现实约会中尝试这种做法，否则你可能再也见不到对方了）。

C3.18. ★

有人要求你用私钥签署一个看起来随机的数。你认为签署这种随机数没有危害。你是否同意？为什么？

C3.19. 在信用卡芯片技术中，终端如何确认一张信用卡是由授权银行发行的？

C3.20. 在信用卡芯片技术中，发卡机构如何确认持卡人已经批准了一笔付款？