数字签名和密码协议习题

1. 在 RSA 数字签名方案中, Bob 的公钥是(n, e), 私钥是 d。Bob 对消息 x_i 进行签名, 并将消息 x_i 与签名 s_i 和他/她的公钥一起发送给 Alice。Oscar 可以实施中间人攻击, 即 Oscar 可以在公开信道上用自己的公钥取代 Bob 的公钥。Oscar 的目标是更改消息 x_i 并为其提供数字签名, 且该签名能被 Alice 验证通过。请给出 Oscar 进行攻击的具体过程。

2. 给定一个 ElGamal 签名方案, 这里不对消息进行 Hash 变换而直接对消息进行签名, 其中 $p = 31$, $g = 3$ 是 Z_{30}^*的一个生成元, 公钥为 $y = 6$。假设收到两次消息 $x = 10$ 的签名(r, s)如下:

   (a) (17, 5)

   (b) (13, 15)

   1) 两个签名都有效吗? 请给出验证过程。

   2) 对于某个特定的消息 x 和上面选择的特定参数存在多少个有效签名?

3. 对于 DSA 数字签名, 如果在签名中使用相同的随机数 k 对两个不同的消息进行签名, 那么这种情况下可以如何进行攻击? (提示: 如何根据这两个消息的签名恢复出签名私钥 x)

4. ECDSA 的参数由曲线 E: $y^2 = x^3 + 2x + 2 \bmod 17$ 给出, 点 P (5, 1)的阶 $q = 19$, Bob 的私钥 $d = 10$。对给定的哈希函数值 $h(x) = 12$ 及所选取的随机数 $k = 11$, 请给出签名(Bob)和验证(Alice)的过程。

   这里给出该曲线上的所有点 $2P = (5, 1)+(5, 1) = (6, 3)$, $3P = 2P+P = (10, 6)$, $4P = (3, 1)$, $5P = (9, 16)$, $6P = (16, 13)$, $7P = (0, 6)$, $8P = (13, 7)$, $9P = (7, 6)$, $10P = (7, 11)$, $11P = (13, 10)$, $12P = (0, 11)$, $13P = (16, 4)$, $14P = (9, 1)$, $15P = (3, 16)$, $16P = (10, 11)$, $17P = (6, 14)$, $18P = (5, 16)$, $19P = O$。

5. 设秘密消息为 $M = 11$, 构造 (3, 5) 门限秘密共享方案。随机选取正整数 7 和 9, 选取多项式 $f(x) = (7x^2 + 9x + 11) \bmod 13$。

   1) 计算 5 个秘密份额 (影子)。

   2) 试从任意 3 个秘密份额 (影子) 中恢复消息 M。