数字签名和密码协议习题答案

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。

解：Oscar 从公开信道中接收到消息 x_i，对 x_i 进行篡改生成 x_i'，然后使用自己的私钥 d' 对 x_i'进行签名得到 s_i'。然后把消息 x_i', 签名 s_i' 以及自己的公钥(n', e')发送给 Alilce。

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?

解：(1) $g^x = 3^{10} \equiv 25 \bmod 31$

(a) 由 $r = 17$，$s = 5$，可得 $t = y^r \cdot r^s = 6^{17} \cdot 17^5 \equiv 26 \cdot 26 \equiv 25 \bmod 31$，即 $t=g^x$ 验证通过。

(b) 由 $r = 13$，$s = 15$，可得 $t = y^r \cdot r^s = 6^{13} \cdot 13^{15} \equiv 26 \cdot 26 \equiv 25 \bmod 31$，即 $t=g^x$ 验证通过。

(2) Elgamal 签名是概率型的签名，对于某个消息存在 p-1 个有效的签名。

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)

解: 假设对消息 x_1，x_2 使用相同随机数进行签名得到 s_1，s_2。即：

$$s_1 \equiv (H(x_1) + dr) \cdot k_E^{-1} \bmod q$$
$$s_2 \equiv (H(x_2) + dr) \cdot k_E^{-1} \bmod q$$

攻击者可以按照如下方式恢复出私钥：

$s_1 - s_2 \equiv k_E^{-1} \cdot (H(x_1) - H(x_2)) \bmod q$

$\Leftrightarrow k_E \equiv \frac{H(x1) - H(x2)}{s1 - s2} \bmod q$

$\Rightarrow\ d\ \equiv\ \frac{s1\cdot kE\ -\ H(x1)}{r}\ \bmod q$

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), $19P = O$。

解：Bob 进行签名的过程如下：

(1) Bob 计算公开密钥 $Q = dP$=(7, 11),。

(2) 计算 $R = kP$ =(13, 10), $c = x(R) \bmod n = 13 \bmod 19$。

(3) 计算 $k^{-1} \bmod n = 7 \bmod 19$。

(4) 计算 $s = k^{-1}(h(x) + dc) \bmod n = 6 \bmod 19$。

得到签名为($h(x)$, c, s)=(12, 13, 6)。

Alice 进行验证的过程如下：

(1) 计算 $k_1 = h(x)\ s^{-1} \bmod n = 2 \bmod 19$ 以及 $k_2 = cs^{-1} \bmod n = 18 \bmod 19$。

(2) $R' = k_1P + k_2Q$ = (13, 10)。

(3) $c = x(R') \bmod 19$, 验证通过。

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。

解：

1) 选取 x = 1，2，3，4，5， 代入公式 $f(x)=(7x^2 + 9x + 11) \bmod 13$，可得 5 个秘密份额分别为：1，1），（2，5），（3，10），（4，3），（5，10）。

2）选择三个秘密份额，如（1，1），（2，5），（3，10）恢复消息 M。

根据公式：$f(x) = \sum_{i=1}^{3} y_i \prod_{j=1, j\neq i}^{3} \frac{(x-x_j)}{(x_i-x_j)} \bmod p$ 可得 M = 11。