应用密码学作业 #6

XXX：202XX80XXXXXXXXX

2023 年 4 月 14 日

1 DSA 签名

若 $s = 0$，则 $k^{-1}(SHA(M) + xr) = 0 \mod q$。而 k^{-1} 必不等于 0 $\mod q$，故 $SHA(M) + xr = 0 \mod q$。

而由于签名中包含 M，故可以计算出 $SHA(M)$，且 r 也已知，则可计算私钥 $x = -SHA(M)r^{-1} \mod q$。即 $s = 0$ 时，私钥是可以被计算出来的。所以应该避免这种情况。

2 ElGamal 签名

(1) 本题中，字母 β 表示的应当是公钥，v 表示的是随机数 k。

要证明 (r, s) 数对是消息 $m = su \mod (p-1)$ 的一个有效签名，只需验证 $\alpha^m = \beta^r r^s$ 即可。

$$\alpha^m = \alpha^{su} = (\alpha^u)^s = (r\beta^{-v})^s = r^s\beta^{-vs} = r^s\beta^{-v(-rv^{-1})} = \beta^r r^s$$

验证成立

(2) 若采用对消息的散列函数进行签名，则需要验证签名的等式应当为 $\alpha^{h(m)} = \beta^r r^s$，那么伪造消息就要找到一个消息，使得其散列值 $h(m) = su$。总所周知，由于散列函数的单向性，对于某一个固定的散列输出，要找到其可能对应的某个输入是困难的，所以攻击者很难找到一个 m，使得 $h(m) = su$，故能抵御存在伪造攻击。

3 Shamir 秘密分享

$$\begin{aligned}
f(x) &= y_1\frac{(x-x_2)(x-x_3)}{(x_1-x_2)(x_1-x_3)} + y_2\frac{(x-x_1)(x-x_3)}{(x_2-x_1)(x_2-x_3)} + y_3\frac{(x-x_1)(x-x_2)}{(x_3-x_1)(x_3-x_2)} \\
&= 8\frac{(x-3)(x-5)}{8} + 10\frac{(x-1)(x-5)}{-4} + 11\frac{(x-1)(x-3)}{8} \\
&= (x-3)(x-5) + 6(x-1)(x-5) + 12(x-1)(x-3) \\
&= 2x^2 + 10x + 13
\end{aligned}$$

故秘密为 13。

4 公平猜拳游戏

设猜拳的两个人分别为 $Alice$ 和 Bob，由于出拳的方式有三种，故每次出拳都包含大约两比特信息。规定，$Alice$ 和 Bob 的通信，其要传递的消息 m 包含两比特，出拳为“锤子”时，$m = 00$；出拳为“剪刀”时，$m = 01$；出拳为“步”时，$m = 10$；现规定游戏流程如下：

(a) $Alice$ 随机选择 r_a，并选择自己的出拳方式 m_a，利用 $Hash$ 函数 h 计算：$H_a = h(r_a, m_a)$，然后把 H_a 发送给 Bob；

(b) Bob 随机选择 r_b，并选择自己的出拳方式 m_b，利用 $Hash$ 函数 h 计算：$H_b = h(r_b, m_b)$，然后把 H_b 发送给 $Alice$；

(c) $Alice$ 将 r_a, m_a 发送给 Bob；

(d) Bob 将 r_b, m_b 发送给 $Alice$；

(e) $Alice$ 和 Bob 验证对方发送的随机数、消息和哈希值是否符合 $H = h(r, m)$，并确定这次猜拳的结果。

说明：步骤 a, b 为出拳方式，没有顺序；步骤 c, d 也没有顺序，但是步骤 c, d 一定要在步骤 a, b 完成之后才可以进行。