ComSec作业11：数字签名

Review

Review:

13.2.数字签名应该具有哪些性质？

①它必须能验证签名者，签名日期和时间

②它必须能认证被签的消息内容

③签名应能由第三方仲裁，以解决争执

因此，数字签名具有认证功能

13.3.数字签名应满足哪些要求？

①签名必须是与消息相关的二进制位串

②签名必须使用发送方某些独有的信息

③产生数字签名比较容易

④识别和验证签名比较容易

⑤伪造数字签名在计算上不可行。无论是从给定的数字签名伪造信息，还是从给定的消息伪造

⑥保存数字签名的副本是可行的。

13.6.直接数字签名方法中会遇到哪些威胁？

这些方法的有效性依赖于发送方的私钥的安全性。如果发送方想否认以前曾发送过某条消息，那么他可以称其私钥已丢失或被盗用，其他人伪造了他的签名。

另一种可能的威胁是，X的私钥可能在时刻T被盗用，但攻击者可用X的签名签发一条消息并加盖一个在T或T之前的时间戳。

13.2.数字签名应该具有哪些性质？

①它必须能验证签名者、签名日期和时间

②它必须能认证被签的消息内容

③签名应能由第三方仲裁，以解决争执

因此，数字签名具有认证功能

13.3.数字签名应满足哪些要求？

①签名必须是与消息相关的二进制位串

②签名必须使用发送方某些独有的信息

③产生数字签名比较容易

④识别和验证签名比较容易

⑤伪造数字签名在计算上是不可行的。无论是从给定的数字签名伪造信息，还是从给定的消息伪造数字签名，在计算上都是不可行的。

⑥保存数字签名的副本是可行的。

13.6.直接数字签名方法中会遇到哪些威胁?

方法的有效性依赖于发送方的私钥的安全性。如果发送方想否认以前曾发送过某条消息，那么他可以称其私钥已丢失或被盗用，其他人伪造了他的签名。

另一种可能的威胁是，X的私钥可能在时刻T被盗用，但攻击者可用X的签名签发一条消息并加盖一个在T或T之前的时间戳。

Problem

13.6.

(a)

显然 Z_p^* 的群阶是 p-1

由费马小定理得

$g^{p-1} \equiv 1 \mod p$

由题可知

$g^q \equiv 1 \mod p$

由拉格朗日定理，不难证明：

有限群里元素的阶整除群的阶

注意到

q 是素数且 $q \mid (p-1)$

设g的阶是r

显然 $r \leq q$ 且 $r|(p-1)$

假设 r < q

则 $q = kr + c$, $c < r$

$g^{kr} = (g^r)^k \equiv 1 \mod p$

$g^q = g^{kr+c} \equiv g^c \equiv 1 \mod p$

与 r 是 g 的阶 相矛盾

所以假设不成立

所以 r = q

即 g 的阶是q

(b)

由费马小定理

$h^{(p-1)} \equiv 1\ mod\ p$

由题可知

$g = h^{(p-1)/q}\ mod\ p$

即

$g^q \equiv h^{(p-1)} \equiv 1 \mod p$

由拉格朗日定理，不难证明：

有限群里元素的阶整除群的阶

注意到

q 是 素数 且 $q \mid (p-1)$

设g的阶是r

显然 $r \leq q$ 且 $r|(p-1)$

假设 r < q

则 $q = kr + c$, $c < r$

$g^{kr} = (g^r)^k \equiv 1 \mod p$

$g^q = g^{kr+c} \equiv g^c \equiv 1 \mod p$

与 r 是 g 的阶 相矛盾

所以假设不成立

所以 r = q

所以 g 的阶是q

(c)

由拉格朗日定理可知一共有

$\phi(q) = q - 1 = 156$ 个生成元

所以

每轮循环找到生成元的概率为：

$p' = 256/40192$

用$\epsilon = k$ 表示 前 k - 1 次均取到非生成元，而第k次取到生成元

因此

$P(\epsilon = k) = (1 - p')^{k-1} * p'$

可见 ϵ 服从几何分布

数学期望：

$E\epsilon = 1/p' = 40192/156$

即为所求

(d)

$p = O(2^{1024})$

$q = O(2^{160})$

$E\epsilon = O(\sqrt{2^{160}}) = O(2^{80})$

不愿意，因为该算法不是一个多项式时间算法

(e)

156/40192