Assignment 5

Tuesday, December 7, 2021 10:09 PM

1. $y = \alpha^k \bmod p$ To verify, we need to compute $B^\delta y^y$

$\delta = (x - ky)a^{-1} \bmod (p-1)$

$a\delta \equiv (x-ky)a^{-1} \cdot a \pmod{p-1}$

$a\delta + ky \equiv x \bmod (p-1)$

$\alpha^x = \alpha^{(a\delta + ky)} = \alpha^{a\delta}\alpha^{ky} = (\alpha^a)^\delta (\alpha^k)^y = B^\delta y^y \pmod p$

so $\alpha^x = B^\delta y^y \pmod p \rightarrow ver_k(x,(y,\delta)) = true$

Because α, B and p are part of A's public key, this proves that with x as the message it is verified using public key of B and p with signature variables of δ and y.

b. With the original scheme, you have to compute the inverse of k in mod $(p-1)$ of y for each message x. For modified scheme, you can invert a, a primitive element, guarenteed to be invertible in mod$(p-1)$, one time for all messages. Resulting in a faster computation

c. The original scheme is dependent on DLP

As given private key a, finding δ:

$B^\delta = \alpha^a y^y$.

finding a:

$y^y = \alpha^a B^{-\delta}$ and both is

$y^y B^\delta = \alpha^a$

So modified scheme has security that is less secure than original

2. $q = 101$, $p = 7879$, $\alpha = 170$, $a = 75$, $B = 4567$

Determine signature of message x so $SHA\text{-}1(x) = 52$ using $k = 49$

$y = (\alpha^k \bmod p) \bmod q = (170^{49} \bmod 7879) \bmod 101 = 1776 \bmod 101$
$= 59 \bmod 101$

$\delta = (SHA\text{-}1(x) + a \cdot y) \cdot k^{-1} \bmod q =$

$(52 + 75(59)) \cdot 33 \bmod 101 = 79$

Signature $(x, 49) = (59, 79)$

Verification:

$e_1 = SHA\text{-}1(x) \cdot \delta^{-1} \bmod q = 52 \cdot 79^{-1} \bmod 101$
$= 52 \cdot 78 \bmod 101 = 16$

$e_2 = y \cdot \delta^{-1} \bmod q = 59 \cdot 78 \bmod 101 = 57$

$(\alpha^{e_1} \cdot B^{e_2} \bmod p) \bmod q = y$

$(170^{16} \cdot 4567^{57} \bmod 7879) \bmod 101 = 59 = y$

so $ver_k(x, (59, 79)) = true$

b. Schnorr Signature Scheme:

k to sign message x_1 and x_2

x_1: $y_1 = h(x_1 \| \alpha^k) \bmod p$
$\delta_1 = k + \alpha y_1 \bmod q$

x_2: $y_2 = h(x_2 \| \alpha^k) \bmod p$
$\delta_2 = k + \alpha y_2 \bmod q$

$\delta_1 - \delta_2 = \alpha(y_1 - y_2) \bmod q$
$\gcd(y_1 - y_2, q) = 1$
$a = (\delta_1 - \delta_2)(y_1 - y_2)^{-1} \bmod q$

If $\gcd(y_1 - y_2, q) = d > 1$ then

$q' = \frac{q}{d}$ $y' = \frac{y_1 - y_2}{d}$ $\delta' = \frac{\delta_1 - \delta_2}{d}$

then: $a'y' = \delta' \bmod q'$
$a' = \delta' y'^{-1} \bmod q'$
$a = a' + iq' \bmod q$ where $0 \le i \le d-1$

So a is found by finding i, so that $B = \alpha^a$

DSA:

x_1: $y = (\alpha^k \bmod p) \bmod q$
$\delta_1 = (SHA\text{-}1(x_1) + ay)k^{-1} \pmod q$

x_2: $y = (\alpha^k \bmod p) \bmod q$
$\delta_2 = SHA\text{-}1(x_2) + ay)k^{-1} \bmod q$

so

$(\delta_1 - \delta_2)k = SHA\text{-}1(x_1) - SHA\text{-}1(x_2) \bmod q$

then if $\gcd(\delta_1 - \delta_2, q) = 1$ then

$k = (SHA\text{-}1(x_1) - SHA\text{-}1(x_2))(\delta_1 - \delta_2)^{-1} \bmod q$

then if $\gcd(\delta_1 - \delta_2, q) = d > 1$ then

$\delta' = \frac{\delta_1 - \delta_2}{d}$ $x' = \frac{SHA\text{-}1(x_1) - SHA\text{-}1(x_2)}{d}$ $q' = \frac{q}{d}$

$k'\delta' = x' \pmod{q'}$

so $k' = \delta'^{-1} x' \pmod{q'}$
$k = \delta'^{-1} x' + iq \pmod q$, $0 \le i \le d-1$

then $\delta_1 = k + ay_1$
$a = (\delta_1 - k)y_1^{-1} \pmod q$

c. $z = (SHA\text{-}1(x))^{-1} \bmod q$ $\epsilon = B^z \bmod p$

$y = ((\alpha\epsilon^y)^{\lambda^{-1} \bmod q}) \bmod p \bmod q$

$\delta = \lambda(SHA\text{-}1(x) \bmod q$

to verify:

$(\alpha^{e_1} B^{e_2} \bmod p) \bmod q = y$

$y = ((\alpha B^{(SHA\text{-}1(x))^{-1} y})^{\lambda^{-1} \bmod q}) \bmod p \bmod q$

$e_1 = SHA\text{-}1(x)\,\delta^{-1}$ $e_2 = y\delta^{-1}$

$\delta = \lambda \cdot SHA\text{-}1(x)$

$\delta^{-1} = \lambda^{-1} \cdot (SHA\text{-}1(x))^{-1}$

$e_1 = \lambda^{-1}$ $e_2 = \lambda^{-1}(SHA\text{-}1(x))^{-1} \cdot y$

so:

$\alpha^{\lambda^{-1}} B^{(SHA\text{-}1(x))^{-1} y \lambda^{-1}}$

$(\alpha B^{(SHA\text{-}1(x))^{-1} y})^{\lambda^{-1} \bmod q}) \bmod p \bmod q = y$

$B = \alpha^k \bmod p \bmod q$

3. public key (p, α, B) $B = \alpha^a \bmod p$

$y = \alpha^k \bmod p$ $\delta = (m - ay)k^{-1} \pmod{p-1}$

$= (13, 7, 5)$

$A \Rightarrow m_1 = 2$ $(y_1, \delta_1) = (11, 1)$
$m_2 = 1$ $(y_2, \delta_2) = (11, 8)$

$\delta = (m - ay)k^{-1} + \lambda(p-1)$

$\delta = mk^{-1} - ayk^{-1} + \lambda(p-1)$

$(\delta - mk^{-1} + ayk^{-1})k = \lambda(p-1)$

$\delta k + ay = m + \lambda(p-1)$

$y_1 = 11 = \alpha^{k_1} \bmod 13$ $\delta_1 = (m_1 - ay_1)k^{-1} \bmod (p-1)$

$y_2 = 11 = \alpha^{k_2} \bmod 13$ $\delta_2 = (m_2 - ay_2)k^{-1} \bmod (p-1)$

so $y_1 = y_2 \Rightarrow k_1 = k_2 = k$

$m_1 = \delta_1 k + ay_1$
$m_2 = \delta_2 k + ay_2$
$\xrightarrow{y_1 = y_2}$ $m_1 - m_2 = k(\delta_1 - \delta_2) \pmod{p-1}$

so

$k = (m_1 - m_2)(\delta_1 - \delta_2)^{-1} \pmod{p-1}$

$a = (m_1 - \delta_1 k)y^{-1}$

$a = (m_1 - \delta_1 (m_1 - m_2)(\delta_1 - \delta_2)^{-1}] y^{-1} \bmod p-1$

$a = (2 - 1(2-1)(1-8)^{-1}) 11^{-1} \bmod 12$

$a = (2 - (1)(-7)^{-1}) 11^{-1} \bmod 12$

$a = (2 - 5) 11 \bmod 12$

$a = -3(11) \bmod 12 = -33 \bmod 12$

$a = -33 \bmod 12 = 3 \bmod 12$

b. If $a = k$ then

$m_1 = (\delta_1 + y_1)k \pmod{p-1}$

$m_2 = (\delta_2 + y_2)k \pmod{p-1}$

then k would be solved, which results in a as $a = k$

also E would notice this as B and y would always be the same no matter the message, m and $m_1 - m_2$ would be scaled by

$(\delta_1, y_1) - (\delta_2, y_2)$

4. public key (p, α, B) $B = \alpha^a$

a. $\delta = ay + km \pmod{p-1}$ instead of $\delta = k^{-1}(m - ay)$

$y = \alpha^k \bmod p$

$\delta = a\alpha^k + km \bmod p-1$

$\alpha^\delta = \alpha^{a\alpha^k + km} = \alpha^{a\alpha^k}\alpha^{km}$

$B^y = \alpha^{a \cdot y} = \alpha^{a\alpha^k}$ $= y^m = \alpha^{km}$

so verification of signature for this scheme is:

$B^y \cdot y^m = \alpha^\delta$ or $y^m = \alpha^\delta (B^y)^{-1}$

b. $\alpha^q = 1$ $B = \alpha^a \bmod p$ $y = m^{-1}\alpha^{5k}$

$\delta = k + ay \bmod q$

$\alpha^\delta = \alpha^k \alpha^{ay}$

$\alpha^\delta = \alpha^k \cdot B^y$ so

$\alpha^k = \alpha^\delta (B^y)^{-1}$

so verification of signature for this scheme is:

$\alpha^k = \alpha^\delta (B^y)^{-1}$

5. $t = g^r$ $g^x = y$

c = random integers

$s = r + cx \bmod p-1$

$g^s = g^{r + cx + \lambda(p-1)} \bmod p = g^r g^{cx} g^{\lambda(p-1)} \bmod p$

$= t(g^x)^c (g^{p-1})^\lambda \bmod p$

$g^s = t \cdot y^c \bmod p$ as $(g^{p-1})^\lambda \bmod p = 1$

so "B" can verify that "A" knows x such that $g^x = y$ mod p by using the given t, known y and c value and see if ty^c matches with g^s with known g and given s