2019 - Exercises VII. - Solutions

Exercise 1

(a) $(d,e,n) = (303703, 7, 1065023)$
$w = 433736$

Signing:
$s = w^d \mod n = 433736^{303703} \equiv 686902 \mod 1065023$

Verification: $w = s^e \mod n = 686902^7 \equiv 433736 \mod 1065023$

(b) Public: $q = 2$, $p = 555557$, $y = q^x \mod p = 552508$
Private: $x = 60221$
Message: $m = 433736$

Signing: (a, b)
$r = 12345$
$a = q^r = 2^{12345} \equiv 148533 \mod 555557$
$b = (w - ax)r^{-1} = (433736 - 148533 \cdot 60221)12345^{-1} \equiv 79543 \cdot 161289 \equiv 511775 \mod 555556$

Verification:

$$y^a a^b \equiv q^w \mod p$$
$$552508^{148533} \cdot 148533^{511775} \equiv 2^{433736} \mod 555557$$
$$98824 \equiv 98824 \mod 555557$$

Exercise 2

(a) Let us suppose a and b defined as

$$a = q^i y^j \mod p$$
$$b = -aj^{-1} \mod (p-1)$$

where $0 \leq i, j \leq p-2$, and j is coprime to $p-1$. As the forger cannot choose arbitrary value of w, let us define it as $w = -aij^{-1} \mod (p-1)$. When verifying the signature (a, b) we plug given equations into verification equation and get

$$y^a a^b \equiv y^a (q^i y^j)^{-aj^{-1}} \mod p$$
$$y^a a^b \equiv y^a q^{-aij^{-1}} y^{-a} \mod p \equiv q^{-aij^{-1}} \mod p \equiv q^m \mod p$$

Verification using defined a, b and w is successful.

(b) We know that $w' = (w + \beta b)\alpha \mod (p-1)$. Using verification equation $y^a a^b \equiv q^w \mod p$, we express w as $w = ax + rb$ knowing that $y = q^x \mod p$ and $a = q^r \mod p$ (via equation $(q^x)^a (q^r)^b \equiv q^w \mod p$).

Transforming $w' = (w + \beta b)\alpha \mod (p-1)$ into $q^{w'} = q^{(w+\beta b)\alpha} \mod p$ we get $q^{w'} = q^{\alpha w + \alpha \beta b}$ mod p. Plugging $w = ax + rb$ into previous equation we get

$$q^{w'} = q^{x\alpha a} q^{r\alpha b} q^{\beta \alpha b} \mod p$$

that can be rewritten as

$$q^{w'} = y^{\alpha a} a^{\alpha b} \alpha^{\alpha b} = y^{\alpha a}(a\alpha)^{\alpha b} \mod p$$

The (a', b') signature can be calculated for arbitrary w' of given form where $a' = \alpha a$, $b' = \alpha b$.

(c) As the same r is used to sign both messages w_1 and w_2, $a = q^r \mod p$, is also the same. Equations for b_1, b_2 expressed as $b_1 r = (m_1 - ax) \mod (p-1)$ and $b_2 r = (m_2 - ax) \mod (p-1)$ can be transformed into $b_1 r - m_1 = -ax \mod (p-1)$ and $b_2 r - m_2 = -ax \mod (p-1)$. Putting those two equations into one we get $b_1 r - m_1 = b_2 r - m_2 \mod (p-1)$ and thus

$$(b_1 - b_2) r = m_1 - m_2 \mod (p-1)$$

If $\gcd(b_1 - b_2,\ p-1) = k$ and $k \mid (m_1 - m_2)$ then there are k possible solutions for r. We compute $q^r \mod p$ for all k solutions and find r such that the equation $a = q^r \mod p$ holds. As r is known, we compute x using equation

$$ax = m_1 - b_1 r \mod (p-1)$$

If $\gcd(a,\ p-1) = d$ and $d \mid (m_1 - b_1 r)$ then there are d possible solutions for x. We compute $q^x \mod p$ for all d solutions and find x such that the equation $y = q^x \mod p$ holds.

Exercise 3

Solution: First of all we have to compute $h = k^{-2} \mod n$.

$$k^{-1} = 20^{-1} \equiv 1544 \mod 3431$$
$$h = k^{-2} \equiv 2822 \mod 3431$$

- *Signature*: The send message is (w', S_1, S_2) where

$$S_1 = \frac{1}{2} \cdot \left(\frac{w'}{w} + w\right) = \frac{1}{2} \cdot (122 \cdot 108^{-1} + 108) \equiv 1230 \mod 3431$$
$$S_2 = \frac{k}{2} \cdot \left(\frac{w'}{w} - w\right) = \frac{20}{2} \cdot (122 \cdot 108^{-1} - 108) \equiv 1854 \mod 3431$$

  The send message is **(122, 1230, 1854)** and the public key is $h = 2822$ and $n = 3431$.

- *Signature verification*: The verification method is $w' \equiv S_1^2 - hS_2^2 \mod n$.

$$S_1^2 - hS_2^2 = 1230^2 - 2822 \cdot 1854^2 \equiv 122 = w' \mod 3431$$

  Therefore the signature was verified.

- *Decryption*: The decryption is $w = \frac{w'}{S_1 + k^{-1} S_2} \mod n$.

$$\frac{w'}{S_1 + k^{-1} S_2} = \frac{122}{1230 + 1544 \cdot 1854} = 122 \cdot 2352^{-1} \equiv 108 \mod 3431$$

  Therefore the secret subliminal message is **108** $= w$.

Exercise 4

1. Blinding by the first party: $m^* = mk^e = 1234 \cdot 8824^{101} \equiv 1234 \equiv 337 \mod 10033$
2. m^* is sent to the second party.
3. Signing by the second party: $s^* = (m^*)^d = 337^{1265} \equiv 4960 \mod 10033$
4. s^* sent back to the first party.
5. Unblinding by the first party: $s = k^{-1}s^* = 8824^{-1} \cdot 4960 \equiv 2946 \cdot 4960 \equiv 4112 \mod 10033$
6. Verification by any other party: $m = s^e = 4112^{101} \equiv 1234 \mod 10033$

Exercise 5

(a) The public keys z_{ij} are computed using the equation

$$z_{ij} = f(y_{ij}) = 17^{y_{ij}} \mod 61$$

in the following table

i	1	2	3	4
z_{i0}	30	31	44	7
z_{i1}	12	9	32	55

(b) The signature of a message $x_1x_2x_3x_4$ is $(y1_{x_1}, y2_{x_2}, y3_{x_3}, y4_{x_4})$. So for our message 0111 we have the signature sig(0111) = $(y_{10}y_{21}y_{31}y_{41})$ = (7, 36, 55, 11). Verification:

$$verif(x_1 \ldots x_k, a_1, \ldots, a_k) = true \Leftrightarrow f(a_i) = z_i, x_i, 1 \leq i \leq k$$

$$verif(0111, 7, 36, 55, 11) = true \Leftrightarrow 17^{a_i} \mod 61 = z_i, x_i, 1 \leq i \leq k$$

So:

$$17^7 \mod 61 = 30$$
$$17^{36} \mod 61 = 9$$
$$17^{55} \mod 61 = 32$$
$$17^{11} \mod 61 = 55$$

(c)

$$verif(x_1 \ldots x_k, a_1, \ldots, a_k) = true \Leftrightarrow f(a_i) = z_i, x_i, 1 \leq i \leq k$$

$$verif(1001, 4, 37, 31, 11) = true \Leftrightarrow 17^{a_i} \mod 61 = z_i, x_i, 1 \leq i \leq k$$

So:

$$17^4 \mod 61 = 12$$
$$17^{37} \mod 61 = 31$$
$$17^{31} \mod 61 = 44$$
$$17^{11} \mod 61 = 55$$

Exercise 6

We can use something like blind signature. The Bob will be receiving encrypted message to make signature of it. If we just send him the c. He will use his signing scheme which is:

$$c^d \equiv (m^e)^d \mod n$$
$$c^d \equiv m \mod n$$

And this is the problem. Bob should not realize, that he is decrypting the message.
Therefore, we can add our secret to the message (random r that has to satisfy $gcd(r, n) = 1$, encrypted with his e):

$$c' \equiv c \cdot r^e \mod n$$

Encrypted random number will be random number. So we send c' to the Bob. Then if we intercept his signature of the message. We can remove the blinding factor (we know our what r we have chosen).

$$m = c' \cdot r^{-1} \mod n$$

This works because $r^{ed} \equiv r \mod n$ so:

$$m \equiv c' \cdot r^{-1} \equiv (c')^d r^{-1} \equiv c^d r^{ed} r^{-1} \equiv c^d r r^{-1} \equiv c^d \pmod n,$$

After this, we have decrypted message m.

Exercise 7

(a) Verification: $g^s y^{H(m||r)} \stackrel{?}{\equiv} r \mod p$
Assuming that the hash function H is publicly available, all the information needed for verification are public or contained in the signature.
$g^s y^{H(m||r)} \equiv g^{k-H(m||r)x} (g^x)^{H(m||r)} \equiv g^{k-H(m||r)x+xH(m||r)} \equiv g^k \equiv r \mod p$

(b) Two intercepted messages with signatures with the same k:
$(m_1, (r_1 = r = g^k \mod p, s_1 = k - H(m_1||r)x \mod q))$
$(m_2, (r_2 = r = g^k \mod p, s_2 = k - H(m_2||r)x \mod q)$

The task is to get the private information x out of them:

$$s_1 - s_2 \equiv k - H(m_1||r)x - (k - H(m_2||r)x) \mod q$$
$$s_1 - s_2 = x \cdot (H(m_2||r) - H(m_1||r)) \mod q$$
$$x = (s_1 - s_2) \cdot (H(m_2||r) - H(m_1||r))^{-1} \mod q$$

All values from the right side of the equation are known. Unless hashes $H(m_2||r)$ and $H(m_1||r)$ are the same, we can compute x. If they are the same, we just wait for another message with different value of this hash.