Question 1.

(a) $(d, e, n) = (303703, 7, 1065023)$
$w = 485441$
Signature $s \equiv w^d \equiv 485441^{303703} \equiv 105153 \bmod 1065023$
The signature can be verified as $s^e \equiv 105153^7 \equiv 485441 \bmod 1065023$

(b) $(x, q, p, y) = (60221, 2, 555557, 552508), r = 12345$
$a \equiv q^r \equiv 2^{12345} \equiv 148533 \bmod 555557$
$r^{-1} \equiv 161289 \bmod 555556$
$b \equiv r^{-1} * (w - a * x) \equiv 161289 * (485441 - 148533 * 60221) \equiv 508404 \bmod 555556$
Signature is sent together with message as $(w, (a, b)) = (485441, (148533, 508404))$
It can be verified without the knowledge of private key x:
$q^w \equiv 2^{485441} \equiv 270960 \bmod 555557$
$y^a * a^b \equiv 552508^{148533} * 148533^{508404} \equiv 270960 \bmod 555557$

Question 2.

If s_1 and s_2 are signatures of m_1 and m_2, we can compute the signature of $m = m_1 m_2 \bmod n$ as $s = s_1 s_2 \bmod n$.

Since $m_3 = m_1 * m_2$, we can compute s_3 as

$$s_3 = s_1 s_2 \bmod n = 192 \cdot 454 \bmod 581 = 18$$

We can use the same principle for finding signature s_4 for $m_4 = 508$, as $33 \cdot 33 \equiv 508 \bmod 581$:

$$s_4 = s_1 \cdot s_1 = 192 \cdot 192 \equiv 261 \bmod 581$$

If s is a signature of m, then s^{-1} is a signature of m^{-1}. We see that $6^{-1} \bmod 581 \equiv 97$, therefore

$$s_5 = s_1^{-1} \bmod m = 454^{-1} \bmod 581 = 398$$

Question 3.

Using the procedure from the lecture:
$h \equiv k^{-2} \equiv (k^{-1})^2 \equiv 4575^2 \equiv 25514 \mod 29737$
Public key $(h, n) = (25514, 29737)$.

$S_1 = \frac{1}{2} \cdot (\frac{w'}{w} + w) \mod n$
$S_1 = \frac{1}{2} \cdot (\frac{2020}{111} + 111) \mod 29737$
$S_1 = 1 \cdot 2^{-1} \cdot (2020 \cdot 111^{-1} + 111) \mod 29737$
$S_1 = 1 \cdot 14869 \cdot (2020 \cdot 27058 + 111) \mod 29737$
$S_1 = 15201 \mod 29737$

$S_2 = \frac{k}{2} \cdot (\frac{w'}{w} - w) \mod n$
$S_2 = \frac{13}{2} \cdot (\frac{2020}{111} - 111) \mod 29737$
$S_2 = 13 \cdot 2^{-1} \cdot (2020 \cdot 111^{-1} - 111) \mod 29737$
$S_2 = 13 \cdot 14869 \cdot (2020 \cdot 27058 - 111) \mod 29737$
$S_2 = 17748 \mod 29737$

Signature $(w', S_1, S_2) = (2020, 15201, 17748)$.

Signature verification:
$w' = {S_1}^2 - h \cdot {S_2}^2 \mod n$
$2020 = 15201^2 - 25514 \cdot 17748^2 \mod 29737$
$2020 = 2020 \mod 29737$
Since this holds the verification was successful.

Recovery of secret message:
$w = \frac{w'}{(S_1 + k^{-1} \cdot S_2)} \mod n$
$w = \frac{2020}{15201 + 13^{-1} \cdot 17748} \mod 29737$
$w = \frac{2020}{15201 + 4575 \cdot 17748} \mod 29737$
$w = 2020 \cdot (15201 + 4575 \cdot 17748)^{-1} \mod 29737$
$w = 2020 \cdot (554)^{-1} \mod 29737$
$w = 2020 \cdot 3489 \mod 29737$
$w = 111 \mod 29737$
From the signature message $w = 111$ was recovered.

Question 4.

The final step to obtain the signature would be $s = \prod_{i=1}^{n} s_i \mod N$.

Since $d = \sum_{i=1}^{n} d_i$, we need all n parties to recover the original private exponent d, therefore this scheme is correct only when $t = n$. It also holds that $m^{d_i} \cdot m^{d_j} \equiv m^{d_i + d_j} \mod N$, therefore $s = m^d = \prod_{i=1}^{n} m^{d_i} \mod N = \prod_{i=1}^{n} s_i \mod N$.

Question 5.

To preserve the security of Lamport one-time signature scheme, for each index i in y_{ij} in the secret key, we can use either the value associated with y_{i0} or y_{i1} bot not both. Otherwise, the attacker could exploit the knowledge of both of these values for some i and craft a valid signature for a message with an arbitrary bit on the i-th position.

There are $2^6 = 64$ possible 6-bit messages in total. For each message, we need a unique combination of the values from the secret key and match them with values in the public key for verification. Choosing 4 out of 8 y_{ij} gives us

$$C(n,k) = \frac{n!}{k!(n-k)!} = \frac{8!}{4!(8-4)!} = 70$$

unique combinations (subsets) of the key values. All we need to do is assign every possible 6-bit message to one of the 70 combinations in a deterministic way, so the verifying party can replicate this process with the public key.

There might exist a more efficient solution, but the most straight-forward one is to order the messages from 000000 to 111111, then we use some deterministic subset selection algorithm to select 64 unique subsets of 4 values from the 8 values in the secret key, order them in a deterministic way by utilizing their indices (for simplicity, we can change the indices to $1 \leq i \leq 8$) and map each of the 64 possible messages to one of the subsets.

The verification process is similar, the verifying party first creates the mapping of the messages to subsets of the values from the public key using the same algorithm as the signing party used for this purpose, which ensures there are equivalent elements in the subsets and preserves mapping of the messages to the subsets with respect to the indices of the elements. For example, if the algorithm mapped the message 100001 to a signature $\{y_1, y_2, y_5, y_8\}$, then the same algorithm needs to map the same message to $\{z_1, z_2, z_5, z_8\}$ values from the public key during verification.

The verifying party then computes $f(y_i)$ for each value in the signature and checks whether the four values match with the corresponding values in the table created from the public key in the previous step (mapping of possible messages to combinations of z_i).

This scheme preserves the security properties of the original Lamport scheme. There are no two different messages, which would get mapped to the same values from the secret key. In other words, there are at most three identical values out of four values in the signature, therefore the attacker would have to reverse the one-way function f for at least one value in the public key to forge a signature of another message.

Question 6.

$(q, p, y) = (2, 567899, 300210)$
$(w_1, (a_1, b_1)) = 172459, (226741, 13448)$
$(w_2, (a_2, b_2)) = 172519, (331901, 326010)$
$(w_3, (a_3, b_3) = 359406, (390725, 78981)$
$(w_4, (a_4, b_4)) = 456149, (144902, 184381)$
$(w_5, (a_5, b_5)) = 459379, (43870, 540485)$
We can see b_1 and b_2 are not invertible mod $p-1$ but $b_3^{-1} \equiv 141455$ mod 567898, so we can write the following equations from the definition $b = r^{-1} * (w - a * x)$ with the substitution $r_4 \equiv 3 * r_3$ mod $p-1$:
$r_3 * b_3 \equiv w_3 - a_3 * x$
$\underline{3 * r_3 * b_4 \equiv w_4 - a_4 * x}$
$r_3 = (w_3 - a_3 * x) * (b_3)^{-1}$
$3 * (w_3 - a_3 * x) * (b_3)^{-1} * b_4 \equiv w_4 - a_4 * x$
$3 * (b_3)^{-1} * b_4 * w_3 - 3 * (b_3)^{-1} * b_4 * a_3 * x \equiv w_4 - a_4 * x$
$3 * (b_3)^{-1} * b_4 * w_3 - w_4 \equiv x * (3 * (b_3)^{-1} * b_4 * a_3 - a_4)$
$x \equiv (3 * (b_3)^{-1} * b_4 * w_3 - w_4) * (3 * (b_3)^{-1} * b_4 * a_3 - a_4)^{-1}$
$x \equiv (3*141455*184381*359406-456149)*(3*141455*184381*390725-144902)^{-1} \equiv 56789$ mod $p-1$
Now we can count $r_3 \equiv (w_3-a_3*x)*(b_3)^{-1} \equiv (359406-390725*56789)*141455 \equiv 160543$ mod 567898
If we perform a simple check using $a = q^r$ mod p for all five signatures, we see it works (we have to get the original $r_1 = 160543 * 9^{-1} \equiv 333337$ mod $p-1$ first).
So we can finally compute the signature of UČO 485441 and add it to the list instead of record 5 (as the list is ordered): $a_6 = q^{r_5} = 2^{9*r_3} = 2^{9*160543} \equiv 43870 = a_5$ mod p
$b_6 = r_5^{-1} * (w_6 - a_6 * x) \equiv 88871 * (485441 - 43870 * 56789) \equiv 240545$ mod 567898
So add there 485441, (43870, 240545) which can be then verified as:
$y^a * a^b \equiv 300210^{43870} * 43870^{240545} \equiv 225548 = q^w = 2^{485441}$ mod p