Question 1.

Public key, in this subliminal channel, is the pair (n, h). We already know that $n = 6059$ and $k = 21$. Since $h \equiv k^{-2} \mod n \Leftrightarrow h \equiv (k^{-1})^2 \mod n$, we have to compute k^{-1}. By using Euclide's algorithm, we have:

$$\begin{aligned}6059 &= 288 \times 21 + 11\\ 21 &= 1 \times 11 + 10\\ 11 &= 1 \times 10 + 1\end{aligned}$$

We can deduce that $1 = 2 \times 6059 - 577 \times 21$, which means that $-577 \times 21 \equiv 1 \mod 6059$, and *in extenso* $-577 \equiv 21^{-1} \mod 6059 \Leftrightarrow 5482 \equiv 21^{-1} \mod 6059$. Therefore, $k^{-1} = 5482$.

Now we can compute h:

$$\begin{aligned}h &\equiv (k^{-1})^2 \mod n\\ h &\equiv 5482^2 \mod 6059\\ h &\equiv 5743 \mod 6059\end{aligned}$$

Now we will sign the message. In this case, two signatures (S_1, S_2) must be computed, according to the following scheme: $S_1 \equiv \frac{1}{2}.\left(\frac{w'}{w} + w\right) \mod n$ and $S_2 \equiv \frac{k}{2}.\left(\frac{w'}{w} - w\right) \mod n$. This can be rewrited $S_1 \equiv 2^{-1}.(w'.w^{-1}+w) \mod n$ and $S_2 \equiv k.2^{-1}.(w'.w^{-1}-w) \mod n$. This implies knowing 2^{-1} and w^{-1}. Since $2 \times 3030 = 6060 \equiv 1 \mod 6059$, we can easily see that $2^{-1} \equiv 3030 \mod 6059$, but for $w = 54$, it is less obvious. We once again use Euclide's algorithm:

$$\begin{aligned}6059 &= 112 \times 54 + 11\\ 54 &= 4 \times 11 + 10\\ 11 &= 1 \times 10 + 1\end{aligned}$$

Then, we have $1 = 5 \times 6059 - 561 \times 54$, and thus we can deduce $w^{-1} \equiv -561 \mod 6059 \equiv 5498 \mod 6059$. Given that, we can compute S_1 and S_2:

$$\begin{aligned}S_1 &\equiv 2^{-1}.(w'.w^{-1} + w) \mod n\\ S_1 &\equiv 3030 \times (2021 \times 5498 + 54) \mod 6059\\ S_1 &\equiv 3030 \times 11111512 \mod 6059\\ S_1 &\equiv 3030 \times 5365 \mod 6059\\ S_1 &\equiv 5712 \mod 6059\end{aligned}$$

$$S_2 \equiv k.2^{-1}.(w'.w^{-1} - w) \mod n$$
$$S_2 \equiv 21 \times 3030 \times (2021 \times 5498 - 54) \mod 6059$$
$$S_2 \equiv 63630 \times 11111404 \mod 6059$$
$$S_2 \equiv 3040 \times 5257 \mod 6059$$
$$S_2 \equiv 3697 \mod 6059$$

Now, we must prove that the signature is correct. To power this verification, $w' \equiv S_1^2 - hS_2^2 \mod n$ must hold:

$$\begin{aligned} S_1^2 - hS_2^2 \mod n &\equiv 5712^2 - 5743 \times 3697^2 \mod 6059 \\ &\equiv 5712^2 - 5743 \times 3697^2 \mod 6059 \\ &\equiv 5288 - 5743 \times 4764 \mod 6059 \\ &\equiv 5288 - 3267 \mod 6059 \\ &\equiv 2021 \mod 6059 \end{aligned}$$

As we can see, $w' \equiv S_1^2 - hS_2^2 \mod n$: as a result, the signature is valid. We can now decrypt the message.

To decrypt the message, we have to compute $w \equiv \frac{w'}{S_1+k^{-1}S_2} \mod n$, which is equivalent to $w \equiv w'.(S_1 + k^{-1}S_2)^{-1} \mod n$. We have $S_1 + k^{-1}S_2 = 5712 + 5482 \times 3697 = 20272666 \equiv 5311 \mod 6059$. Therefore, we have to calculate $5311^{-1} \mod 6059$, and we will once again use the Euclide's algorithm:

$$\begin{aligned} 6059 &= 1 \times 5311 + 748 \\ 5311 &= 7 \times 748 + 75 \\ 748 &= 9 \times 75 + 73 \\ 75 &= 1 \times 73 + 2 \\ 73 &= 36 \times 2 + 1 \end{aligned}$$

We obtain $1 = 2620 \times 6059 - 2989 \times 5311$. Consequently, $-2989 \mod 6059 \equiv 3070 \mod 6059 \equiv 5311^{-1} \mod 6059$.

Finally, since we know all needed values, we can compute w:

$$w \equiv w'.(S_1 + k^{-1}S_2)^{-1} \mod n$$
$$w \equiv 2021 \times 5311^{-1} \mod 6059$$
$$w \equiv 2021 \times 3070 \mod 6059$$
$$w \equiv 54 \mod 6059$$

We find the value of w given in the statement.

Question 2.

See excel table

Question 3.

From $(m_1, sig(m_1))$ we have $12^d = 46 \mod 1591$.

From $(m_2, sig(m_2))$ we have $33^d = 1080 \mod 1591$

From the exercise book, we know that for the RSA signature scheme it holds: if s_1 and s_2 are signatures of messages m_1 and m_2, we can easily compute the signature of the message $m = m_1 * m_2 \mod n$ as $s = s_1 * s_2 \mod n$.

$m_3 = m_1 * m_1$

$s_3 = s_1 * s_1 \mod 1591$

$s_3 = 525$

Verify: $525^{13} \mod 1591 = 144$

$m_4 = m_1 * m_2$

$s_4 = s_1 * s_2 \mod 1591$

$s_4 = 359$

Verify: $359^{13} \mod 1591 = 396$

From the exercise book, we know that if s is a signature of a message m then $s^{-1} \mod n$ is the signature of the message $m^{-1} \mod n$.

$m_5 = m_4^{-1} \mod 1591$

EEA for $359, 1591 = 195 * 359 + (-44) * 1591 = 1$

$s_5 = 195 \mod 1591$

Verify: $195^{13} \mod 1591 = 454$

Question 4.

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.
For every n, we have $2n$ possible keys and we want to find bit size of messages, which give us the highest number of created messages.
If we choose the bit length $= 2n$, there is only one possible message, as $\binom{2n}{2n} = 1$. However we know from the Pascal triangle, that the highest result of combination number is when $k = n/2$, if n is even, and $k = n/2 + 1$ or $k = n/2 - 1$ if n is odd. So the maximum number of distinct messages one can sign with such scheme for n is $\binom{2n}{n}$ as $2n$ is always even.

For $n = 10$ we are choosing 10 out of 20 y_{ij}, which give us:

$$C(n,k) = \frac{n!}{k!(n-k)!} = \frac{20!}{10!(20-10)!} = 184756$$

unique combinations (subsets) of the key values, so we can sign 184756 distinct messages with such scheme.

Question 5.

(a) We have the public key $(p = 101, q = 27, y = 14)$, a message $w = 61$ and the signature is $(27, 51)$. We verify if the Elgamal signature verification equality holds :

$$y^a a^b \mod n = 14^{27} 27^{51} \mod 101$$

$$y^a a^b \mod n = 40$$

$$q^w \mod 101 = 27^{61} \mod 101$$

$$q^w \mod 101 = 40$$

The equality holds, $y^a a^b = q^w \mod n$, which means the signature is valid.

(b) We can observe that $q = a = 27$. As we have :

$$a \equiv q^r \mod p$$

$$27 \equiv 27^r \mod p$$

Then r can only be 1. Knowing that $r = 1$, we can easily compute x with the formula :

$$x = (w - r.b)a^{-1} \mod (p1)$$

$$x = (61 - 51) \times 27^{-1} \mod 100$$

$$x = 630 \mod 100$$

$$x = 30$$

We have $x = 30$. As an additional proof to verify this hypothesis, let us see if $x = 30$ works to compute $b = 51$ we were given :

$$b = (w - x.a)r^{-1} \mod (p - 1)$$

$$b = (61 - 30 \times 27) \mod 100$$

$$b = 51$$

We find the b that we were given, $x = 30$ seems to be valid.

Question 6

(a) If the protocol is followed properly then

$$\prod_{i=1}^{t} y_{p_i}^{a_{p_i}} a_{p_i}^{b_{p_i}} = \prod_{i=1}^{t} q^w \mod p = q^{wt} \mod p$$

(b) The protocol is not unforgeable. The sectes x_i do not have to be unique. If it happens that $x_i = x_j$, $i \neq j$, then the party i can forge j's part of the signature a_j, p_j with his own r'_j (and vice-versa), leading to a possible signature created by less than t parties.