Question 1.

$$\begin{aligned} x &\equiv 6 \pmod{17} \\ x &\equiv 3 \pmod{7} \\ x &\equiv 9 \pmod{11} \end{aligned}$$

First we check that $gcd(17,7) = 1$, $gcd(17,11) = 1$ and $gcd(7,11) = 1$, therefore we can use the Chinese remainder theorem.

Let's denote the numbers from the assignment as $a_1 = 6$, $m_1 = 17$, $a_2 = 3$, $m_2 = 7$, $a_3 = 9$, $m_3 = 11$.

We have three integers m_1, m_2 and m_3 st $gcd(m_i, m_j) = 1$ if $i \neq j$ and integers a_1, a_2, a_3 st $0 < a_i < m_i$, $1 \leq i \leq 3$. The system of congruences

$$x \equiv a_i \mod m_i, 1 \leq i \leq 3$$

has the solution $x = \sum_{i=1}^{3} a_i M_i N_i$, where $M = \prod_{i=1}^{3} m_i$, $M_i = \frac{M}{m_i}$, $N_i = M_i^{-1} \mod m_i$ and the solution is unique up to the congruence modulo M. Since we are looking for $0 \leq x \leq M$, we can do the computation of $x = \sum_{i=1}^{3} a_i M_i N_i \mod M$.

First we compute $M = m_1 \cdot m_2 \cdot m_3 = 17 \cdot 7 \cdot 11 = 1309$. Then we can compute M_i:

$$\begin{aligned} M_1 &= \frac{1309}{17} = \frac{17 \cdot 7 \cdot 11}{17} = 7 \cdot 11 = 77 \\ M_2 &= \frac{1309}{7} = \frac{17 \cdot 7 \cdot 11}{7} = 17 \cdot 11 = 187 \\ M_3 &= \frac{1309}{11} = \frac{17 \cdot 7 \cdot 11}{11} = 17 \cdot 7 = 119 \end{aligned}$$

Now we need the inverses of M_i.

$$\begin{aligned} N_1 &= M_1^{-1} \mod m_1 \\ &= 77^{-1} \mod 17 \\ &= 9^{-1} \mod 17 \\ &= 2 \mod 17 \end{aligned}$$

We found the last equation simply, since $2 \cdot 9 = 18 = 1 \mod 17$.

$$\begin{aligned} N_2 &= M_2^{-1} \mod m_2 \\ &= 187^{-1} \mod 7 \\ &= 5^{-1} \mod 7 \\ &= 3 \mod 7 \end{aligned}$$

Again we simply find the last equation, since $3 \cdot 5 = 15 = 1 \mod 7$.

$$\begin{aligned} N_3 &= M_3^{-1} \mod m_3 \\ &= 119^{-1} \mod 11 \\ &= 9^{-1} \mod 11 \\ &= (-2)^{-1} \mod 11 \\ &= 5 \mod 11 \end{aligned}$$

Again $-2 \cdot 5 = -10 = 1 \mod 11$.

Now we can compute the x:

$$\begin{aligned} x &= \sum_{i=1}^{3} a_i M_i N_i \mod M = \\ &= 6 \cdot 77 \cdot 2 + 3 \cdot 187 \cdot 3 + 9 \cdot 119 \cdot 5 \mod 1309 = \\ &= 924 + 1683 + 5355 \mod 1309 = \\ &= 7962 \mod 1309 = \\ &= 108 \end{aligned}$$

So we have the result $x = 108$. We can easily check that $108 \equiv 6 \mod 17$, $108 \equiv 3 \mod 7$ and finally $108 \equiv 9 \mod 11$.

Question 2.

I'm gonna use Euler's criterion:

$$a^{\frac{p-1}{2}} \equiv \begin{cases} 1 \mod p & \text{if there is an integer } x \text{ such that } a \equiv x^2 \mod p, \\ -1 \mod p & \text{if there is no such integer.} \end{cases}$$

Let's look at the number $\{1, \dots, 10\}$:

$$\begin{aligned}
1^{\frac{8009-1}{2}} &\equiv 1^{4004} \equiv 1 \mod p \\
2^{\frac{8009-1}{2}} &\equiv 2^{4004} \equiv 1 \mod p \\
3^{\frac{8009-1}{2}} &\equiv 3^{4004} \equiv -1 \mod p \\
4^{\frac{8009-1}{2}} &\equiv 4^{4004} \equiv 1 \mod p \\
5^{\frac{8009-1}{2}} &\equiv 5^{4004} \equiv 1 \mod p \\
6^{\frac{8009-1}{2}} &\equiv 6^{4004} \equiv -1 \mod p \\
7^{\frac{8009-1}{2}} &\equiv 7^{4004} \equiv 1 \mod p \\
8^{\frac{8009-1}{2}} &\equiv 8^{4004} \equiv 1 \mod p \\
9^{\frac{8009-1}{2}} &\equiv 9^{4004} \equiv 1 \mod p \\
10^{\frac{8009-1}{2}} &\equiv 10^{4004} \equiv 1 \mod p
\end{aligned}$$

So numbers $1, 2, 4, 5, 7, 8, 9, 10$ are *quadratic residui* modulo 8009, and number $3, 6$ are not.

Question 3.

(a) Rabin cryptosystem

$n = 698069 = 887 \cdot 787$

Encryption: Since $w = 456556$ and $w < n$:

$$c = w^2 \pmod{n} = 456556^2 = 675805 \pmod{698069}$$

Decryption:
The formula is $w \equiv \sqrt{c} \pmod{n}$. Firstly we use Chinese remainder theorem:

$$\begin{aligned} w_p &\equiv 675805 \pmod{887} & \qquad w_q &\equiv 675805 \pmod{787} \\ w_p &\equiv 675805^{\frac{887+1}{4}} \pmod{887} & \qquad w_q &\equiv 675805^{\frac{787+1}{4}} \pmod{787} \\ w_p &\equiv 675805^{222} \pmod{887} & \qquad w_q &\equiv 675805^{197} \pmod{787} \\ w_p &\equiv 249 \pmod{887} & \qquad w_q &\equiv 96 \pmod{787} \end{aligned}$$

Secondly we have to find y_p and y_q (can be found as Bezout's coefficients) for $p = 887$ and $q = 787$:

$$\begin{aligned} y_p &\equiv p^{-1} \pmod{q} & \qquad y_q &\equiv q^{-1} \pmod{p} \\ y_p &\equiv 887^{-1} \pmod{787} & \qquad y_q &\equiv 787^{-1} \pmod{887} \\ y_p &\equiv -181 \pmod{787} & \qquad y_q &\equiv 204 \pmod{887} \end{aligned}$$

Lastly we calculate four possible solutions as follows:

$$w_i \equiv \pm w_p \cdot q \cdot y_q \pm w_q \cdot p \cdot y_p \pmod{n}$$

$$\begin{aligned} w_1 &\equiv 249 \cdot 787 \cdot 204 + 96 \cdot 887 \cdot (-181) \equiv 131525 \pmod{698069} \\ w_2 &\equiv 249 \cdot 787 \cdot 204 - 96 \cdot 887 \cdot (-181) \equiv 241513 \pmod{698069} \\ w_3 &\equiv -249 \cdot 787 \cdot 204 + 96 \cdot 887 \cdot (-181) \equiv 456556 \pmod{698069} \\ w_4 &\equiv -249 \cdot 787 \cdot 204 - 96 \cdot 887 \cdot (-181) \equiv 566544 \pmod{698069} \end{aligned}$$

The original message is w_3.

(b) El Gamal cryptosystem

$p = 567899$	$x = 12345$
$q = 2$	$r = 938$

Encryption:
Firstly, we need $y = q^x \pmod{p} \equiv 2^{12345} \equiv 222588 \pmod{567899}$.
Now we can encrypt the message $w = 456556$ as follows:

$$\begin{aligned} &c = (a, b) & \\ &a \equiv q^r \pmod{p} & b \equiv w \cdot y^r \pmod{p} \\ &a \equiv 2^{938} & b \equiv 456556 \cdot 222588^{938} \\ &a \equiv 201104 \pmod{567899} & b \equiv 325068 \pmod{567899} \end{aligned}$$

The encrypted message is (201104, 325068)

Question 4.

To show this, we prove that the discrete logarithm problem is reducible to finding two collisions, i.e. we can solve the discrete logarithm by finding two colliding messages.
First we find the two colliding messages $m = x + yq$ and $m' = x' + y'q$. We want to find l such that $\log_\alpha \beta = l \bmod p$ (or $\beta = \alpha^l \bmod p$).
Because the messages m, m' have the same hash value, it holds that $\alpha^x \beta^y = \alpha^{x'} \beta^{y'} \bmod p$.
We replace β with α^l: $\alpha^x (\alpha^l)^y = \alpha^{x'} (\alpha^l)^{y'} \bmod p$
$\alpha^x \alpha^{ly} = \alpha^{x'} \alpha^{ly'} \bmod p$
$\alpha^{x+ly} = \alpha^{x'+ly'} \bmod p$
$x + ly = x' + ly' \bmod p - 1$ (for exponents we use modulus order of $\alpha = p - 1$)
$l(y' - y) = (x - x') \bmod p - 1$
We can replace $p - 1 = 2q$ and get $l(y' - y) = (x - x') \bmod 2q$
We can solve this using these two equations and CRT:
$l(y' - y) = (x - x') \bmod q$
$l(y' - y) = (x - x') \bmod 2$
For the first one we have to show that inversion of $y' - y$ exists, i.e. $y' - y \neq 0 \pmod{q}$.
If $y \neq y'$, it holds that $y' - y \neq 0 \pmod{q}$ because $0 \leq y', y \leq q - 1$.
If $y = y'$ it holds that $\alpha^x = \alpha^{x'} \pmod{p}$ (because $h(m) = h(m')$), $x = x' \pmod{p-1}$, $x = x' \pmod{2q}$ and because $0 \leq x', x \leq q - 1$ that means $x = x'$, but that breaks the condition $m \neq m'$ - contradiction. Therefore $y \neq y'$.
For the first equation we have one solution $l = (x - x') * (y' - y)^{-1} \pmod{q}$
For the second equation we have two different solutions (because we are using modulus 2) and we can try both without changing the complexity to get the final value of l (there is only one because α is primitive root).
We showed that we can solve the discrete logarithm problem by finding two colliding messages and therefore finding two colliding messages is at least as hard as solving the discrete logarithm problem.

Question 5.

(a) Probability that at least two people were born on the same day of the week is easier to calculate with complementary probability - everyone was born on different day of the week and subtract it from 1. (variation without repetition, how many ways to pick 5 digits from 7 numbers, order is important)!

$$1 - Pr(\text{all distinct}) = 1 - \frac{7!}{7^5 \cdot 2!} = 0.8500624$$

(b) The probability that exactly two people (couple) were born on the same day of the week (and three other people in different days) is: How many ways can we select a pair, couple - **two from five** people each person from pair was born on the same **(one) day from seven** possible days. The other **three remaining** people have respectively **six, five and four** possible born days, divided by **all possible outcomes**

$$\frac{\binom{5}{2} \cdot \binom{7}{1} \cdot 6!}{7^5 \cdot 3!} = 0.5002082$$

(c) the probability for at least three people were born on the same day of the week is equal to probability that exactly two people were born on the same day of the week (prob. from (b)) subtracted from probability that at least two people were born on the same day of the week (prob. from (a)). We have to be careful and don't forget to subtract also the probability of two pairs, because (b) is probability of exactly one pair. So we have to choose **two from five** people - first pair and **two from three** people - second pair now assign **two from seven** days to each pair and finally assign last day from **5 residual days** to last the person:

$$(a) - (b) - \frac{\binom{7}{2} \cdot \binom{5}{2} \cdot \binom{3}{2} \cdot 5}{7^5} = 0.1628488$$

Question 6.

First, we will show that there are exactly two decryptions x_i, x_j of even parity and exactly two decryptions x_k, x_l of odd parity, where $i \neq j \neq k \neq l$.

The decryptions are in the following form:

$$\begin{aligned}
x_1 &\equiv m_p \cdot q \cdot y_q + m_q \cdot p \cdot y_p && \bmod n \\
x_2 &\equiv m_p \cdot q \cdot y_q + (-\ m_q) \cdot p \cdot y_p && \bmod n \\
x_3 &\equiv (-\ m_p) \cdot q \cdot y_q + m_q \cdot p \cdot y_p && \bmod n \\
x_4 &\equiv (-\ m_p) \cdot q \cdot y_q + (-\ m_q) \cdot p \cdot y_p && \bmod n
\end{aligned}$$

where $m_p \equiv \sqrt{c} \bmod p$, $m_q \equiv \sqrt{c} \bmod q$, $y_p \equiv p^{-1} \bmod q$ and $y_q \equiv q^{-1} \bmod p$.

Since p, q are prime numbers such that $p \equiv q \equiv 3 \bmod 4$, then p and q are odd prime numbers.

Since p is an odd prime number and $-m_p \equiv p - m_p \pmod p$, then m_p is of opposite parity from $-m_p$.
This holds also for m_q and $-m_q$ – i.e. since q is an odd prime number and $-m_q \equiv q - m_q \pmod q$, then m_q is of opposite parity from $-m_q$.

Let m_p and m_q have the same parity. Then $-m_p$ and $-m_q$ also have the same parity (opposite from m_p and m_q).

Then the decryption x_1 can be written as:

$$\begin{aligned}
x_1 &\equiv m_p \cdot q \cdot y_q + m_q \cdot p \cdot y_p && \bmod n \\
&\equiv -((-m_p) \cdot q \cdot y_q + (-m_q) \cdot p \cdot y_p) && \bmod n \\
&\equiv -x_4 && \bmod n \\
&\equiv n - x_4 && \bmod n
\end{aligned}$$

And the decryption x_2 can be written as:

$$\begin{aligned}
x_2 &\equiv m_p \cdot q \cdot y_q + (-m_q) \cdot p \cdot y_p && \bmod n \\
&\equiv -((-m_p) \cdot q \cdot y_q + m_q \cdot p \cdot y_p) && \bmod n \\
&\equiv -x_3 && \bmod n \\
&\equiv n - x_3 && \bmod n
\end{aligned}$$

Since $n = p \cdot q$ is an odd number, the decryptions x_1 and x_4 are clearly of opposite parity. And so are the decryptions x_2 and x_3.

Second, we will show that for each pair x_s, x_t of decryptions of the same parity, where $s \neq t$, the value of Jacobi symbol modulo n of x_s is opposite from the Jacobi symbol modulo n of x_t.

The Jacobi symbols modulo n for the decryption x_1 is as follows:

$$\begin{aligned}\left(\frac{m_p \cdot q \cdot y_q + m_q \cdot p \cdot y_p}{n}\right) &= \left(\frac{m_p \cdot q \cdot y_q + m_q \cdot p \cdot y_p}{p \cdot q}\right) \\ &= \left(\frac{m_p \cdot q \cdot y_q + m_q \cdot p \cdot y_p}{p}\right) \cdot \left(\frac{m_p \cdot q \cdot y_q + m_q \cdot p \cdot y_p}{q}\right) \\ &= \left(\frac{m_p \cdot q \cdot y_q}{p}\right) \cdot \left(\frac{m_q \cdot p \cdot y_p}{q}\right) \\ &= \left(\frac{m_p}{p}\right) \cdot \left(\frac{m_q}{q}\right)\end{aligned}$$

And in an analogous way we get the Jacobi symbol modulo n for the decryption x_2:

$$\begin{aligned}\left(\frac{m_p \cdot q \cdot y_q + (-m_q) \cdot p \cdot y_p}{n}\right) &= \left(\frac{m_p}{p}\right) \cdot \left(\frac{-m_q}{q}\right) = \left(\frac{m_p}{p}\right) \cdot \left(\frac{-1}{q}\right) \cdot \left(\frac{m_q}{q}\right) \\ &= -\left(\frac{m_p}{p}\right) \cdot \left(\frac{m_q}{q}\right)\end{aligned}$$

For the decryption x_3:

$$\begin{aligned}\left(\frac{(-m_p) \cdot q \cdot y_q + m_q \cdot p \cdot y_p}{n}\right) &= \left(\frac{-m_p}{p}\right) \cdot \left(\frac{m_q}{q}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{m_p}{p}\right) \cdot \left(\frac{m_q}{q}\right) \\ &= -\left(\frac{m_p}{p}\right) \cdot \left(\frac{m_q}{q}\right)\end{aligned}$$

And for the decryption x_4:

$$\begin{aligned}\left(\frac{(-m_p) \cdot q \cdot y_q + (-m_q) \cdot p \cdot y_p}{n}\right) &= \left(\frac{-m_p}{p}\right) \cdot \left(\frac{-m_q}{q}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{m_p}{p}\right) \cdot \left(\frac{-1}{q}\right) \cdot \left(\frac{m_q}{q}\right) \\ &= \left(\frac{m_p}{p}\right) \cdot \left(\frac{m_q}{q}\right)\end{aligned}$$

Since $\gcd(m_p, p) = \gcd(m_q, q) = 1$ none of the Jacobi symbols modulo n for any decryption will be equal to zero.

This implies that the Jacobi symbols modulo n are the same for the decryptions x_1 and x_4 (which are of opposite parity).
And also for the decryptions x_2 and x_3 (again of opposite parity) the Jacobi symbols modulo n are the same (and they have an opposite value from the Jacobi symbols modulo n for x_1 and x_4).

Therefore, we can see that each of the four possible decryptions x_1, x_2, x_3 and x_4 of ciphertext c is uniquely determined by two bits of information – its parity and Jacobi symbol.