6.1 (a) Encrypt your UČO using the Rabin cryptosystem with $n = 698069$. Then calculate all four possible decryptions of the ciphertext you calculated, with the knowledge that $n = 887 \times 787$.

Solution:

- *Encryption*: $m = 456149$ and $m < n$, therefore we can compute the ciphertext

$$c = m^2 = 456149^2 \equiv \mathbf{577578} \mod 698069.$$

- *Decryption*: The decryption formula is $m \equiv \sqrt{c} \pmod{n}$. We use Chinese remainder theorem to calculate the possible results.

$$\begin{aligned} x &\equiv 577578 && \mod 887 \\ x &\equiv 577578^{\frac{887+1}{4}} && \mod 887 \\ x &\equiv 577578^{222} && \mod 887 \\ x &\equiv 231 && \mod 887 \end{aligned} \qquad \begin{aligned} y &\equiv 577578 && \mod 787 \\ y &\equiv 577578^{\frac{787+1}{4}} && \mod 787 \\ y &\equiv 577578^{197} && \mod 787 \\ y &\equiv 311 && \mod 787 \end{aligned}$$

We are looking for the Bezout's coefficients (k and l) for $p = 887$ and $q = 787$

$$204 \cdot 787 - 181 \cdot 887 = 1.$$

Therefore $k = -181$ and $l = 204$.
Finally we can calculate all four possible decryptions, using this statement

$$\pm x \cdot l \cdot q \pm y \cdot k \cdot p \equiv m_i \mod n.$$

$$\begin{aligned} m_1 &\equiv 231 \cdot 204 \cdot 787 + 311 \cdot (-181) \cdot 887 \equiv 419782 \mod 698069 \\ m_2 &\equiv 231 \cdot 204 \cdot 787 - 311 \cdot (-181) \cdot 887 \equiv 456149 \mod 698069 \\ m_3 &\equiv -231 \cdot 204 \cdot 787 + 311 \cdot (-181) \cdot 887 \equiv 241920 \mod 698069 \\ m_4 &\equiv -231 \cdot 204 \cdot 787 - 311 \cdot (-181) \cdot 887 \equiv 278287 \mod 698069 \end{aligned}$$

The original message is m_2.

□

(b) Encrypt your UČO with the ElGamal cryptosystem with $p = 567899$, $q = 2$, $x = 12345$ and random choice $r = 938$.

Solution: First of all, the part of public key is $y = q^x \mod p$, therefore $y = 2^{12345} \equiv 222588 \mod 567899$.
Now we are able to encrypt the message $m = 456149$ The ciphertext is $c = (a, b)$, where $a = q^r \mod p$ and $b = y^r w \mod p$.

$$\begin{aligned} a &= 2^{938} && \equiv 201104 \mod 567899 \\ b &= 222588^{938} \cdot 456149 \equiv 25233 \mod 567899 \end{aligned}$$

The message $m = 456149$ is encrypted as $(\mathbf{201104}, \mathbf{25233})$. □

Question 2.

$q = 7, y = 505, p = 541$

$m = \sqrt{p-1} = \sqrt{540} = 24$

$0 \geq i, j \geq 23$:

L_1 :

j	0	1	2	3	4	5	6	7	8	9	10	11
$q^{m \cdot j} \pmod p$	1	110	198	140	252	129	124	115	207	48	411	307

j	12	13	14	15	16	17	18	19	20	21	22	23
$q^{m \cdot j} \pmod p$	228	194	241	1	110	198	140	252	129	124	115	207

L_2 :

i	0	1	2	3	4	5	6	7	8	9	10	11
$y \cdot q^{-i} \pmod p$	505	304	198	492	534	540	309	276	194	105	15	234

i	12	13	14	15	16	17	18	19	20	21	22	23
$y \cdot q^{-i} \pmod p$	188	336	48	316	277	426	370	362	129	173	102	401

Pairs with common second values, and resulting exponents:

$(9, 48), (14, 48)$, $x_1 = 24 \cdot 9 + 14 = 230 \pmod{540}$
$(5, 129), (20, 129)$, $x_2 = 24 \cdot 5 + 20 = 140 \pmod{540}$
$(20, 129), (20, 129)$, $x_3 = 24 \cdot 20 + 20 = 500 \pmod{540}$
$(13, 194), (8, 194)$, $x_4 = 24 \cdot 13 + 8 = 320 \pmod{540}$
$(2, 198), (2, 198)$, $x_5 = 24 \cdot 2 + 2 = 50 \pmod{540}$
$(17, 198), (2, 198)$, $x_6 = 24 \cdot 17 + 2 = 410 \pmod{540}$

Question 3.

We assume that year has 365 days. People born on 29^{th} of February usually celebrate birthday on the 28^{th} anyway.

(a) The birthday co-incidence probability given by the birthday paradox equation is:

$$1 - \frac{365!}{365^n(365-n)!}$$

For $n = 135$, this gives:

$$1 - \frac{365!}{365^{135}(365-135)!} \approx 0.99999999999960$$

Meaning the probability is around 99.999999999960%, or, in other words, practically certain.

(b) Since the chance of some specific other student sharing birthday with me is $\frac{1}{365}$, the chance of him not sharing is $\frac{364}{365}$, the probability of all the 134 students other than me not sharing is $\left(\frac{364}{365}\right)^{134}$ and finally the probability of some other student sharing birthday is:

$$1 - \left(\frac{364}{365}\right)^{134} \approx 0.3076$$

Meaning the probability is around 30.76%.

Question 4.

Given problem is an equivalent to solving the birthday paradox for a year with 2^{64} days. Let's consider the complementary event, that is that no collision occurred. The probability of such event considering n 2^{64}-bit hashes (by the pigeonhole principle $n \leq 2^{64}$) is equal to

$$P(A^{'}) = \prod_{i=0}^{n-1}(1 - \frac{i}{2^{64}}) = \prod_{i=0}^{n-1}\frac{1}{2^{64}}(2^{64} - i) = \frac{1}{2^{64n}} \cdot \frac{2^{64}!}{(2^{64} - n)!}$$

However as the size of hash is large, an approximation can be used. Assuming $n << 2^64$ we will use the fact that for $ln(1 - \epsilon) = -\epsilon$ for small positive ϵ. We obtain:

$$ln(P(A^{'})) = \sum_{i=0}^{n-1} ln(1 - \frac{i}{2^{64}}) = \sum_{i=0}^{n-1} -\frac{i}{2^{64}} = -\frac{1}{2^{64}} \cdot \frac{n(n-1)}{2} \approx -\frac{1}{2^{64}} \cdot \frac{n^2}{2} \text{ (for large n)}$$

$$e^{ln(P(A^{'}))} = P(A^{'}) \approx e^{-\frac{n^2}{2 \cdot 2^{64}}}$$

The probability P(A) of generating at least one collision in a set of n 2^{64}-bit hashes is at least $\frac{3}{4}$ when $P(A^{'}) \leq \frac{1}{4}$. Therefore we obtain:

$$\begin{aligned} e^{-\frac{n^2}{2 \cdot 2^{64}}} &\leq \frac{1}{4} \\ -\frac{n^2}{2 \cdot 2^{64}} &\leq ln(\frac{1}{4}) \\ n^2 \leq -2 \cdot 2^{64} \cdot ln(\frac{1}{4}) &\approx 5.11452 \ldots \cdot 10^{19} \\ n &\approx 7.15159 \ldots \cdot 10^{9} \end{aligned}$$

At leas $\approx 7.15159 \ldots \cdot 10^{9}$ guesses must be made in order to obtain probability of a collision at leas $\frac{3}{4}$.

Question 5.

We are encrypting message $x = 1111_2$, $s_0 = 195$ with parameters $p = 11$ and $q = 43$.

$$\begin{aligned} n = p \times q &= 473 \\ s_1 = 195^2 \ mod \ 473 &= 185 \\ s_2 = 185^2 \ mod \ 473 &= 169 \\ s_3 = 169^2 \ mod \ 473 &= 181 \\ s_4 = 181^2 \ mod \ 473 &= 124 \\ s_5 = 124^2 \ mod \ 473 &= 240 \\ \sigma_1\sigma_2\sigma_3\sigma_4 = 1110 (least \ significant \ bits \ of \ s_1, \ s_2, \ s_3, \ s_4) & \end{aligned}$$

$$c = (s_5, \ x \oplus \sigma_1\sigma_2\sigma_3\sigma_4) = \underline{\underline{(240, 0001)}}$$

Question 6.

(a) The function is not negligible because if we set $p(n) = n^2$ and suppose the inequality $ln(1 + \frac{1}{n}) > \frac{1}{n^2}$, then $\lim_{n\to\infty} ln(1 + \frac{1}{n}) * n^2 = \infty$ which is > 1 for at least most of n values, meaning $f(n) \leq \frac{1}{p(n)}$ can not hold "for almost all n" as the definition states.

(b) It is easy to see that for any polynomial $p(m) = a_m n^m + \cdots + a_0$ the function $r_p(n) = \sum_{i=0}^{m} |a_i| * n^m$ produces greater values than the polynomial. Therefore, if $f(n) \leq \frac{1}{r_p(n)}$, then $f(n) \leq \frac{1}{p(n)}$.

$e^{\frac{1}{n}} e^{-n} \leq \frac{1}{r_p(n)}$

$e^{\frac{1-n^2}{n}} \leq \frac{1}{r_p(n)}$

$ln(e^{\frac{1-n^2}{n}}) \leq ln(\frac{1}{r_p(n)})$

$\frac{1-n^2}{n} \leq ln(\frac{1}{\sum_{i=0}^{m} |a_i| * n^m})$

$\frac{1-n^2}{n} \leq -ln(\sum_{i=0}^{m} |a_i| * n^m)$

$\frac{1-n^2}{n} \leq -ln(\sum_{i=0}^{m} |a_i|) - m * ln(n)$

$\frac{\frac{1-n^2}{n} + ln(\sum_{i=0}^{m} |a_i|)}{-ln(n)} \geq m$

$\lim_{n\to\infty} \frac{\frac{1-n^2}{n} + ln(\sum_{i=0}^{m} |a_i|)}{-ln(n)} = \infty$

From the reason similar as in (a), m is lower than at least most of n values for any polynomial, hence the function is negligible.

Question 7.

(a) Suppose you know a valid plaintext-ciphertext pair $w_1 = 457, (a_1, b_1) = (663, 2138)$, constructed using the ElGamal cryptosystem with public key $p = 6661$, $q = 6$, $y = 6015$. Also you know that instead of using a new random r to encrypt each new message, the sender just increments the previous one, i.e. $r_2 = r_1 + 1$. With this knowledge decrypt the following ciphertext $(a_2, b_2) = (3978, 1466)$ without calculating discrete logarithms.

we know that:
$w_1 = 457$
$a_1 = q^{r_1} \mod p$
$b_1 = y^{r_1} w_1 \mod p$
$w_1 = b_1 a_1^{-x} \mod p$
and therefore $a_1^x = w_1^{-1} b_1 \mod p$
and we also know:
$r_2 = r_1 + 1$
$a_2 = q^{r_2} = q^{r_1+1} = a_1 q \mod p$
$b_2 = y^{r_2} w_2 = y^{r_1+1} w_2 \mod p$
$w_2 = b_2 a_2^{-x} \mod p$

To calculate w_2 now we can use this knowledge

$$\begin{aligned} w_2 &= \frac{b_2}{a_2^x} && \mod p \\ &= \frac{b_2}{(a_1 q)^x} && \mod p \\ &= \frac{b_2}{a_1^x q^x} && \mod p \\ &= \frac{b_2}{w_1^{-1} b_1 y} && \mod p \\ &= b_2 w_1 b_1^{-1} y^{-1} && \mod p \end{aligned}$$

Now to actually decrypt w_2 we need to calculate $b_1^{-1} \mod p$ and $y^{-1} \mod p$ (we can use for example extended eucklidean algorithm)
$b_1^{-1} \equiv 4153 \mod 6661$
$y^{-1} \equiv 464 \mod 6661$
and now we can calculate w_2
$w_2 = b_2 w_1 b_1^{-1} y^{-1} = 1466 \cdot 457 \cdot 464 \cdot 4153 = 888$

(b) Show that the same attack is possible for any linear update function of the random seed, i.e. whenever $r_2 = kr_1 + \ell \mod p - 1$.

we know that:
$a_1 = q^{r_1} \mod p$

$b_1 = y^{r_1} w_1 \mod p$
$w_1 = b_1 a_1^{-x} \mod p$
and therefore $a_1^x = w_1^{-1} b_1 \mod p$
and we also know:
$r_2 = kr_1 + \ell \mod p - 1$
$a_2 = q^{r_2} = q^{kr_1+\ell} = a_1^k q^\ell \mod p$
and therefore:

$$\begin{aligned} w_2 &= b_2 a_2^{-x} && \mod p \\ &= b_2 (a_1^k q^\ell)^{-x} && \mod p \\ &= b_2 (a_1^{xk} q^{x\ell})^{-1} && \mod p \\ &= b_2 ((w_1^{-1} b_1)^k y^\ell)^{-1} && \mod p \\ &= b_2 (w_1^{-k} b_1^k y^\ell)^{-1} && \mod p \\ &= b_2 w_1^k b_1^{-k} y^{-\ell} && \mod p \\ &= b_2 w_1^k (b_1^{-1})^k (y^{-1})^\ell && \mod p \end{aligned}$$