Exercise 9.1 (small public exponent RSA). (6 points) In a public domain
the exponent $e = 3$ is used as public exponent, thus every user chooses a
public modulus $N$ such that $\gcd(\varphi(N), 3) = 1$ and computes his respective
secret exponent $d$ such that $3 \cdot d = 1 \mod \varphi(N)$. Suppose that the users $A,$
$B, C$ have the following public moduli:

$$N_1 = 5000746010773, \quad N_2 = 5000692010527, \quad N_3 = 5000296004107.$$  

(i) ALICE sends a message $m$ to $A, B, C$ by encrypting: $m_i = m^3 \mod N_i$. 
An eavesdropper EVE intercepts the following values:

$$m_1 = 1549725913504, \quad m_2 = 2886199297672, \quad m_3 = 2972130153144.$$  

Show that EVE can recover the value of $m$ without factoring $N_i$ and 
compute this value. (Hint: Use the Chinese Remainder Theorem.)

(ii) Generalize the method used by EVE above for a general public exponent
$e$. How many messages should EVE intercept in order to recover the 
clear text message?

(iii) For $N_1$, the information $\varphi(N_1) = 5000740010560$ has leaked. Use this 
to factor $N_1$ and find the secret key of A. Do not use brute force.

Exercise 9.2 (a discrete log hash function). (6 points) A prime number $q$ so
that $p = 2q + 1$ is also prime, is called a Sophie Germain prime. We choose
$q = 7541$ and $p = 2 \cdot 7541 + 1$ both prime and want to define a hash function
on the set $\mathbb{Z}_q \times \mathbb{Z}_q$.

(i) Let $\alpha = 604$ and $\beta = 3791$. Prove that $\text{ord}(\alpha) = \text{ord}(\beta) = q$.

The elements $\alpha$ and $\beta$ actually generate the same subgroup of $\mathbb{Z}_p^*$, i.e. $\langle \alpha \rangle = \langle \beta \rangle$. Call this subgroup $G$. 
(ii) Now, we can define a hash function
\[ h : \mathbb{Z}_q \times \mathbb{Z}_q \to G, (x_1, x_2) \mapsto \alpha^{x_1} \beta^{x_2}. \]
Compute \( h(7431, 5564) \) and \( h(1459, 954) \) and compare them.

(iii) In (ii) you found a collision for the hash function \( h \). This enables you to compute the discrete logarithm \( \text{dlog}_{\alpha} \beta \). Do it.

(iv) Conversely, use your knowledge of \( \text{dlog}_{\alpha} \beta \) to compute another collision for \( h \).

Exercise 9.3 (correctness of RSA). (4+2 points) It is a common requirement for an encryption scheme to guarantee that the decryption of an encrypted text yields the original message. In short:
\[ \text{dec(enc(m))} = m. \]
This is property is called correctness.

(i) Use Euler’s Theorem to prove the correctness of RSA for messages \( m \in \mathbb{Z}_N^\times \).

(ii) RSA also works correctly for messages \( m \in \mathbb{Z}_N \setminus \mathbb{Z}_N^\times \). Prove that, too. Hint: Use the Chinese Remainder Theorem to transform a congruence modulo \( N \) into a system of two congruences modulo \( p \) and \( q \).