1. [10 points] Suppose that Alice's RSA public key is the pair (N, e).
   (a) Once Alice has decided on (N, e), how does she determine her decrypting exponent d? Why isn't Eve able to do the same thing, and decrypt messages intended for Alice?
   (b) Suppose that Alice wishes to use the same public key (N, e) to sign a document D. How does she compute the signature S? How does Victor (who only knows the public key) verify that the signature is correct?

2. [10 points] (a) State the Prime Number Theorem.
   (b) Estimate the number of primes between $1,000,000$ and $1,001,000$ (your answer may include logarithms, and will be marked correct if it is within 20% of the true value).
   (c) Estimate how many of these prime numbers are congruent to $1 \pmod 6$.

3. [10 points] Suppose that Samantha is using ElGamal parameters (p, g), and her public key is $A \in \mathbb{Z}/p\mathbb{Z}$. You may assume that g is a primitive root modulo p. Samantha has just generated a valid ElGamal signature (S_1, S_2) for a document D.
   (a) What congruence must be verified to check that this is a valid signature?
   (b) Suppose that Eve examines this signature and discovers that $S_1 \equiv g^3 \pmod p$. Describe how Eve can use this information to compute Alice's private key a (such that $g^a \equiv A \pmod p$). You may assume that $\gcd(S_1, p-1) = 1$.

4. [10 points] The number $p = 397$ is prime, and $g = 5$ is a primitive root modulo p. The prime factorization of $p - 1$ is $396 = 2^2 \cdot 3^2 \cdot 11$.

   Eve has computed the following three $\pmod p$ discrete logarithms.

$$\begin{aligned} \log_{5^{99}\%p}\left(311^{99}\%p\right) &= 3 \\ \log_{5^{44}\%p}\left(311^{44}\%p\right) &= 6 \\ \log_{5^{36}\%p}\left(311^{36}\%p\right) &= 2 \end{aligned}$$

   Using these three values, determine the value of $\log_5(311)$.

5. [10 points] Note (2024): you may omit this question, since our course does not assume the vocabulary of groups. Suppose that G is a finite group. Assume that you have access the following:

   - A function `Gmult(a,b)`, which takes $a, b \in G$ and returns their product in G.
   - A function `Ginv(a)`, which takes an element $a \in G$ and returns its inverse in G.
   - A constant `Gid`, which is the identity element of G.
   - A constant `Gord`, which is the integer $|G|$.

   (a) Write a function `Gpow(a,k)`, which receives an element $a \in G$ and an integer $k \in \mathbb{Z}$, and returns the group element g^k. For full credit, your function should call the function `Gmult` at most $\mathcal{O}(\log |k|)$ times.

(b) Assume that you also have access to a function `mod_inv(c,M)`, which takes integers $c, M \in \mathbb{Z}$ such that $\gcd(c, M) = 1$ and returns the inverse of c modulo M. Write a function `Groot(a,k)`, which receives an element $a \in G$ and an integer $k \in \mathbb{Z}$ such that $\gcd(k, |G|) = 1$, and returns an element $x \in G$ such that $x^k = a$. You may assume that the function `Gpow` from part (a) has been implemented correctly, and use it in your solution. For full credit, your function should call `Gmult` at most $\mathcal{O}(\log |k|)$ times (including the times it is called by `Gpow`).

6. [10 points] Suppose that Samantha and Victor agree to use a digital signature system that differs slightly from DSA. In this system, the parameters (p, q, g), public key A, and private key a are as in DSA. However, the equations describing a signature of a document D are now the following.

$$\begin{aligned} S_1 &= g^k \% p \% q \\ S_2 &= a^{-1}(kD - S_1) \% q \qquad \text{(where } a^{-1} \text{ denotes the inverse modulo } q\text{)} \end{aligned}$$

Describe a verification procedure for this signature scheme. Your answer should be similar to the verification procedure of DSA.