Assignment 3

June 2025

Question 1.

[ungraded] You must have learnt about Extended Euclid's GCD? If a and b are co-prime non-zero natural numbers, can you use it to find the modular inverse of a with respect to b, that is, $a^{-1} \mod b$?

Question 2.

Would you like to know more about the Miller Rabin Primality test? Learn about the Jacobi symbol $\left(\frac{a}{b}\right)$ from Wikipedia or Ireland-Rosen (chapter 3). Given that $a = 5$ and $b = 10^{256}+1$, can you use a property to compute $\left(\frac{a}{b}\right)$ on pen and paper?
Solution. We can use the properties:

$$a \equiv b \pmod{p} \tag{1}$$

$$\Rightarrow \quad \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) \tag{2}$$

$$\text{and} \quad \left(\frac{a}{b}\right) \cdot \left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\frac{b-1}{2}} \quad \text{since } a, b \text{ are coprime odd positive integers} \tag{3}$$

using these properties, we can see that since $10^{256} + 1 \equiv 1 \pmod 5$ therefore,

$$\left(\frac{10^{256}+1}{5}\right) = \left(\frac{1}{5}\right) = 1$$

and

$$\left(\frac{5}{10^{256}+1}\right) = \left(\frac{10^{256}+1}{5}\right) \cdot (-1)^{\frac{5-1}{2}\frac{10^{256}+1-1}{2}} = 1 \cdot 1 = 1$$

□

Question 3.

Read up the Miller-Rabin primality test (with or without proof). Suppose for our choice of public key and private key, $p-1 \mid n-1$ and $q-1 \mid n-1$. Does the Miller Rabin Primality Test cause a problem? (Hint: Carmichael numbers have a criterion called Korselt Criterion).
Solution.
According to the given properties, with the use of **Korselt Criterion**, we can say that n is a **Carmichael number**. If we apply Miller-Rabin test on this number n, we can easily factorise the number, which looses the main security aspect of RSA, hence Miller-Rabin does cause a problem with these properties. □

Question 4.

[ungraded] Read up about the Coppersmith Theorem based attacks on RSA (This will be fairly complicated). Is there an apparent criteria that the public key and private key must satisfy for the attack to be legitimate?

Question 5.

[ungraded] Is there an efficient way to compute the LCM of two numbers inputted as strings? Try and learn about the Carmichael Totient function and how the LCM can be used to efficiently encrypt in RSA.

Optional Reading

If you have a subtle idea about Quantum Computing, read up a bit about Shor's algorithm attack on RSA.

Coding Question

Take p as the smallest prime bigger than 10^{50} and take q to be the smallest prime bigger than 10^{52}. You will have to store them as strings due to their mass size. You are free to use any methods to find these primes; there are good libraries in C and C++ for this, you can use any generative AI to your help, however the direct response might be garbage so try to find a way to code it with its help and run it on your computer instead. Given the input as a string for an integer in base 10, implement a simple RSA Cryptosystem for encryption and decryption. Take e to be any 20 digit number satisfying the necessary parameters. To find the parameter d, try using basic recurrence for extended Euclid GCD, but you're free to try any method. Let your output be first the encoded string c and the decoded message d in next line. Except the procedure to find p and q, you should try to code everything, including all the necessary operations on the strings yourself.