4130 HW 4

Matthew Fisher

To better understand the cryptographic principles behind key pair generation, I constructed an unique RSA key generator for this homework. In order to ensure a solid understanding of each phase, I manually coded the process rather than depending on pre-built libraries for key creation. The software creates a public-private key pair, where the private key has two corresponding values and the public key has two values, using the required key size as input.

Selecting two huge prime numbers, p and q, whose bit lengths were roughly half the intended key size, was the first stage in the key generation process. For instance, p and q were each at least 512 bits for a 1024-bit key. I used the Miller-Rabin primality test to find appropriate prime integers. A probabilistic approach to determining if a number is prime, this test provides an effective trade-off between dependability and performance.

I determined the the product of the two prime numbers after choosing the prime numbers. The totient of the modulus, a value that the RSA technique uses to specify the relationship between the public and private keys, was then calculated. I decided on 65537 for the public exponent since it provides a fair mix between security and computing efficiency.

I determined the public exponent's multiple inverse with regard to the totient in order to construct the private key. By ensuring that the public and private keys function properly together, this step enables the creation of digital signatures as well as encryption and decryption. I utilized Python's sympy module, which offers functions for handling huge integers and carrying out modular arithmetic effectively, to manage the massive numbers needed in these computations.

Both the public and private keys are output by the program at the conclusion of the procedure. I developed a deeper understanding of the mathematics behind RSA encryption by manually carrying out the process, particularly how prime numbers, modular arithmetic, and key generation interact. The significance of safe and effective key creation in cryptography was emphasized by this homework.