CS553 Cryptography

BitBees

Question 7

Number Theory with SageMath

We have implemented the Euclidean GCD and Extended Euclidean GCD on Sage. Please refer to `q7_part1.sage` for the implementation of the same.

The first output simply is the modular inverse of 11 in $\mathbb{Z}_4$

The second output, separated by * is the number of invertible elements in $\mathbb{Z}_4$ along with checking for each element in $\mathbb{Z}_4$.

These inputs can be customized according to your choice.

The implementation using inbuilt functions can be found in `q7_part2.sage` A more efficient way to calculate the number of invertible elements in is by using Eulers Toitent function.

$$\Phi(n) = |\{1 \leq a < n | (a, n) = 1\}|$$

And $\Phi(p) = p - 1$ for prime numbers, we can factorize our given m to its prime factors.

$$\Phi(mn) = \Phi(m)\Phi(n)$$

$$\Phi(35) = \Phi(7)\Phi(5) = 6 \cdot 4 = 24$$

Implementation of this can be found in `q7_part3.sage`