Assignment 1

Task 1. Implement the ElGamal Enc algorithm in Sage

1. submit the code
2. Implement ElGamal based on Diffie-Hellman over Group 14 of RFC 3526
3. Provide "known answer-test" (KAT) values （i.e., an example of pk, sk, m and c）

Task 2. Implement the Textbook RSA signature in Sage

1. submit the code
2. the length of n should be 2048 bits
3. Show the attack that if $\sigma_1 = M_1^d$, $\sigma_2 = M_2^d$, then $\sigma_1\sigma_2$ is the Textbook RSA signature of M_1M_2
4. Provide "known answer-test" (KAT) values (i.e., an example of vk=(n, e), sk=d, m and σ)

SageMath is a free open-source mathematics software system licensed under the GPL. It builds on top of many existing open-source packages.

You may install SageMath on your laptop by following guide provided by https://www.sagemath.org/

Or just run your code using online project https://sagecell.sagemath.org/