Assignment 1 (Deadline 10 March)

- Implement the ElGamal Enc algorithm in Sage (or other languages)
    - submit the code
    - Provide “known answer-test” (KAT) values （i.e., example of pk, sk, m and c）

- Implement the Textbook RSA signature in Sage (or other languages)
    - submit the code
    - And 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 $M_1\ M_2$
    - run the attack to Hash-then-sign of RSA and show it does not work for Hash-then-sign of RSA
    - Provide “known answer-test” (KAT) values (i.e., example of vk=(n, e), sk=d, m and σ）

- Write a report about the algorithms and implementation
- Assignment 1 will be available on the blackboard