# INTE2401/2402 Lab 10

Student ID: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

This week’s lab concentrates on Shamir identity-based signature scheme based on RSA.

* Apache commons codec lib provides binary encoding methods, e.g. Base64. Download at (<https://commons.apache.org/proper/commons-codec/download_codec.cgi> ). User guide is provided at (<https://commons.apache.org/proper/commons-codec/userguide.html> ).

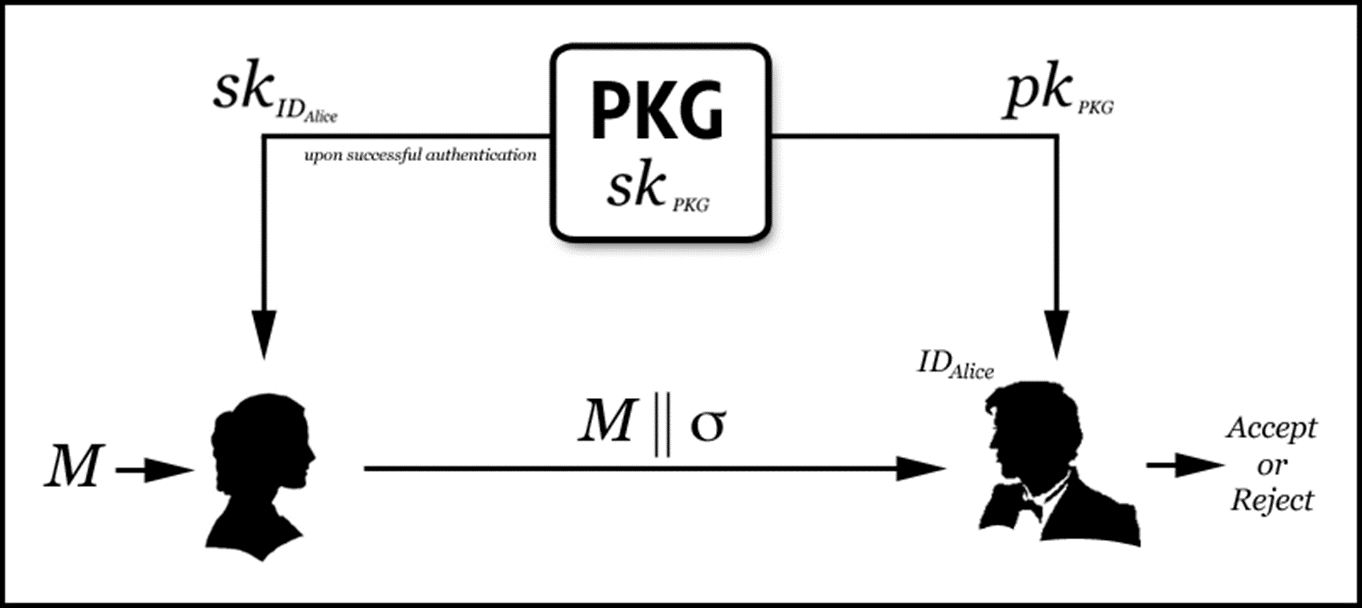


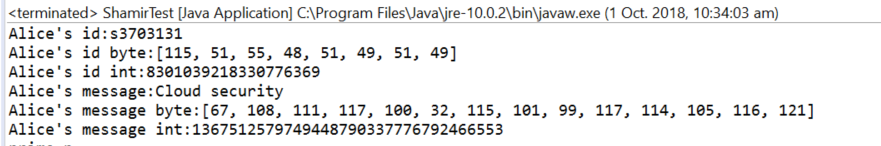
Figure 2. Shamir IDS

Fig 2 displays the Shamir Identity-based Digital Signature (IDS) scheme based on RSA. In this task, we use Java to implement scheme. We use our ***student no as Alice’s ID***, and we specify the ***message as “Cloud security”***. In this scheme, we have three functions.

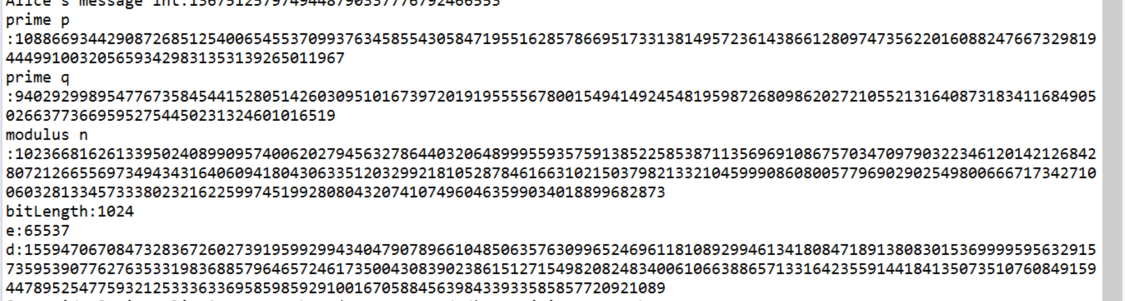
Q1. Implement a Java program of Shamir IDS scheme based on RSA to check the authenticity of a message and output the intermediate results sk\_Alice, signature (s,t).

Sample:

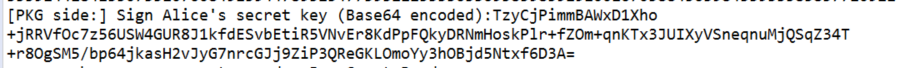
1) Choose message and id.



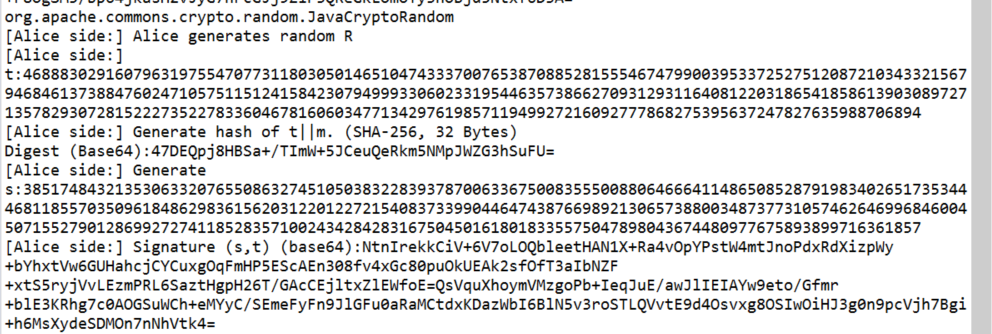
2) Generate RSA keys (RSA-1024).



3) PKG side computes sk\_Alice.



4) Alice side computes signature(s, t).



5) Bob side verifies the validity.

