# COMP 522: Privacy and Security
# Lab session 4

Lecturer: Alexei Lisitsa

## RSA encryption and SHA-1 digests

Download, compile and run the following simple programs available at the web page `www.csc.liv.ac.uk/~alexei/COMP522/index.html` of COMP522 course:

- RSA encryyption/decryption with random keys (`RandomKeyRSAExample.java`)
- SHA-1 hashing (`MessageDigestExample.java`)

Look into the code and see how the encryption and hashing are implemented.

## Message authentication using SHA-1 hash algorithm and RSA encryption

This exercise asks you to write a simple program in Java using JCA which combines both RSA encryption and SHA-1 to demonstrate the message authentication protocol shown as variant b) on page 9 of lecture notes on Message Authentication and Hash Functions.
The program needs to model activities of two participants, Sender and Verifier.
**Sender:**

- takes a text of the message;
- calculates the message digest (hash function) using SHA-1 algorithm;
- generates a pair of RSA private/public keys;
- encrypts the produced digest (hash) with a private key;
- passes the original message, encrypted digest and public key to the Verifier.

**Verifier:**

- decrypts the digest produced by the Sender with the Sender's public key;
- recalculates a new digest from the text of the message he has recieved;
- compare and prints these two digests.

By experimenting with this program, show that the Verifier can detect the following attacks:

- The message has been changed in passing from Sender to Verifier;
- The encrypted digest has been changed in passing from Sender to Verifier;
- Both message and encrypted digest have been changed.

# Digital Signature Algorithm

Implement a version of a program for the message authentication which utilizes Digital Signature Algorithm (DSA) available in JCA. See details on use of DSA in
`http://docs.oracle.com/javase/7/docs/technotes/guides/security/crypto/CryptoSpec.html#SigEx`.
Show that again Verifier may detect Adversary's attacks.