COMP 522: Privacy and Security
Lab session 3

Lecturer: Alexei Lisitsa

For this session, I should like you to try to estimate how fast the password - based encryption/decryption can be done using JCA.

How to Measure Execution time in Java

You can use either System.nanoTime() to measure *elapsed time* or System.currenTimeMillis() to measure *wall-clock* time. A good discussion of differences between two with examples of code can be found at https://www.techiedelight.com/measure-elapsed-time-execution-time-java/

How fast is password-based DES encryption?

In order to estimate how long brute-force search attack would take on a password-based encryption, one needs to estimate an average time required to perform one encryption/decryption.

Task 1 Modify Password-Based Encryption Program PBEs.java considered in Lab 2, so it can measure execution time of

- key generation and encryption (repeated 5 times);
- key generation and decryption (repeated 5 times).

Measure the above times for a fixed password, fixed plain text, salt and iteration count. Repeat experiments a few times for each measurement. Make a record of your measurements. **Task 2**

- Change your program to try different iteration counts: 1,5,10,100,1000,2000.
  How does it affect time measurements above?
- Try various passwords. Are time measurements affected?
- Try plain texts of different sizes. Are time measurements affected?

Question 3
Should we increase or decrease iteration count to make an encryption more resistant to brute-force search attack? What are potential disadvantages of doing that?