Department of Computer Science
COMP522 Individual coursework
Assignment 1

Alexei Lisitsa
a.lisitsa@liverpool.ac.uk

1 Overall marking scheme

The coursework for COMP522 consists of two assignments, contributing to 25% of the final mark. The contribution of the single assignments is as follows:

Assignment 1	20%
Assignment 2	20%
TOTAL	40%

Failure in any assignment may be compensated for by higher marks in other components of the module.

This document describes Assignment 1. Assignment 1 will be marked according to the following broad criteria:

- correctness of the arguments;
- presence/absence of the evidence on the experiments;
- original contribution either in implementation, or analysis.

2 Aims of the Assignment 1

- to illustrate the practical complexity of brute-force search attacks on the password-based encryption;
- to test the students skills of using symmetric cryptography primitives in Java programmes;
- to test the students skills in the analysis of the experiments.

3 Estimation of time required for brute-force search attack on the password-based encryption

This assignment asks you to estimate the time required for successful brute-force search attack on *password-based encryption* using JCA in Java. It assumes that you have done Lab 1, Lab2, Lab3 (see web page of the module).

1. Make a list of passwords, mentioned in item 3, and asked for in item 4 of section Lab1.1 of Lab 1 instructions (page 1);
2. For password-based DES encryption implementation in JCA (Lab 2 and Lab 3) fix some salt and iteration count and record an average time required for encryption/decryption (done in Lab 3);
3. For each of the passwords above estimate the time required for successful brute-force search attack, assuming that an attacker knows:
    - the predefined plaintext;
    - the ciphertext produced;
    - the salt;
    - the iteration count;
    - but **no password**.
4. Investigate how the time required for the attack depends on the iteration count;
5. Consider a variant of the attack, in which an attacker knows everything as above,except the iteration count, and estimate the time required to recover the passwords;
6. Compare your estimated time with the estimated time returned for the same passwords by online services (Lab 1, page 2) and propose plausible explanation of any observed differences.
7. Write a report on the above, providing an evidence for your arguments (e.g. snippets of code used to estimate time required for one encryption).

Please notice that the assignment tasks above *do not assume* that you will implement a program for full brute-force search.

4 Useful information

You may find it useful to have a look again on the simple program implementing password-based encryption (used in Labs 2 and 3): PBEs.java
Direct link: http://www.csc.liv.ac.uk/~alexei/COMP522_18/PBEs.java

JCA Reference Guide can be found at
http://java.sun.com/javase/6/docs/technotes/guides/security/crypto/CryptoSpec.html

5 Submission

You need to submit:

- Report (in *.pdf, *.doc,or *.docx format)

The work must be submitted electronically via Electronic Coursework Submission System. This must be done by

17.00 on Wednesday, 2nd of November, 2022

Please be aware that the standard University policies

- on plagiarism, collusion and fabricated data www.liv.ac.uk/tqsd/pol_strat_cop/cop_assess/cop_assess.doc, Section 8 and
- on late submission www.liv.ac.uk/tqsd/pol_strat_cop/cop_assess/cop_assess.doc, Section 6 are applied to this assignment.