Department of Computer Science
COMP522 Individual coursework
Assignment 2

Alexei Lisitsa
a.lisitsa@liverpool.ac.uk

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 2. Assignment 2 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.

Aims of the Assignment 2

- to illustrate the practical aspects of using asymmetric cryptography, hash functions, digital signatures for the message authentication;
- to illustrate the practical aspects of key exchange algorithms
- to test the students skills of using cryptographic primitives in programming with JCA;
- to test the students skills in the analysis of the experiments.

This assignment consists of two parts: on message authentication and on key exchange.

Comparison of methods for message authentication

This part of the assignment asks you to overview and compare the following methods for message *integrity*, *authentication* and *non-repudiation* considered at lectures and Labs 4 and
6:

- hash functions (for example SHA-256);
- RSA + SHA1 method considered at Lab 4;
- DSA method considered at Lab 4;
- HMAC-SHA256 considered at Lab 6.

For each method please give a short description, including the statement of what it can be used for and under which assumptions, as well as what are possible advantages and disadvantages of these methods. Illustrate your arguments by the results of experiments (Lab 4, Lab 6, or of your own design).

Key Exchange for Four parties

This part of the assignment asks you to design and implement a variant of Diffie-Hellman Key exchange protocol which would allow to exchange the secrets between four parties. Please

- describe a theoretical design, similar to that presented at the lecture for two-party DH protocol;
- using provided reference implementations of DH for two and three parties (Lab 5) implement your design and demonstrate it works;
- write a report on the above, providing an evidence for your arguments.

1 Submission

You need to submit:

- Report (in *.pdf, *.doc,or *.docx format)
- Java code for your implementation

The work must be submitted electronically via Electronic Coursework Submission System (part of SAM system).
This must be done by

17.00 on Wednesday, 7th of December, 2022

Please be aware that the standard University policies on plagiarism, collusion and fabricated data and on late submission are applied to this assignment.