University of London International Programmes
Computing coursework assignments 2015–16

CO3326 Computer security
Coursework assignment 2

This coursework assignment is designed to help you enrich your learning experience and to encourage self-study and creativity. Assumptions may be added if necessary in your coursework answers to simplify implementation tasks or help with understanding issues. You should, however, attempt the exercises at the end of each chapter in the textbook or subject guide before doing the coursework. Otherwise, you may find the tasks in the coursework assignment difficult and the experience less rewarding. You should read the coursework assignments or questions carefully and pay particular attention to the Submission Requirements on page 2 and the ***Code specification CO3326 cw2*** *on the VLE.*

Based on the software prototype that you have developed in Coursework 1 and the code specification, analyse and implement the protocol below about authentication using a trusted server S.

Suppose a trusted server S that distributes public keys on behalf of others. Thus S holds Alice's public key K_A and Bob's public key K_B. S's public key, k_S, is well known. Now Alice (A) and Bob (B) wish to authenticate with each other and they propose to use the following protocol.

1) Dear S, This is A and I would like to get B's public key. Yours sincerely, A.
2) Dear A, Here is B's public key signed by me. Yours sincerely, S.
3) Dear B, This is A and I have sent you a nonce only you can read. Yours sincerely, A.
4) Dear S, This is B and I would like to get A's public key. Yours sincerely, B.
5) Dear B, Here is A's public key signed by me. Yours sincerely, S.
6) Dear A, Here is my nonce and yours, proving I decrypted it. Yours sincerely, B.
7) Dear B, Here is your nonce proving I decrypted it. Yours sincerely, A.

1. Implement this protocol in Java to demonstrate how it works (again in decimal) according to the implementation details to be given in the **Code specification CO3326 cw2** on the VLE. This part of the program source code is worth up to [40%] credits.

2. Identify and in your program demonstrate if there is a subtle vulnerability of this protocol. [Hint: Consider if A uses this protocol to authenticate with a third-party Z.] This part of the program source code is worth up to [20%].

You may add if necessary assumptions for details to ease your implementation, but you must explain them clearly to gain credits. Also, you may decide where to start your implementation but it might be easier for you to first work out the keys and notations involved in each step. For example, let n_A and n_B be the nonce of A and of B respectively, and $(x, y)k$ be (x, y) with a signature k. The following lines denote the protocol with information flows to be transmitted.

1) A → S: A, B
2) S → A: $(K_B, B)k_S$
3) A → B: $(n_A, A)K_B$
4) B → S: B, A
5) S → B: $(K_A, A)k_S$
6) B → A: $(n_A, n_B)K_A$
7) A → B: $(n_B)K_B$

[END OF COURSEWORK ASSIGNMENT 2]

Submission requirements

The available marks are given in square brackets.

1. Your coursework submission must include a report Document [40%] and the program Code [60%]. The Document (preferable in .pdf format) should include the following sections:
   (a) Algorithms (in flow-chart)
   (b) Design (in block diagram or class-diagram in UML)
   (c) Demonstration (in 5 best screen-shots)
   (d) Discussion (including answers to any questions/problems in the Coursework assignment, your experience in attempt of the coursework, and full bibliography)

2. Your pdf. document should be named using the following conventions.

   FamilyName_SRN_COxxxxcw#.pdf (e.g. Zuckerberg_920000000_CO3323cw2.pdf)
   - **FamilyName** is your family name (also known as last name or surname) name as it appears in your student record (check your student portal),
   - **SRN** is your Student Reference Number, for example 920000000
   - **COXXXX** is the course number, for example CO1108, and
   - **cw#** is either cw1 (coursework 1) or cw2 (coursework 2).

3. The program code must meet the requirements as detailed **Code specification CO3326 cw2.**

4. You should monitor and report the time you have spent for each part of the coursework answers, and leave a note to the examiner if you need to raise any issue at the beginning of your coursework answers as follows:

Total Number of Hours Spent	
Hours Spent for Algorithm Design	
Hours Spent for Programming	
Hours Spent for Writing Report	
Hours Spent for Testing	
Note for the examiner (if any):	

5. Show *all* your work. Any use of others' work should be declared at the point of use and referred to in the *Bibliography* section at the end of your coursework answers.

[END OF SUBMISSION REQUIRMENTS]