Take home 2 (05/16/2017) - Extra Credit Assignment

(Assigned on 05/16/2017, deadline (sharp) on 05.30.2017)

Nature of the Assignment: This take home focuses on foundational tools required to establish and defend secure network systems. In particular, the modern internet communication heavily relies on SSL/TLS security suite. This suite itself relies on some basic algorithms, number theoretical and probabilistic tools. This take home aims establishing a minimum basic towards understanding these tools. This assignment aims at extending your knowledge on the complementary aspects of the topics covered during the class (so it goes beyond the material simply put on the slides, as described and emphasized before).

Requirements: Assignment will be completed by each student individually (no collaboration). Directly borrowing (e.g., copy-paste) from any material and putting in solutions (e.g., from online solutions, Wikipedia, or research papers) is plagiarism (see Syllabus for its corresponding actions). Please cite very carefully each resource you use, but citing a solution does not give a license to directly put it as an answer. All of your answers must be in your in own words and interpretations.

Format: Assignment should be prepared by a text editor (e.g., Microsoft Word or Latex). Handwritten submissions are not accepted.

Grading: Note that this is an all or nothing assignment, meaning that your submission will not be accepted unless you solve all the questions.

Extra Credit: This is an extra-credit assignment, and it will be added on top of your overall score at the end of the term. This means that not doing it will not impact your overall score, but doing so will support your grade.

Further Extra Credit: Latex is the de-facto tool for scientific writing. To encourage the use of this critical tool, we will provide further extra credit if you type your assignment with Latex. You can use any package of your choice, but may also consider IEEE conference format. You must attach your Latex code to prove you typed assignment with Latex.
1) Large Number Arithmetic to Enable Basic Primitives,
   a) What is the purpose of the Square-and-Multiply algorithm?
   b) Describe Square-and-Multiply algorithm with a pseudo-code.
   c) What is the time complexity of the Square-and-Multiply algorithm? Describe your answer to supplement your asymptotic analysis result.

2) The primitives of RSA,
   a) What is Totient function?
   b) What is the purpose of Extended Euclid Algorithm?
   c) Describe the Extended Euclid Algorithm with a pseudo-code.

3) RSA Scheme,
   a) Describe RSA encryption and decryption scheme in detail.
   b) How does Square-and-Multiply algorithm, Totient function, and Extended Euclid Algorithm play a role in RSA? Explain where they are used in your scheme description above.
   c) A naive implementation of RSA is vulnerable to timing based side channel attacks. Describe how such a timing attack on RSA can be launched based on the properties of the Square-and-Multiply algorithm.

4) DLP Concept and DSA Scheme,
   a) Describe what the generator for a given prime group is.
   b) Define Discrete Logarithm Problem (DLP) and its relation to generators.
   c) Give the pseudo-code of Digital Signature Algorithm (DSA), and explain how it is related to DLP problem.

5) What is the main cryptographic algorithm used in the most recent SSL/TLS suite? Provide at least the name of five important algorithms, and briefly explain their functionalities in SSL/TLS.