COMP3334 Computer Systems Security

Individual Assignment (15%)

[Deadline: 23:59:00 19th March 2021 (Sat)]

For ALL questions, type the steps for your solutions. For mathematical calculations, you must not rely on computer programs, and you have to show the steps of your calculations. Otherwise, NO marks will be awarded, even though your final answer is correct.

Question 1 One-time pad (5 marks)

Given *X*, which is the first 10 letters of your name in lowercase in the form of "<last_name><first_name>", e.g., "chantaiman", and a secret key, *K*, "polyucomputing"

a) Convert each letter of *X* and *K* to 8 bits using the ASCII code standard. If your name does not have 10 letters, append it with sufficient number of the letter, 'y'. [2 marks]
b) Encrypt *X* by *K* using one-time pad. [3 marks]

Question 2 Playfair Cipher (5 marks)

Encrypt the text, "apoonchoi", using Playfair Cipher. The key is your last name.

Question 3 RSA (15 marks)

In an RSA cryptosystem, you intercept a ciphertext C = 2022 sent to a user whose public key is (e = 27893, n = 124711). What is the plaintext M? Show your steps.

Question 4 Brute-force Attack (10 marks)

Suppose you need to find the key, by brute-force attack, of a ciphertext encrypted using Advanced Encryption Standard (AES). Assume the time of checking a key requires 1000 floating point operations. Find out the time (in terms of years in scientific notation) for the current fastest supercomputer (Check here) to exhaust the whole 256-bit key space. Assume each year has 365 days.

Question 5 Diffusion in ChaCha20 (25 marks)

The quarter-round function in ChaCha20 is based on add-rotate-XOR (ARX) structure. Refer to the paper: https://cr.yp.to/chacha/chacha-20080128.pdf, perform the followings:

a) Write a program in C/C++, Java, JavaScript or Python to implement the quarter-round function. Your program should include 5 test cases which clearly show the inputs and outputs in the console. [10 marks]

b) Diffusion is one of the properties of encryption algorithms that a small change in the input bits should have a large change in the output bits. In this question, you are required to measure the diffusion of the quarter-round function, which is defined as the average of the total number of output bits that is not the same as the input bits. Use a 4-bit input/output as an example. The input bits are 1011 and the output is 1000. The number of different bits is 2 (the latter two bits). Another set of input bits are 1111 and the output is 0000. The number of different bits is 4. So, the average is (2 + 4) / 2 = 3. Elaborate how you perform the measurement for the quarter-round function in a) and explain your findings, with the aid of your program. Also, state your assumptions. [15 marks]

Question 6 Case Study – Security Requirement Analysis (40 marks)

Exposure Notifications Systems (ENS) are widely adopted by numerous governments in the world for contact tracing in the pandemic. It allows public health authorities to collect relevant information of individuals and deliver prompt notifications to those who had contact with people contracted COVID-19.

One popular implementation of ENS is to have an app, installed in a smartphone, which (may) utilize various phone facilities and services, including GPS, Bluetooth, and camera, to collect information of the user manually/automatically, and alert the user if there is potential

exposure to COVID-19.

There have been extensive discussions about the privacy issue (and other security concerns) of ENS apps. In this case study, you are going to perform a thorough security requirement analysis on ENS systems and examine to what extent some ENS apps available in the market are able to fulfill the security requirements.

Write a 1500-word report that includes the followings:

1. An analysis of the security requirements of ENS. As a starting point, you may first use the C.I.A. model for your analysis. Then, consider other security requirements that you think important for this type of system. [15 marks]
2. Choose ONE of the following ENS apps and describe what security mechanisms are adopted to fulfil the security requirements you mentioned in 1. [15 marks]
    - LeaveHomeSafe - https://www.leavehomesafe.gov.hk/en/
    - TraceTogether - https://www.tracetogether.gov.sg/
    - NHS COVID-19 - https://covid19.nhs.uk/
3. Comment on the insufficiency(s) of the implementation and propose new requirement(s) and possible security mechanism(s). [10 marks]

Provide detailed justifications of any claims in your report.

Submission

The deadline of this assignment is **23:59:00 19th March 2022 (Sat)**. No late submission is allowed.

Submit your typed solutions in a single document file, in .doc, docx or .pdf format, to the "Individual Assignment" entry under "Assessments" in Blackboard.

Name the document file as:

<student_name>_<student_id>.<file_extension>

E.g., CHANTaiMan_12345678d.docx

For your program in Q5, only the source file(s) have to be submitted:

1. Create a folder and name it as Q5_<student no>_<your name>.
   E.g., Q5_12345678d_CHANTaiMan
2. Prepare a "readme.txt" file to briefly describe how your program can be run.
3. Put the program source and readme files into the folder.
4. Compress the folder (.zip, .7z, or .rar).
5. Submit the file to the "Individual Assignment (Program)" entry under "Assessments" in Blackboard.

A maximum of 3 submission attempts are allowed. Only the last attempt will be assessed.

Any wrong file naming and submission will receive 0 mark for the whole assignment. You have the obligation to check the correctness of your submission.

Note that plagiarism is serious offense. The similarity index in Turnitin will serve as an indicator of how much of your work was copied from other sources. Your submission with similarity index higher than 25% will be treated as plagiarizing unless proper justification and explanation. A rule of thumb is that you work by yourself alone and use your own words to write the report.

Both copiee and copier will receive 0 mark. Serious cases would be submitted to the Departmental Learning and Teaching Committee (DLTC) for further disciplinary actions.