Computer Science COMP4670/8640

Assignment 1

Due: End of Friday, October 18, 2019

Note

Some questions might be open-ended and therefore require your own opinions and/or creativity, as the answers can vary considerably.

Question 1 (15%)

Based on the definitions we had for “Threats”, “Vulnerabilities”, and “Controls”, bring two separate examples or scenarios, and indicate each of these three aspects in each scenario.

Question 2 (10%)

Using some sentences or examples, show how the four kinds of threats, “Interception”, “Interruption”, “Fabrication”, and “Modifications” relate to the three concepts, preserving “Confidentiality”, “Integrity”, and “Availability”. Is there a one-to-one correspondence between any pair of these concepts?

Question 3 (10%)

Do you believe attempting to break into a computing system without authorization should be illegal? Why or why not? Bring at least two examples and/or scenarios to support your answer.

Question 4 (15%)

For each of the following two programs, answer the three questions followed:

1. A program that accepts and tabulates votes in an election.
2. A program that allows consumers to order products from the web.

- Who might want to attack the program?
- What type of harms might they want to cause?
- What kinds of vulnerabilities might they exploit to cause harm?

After completion, submit your answers as a single pdf file into Blackboard.

Question 5 (10%)

One-time Pad is the only cryptosystem that provides ***Perfect Secrecy***.

- Describe advantages and disadvantages of this cryptosystem.
- Bring one example in real-word, in which one-time pad is suitable to be used, and one example that is not. Justify your answers.

Question 6 (10%)

Rotor machines were used by both Germany (Enigma) and Japan (Purple) in World War II. Watch this short clip on Enigma rotor machine:

http://www.khanacademy.org/math/applied-math/cryptography/crypt/v/case-study--ww2-encryption-machines

It consists of a set of independently rotating cylinders, each of which has 26 input pins and 26 output pins. Each input pin is connected to a unique output pin using internal wiring. You can see a related diagram in the following link, under the title "Rotor Machine":

http://sjsu.rudyrucker.com/~haile.eyob/paper/#3.%20Classic%20Cryptography

- A single cylinder defines a mono-alphabetic substitution. Considering a 5-rotor machine, what would be the equivalent key length of a Vigenere cipher for this machine? Explain your answer.

- Humans are said to be the weakest link in any security system. Give two examples of human failure that could lead to compromise of encrypted data.

Question 7 (5%)

Based on the convention we use to represent English alphabet using numbers 0 to 25, try to formulate Atbash Cipher by showing two mathematical expressions, one for encryption and one for decryption. Show the correctness of your expressions with one example.

Question 8 (15%)

After completion, submit your answers as a single pdf file into Blackboard.

Affine Caesar cipher is a generalization of the Caesar cipher, with the following form:

$$C = E([a,b],p) = (ap + b) \bmod 26$$

- What would be the limitations for the possible values of a and b? Explain why. Provide your answer as a general statement.
- Based on your answer to the first part of this question, how many distinct affine Caesar cipher exist? Explain your answer.
- The following ciphertext has been generated with an affine Caesar cipher. Break the code. **(It is important to show all the cryptanalysis steps you perform, and not just writing the final answer.)**

  `rarxl jobfp lobvb egler jnoob jgbej ozwgl`

  `nelxg crglg xcnpm sabne bgnne b`

  Hint:

  First indicate the first two most frequent letters in the cipher.

Question 9 (10%)

- How would you test a piece of ciphertext to determine quickly if it was likely the result of a simple substitution?
- How would you test a piece of ciphertext to determine quickly if it was likely the result of a transposition?

After completion, submit your answers as a single pdf file into Blackboard.