Assignment 1

CS-UH-3210: Computer Security

Due: Friday, September 14, by 8:00pm

The assignment is to be submitted electronically (no paper hand-in required). Upload your solutions to NYU classes as one PDF file with your name on the first page (only). The file name should contain your full name. Make sure you provide your own, individual solution.

Problem 1. Security Goals [11 points]
Read Chapter 1, subsections 1.1 to 1.3, of *Introduction to Computer Security* by Michael Goodrich and Roberto Tamassia.

1. Answer the exercises R-13, R-14, R-15, and C-3 at the end of the chapter. Explain your answers.
2. Classify each of the following as a violation of confidentiality, of integrity, of availability, or of some combination thereof.
   (a) John copies Marys homework.
   (b) Paul crashes Lindas system.
   (c) Carol changes the amount of Angelos check from $100 to $1,000.
   (d) Gina forges Rogers signature on a deed.
   (e) Rhonda registers the domain name "FancyCompany.com and refuses to let the company FancyCompany buy or use that domain name.
   (f) Jonah obtains Peters credit card number and has the credit card company cancel the card and replace it with another card bearing a different account number.
   (g) Henry spoofs Julies IP address to gain access to her computer.

Problem 2. Identify encryption schemes [6 points]
The task of this exercise is to identify which type of encryption was used for encrypting messages. The possible types are: Shift cipher (e.g., Caesar Cipher), Substitution Cipher, and Vigenere. For each pair of plaintext and ciphertext find out which method of encryption was used, explain why, and write down the key that was used for this method. Multiple correct answers are possible.

- **Plaintext**: `NEVERTRUSTINSECURITYBYOBSCURITY`
  Ciphertext: `ARIREGEHFGVAFRPHEVGLOLBOFPHEVGL`
- **Plaintext**: `THISISASECRETMESSAGE`
  Ciphertext: `GSRHRHZHVXIVGNVHHZTV`
- **Plaintext**: `GOOD`
  Ciphertext: `OVUA`

Problem 3. Substitution Ciphers [9 points]
Read Chapter 1 of *Understanding Cryptography* by Paar and Pelzl. Solve problem 1.1 at the end of the chapter. You can find a `txt`-file with the ciphertext provided on NYU classes. Do not use an existing tool or webpage to solve the problem but instead describe your approach on solving the problem and answering the questions. If you write code, append it to your solution.

Problem 4. Shift Ciphers [4 points]
In *Understanding Cryptography* by Paar and Pelzl, solve problem 1.2. You can find a `txt`-file with the ciphertext provided on NYU classes. Describe your approach and solution. Answer the questions.

Problem 5. Modular Arithmetic – Do NOT hand in!
To get practice with modular arithmetic – the basis of many cryptosystems –, work on the following exercises: 1.5, 1.6, 1.7, 1.8, and 1.9 in Chapter 1 of Paar and Pelzl. Do NOT hand in your solutions, but make sure you understand how to solve these exercises.