CS458-01/02/03 - Fall 2018
Problem Set 2
Due in Blackboard on Thursday, September 20 (11:59pm)

Problem 0

- Read Chapters 2 & 20 form textbook

Problem 1

Classify each of the following as a violation of `confidentiality`, of `integrity`, of `availability`, or of some combination thereof.

a. John copies Mary's homework.

b. Paul crashes Linda's system.

c. Carol changes the amount of Angelo's check from $100 to $1,000.

d. Gina forges Roger's signature on a deed.

e. Rhonda registers the domain name "AddisonWesley.com" and refuses to let the publishing house buy or use that domain name.

f. Jonah obtains Peter's 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 Julie's IP address to gain access to her computer

Problem 2

Computer viruses are programs that, among other actions, can delete files without a user's permission. A U.S. legislator wrote a law banning the deletion of any files from computer disks. What was the problem with this law from a computer security point of view? Specifically, state which security service would have been affected if the law had been passed.

Problem 3

Suppose that someone suggest the following way to confirm that the two of you are both of you are in possession of the same secret key. You create a random bit string the length of the key, XOR it with the key, and send the result over the channel. Your partner XORs the incoming block with the key (which should be the same as your key) and sends it back. You check, and if what you receive is your original random string, you have verified that your partner has the same secret key, yet neither of you has ever transmitted the key. Is there a flaw in this scheme? Explain.

Problem 4

Simplify the following XOR arithmetic expressions, where a, b, and c are bits such that $a \oplus b = c$, where $\oplus$ is shorthand for XOR, and a' stands for the complement of a (opposite bit value).

- $a \oplus a$
- $a \oplus a'$
- $a \oplus b'$
- $a' \oplus b'$
- $a \oplus b \oplus a$
- $b \oplus c$

Problem 5

Find the plaintext and the key, given the ciphertext CSYEVIXIVQMREXIH. *Hint: The key is a shift of the alphabet.*