**CS 4732/57322 Homework #1**

***Due electronically by midnight 6/26/2018***. There will be a one letter grade penalty for every day late, until 3 days after this date. No homework will be accepted after that time.

For submission, if done on paper please scan and submit as a pdf. If done in word, please submit the .docx or .doc format.

**IMPORTANT**: Clearly indicate outside resources utilized and sign below. Failure to cite use of outside resources will be reported for appropriate disciplinary actions. Note that discussions with other students are encouraged; copying – with or without modifications – is unacceptable and will also be reported.

<https://stackoverflow.com/questions/533965/why-is-security-through-obscurity-a-bad-idea>

http://crypto.interactive-maths.com/simple-transposition-ciphers.html

course powerpoints and book

I discussed one or more problems with the following people:

I hereby certify that any outside resources utilized, other than the textbook and class materials, are clearly cited. All other material I provide for this homework submission is my own original work.

THOMAS MARK MINTUN

*Printed name*

1. (8 points) In regards to the requirements of computer security:

a) What is the difference between confidentiality and integrity?

Confidentiality covers two concepts: data confidentiality and privacy. Data confidentiality assures that private or confidential information is not made available or disclosed to unauthorized individuals. Privacy assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

Integrity is composed of the two concepts of data integrity and system integrity. Data integrity assures that information and programs are changed only in a specified and authorized manner. System Integrity assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system. System integrity ensures that the system is not manipulated by an outside force.

**A loss of integrity is the unauthorized modification or destruction of information. A loss of confidentiality is the unauthorized disclosure of information. Integrity refers to the modification of the information, and confidentiality refers to the users of that information.**

b) Give an example of some scheme that would protect integrity but not give confidentiality and vice versa.

Symmetric encryption and data integrity algorithms would ensure data integrity but not confidentiality. Authentication protocols would protect confidentiality but not integrity. Non repudiation ensures confidentiality but not integrity. A connectionless integrity service that deals with independent messages provides data integrity only, and not confidentiality.

2. (4 points) Suppose an organization could not break the encryption used by another organization. What other possible technique could they use to try and gain information?

They could do traffic analysis which analyzes the pattern of messages, frequency of messages, length of messages, and location and identity of the communicating hosts. They could also do active attacks including: masquerade attack, replay attack, modification of messages, or denial of service attack to gain some information or at the least mess up the messages and see if the other organization makes a public statement that someone is attacking them, and use that info to attack another way. They could also brute force all possible keys, but this is essentially breaking the encryption which is said to not be possible in the question.

3. (5 points) Describe security by obscurity. Does this conflict with any security design principles? If so, list the ones that it violates.

Security by obscurity refers to making your data or system unknown/uncertain. Steganography can be used as an example of security by obscurity, because changing the least significant digit of a color in RGB of an image leaves the data out there in the open, but the data is obscure enough that most will not know there is a message being passed in the image.

The principle that this goes against is using known secure encryption algorithms that have been studied and believed to be effective. Security through obscurity violates the principles of least astonishment, separation of privilege, and most notably violates the open design principle.

4. (9 points) Assign low, moderate, or high impact level for the loss of confidentiality, availability,and integrity of an organization that handles student loan data for students at a university. Justify your answers.

Losing confidentiality, availability, and integrity of a system that handles student loan data for students at a university is a **HIGH** impact level. First, the information lost is very sensitive to customers, and malicious actors can do a lot of harm with the information. In other words, the loss of integrity of the system would have severe or catastrophic adverse effects resulting in major damage to assets belonging to the students at the university namely bank account and credit information. Also, this loss of security would almost certainly cause major financial loss as well so **HIGH** impact level loss.

Loss of availability in and of itself would be considered a low impact level threat because students assets are not lost, corrupted, or stolen. The downtime of the system would be the biggest issue to users of the system, which is NOT catastrophic.

If the data integrity breach is anything at all it is a high level threat because there are attacks to get key access which would compromise the entire system.

Data confidentiality threat would be considered low to medium for this system. The attackers could try to correlate information and prove you go to the university and have a loan, but this information is most likely public anyways. This threat has medium potential because the attackers could use this information with the help of other attacks to break the system.

5. (10 points) Write an attack tree for getting into a professor’s office in order to gain information about a test. Do not try this in practice.

The security incident that is the goal of the attack is represented as the root node of the tree, and the ways that an attacker could reach that goal are represented as branches and subnodes of the tree. The final nodes on the path outwards from the root (leaf nodes) represent a way to initiate an attack.

**On separate sheet! → I would add another leaf node to attack the school’s and your networks but scanned already**

6. (9 points) Find an integer x such that:

a)

4 % 31 ⇒ (5 \* 2) (mod 3) = 10 (mod 3) = 1 Hence x = 2

b)

6 % 5 1 ⇒ (7 \* 3) (mod 5) = 21 (mod 5) = 1 Hence x = 3

c)

8 % 7 = 1 ⇒ (9 \* 4) (mod 3) = 36 (mod 7) = 1 Hence x = 4

7. (10 points) Using Euler’s algorithm to find the GCD, calculate GCD(816,1071). Show each step of the algorithm.

1071 / 816 = 1 Remainder 255 ⇒ 816 / 255 = 3 Remainder 51 ⇒ 255 / 51 = 5 Remainder 0 → Hence GCD(816,1071) = 51

1) a is larger than b 2) set up a / b = c Raminder r do the division then replace a with b and replace b with r and repeat division 3) continue till remainder = 0

8. (6 points) Describe the difference between transposition and substitution in cryptography. Give a brief example of each.

Substitution and transposition are techniques used to change plain text into cipher text. Substitution involves replacing plaintext letters with different letters, numbers, or symbols. If bits, plaintext bit patterns are changed with ciphertext bit patterns. The Caesar Cipher was the first known example of this. The plaintext letters are substituted with the letter three places downstream from it in the alphabet, and X,Y,Z wrap around to A,B,C. Each letter is substituted by the letter 3 places downstream from it when the key equals 3.

Transposition involves moving the original letters around in the plaintext and/or ciphertext so as to jumble the letters in a non correct order. The letters or words of the plaintext are reordered by some way, fixed by a given rule. One simple example of this is to reverse the order of the letters. Plaintext is: transposition ---> ciphertext: noitisopsnart.

9. (5 points) Describe the difference between a monoalphabetic cipher and a polyalphabetic cipher.

A monoalphabetic cipher uses only the letters in one alphabet; a single cipher alphabet is (mapping from plain alphabet to cipher alphabet) is used per message. A cryptanalysis can still correlate letter frequencies and most likely break the code. **A monoalphabetic cipher uses fixed substitutions.** An example is Caesar’s cipher.

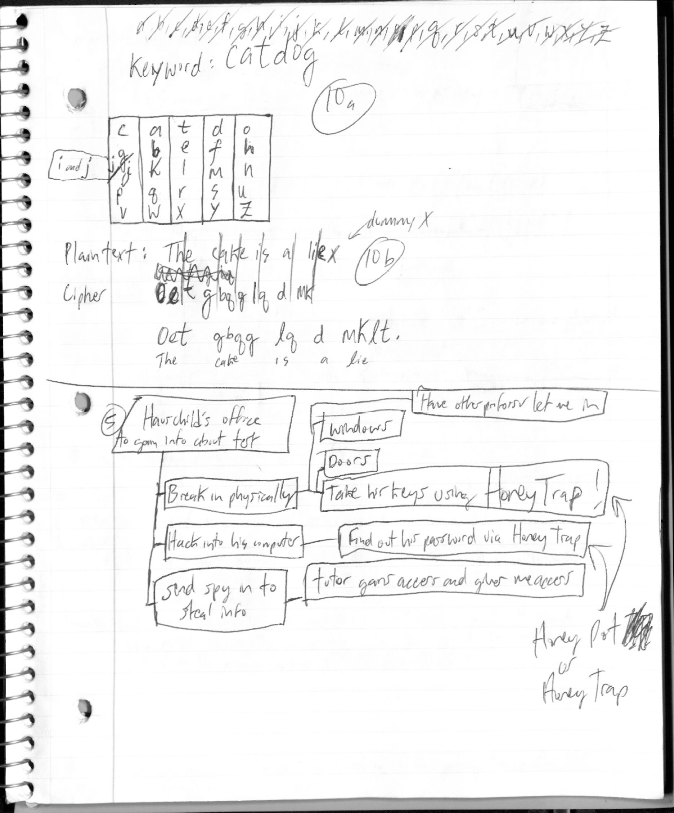
A polyalphabetic cipher uses different monoalphabetic substitutions as one proceeds through plaintext message. A set of monoalphabetic substitution rules is used, and a key determines which particular rule is chosen for a given transformation. **The strength of polyalphabetic cipher is that there are multiple ciphertext letters for each plaintext letter, one for each unique letter of the keyword. Thus the letter frequency is obscured.** A polyalphabetic cipher uses multiple substitution alphabets.

10. a)(10 points) Construct a Playfair matrix with the keyword catdog

**Done by hand on separate sheet.**

b) (5 points) Using your matrix above, encrypt the plaintext using the playfair cipher: The cake is a lie

**On separate sheet! Answer is: Oet qbqg lq d mklt**

****