Unit 6: Information Security — CS 101, Fall 2019

Learning Objectives

After completing this unit, you should be able to:

- Define confidentiality, integrity, and availability using examples.
- Discuss security threats/solutions within an operating system.
- Discuss security threats/solutions within a computer network.
- Explain the terms: firewall, malware, denial of service, phishing.
- Explain the limitations of random substitution and shift ciphers.
- Describe (in general terms) how public/private encryption works.
- Describe spoofing and how digital signatures establish identity.

Textbook Sections

3.5 Operating System Security

4.5 Network Security and Encryption

Video Lectures

- Security Part 1
- Security Part 2
- How the Internet Works (Videos 6–8)

Assignments

Act06 Encryption; Chapter 3 & 4 Problems

Lab06 Command Line Review; Telnet vs ssh, Encryption

Unit 6 Checklist: Sep 30 – Oct 06

Before Wednesday	**Date Completed**
FINISH models 1 and 2 of Encryption activity	
READ textbook 3.5 Operating System Security (take notes) ANSWER questions 1 and 3 in your notes	
WATCH video lecture: Security Part 1 (take notes)	
WATCH video lecture: Security Part 2 (take notes)	
READ tutorial: Command Line Review	
START Lab06: Telnet vs ssh, encryption	(10 pts)
Before Friday	**Date Completed**
READ textbook 4.5 Network Security and Encryption (take notes) ANSWER questions 3, 4, and 5 in your notes	
WATCH Code.org #6: Encryption & Public Keys (take notes)	
WATCH Code.org #7: Cybersecurity & Crime (take notes)	
WATCH Code.org #8: How Search Works (take notes)	
START Act06 exercises (complete at least 75%)	(15 pts)
UPLOAD and summarize references for PT1 in Google Drive	(10 pts)
Before Monday	**Date Completed**
COMPARE your Lab06 and Act06 with the solutions in Canvas	
SUBMIT Quiz06 – 1st attempt closed: see what you don’t know	
STUDY your notes, ask questions on Piazza, meet with the TAs	
SUBMIT Quiz06 – 2nd attempt open: try to get the full 10 points	(10 pts)

TAKE Exam06	(40 pts)

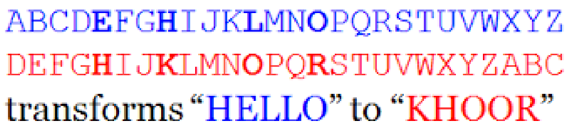
Activity 6: Encryption

Model 1   Caesar Cipher

Julius Caesar famously used a "Cipher Wheel" to encrypt his messages to Cicero. This website provides an electronic version of the cipher wheel:

http://cryptoclub.org/tools/caesar_cipher.php

The Cipher Wheel uses a shift of the alphabet to determine which letters should be substituted. The outer ring is the original characters in **plaintext** (the first row of characters); the inner ring is the encrypted characters in **ciphertext** (the second row of characters).



ABCD**E**FG**H**IJK**L**MN**O**PQRSTUVWXYZ
DEFG**H**IJ**K**LMN**O**PQ**R**STUVWXYZABC
transforms "HELLO" to "KHOOR"

Questions (10 min)   Start time: ________

1. In both the above model and in the electronic cypher wheel, blue (1st line) and red (2nd line) display the same set of characters. Which color/line represents the original characters, and which color/line represents the encrypted characters?

2. Rotate the electronic cypher wheel to match the blue and red characters above, by clicking on the white arrows. What is the key (the shift)?

3. Assume we do not know the key, but we know a Caesar encryption was used to encrypt this following ciphertext. Using trial and error, decrypt the phrase:

PDA XAOP PDEJCO EJ HEBA WNA BNAA

a) What is the original text?

b) What is the key (the shift)?

4. Consider how we might decrypt the phrase without the key.

a) How many different keys are there?

b) Describe the process that YOU used to decrypt a phrase when the key was unknown.

c) In contrast, describe the process a COMPUTER could use to decrypt a phrase when the key is unknown.

5. Think about the examples you brainstormed at the beginning of the activity. What is one advantage and one disadvantage of using Caesar Cipher encryption for online security?

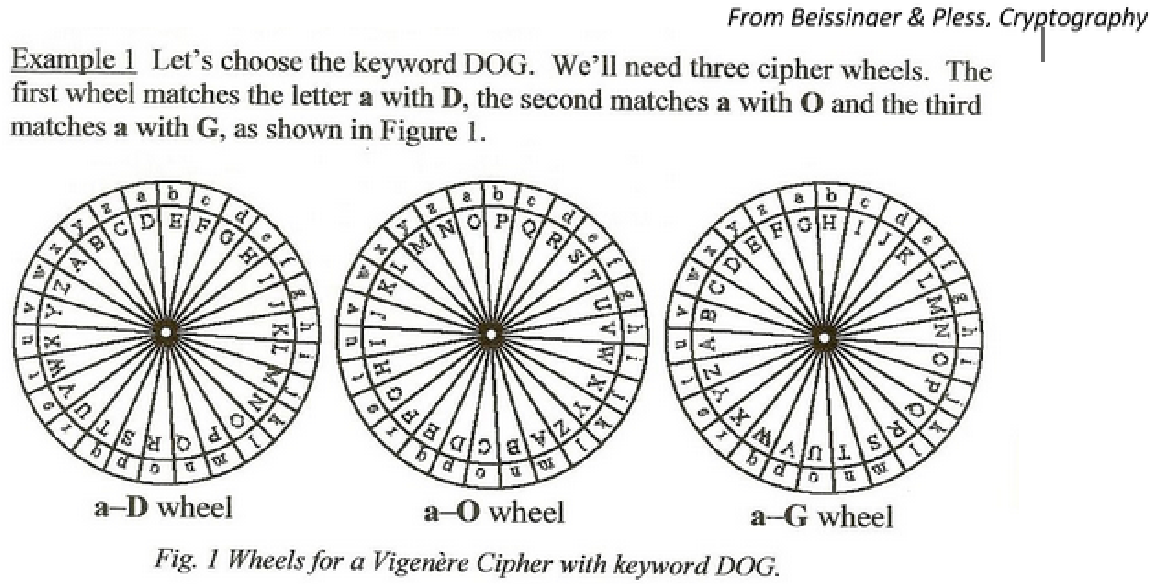
a) one advantage:

b) one disadvantage:

Model 2 Vigenère Cipher

Vigenère Ciphers are a value-added Caesar Cipher that is very difficult to crack. Instead of using a single number, the key is a word. Each character in the key is encoded with its own Caesar Cipher. For example, here is how you encrypt the word `UMBRELLA` using the key `DOG` shown below.

1. Enter plaintext: `UMBRELLA`
2. Apply the key: `DOGDOGDO`
3. Get ciphertext: `XAHUSROO`



From Beissinger & Pless, Cryptography

Example 1 Let's choose the keyword DOG. We'll need three cipher wheels. The first wheel matches the letter **a** with **D**, the second matches **a** with **O** and the third matches **a** with **G**, as shown in Figure 1.

a–**D** wheel

a–**O** wheel

a–**G** wheel

Fig. 1 Wheels for a Vigenère Cipher with keyword DOG.

Questions (15 min) **Start time:** ________

6. Which letters in `UMBRELLA` use:

   a) the a-D wheel for encryption?

   b) the a-O wheel for encryption?

   c) the a-G wheel for encryption?

7. Why do you think the online cipher wheel uses lower-case letters for the outer wheel and upper-case letters for the inner wheel?

8. If you were encrypting the word `PEANUT` using the keyword `CAT`, list which letters would use which cipher wheel.

9. Encrypt `PEANUT` using the keyword `CAT`.

10. Consider the length of the keyword.

a) If we knew the keyword was two letters long, how many combinations of cipher wheels are there? Show your work.

b) If we knew the keyword was three letters long, how many combinations of cipher wheels are there? Show your work.

c) Ideally, if we needed to encrypt a 1000 character document, how long should the keyword be? Explain your answer.

11. Think about the examples you brainstormed at the beginning of the activity. What is one advantage and one disadvantage of using Vigenère Cipher encryption for online security?

a) one advantage:

b) one disadvantage:

Conclusion

Modern encryption techniques (e.g., RSA and AES) are much more sophisticated than the shift ciphers we've looked at in this activity. But the idea is the same: you apply a "key" to some plaintext and transmit the resulting ciphertext.

Chapters 3 & 4: Information Security

Use the textbook, your individual notes, the video lecture slides, and the Internet to answer the following questions. Do NOT divide and conquer! Discuss each question as a group and work together to identify as many details as possible. Spend about five minutes of class time on each question.

1. Why is it a bad idea to log into your computer as an administrator to perform everyday tasks like browsing websites, writing documents, and playing games?

2. Describe how an operating system and CPU work together to prevent malicious code from gaining control over the system. (Hint: privileged instructions)

3. What is a firewall? What does it do? How does it work? Is it hardware or software? What security threats can it protect against?

4. What are the differences between viruses, worms, and Trojan horses? How can a user defend against them? What should someone do if their computer gets infected?

5. Describe a denial of service attack. What resources are necessary to carry out such an attack? How are these resources acquired?

6. What is a proxy server and what are its benefits? What are potential concerns of using a public proxy server?

7. What are the three security principles described by the CIA Triad? For each one, give an example of how it can be violated.