

choose one: Received Received help from:
 (or more) no help Collaborated with: _____

Homework: /SI110/Models & Tools/Symmetric Encryption

1. Decrypt the ciphertext "uwwv zwks", which was encrypted using the Ceasar Cipher with shift value 8. You may use the below link to help, but otherwise do this by hand!

<http://rona.cs.usna.edu/~sil10/resources/ceasar-shift/shiftTable.html>

10/8/6/0

2. You are in the middle of class, with everyone sitting at their desks, unable to get up for any reason. You have no cell phones or computers. So the only way you can communicate is by passing notes. There's a new student sitting across the room from you, whom you've never met before. Explain why you can't carry on a Ceasar Shift Encrypted note passing correspondence with the new person with any real hope of secrecy - even ignoring the possibility of someone doing a brute force attack (they should be paying attention!).

10/8/6/0

3. Use the Ceasar Cipher Frequency Analysis page from the SI110 website's Resources page (link below) to fill in the table below. Note: Refreshing the page clears all fields.

<http://rona.cs.usna.edu/~sil10/resources/ceasar-shift/freqAnalysis.html>

Ciphertext	Deduced Shift	Probability Correct	Plaintext
NWWB			
NWWBJITT			
NWWBJITTBMIU			

10/8/6/0

Explain why the deduced shift value changes from row to row.

10/8/6/0

4. Circle the correct answer. In the Vigenere Cipher, with a longer key ...

- a. communication is more secure.
- b. communication is less secure.
- c. the security of the communication is unchanged.

5/0/0/0

5. In what situation does the Vigenere Cipher provide provably perfect security? What alternative name do we use in this case?

10/8/6/0

6. Encrypt the message "GROUNDOUT" with the key "WRIT" using the Vigenere Cipher (link below). Show your work using the below table.

<http://rona.cs.usna.edu/~sil10/resources/vigenere/vctable.html>

Key										
Plaintext										
Ciphertext										

10/8/6/0

7. Using a chosen-plaintext attack, you've tricked your enemy into sending a message with plaintext "PARTYROCKERS". You intercept the ciphertext GEUKCUFGNVVV, and you suspect that your enemy is using the Vigenere Cipher (link below). Figure out your enemy's secret key! Show your work using the below table.

<http://rona.cs.usna.edu/~sil10/resources/vigenere/vctable.html>

Key											
Plaintext											
Ciphertext											

10/8/6/0

Secret Key:

5/3/3/0

8. Suppose I wanted to create a special kind of secret key encryption that splits the secret key between two people (Bob1 and Bob2), so that neither could encrypt/decrypt messages individually, rather it would take both of them together to encrypt/decrypt messages. Here are two ways to do this:

a) Use a vigenere cipher with key of length k , such that Bob1 has the first $k/2$ characters of the key and Bob2 has the second $k/2$ characters of the key.

Ex: $k_1 = \text{foo}$, $k_2 = \text{bar}$. Plaintext "happyday" gets encrypted with key **foobar** as **MODQYUFM**.

b) Use a vigenere cipher such that both Bob1 and Bob2 have k -character keys, k_1 and k_2 , but the real key needed to encrypt/decrypt is actually the result of applying a vigenere cipher to encrypt k_1 using k_2 as the key.

Ex: $k_1 = \text{foobar}$, $k_2 = \text{putter}$. Encrypt **foobar** with key **putter** to get key $k = \text{UIHUEI}$. Now plaintext "happyday" gets encrypted with key **UIHUEI** as **BIWJCLUG**.

Which of these is better at achieving the goal of only having encryption/decryption possible when Bob1 and Bob2 cooperate? Explain your answer!

10/8/6/0

9. Download and test software install following the directions below. You will lose HW points if this program doesn't work properly on Wed/Thurs.

Download

- a. Use the Google-Chrome
- b. Go to the course Resources web page.
- c. Towards the top left of that page: Right click "9. VM remote Console" Select "Save Link As..." SAVE IT TO YOUR **DESKTOP!**

Install

- a. Double click this icon on your Desktop: **vmLogin.msi**
- b. Install in **C:\SI110Programs**. Click through, affirming any security prompts.

Run

- a. Further down on the left of the Resources web page look for: "Virtual Machine Login". Open that page and follow the directions. Click through, affirming any security prompts. You do not have to use an Admin shell.