

Name: _____

Introduction to Information Assurance
Cryptology Lab

Lab: Caesar, Hill, Vigenère, XOR and Vernam, Transposition and Substitution

For this lab, you will use the Cryptool 2 to encrypt and decrypt sample messages. You will be learning about the different kinds and types of ciphers and how they work. We will look at four main ciphers: Caesar, Hill, Vigenère, Vernam and the XOR Cipher. The goal is to understand how each cipher works and to be able to identify and crack each individual type. These skills may be applied later during the CTF portion of the day.


You may want to save each workspace to use for decrypting CTF problems later.

Investigation/Specific Questions

- These are found in the lab instructions. Questions in bold are to be answered.

Name: _____

Caesar Cipher

1. Begin by pressing  + R
2. Start CrypTool 2: This may work - Type **C:\Program Files (x86)\CrypTool 2\CrypWin.exe** into the Run window – this will open up Cryptool 2.
3. In the Main Functions section, click on the “Create a new workspace” button.
4. Under the Classic Ciphers tab in the tool bar on the left, drag and drop a Caesar module into your workspace.
5. Resize the module so you can see all of the options.
6. Drag out the input arrow (top arrow) on the left hand side of the Caesar module and create a Text Input box. Do the same for the Text Output box on the right.
7. Enter some sample text into the Input Box on the left and click Play on the top menu bar.

8. **Make observations. What happened to the text? How did it change? What is the default key provided (key is an integer)? [3 points]**

9. **What happens when you enter something other than a letter (e.g. special characters)? [1 point]**

10. **What is cipher text “ZBWLY ZLJYLA TLZZHNL” decrypted with key 7? [1 point]**

DON'T FORGET TO HIT STOP AFTER THE PROCCES IS COMPLETED

You cannot make any other changes until you hit stop.

11. Now let's take a look at the frequency of the letters used. This information can be helpful in many different kinds of ciphers.
12. Right click the line connecting your Caesar module and the text output and select Delete.
13. Drag and drop a Frequency Test module from the Cryptanalysis menu in its place.
14. Connect the Caesar Ciphers string output to the String input on the Frequency test. Notice how the types are the same so when you connect them you get an OK! dialog.
15. Run the program and you should get a nice graph on the frequency of the letters.

Name: _____

Vigenère Cipher

1. Start off by creating a new workspace. Click the dropdown arrow next to “New” and click Workspace.
2. Under the Classic Ciphers menu drag in a new Vigenère module.
3. Create a Text Input Box by dragging the top left arrow outwards on the module. Do the same for the output on the left.
4. Before you dive into encrypting and decrypting with a Vigenère cipher you need to understand how they work. Every letter has a corresponding number associated with it. For example A is 1, B is 2, etc. The Vigenere Cipher has a text input and a key to shift by. For example, if you had the key “key” and the text “super secret message”, it would be visualized like this:

```
s u p e r   s e c r e t   m e s s a g e
k e y k e   y k e y k e   y k e y k e y
```

The cipher takes the corresponding value of each individual input letter in the message and the “shift value” represented by the key and adds them together. For example, the first letter of the message, “s” has a value of 19 and the first letter of the key, “k” has “shift value” value of 10. Then $19 + 10 = 29$. Now $29 \bmod 26$ is 3 which is “c”. Doing that for each letter through should give you the encrypted text “CYNOV QOGPOX KOWQKKC”

5. What would be the output if the first letter of the message was m and the first letter of the key was a? **[1 point]**

6. What is the cipher text “ZINCS PGVNU” decrypted? **[1 point]**

7. What was the key word used to encrypt the text? **[1 point]**

Name: _____

General Substitution Cipher

1. Create a new workspace by clicking the dropdown arrow next to “New” and click Workspace.
2. Under the Classic Ciphers menu drag in a new Substitution module.
3. Create 3 Text Input boxes and connect them to the Substitution module. Also create a Text output on the right. The three input boxes are the text to encrypt/decrypt, the alphabet, and what each letter should change to. For example, if you define the alphabet as A C E G I K and the shifts to B D F H J L then A → B, C → D.
4. **Decrypt the text “EOHITKZTBZ” using the standard alphabet source and the standard QWERTY layout from left to right starting with Q ending with M for the destination alphabet. [1 point]**

5. **What happens if you have a letter in the message that is not defined in your alphabet? [1 point]**

6. **What is a potential issue with not using the whole alphabet when you encrypt your message? [2 points]**

MAKE SURE YOUR ALPHABET AND TEXT ARE THE SAME CASE

The substitution cipher is case sensitive

Name: _____

Transposition Cipher

1. Create a new workspace by clicking the dropdown arrow next to “New” and click Workspace.
2. Under the Classic Ciphers menu drag in a new Transposition module.
3. From the Tools menu, drag 2 new text inputs into your workspace.
4. Connect the output arrows from the Text input to the Input arrows on the Transposition module.
5. Type a message into the top Input Box of the Transposition Module and a key into the bottom.
6. The Transposition module will show you the steps it is doing to encrypt the text and in the end it will print out the encrypted text.

7. Encrypt the text “SECRET MESSAGE” using the key “KEY” . **[1 point]**

8. Encrypt the text “AAWKDATTM ACT” using the key “CRYPTO” . **[1 point]**

9. What would happen if you had a key of only one letter? Does it matter what letter it is? **[1 point]**

Name: _____

The XOR Cipher

1. Create a new workspace and drag an XOR Cipher module into your workspace.
2. The XOR Cipher works by taking the binary value of the ASCII Code and combining them using a XOR Truth Table.

| INPUT | | OUTPUT |
|-------|---|--------------|
| A | B | $A \oplus B$ |
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

3. Start by dragging out the Data Input and XOR Key input and make them into Text Input Boxes. Do the same for the Data Output on the right.
4. **Encrypt the text “ATTACK AT DAWN” with the key ABCXYZ. What’s the encrypted text? [1 point]**

5. **Encrypt the text 101010 with the key 010111. What’s the encrypted text? [1 point]**

Name: _____

The Vernam Cipher

1. Create a new workspace by clicking the dropdown arrow next to “New” and click Workspace.
2. Under the Classic Ciphers menu drag in a new Vernam Cipher module.
3. Drag two new Text Inputs into your workspace from the Tools menu and connect them to the Vernam Cipher Module. Do the same for the Text Output.
4. Type a message into the top Input Box and a key into the bottom Input box.
5. A Vernam Cipher works by taking the first letter of the message and the first letter of the key and doing a XOR.
6. You can fix the Alphabet Input to only capital letters.

The Hill Cipher

1. The Hill Cipher takes in the string you would like to encrypt/decrypt and a matrix. You lay out the string into a matrix format and replace every letter with its position in the alphabet, A being 1, B being 2, etc. and perform matrix multiplication with the other matrix. You then go through and divide each number by 26 and use the remainder for the new number because you could have negative numbers after the multiplication. Convert those back to ASCII and you're golden.

2. An example Hill Cipher setup would look like this:

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \begin{pmatrix} 2 \\ 0 \\ 19 \end{pmatrix} \equiv \begin{pmatrix} 31 \\ 216 \\ 325 \end{pmatrix} \equiv \begin{pmatrix} 5 \\ 8 \\ 13 \end{pmatrix} \pmod{26}$$

3. The matrix on the left (The string) is multiplied with the matrix on the right (The key) to get the matrix [31, 216, 325] which when you perform a modulus operation on, you get the matrix [5,8,13]
4. To do this in Cryptool, start off by creating a new workspace by clicking the dropdown arrow next to “New” and click Workspace.
5. Under the Classic Ciphers menu drag in a new Hill Cipher module.
6. Drag a Text Input & Output module onto your workspace and connect it to the Hill Cipher module. Type in your matrix and hit run.

7. **Encrypt the text “MEETTONIGHT” with the matrix [3, -2, -1, 1] [1 point]**

8. **What happens if you have a non-alphanumeric character in your string? Why does this happen? [2 points]**

Name: _____

BONUS:

1. Why do some ciphers handle special characters different than others? **[1 point]**

2. Which one of these ciphers seems the most secure? Why? **[2 points]**

3. What's a real world situation where these ciphers can be used? **[1 point]**
