CIS313, Cryptography
Module 1 Lab – Caesar and Vigenere Ciphers

In this first week, we will be using a variety of tools to encrypt and decrypt using classic ciphers that we have learned about this week. Remember that the Caesar cipher is a simple shift cipher. It is called a shift cipher because the letters of the original plaintext are shifted by a key or number between 1 and 25. For example, if we use a key of 1, the letter C and A in the word cat would be shifted one to the right. C would become D, A would become B, and T would become U. The encrypted text would be DBU.

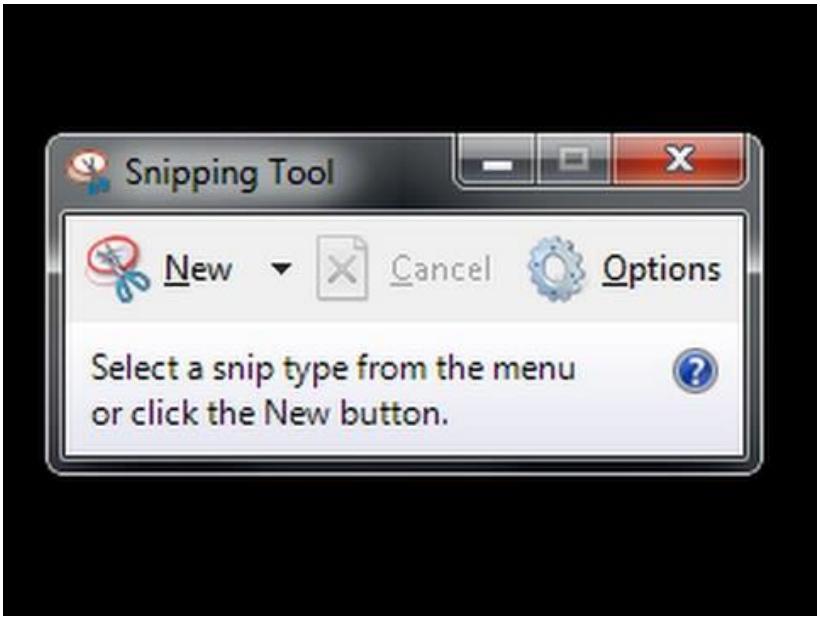
A more complex cipher is called the Vigenere cipher. This cipher uses a tabula recta which is an alphabetic square. Using this tabula recta, the plaintext, and a word or series of words as a key. The intersection between the plaintext letter and the corresponding letter in the key is found on the tabula recta and the letter found at the intersection becomes the corresponding ciphertext letter. The Vigenere cipher improves on the Caesar cipher and other monoalphabetic ciphers by obscuring or distributing the frequency of letters in the ciphertext and making the ciphertext harder to crack. From its invention in 1553 it remained secure until it was cracked in 1863, nearly 300 years.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Figure 1Tabula Recta: Image from https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher#/media/File:Vigen%C3%A8re_square_shading.svg

In this lab we will use a variety of tools including some websites as well as a tool you will become familiar with called Cryptool 2. Cryptool 2 is a program that helps you visualize and learn common cryptographic algorithms and how they work in operation.

You will need to take screenshots of your work. Please make sure you are familiar with the Windows Snipping tool. You can find a quick tutorial on the tool here:



You will be required to submit the following graded items as part of this lab:

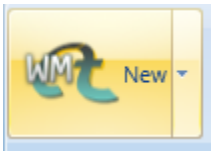
- A screenshot and text of the Caesar encrypted plaintext in Cryptool 2
- A screenshot and text of the Caesar decrypted plaintext in Cryptool 2
- Text of the Vigenere cipher encrypted ciphertext from https://studio.code.org/s/vigenere/stage/1/puzzle/1
- A list of the five most likely key lengths of Vigenere ciphertext from: https://www.dcode.fr/vigenere-cipher
- The broken Vigenere plaintext and source of the quote from Cryptool 2 and a Google (if the answer is not obvious)

Ensure you paste the required items in this document under the **BOLD** text.

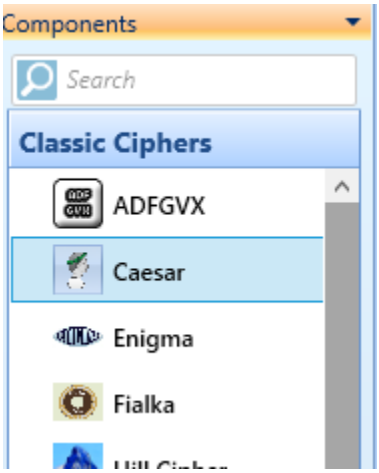
Lab 1 – Caesar Cipher Encryption and Decryption with Cryptool 2

1. Start by opening Cryptool 2. If you are using the Cybersecurity Desktop the tool can be opened by navigating to the Software folder and clicking on the Cryptool 2.1 (Stable Build 88553.1). If you can install the Cryptool 2 binary on your own Windows computer by downloading and installing it yourself. You can download the tool here: https://www.cryptool.org/en/cryptool2

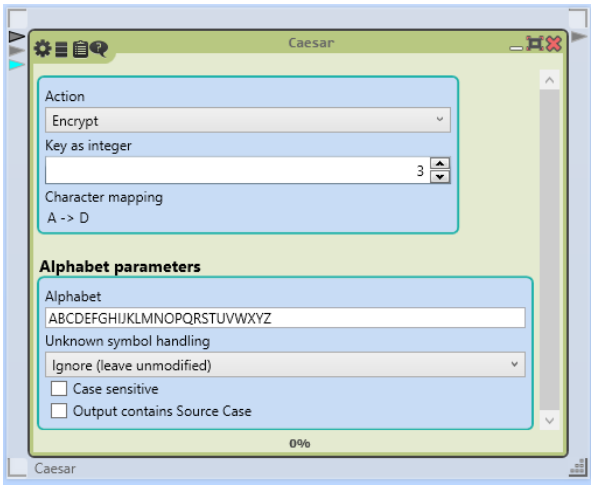
2. After opening Cryptool click on new workspace.



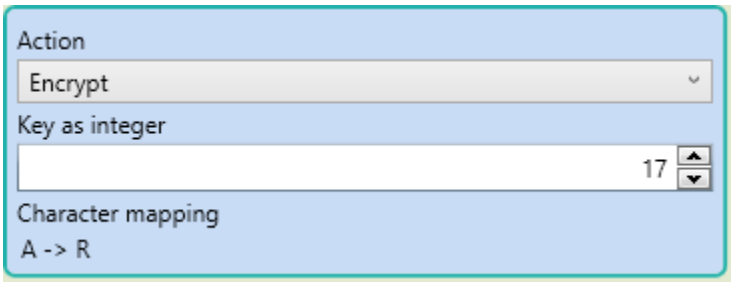
3. On the left side of the screen you will see components. Click the on the Classic Ciphers box to expand those components and then drag the component labeled Caesar to the workspace/canvas area on the right.



4. Expand the Caesar cipher component by dragging the lower left corner of the component right and down until you can see the components options. If your Caesar component doesn't show all the settings.



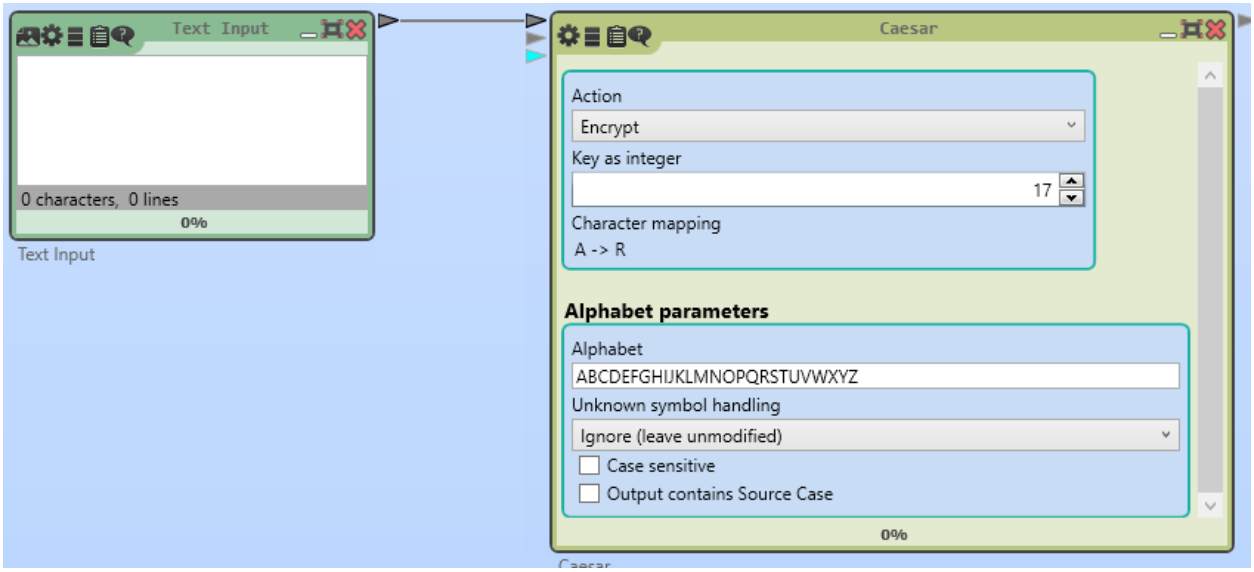
5. Change the Key as Integer field to 17.



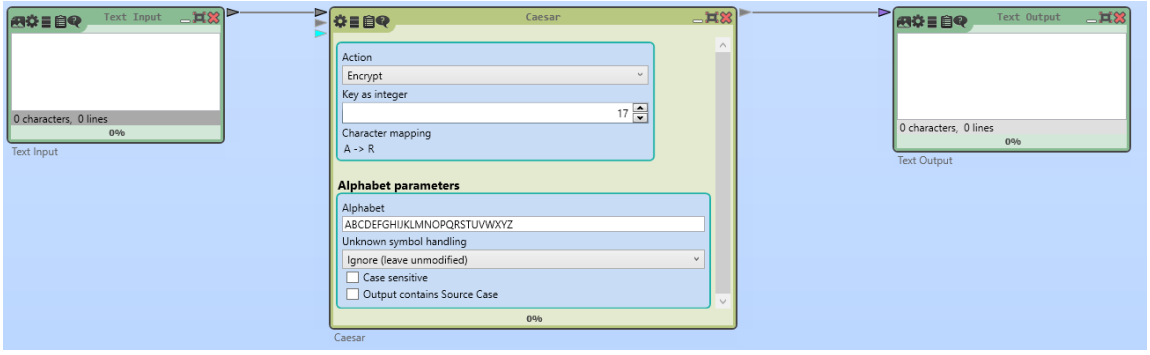
6. In the upper right-hand corner of the Caesar cipher component you will see three arrow that are dark gray, gray, and light blue. Hover your mouse cursor over each and you should see boxes that identify each as Text Input, External Alphabet Input, and Shift Value (Integer). Take your mouse on the top arrow labeled Text Input, click, and hold on it, and drag the line to an empty area of the canvas left of the Caesar component. Click on the Text Input < Text button that appears when you release the mouse. Click on the image below for an example.

   Animated Example

   Your canvas should now look like this:



7. Now that we have a Text Input component, we will also need to create a Text Output component. You can do this by clicking the gray arrow on the top right of the Caesar cipher component and dragging it to the right of to a blank area of the workspace/canvas. Click on the Text Output option that appears when you release the mouse button. Your canvas should now look like this:



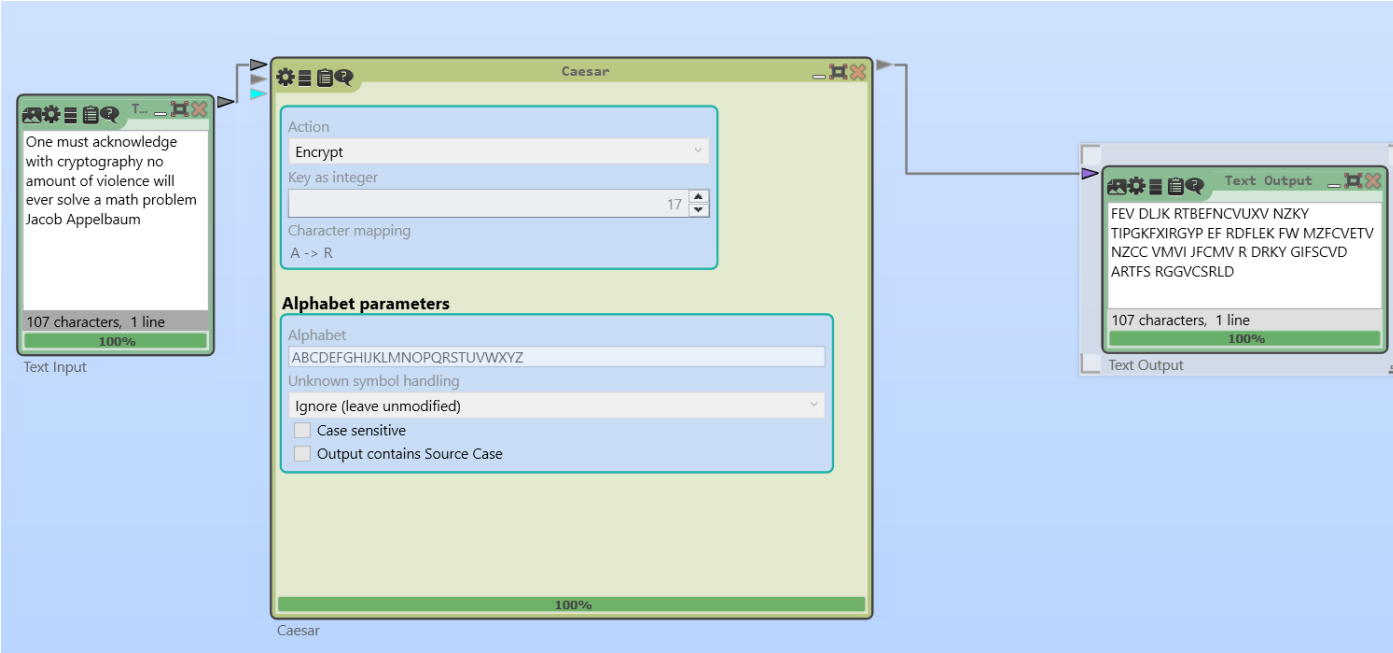
8. Now paste the following text into the Text Input component and hit the Play button in the ribbon at the top of the screen. Take a screenshot of your canvas with the Text Output showing

the encrypted text and paste it into the answer sheet. Paste the Text Output/Encrypted Text into the answer sheet.

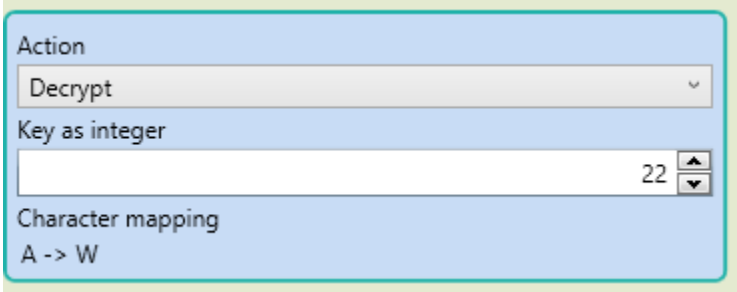
Text to Encrypt: One must acknowledge with cryptography no amount of violence will ever solve a math problem Jacob Appelbaum

Copy the answer text and take a screenshot of your completed canvas and paste them here:

FEV DLJK RTBEFNCVUXV NZKY TIPGKFXIRGYP EF RDFLEK FW MZFCVETV NZCC VMVI JFCMV R DRKY GIFSCVD ARTFS RGGVCSRLD



9. Click the Stop button in the ribbon at the top of the screen. Now change the Action in the Caesar component to Decrypt and change the Key as Integer to 22.

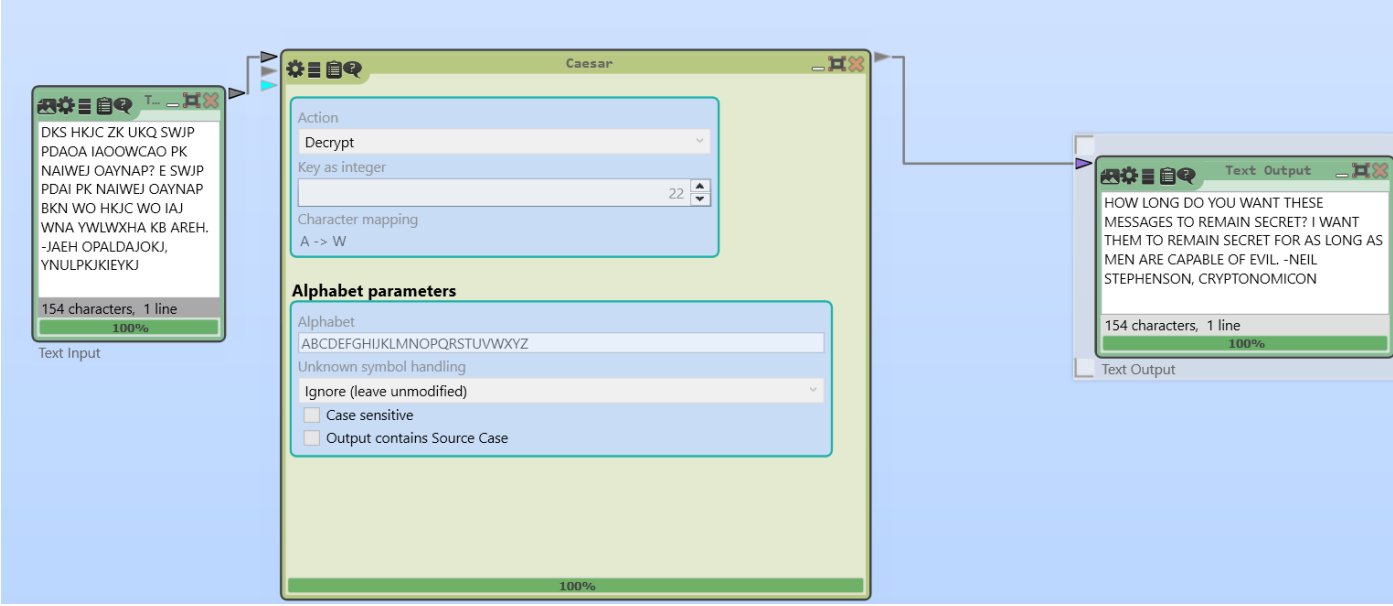


10. Decrypt the following encrypted text by pasting the encrypted text into the Text Input component and hitting play.

Text to Decrypt: DKS HKJC ZK UKQ SWJP PDAOA IAOOWCAO PK NAIWEJ OAYNAP? E SWJP PDAI PK NAIWEJ OAYNAP BKN WO HKJC WO IAJ WNA YWLWXHA KB AREH. -JAEH OPALDAJOKJ, YNULPKJKIEYKJ

Copy the answer text and take a screenshot of your completed canvas and paste them here:

HOW LONG DO YOU WANT THESE MESSAGES TO REMAIN SECRET? I WANT THEM TO REMAIN SECRET FOR AS LONG AS MEN ARE CAPABLE OF EVIL. -NEIL STEPHENSON, CRYPTONOMICON



Lab 2 – Vigenere Cipher Encryption

1. Navigate to the following website: https://studio.code.org/s/vigenere/stage/1/puzzle/1

2. In the Enter Your Message box copy or type the following message:
   In_God_we_trust_Everybody_else_we_verify_using_PGP_Tim_Newsome

3. In the Enter Your Secret Key box type CRYPTOGRAPHY and then click the Play button. Make sure you adjust the encryption speed so that you can observe the encryption in progress. Notice how the plaintext is combined with the encryption key and how the key is repeated. Click the picture below for an example. Notice how he left/vertical column repeats the key MY_SECRET_KEY.

   Animated Example

4. **Copy the resulting ciphertext in the area below as this will be your answer:**

   KDXVGRFMEO_OWIQOXIKHYQVA_QB_KSFMEOBBTZCMSHYZNVGMIFXHA_FDEKZLOV

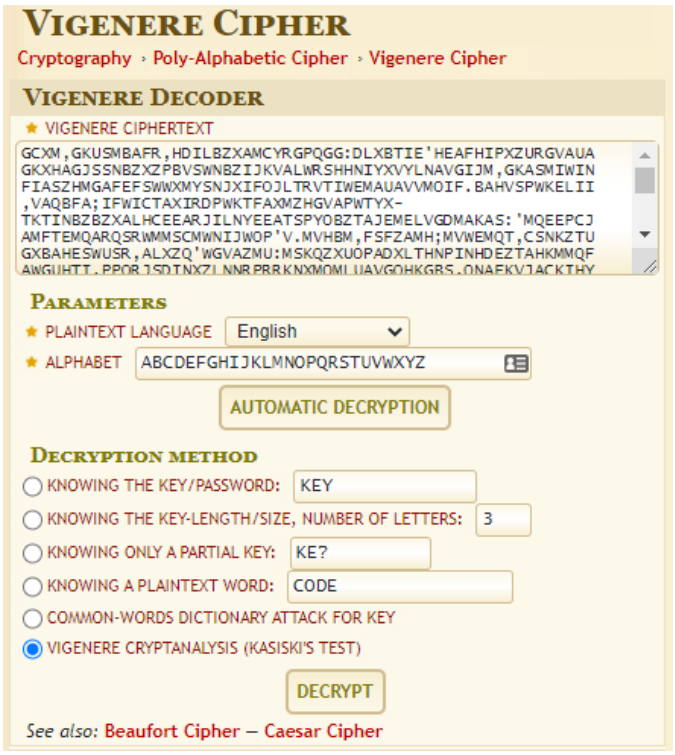
Lab 3 – Breaking the Vigenere Cipher

Ciphertext to Break:

GCXM,GKUSMBAFR,HDILBZXAMCYRGPQGG:DLXBTIE'HEAFHIPXZURGVAUAGKXHAGJSSNBZXZPBVSW
NBZIJKVALWRSHHNIYXVYLNAVGIJM,GKASMIWINFIASZHMGAFEFSWWXMYSNJXIFOJLTRVTIWEMAUA
VVMOIF.BAHVSPWKELII,VAQBFA;IFWICTAXIRDPWKTFAXMZHGVAPWTYX-
TKTINBZBZXALHCEEARJILNYEEATSPYOBZTAJEMELVGDMAKAS:'MQEEPCJAMFTEMQARQSRWMMSC
MWNIJWOP'V.MVHBM,FSFZAMH;MVWEMQT,CSNKZTUGXBAHESWUSR,ALXZQ'WGVAZMU:MSKQZX
UOPADXLTHNPINHDEZTAHKMMQFAWGUHTI,PPQRJSDINXZLNNRPRRKNXMOMLUAVGOHKGBS,QNA
FKVJACKIHYLMFLRFA'ALALVXABIPHPPSMTEDMEGNZWUAMFSYAAPBBCTAYL.JHZILBKKCDWIITZFLRK
DQHLHRWAOSEBOWXMPQX,BT'SCDNMKLVV'LEDSAU,PPWIYSNLYEA'GYWFMBQXTK,XUSLIFZZSYLU
WCFEH'VEVZX,BTIYOS'AVXSER,BTIVBOWDXUGXWRSSTEKW,TUHMPQWCINVKMOEMXMXVSJBEXYM
MWRXU'IJEGKALRBMORG,SPWGOIAQYWRZBUAZOXAQEUHWABMLTEDMIMGVWJSKLFHLWMAKDW
OHBPWNMVQSHATXHV,MWSVHBPIFWZAXIFYARAZSPLEKGXMSS,XCLMOEMBTIQFAIVHMWHUQXU
WJOSYAIKLQEGV,PPWNUHBAOSISNM'VVVYGBDC,SFKUOAVWXJAYEBJWLKHZXTXIEFABMKUW,ICLDY
SOBZXDMET,MRQAWSWLBWKIFLRFXMSKALHAQMYZOEWAHZXBTEATHGLHVXAMDWGVWBOXRRH
EZSGCBBZNZGHVEGVSJKWWVILUMORQKESKKWHNGWNZH,IFWALNAFLRBWBAOLLNMAJESOWDNA
MHVUWFWYSDBLHH'MDAVHDBZXWEEMOEFHKNLAVYZPF,EARAVLXYTKQEIFCBOJXHXIQFGUOJLEHTI
GBIMGVPPALYIZIDHGVAQJVBVKMZXFHQZFTDVRIZHYCOMLALRTUQSSOYBAHU.

1. The first step in breaking the Vigenere cipher is to find the key length. This can be done by taking every I'th letter starting at the number 2 and checking to see if the distribution is uniform (each number appears at the same relatively frequency) or if the distribution matches the languages distribution of letters shifted by some amount (shifted e's, t's, a's, o's match the English language). If use a key that is four letter long, we would expect every fourth character to be shifted by the same amount and therefore the distribution of letters should resemble the distribution of letters in the English language. We can automate this process here: https://www.dcode.fr/vigenere-cipher. Make sure you change the language to English in the upper right-hand corner of the page.

2. Copy the Ciphertext to Break into the Vigenere Ciphertext box and then select VIGENERE CRYPTANALYSIS (KSISKI'S TEST) then click DECRYPT. You will see the most likely key sizes listed from most likely to least likely displayed in the left-hand column of the page.



Record the five most likely key lengths here:

6 letters

4 letters

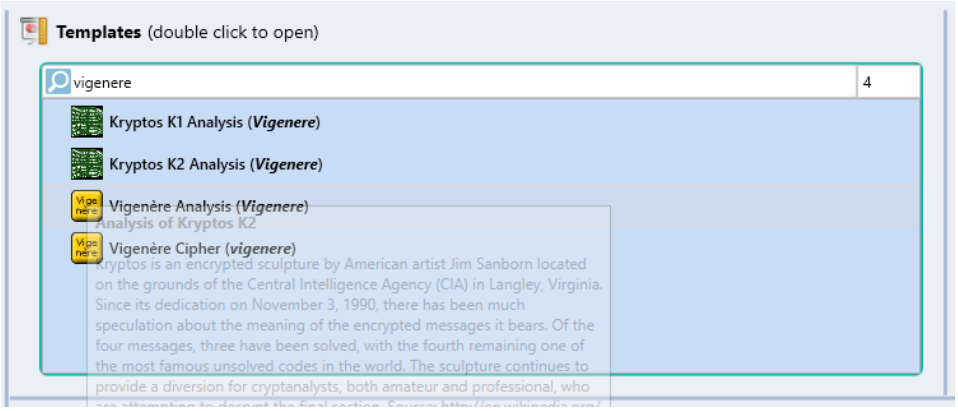
3 letters

5 letters

8 letters

3. Next, we will use Cryptool 2 to determine the shift of each character of the key and decrypt the text. This can be done by either brute force or frequency analyses of every i`th character for the length of the key. For example, if the key is four, we will look at every fourth character and see if it matches the frequency of the English language. Launch Cryptool 2.

4. Make sure you are on the tab labeled Startcenter. In the center of this screen you will see a section labeled Templates with a search box underneath. Type Vigenere in the search box and then select Vigenere Analysis (Vigenere).



5. Copy the Ciphertext to Break into the Text Input Component (Note: when using the Cybersecurity Desktop in the VMWare Horizon client, you can copy text from your computer into the remote Cybersecurity Desktop). In the Vigenere Analyzer, click on the settings gear in the upper right-hand Vigenere Analyzer component and set the Lower Bound of Keylength and Upper Bound of Keylength to the length of the first of your five possible keylengths. For example, if my first possible keylength is 7, the settings will appear as follows:

6. Click the Play button and see if the Text Output has intelligible text. If not change the Lower Bound of Keylength and Upper Boudn of Keylength to your next potential keylength and run the Vigenere Analyzer again. Check for intelligible text in the Text Output Box. Do this until you recognize English characters in the Text Output.

Paste the decrypted text here (Note: there will be no spaces in the decrypted text):

TOBEORNOTTOBETHATISTHEQUESTIONWHETHERTISNOBLERINTHEMINDTOSUFFERTHESLINGSAANDARROWSOFOUTRAGEOUSFORTUNEORTOTAKEARMSAGAINSTASEAOFTROUBLESANDBYOPPOSINGENDTHEMTODIETOSLEEPNOMOREANDBYASLEEPTOSAYWEENDTHEHEARTACHEANDTHETH

OUSANDNATURALSHOCKSTHATFLESHISHEIRTOTISACONSUMMATIONDEVOUTLYTOBEWISHDTO
DIETOSLEEPTOSLEEPPERCHANCETODREAMAYTHERESTHERUBFORINTHATSLEEPOFDEATHWHAT
DREAMSMAYCOMEWHENWEHAVESHUFFLEDOFFTHISMORTALCOILMUSTGIVEUSPAUSETHEREST
HERESPECTTHATMAKESCALAMITYOFSOLONGLIFEFORWHOWOULDBEARTHEWHIPSANDSCORNS
OFTIMETHOPPRESSORSWRONGTHEPROUDMANSCONTUMELYTHEPANGSOFDISPRIZDLOVETHEL
AWSDELAYTHEINSOLENCEOFOFFICEANDTHESPURNSTHATPATIENTMERITOFTHUNWORTHYTAKE
SWHENHEHIMSELFMIGHTHISQUIETUSMAKEWITHABAREBODKINWHOWOULDFARDELSBEARTOG
RUNTANDSWEATUNDERAWEARYLIFEBUTTHATTHEDREADOFSOMETHINGAFTERDEATHTHEUNDIS
COVEREDCOUNTRYFROMWHOSEBOURNNOTRAVELLERRETURNSPUZZLESTHEWILLANDMAKESUS
RATHERBEARTHOSEILLSWEHAVETHANFLYTOOTHERSTHATWEKNOWNOTOFTHUSCONSCIENCED
OESMAKECOWARDSOFUSALLANDTHUSTHENATIVEHUEOFRESOLUTIONISSICKLIEDOERWITHTHEP
ALECASTOFTHOUGHTANDENTERPRISESOFGREATPITCHANDMOMENTWITHTHISREGARDTHEIRCU
RRENTSTURNAWRYANDLOSETHENAMEOFACTION

The plaintext message is a quote taken from which famous play?

Hamlet