

What is Gryptography?

Some Vocabulary:

- The prefix *crypto* means secure communication.
- A cipher is a code.
- To encrypt means to convert text into a code.
- To decrypt means to convert the code back into text.

Facts:

- Cryptography the science and art of writing in secret code - was first used by Egyptians to portray messages using hieroglyphs.
- Now it is used to encrypt messages for security reasons.
- Computers helped advance cryptography.

130F7	13107	13117	HH+ 13127	13137	13147	13157	13167	13177	O 13187	13197	131A7
2777 130F8	¥ 13108	13118	13128	13138	13148	13158	13168	2323 13178	13188	13198	131A8
130F9) 13109	13119	13129	O 13139	13149	13159	13169	13179	13189	U 13199	() 131A9
130FA	1310A	1311A	1312A	999 1313A	1314A	1315A	1316A	1317A	1318A	1319A) 131AA
130FB	1310B	R 1311B	1312B	1313B	1314B	1315B	1316B	1317B	1318B	1319B	131AB
130FC	1310C	7 1311C	1312C	S 1313C	1314C	315C	1316C	1317C	1318C	1319C) 131AC

History of the Caesar Cipher

- Julius Caesar, leader of Ancient Rome, first used this simple cipher to send coded messages to people in the military.
- This is most likely where the name Caesar Cipher came from.
- It was effective at the time because many people were illiterate.



How does the Caesar Cipher Work?

- Each letter of the alphabet is replaced with a letter a certain number of positions further along.
- It goes from: Plaintext → Ciphertext → Plaintext
- Each letter is shifted a certain amount to create the ciphertext.
- To encode, first change each letter into its corresponding number (a=1, b=2, c=3, etc.) and add the shift number. Then change your new number back into its corresponding letter.



Gaesar Cipher Demonstration

- The <u>Caesar Cipher Wheel</u> is used to help code and decode the letters.
- To demonstrate, let's code the word "Artemis" using a shift of three letters.
- The coded word would be "Duwhplv."
- The decoder would have to know the key shift to decode the message

Cons of the Caesar Cipher

- There are only 25 different combinations, so it is easy to break with brute force.
- Each input can only have one output, so you have limited options.
- Can easily use frequency analysis to decode a message.
- If you know a word that is frequently used, you can decode the message easily

What is Frequency Analysis?

0.14

0.12

0.1 -

0.08

0.06

0.04

0.02

0

- Frequency analysis is a way to measure how frequent or often each letter is used in any language.
- When given a string of ciphertext, one way to attempt to decipher it is by making a frequency analysis chart. After creating the chart, look for the highest and lowest bars to try to match them up with the original frequency analysis chart.

Below: Frequency Analysis chart of the English language

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

Cons of Frequency Analysis

- Frequency analysis becomes less and less accurate as the message gets shorter, because there are fewer letters.
- If the coded message uses a letter that has a low frequency, the frequency analysis of the message will be inaccurate. For example, if the message is about zebras, there will be a greater proportion of 'z's than expected.
- Use of punctuation in the message will also make it harder to decode.

- The Vigenère cipher, which first appeared in 1585 in a book by Blaise de Vigenère, is a more advanced version of the Caesar Cipher.
- It consists of a 26x26 table called the Vigenère Table with headings A-Z on
- the top and side.
- The rows and columns shift one letter at a time.
- You must have a plaintext and a keyword.

	8 - 3 	A	в	С	D	Ε	F	G	Η	T	J	к	L	М	Ν	0	Ρ	Q	R	S	Т	U	۷	W	Х	Y	Ζ
	Α	A	В	С	D	Е	F	G	Н	1	J	K	L	М	Ν	0	Ρ	Q	R	S	Т	U	۷	W	Х	Y	Ζ
8	в	В	С	D	Е	F	G	Н	1	J	Κ	L	М	Ν	0	Ρ	Q	R	S	Т	U	۷	W	Х	Y	Ζ	Α
	0	С	D	Е	F	G	Η	-	L	Κ	Г	Μ	Ν	0	Ρ	Q	R	S	Т	С	<	W	Х	Y	Ζ	Α	В
	D	D	Ε	F	G	Η	1	L	х	L	М	Ν	0	Ρ	Ø	R	S	Т	U	<	M	Х	Y	Ζ	Α	В	С
	Ш	Е	F	G	Η	1	ſ	ĸ	Г	М	Ν	0	Ρ	Ø	R	S	Т	U	V	W	Х	Y	Ζ	A	В	С	D
	Т	F	G	Η	Ι	J	Κ	Г	Μ	Ν	0	Р	Ø	R	S	Т	U	۷	W	Х	Y	Ζ	Α	В	С	D	Е
4	G	G	Н	-	J	K	L	Μ	Ζ	0	Ρ	Ø	R	S	Т	U	٧	W	Х	Υ	Ζ	Α	В	C	D	Е	F
8	Η	Н	1	L	Κ	L	Μ	Ν	0	Ρ	Ø	R	S	Т	U	۷	W	Х	Y	Ζ	Α	В	С	D	E	F	G
	-	1	J	ĸ	L	М	Ν	0	Ρ	Ø	R	S	Т	U	V	W	Х	Υ	Ζ	Α	В	С	D	Е	F	G	Н
	c	J	Κ	Г	М	Ν	0	Ρ	Ø	R	S	Т	U	٧	W	Х	Υ	Ζ	Α	В	0	D	Е	F	G	Η	1
	κ	К	L	Μ	Ν	0	Ρ	Ø	R	S	Т	С	V	W	Х	Y	Ζ	Α	В	С	D	E	F	G	Η	1	J
	L	L	М	Ν	0	Ρ	Q	R	S	Т	U	۷	W	Х	Υ	Ζ	Α	В	С	D	Ε	F	G	Η	1	J	Κ
	Μ	Μ	N	0	Ρ	Q	R	S	Т	U	٧	W	Х	Y	Ζ	A	В	С	D	Е	F	G	Η	1	J	K	L
1	Ν	Ν	0	Р	Ø	R	S	Н	С	Υ	W	Х	Υ	Ζ	Α	В	С	D	Е	F	O	Η	Τ	Ĺ	Κ	L	М
	0	0	Ρ	Ø	R	S	Т	С	K	W	Х	Υ	Ζ	Α	В	С	D	E	F	G	Η	I.	J	K	L	М	Ν
	Р	Ρ	Q	R	S	Т	U	<	M	Х	Y	Ζ	Α	В	С	D	E	F	G	Н	-	J	K	Г	Μ	Ν	0
	Q	Q	R	S	Т	U	٧	W	Х	Y	Ζ	Α	В	С	D	Ε	F	G	Η	1	J	Κ	L	Μ	Ν	0	Ρ
4	R	R	S	Т	U	۷	W	Х	Y	Ζ	Α	В	С	D	E	F	G	Η	-	J	K	L	М	Ν	0	Ρ	Q
7	S	S	Т	U	٧	W	X	Y	Ζ	Α	В	С	D	E	F	G	Η	-	J	K	L	М	Ν	0	Ρ	Q	R
	Т	Т	U	۷	W	Х	Y	Ζ	Α	В	С	D	E	F	G	Η	1	J	К	L	М	Ν	0	Ρ	Q	R	S
	U	J	٧	W	Х	Y	Ζ	Α	В	С	D	Е	F	G	Η	1	J	K	L	М	Ν	0	Ρ	Q	R	S	Τ
	۷	۷	W	Х	Y	Ζ	Α	В	С	D	Е	F	G	Η	-	J	K	L	Μ	Ν	0	Ρ	Q	R	S	Т	U
	W	W	Х	Y	Ζ	A	В	С	D	Е	F	G	Η		J	K	L	М	Ν	0	Ρ	Q	R	S	Т	U	D
7	X	Х	Y	Ζ	A	В	С	D	Е	F	G	Η	1	J	Κ	L	М	Ν	0	Ρ	Q	R	S	Т	U	۷	С
	Y	Y	Ζ	Α	В	С	D	Е	F	G	Η	1	J	K	L	М	Ν	0	Ρ	Q	R	S	Т	U	V	W	В
	Ζ	Ζ	Α	В	С	D	Е	F	G	Н	1	J	K	L	М	Ν	0	Ρ	Q	R	S	Т	U	V	W	Х	Y

Encryption using the Vigenère Cipher

- Line up your plaintext and your keyword, repeating the keyword as many times as needed.
- In the table, find the cross-section of each set of letters to create your ciphertext.
- Example:

Plaintext: ARTEMIS PROJECT Keyword: CODECOD ECODECO

Encoded Message:

CFWIOWV TTCMIEH

	2 2	A	в	5	D	E	F	G	Н	L.	L	κ	L	М	Ν	0	Ρ	Q	R	S	L	U	۷	W	Х	Υ	Ζ	
	Α	Α	E	С	D	Е	F	G	Н	1	J	K	L	М	Ν	0	Ρ	Q	R	S	Т	U	٧	W	Х	Y	Ζ	
	в	В	С	Ģ	Е	F	G	Н	1	J	Κ	L	М	Ν	0	Ρ	Q	R	S	Т	U	٧	W	Х	Y	Ζ	Α	
	С	С	D	Е	F	G	H	I	J	K	L	М	Ν	0	Ρ	Q	R	S	Т	U	٧	W	Х	Y	Ζ	Α	В	
	D	D	E	F	G	Η	1	J	K	L	М	Ν	0	Ρ	Q	R	S	Т	U	٧	W	Х	Υ	Ζ	Α	В	С	
	Ε	Е	F	G	Н	1	J	K	L	М	Ν	0	Ρ	Q	R	S	Т	U	٧	W	Х	Y	Ζ	Α	В	С	D	
	F	F	G	Н	Ι	J	Κ	L	Μ	Ν	0	Ρ	Q	R	S	Т	U	٧	W	Х	Y	Ζ	Α	В	С	D	Е	
	G	G	Н	1	J	K	L	М	N	0	Ρ	Q	R	S	Т	U	٧	W	Х	Y	Ζ	Α	В	С	D	Е	F	
	Η	Н	T	J	K	L	М	Ν	0	Ρ	Q	R	S	Т	U	۷	W	Х	Y	Ζ	Α	В	С	D	Е	F	G	
	1	1	J	K	L	М	Ν	0	Ρ	Q	R	S	Т	U	٧	W	Х	Υ	Ζ	Α	В	С	D	Е	F	G	Н	-
	c	J	K	L	М	Ν	0	Ρ	Ø	R	S	Т	U	۷	W	Х	Υ	Ζ	А	В	С	D	Е	F	G	Η	1	
	κ	К	L	М	Ν	0	Ρ	Q	R	S	Т	U	٧	W	Х	Y	Ζ	Α	В	С	D	E	F	G	Η	1	J	
	L	L	М	Ν	0	Ρ	Q	R	S	Т	U	۷	W	Х	Υ	Ζ	Α	В	С	D	Е	F	G	Η	1	J	Κ	
	Ν	М	N	0	Ρ	Q	R	S	Т	U	٧	W	Х	Y	Ζ	A	В	С	D	E	F	G	Η	1	ſ	Κ	L	
	Ν	Ν	0	Ρ	Q	R	S	Т	С	٧	W	Х	Y	Ζ	Α	В	С	D	E	F	G	Η	Ι	J	Κ	L	М	
~	0	0	Ρ	Q	R	S	Т	U	V	W	Х	Y	Ζ	Α	В	С	D	Е	F	G	Н	I.	J	K	L	М	Ν	
\neg	Ρ	Ρ	Q	R	S	Т	J	۷	W	Х	Y	Ζ	Α	В	С	D	E	F	G	Н	1	J	Κ	L	Μ	Ν	0	
	Q	Q	R	S	Т	T.	V	W	Х	Y	Ζ	Α	В	С	D	E	F	G	Η	1	J	Κ	L	Μ	N	0	Ρ	
	R	R	S	Т	U	۷	W	Х	Y	Ζ	Α	В	С	D	Е	F	G	Η	1	J	K	L	М	Ν	0	Ρ	Q	
	S	S	Т	U	۷	W	Х	Y	Ζ	Α	В	С	D	E	F	G	Η	I.	J	K	L	М	Ν	0	Ρ	Q	R	
	Т	Т	U	۷	W	Х	Y	Ζ	Α	В	С	D	E	F	G	Η	1	J	Κ	L	М	Ν	0	Ρ	Q	R	S	
	U	U	V	W	Х	Y	Ζ	Α	В	С	D	E	F	G	Η	1	J	Κ	L	М	N	0	Ρ	Q	R	S	Т	
	۷	۷	W	Х	Y	Ζ	Α	В	С	D	Ε	F	G	Η		J	K	L	М	Ν	0	Ρ	Q	R	S	Т	U	
	W	W	Х	Υ	Ζ	Α	В	С	D	Е	F	G	Η	-E	J	K	L	М	Ν	0	Ρ	Q	R	S	Т	U	D	
	Х	Х	Y	Ζ	Α	В	С	D	Е	F	G	Η	1	J	Κ	L	Μ	Ν	0	Ρ	Q	R	S	Т	U	۷	С	
	Y	Y	Ζ	Α	В	С	D	E	F	G	Η	1	J	K	L	М	Ν	0	Ρ	Q	R	S	Т	U	V	W	В	
	Ζ	Ζ	A	В	С	D	Е	F	G	Н	1	J	K	L	Μ	Ν	0	Ρ	Q	R	S	Т	U	۷	W	Х	Y	

Decryption using the Vigenère Cipher

- It is necessary to know the keyword to decode a message written using the Vigenère Cipher.
- Line up the keyword with the ciphertext and go across or down to find the plaintext, for example:
 Ciphertext: CFWIOWV TTCMIEH Key: CDDECOD ECODECO
- Because each letter has its own shift, there are many more combinations, making it much more secure than the original Caesar Cipher.

	_	_		$\mathbf{\nabla}$			_	_		_	_	-																	
		Α	в	С	D	Е	F	G	Η	T	J	Κ	L	Μ	Ν	0	P	Q	R	S	Τ	U	۷	W	X	Y	z		
(Α	А	В	С	D	Е	F	G	Н	1	J	K	L	М	Ν	0	Ρ	Q	R	S	Т	U	٧	W	Х	Y	Ζ		
	4	В	С	D	^ ٦	F	G	Н	1	J	Κ	L	М	Ν	0	Ρ	Q	R	S	Т	U	۷	W	Х	Y	Ζ	Α		
	С	С	D	Е	F	$\overline{\mathbf{N}}$	H	Ι	J	K	L	Μ	Ν	0	Ρ	Q	R	S	Т	U	۷	W	Х	Y	Ζ	Α	В		
	D	D	Е	F	G	H	1	J	Κ	L	М	Ν	0	Ρ	Q	R	S	Т	U	٧	W	Х	Υ	Ζ	Α	В	С		
	Ε	Е	F	G	Η	1	J	K	L	Μ	Ν	0	Ρ	Q	R	S	Т	U	۷	W	Х	Y	Ζ	Α	В	С	D		
	F	F	G	Η	Ι	J	Κ	L	М	Ν	0	Ρ	Q	R	S	Т	U	۷	W	Х	Y	Ζ	Α	В	С	D	Е		
	G	G	Н	1	J	K	L	М	N	0	Ρ	Q	R	S	Т	U	٧	W	Х	Υ	Ζ	Α	В	С	D	Е	F		
	Η	Н	1	J	К	L	М	Ν	0	Ρ	Q	R	S	Т	U	۷	W	Х	Y	Ζ	Α	В	С	D	E	F	G		
	-	1	J	K	L	Μ	Ν	0	Ρ	Q	R	S	Т	U	٧	W	Х	Υ	Ζ	Α	В	С	D	Е	F	G	Н		
	c	J	Κ	L	М	Ν	0	Ρ	Ø	R	S	Т	U	۷	W	Х	Υ	Ζ	Α	В	С	D	Е	F	G	Н	1		
	κ	К	L	М	Ν	0	Ρ	Q	R	S	Т	U	V	W	Х	Y	Ζ	Α	В	С	D	Е	F	G	Η	1	J		
	L	L	М	Ν	0	Ρ	Q	R	S	Т	U	۷	W	Х	Υ	Ζ	Α	В	С	D	Е	F	G	Н	1	J	Κ		
	Μ	М	Ν	0	Ρ	Q	R	S	Т	U	٧	W	Х	Y	Ζ	Α	В	С	D	Е	F	G	Η	1	J	Κ	L		
	Ν	Ν	0	Ρ	Q	R	S	Т	U	۷	W	Х	Y	Ζ	Α	В	С	D	Е	F	G	Н	Ι	J	Κ	L	М		
	0	0	Ρ	Q	R	S	Т	U	٧	W	Х	Y	Ζ	Α	В	С	D	Е	F	G	Н	L	J	K	L	М	Ν		
	Ρ	Ρ	Q	R	S	Т	U	V	W	Х	Υ	Ζ	Α	В	С	D	Е	F	G	Н	1	J	Κ	L	Μ	Ν	0		
	ų	Q	R	S	Т	U		Å	Х	Y	Ζ	Α	В	С	D	E	F	G	Η	1	ſ	K	L	Μ	Ν	0	Ρ		
	R	R	S	Т	U	۷	W		Y	Ζ	Α	В	С	D	Е	F	G	Н	1	J	K	L	Μ	Ν	0	Ρ	Q		
	S	S	Т	U	۷	W	Х	Y	Ζ	Α	В	С	D	Е	F	G	Η	-	J	Κ	Г	М	Ν	0	Ρ	Q	R		
	T	Т	U	٧	W	Х	Υ	Ζ	Α	В	С	D	E	F	G	Η	1	J	К	L	М	Ν	0	Ρ	Q	R	S		
	C	U	V	W	Х	Y	Ζ	Α	В	С	D	E	F	G	Η	1	J	Κ	L	М	Ν	0	Ρ	Ø	R	S	Т		
	<	۷	W	Х	Y	Ζ	Α	В	0	D	Е	F	G	Η	Ι	J	Κ	L	Μ	Ν	0	Ρ	Ø	R	S	Т	U		
	W	W	Х	Y	Ζ	Α	В	С	D	Е	F	G	Η	-E	J	K	L	Μ	Ν	0	Ρ	Q	R	S	Т	U	D		
	Х	Х	Y	Ζ	A	В	С	D	E	F	G	Η	1	J	Κ	L	Μ	Ν	0	Ρ	Q	R	S	Т	U	V	С		
	Y	Y	Ζ	Α	В	С	D	E	F	G	Η	1	J	K	L	М	Ν	0	Ρ	Q	R	S	Т	U	V	W	В		
	Ζ	Ζ	A	В	С	D	Е	F	G	Н	1	J	K	L	М	Ν	0	Ρ	Q	R	S	Т	U	٧	W	Х	Y		

Gryptography Today

- Modern algorithms for cryptography are too complex for humans to complete by hand. Now, computers or specialized hardware devices carry out the algorithms.
- It ensures security in everyday things that people do, including cybersecurity, credit card information, and passwords.
 - Cryptography is essential to protect personal information from hackers.
 - There are many ways to encrypt your information using cryptography and make sure it is safe.
- Cryptography is constantly expanding and becoming more complex. In the future, cryptography could be even more advanced and useful.



Websites:

Practical Cryptography - Caesar Cipher Cryptography Presentation (by the Coordinators) Crypto Corner - Frequency Analysis MTU - The Vigenère Cipher Encryption and Decryption MTU - The Vigenère Cipher: Introduction Caesar Cipher Wheel Online Caesar Cipher Wheel Vigenère Encoder and Decoder

<u>Some of our Images:</u> <u>Frequency Analysis</u> <u>Person Thinking</u> <u>Vigenère Table</u>