Introductory Codebusters - Vigenere

3/7/21

Looking Ahead

(6) Baconian

Pollux & Morbit - Rail Fence

Patristocrat - Xenocrypt

Review (11)

Getting fast at letter-number conversions is essential

https://quizlet.com/393552971/codebusters-letters-to-numbers-flash-cards/

Put this Quizlet I made on Write mode or however you learn best

- Eventually, conversions will be effortless and take less than a second

Vigenere Basics

Pretty sure we know how to add and subtract

For Vig, we have two main skills to exercise:

- Letter-number conversions
- Modular arithmetic

Modular Arithmetic

Taking x mod y (same thing as x modulo y) means: **when you divide x by y, what is the remainder?**

- Ex: 5 mod 4 = 1, 10 mod 5 = 0, 42 mod 12 = 6
- Whenever we're doing math in Codebusters, we are taking the number in question **modulo 26** because there are 26 letters in the alphabet
    - Don't get this confused with letter-number conversions! A still equals 0, just as Z still equals 25.

Vigenere Encryption Intro

When you **encrypt**, you will be given **two parameters** in the question: the ciphertext and the **keyword**..

- Example question prompt: **Encode “HELLO” with a Vigenere cipher using keyword “LOCA”.**

Encryption is literally just addition!

- Convert letters to numbers, add, repeat.

Vigenere Encryption Continued

Saying we're encoding "HELLO" with keyword "LOCA".

- Write HELLO and LOCA next to each other vertically, repeating the keyword as much as you need to
- Convert "HELLO" to numbers: "7,4,11,11,14"
- Convert "LOCA" to numbers: "11, 14, 2, 0"
- Add!
- Apply modular arithmetic if necessary

Vigenere Encryption Example

19) **[200 points]** Encode this sentence with the Vigenere cipher using the keyword compiler.

W	H	A	T	M	A	K	E

S	T	H	E	D	E	S	E

R	T	B	E	A	U	T	I

F	U	L	I	S	T	H	A

T	S	O	M	E	W	H	E

R	E	I	T	H	I	D	E

S	A	W	E	L	L

Try another!

7) **[200 points]** Encode James G. Watt's strong opinion on journalism using the Vigenere cipher (key ARBOL)

T	H	E	Y	K

I	L	L	G	O

O	D	T	R	E

E	S	T	O	P

U	T	O	U	T

B	A	D	N	E

W	S	P	A	P

E	R	S

Vigenere Decryption Intro

Instead of adding, subtract!

- Apply modular arithmetic when necessary
  - Remember, always mod 26
- Letter-number conversions are still a thing

Vigenere Decryption Example

18) **[175 points]** Decode this sentence with the Vigenere cipher using the keyword digital.

E	M	R	M	L	S	N

X	Z	O	W	N	S	L

E	W	A	B	I	E	Z

S	T	K	I	G	D	X

R	Z	K	K	N	R	T

R	C	Y	I	U	O	F

W	Q	J	M	T	S

Again!

18) **[175 points]** Decode this sentence with the Vigenere cipher using the keyword beings.

J	I	V	W	U	Q

X	E	T	X	O	F

H	Q	G	Q	U	Y

B	R	L	P	U	E

Q	P	M	G	O	F

H	G	Z	B	Y	K

X	S	Z	Q	V	M

A	D	T	R	Y

What if I’m not given a keyword?

Time to big brain

Vigenere Cryptanalysis Example

19) **[175 points]** Decode this sentence with the Vigenere cipher. The first 5 characters of the sentence is Peopl.

G	S	Q	Z	J

V	K	K	D	F

X	C	C	V	Q

J	I	E	M	C

V	R	D	O	A

R	I	U	O	R

Y	S	A	U	L

F	K	Y	R	C

I	S	V	R	C

P	F	G	Q	M

Z	B	I

Up Next

Keep practicing on Puzzle Baron's Cryptograms

I'll post a new homework json for this week on Google classroom

Keep practicing your letter-number conversions!

Baconian scheduled for next lesson if you want to take a look ahead (binary)