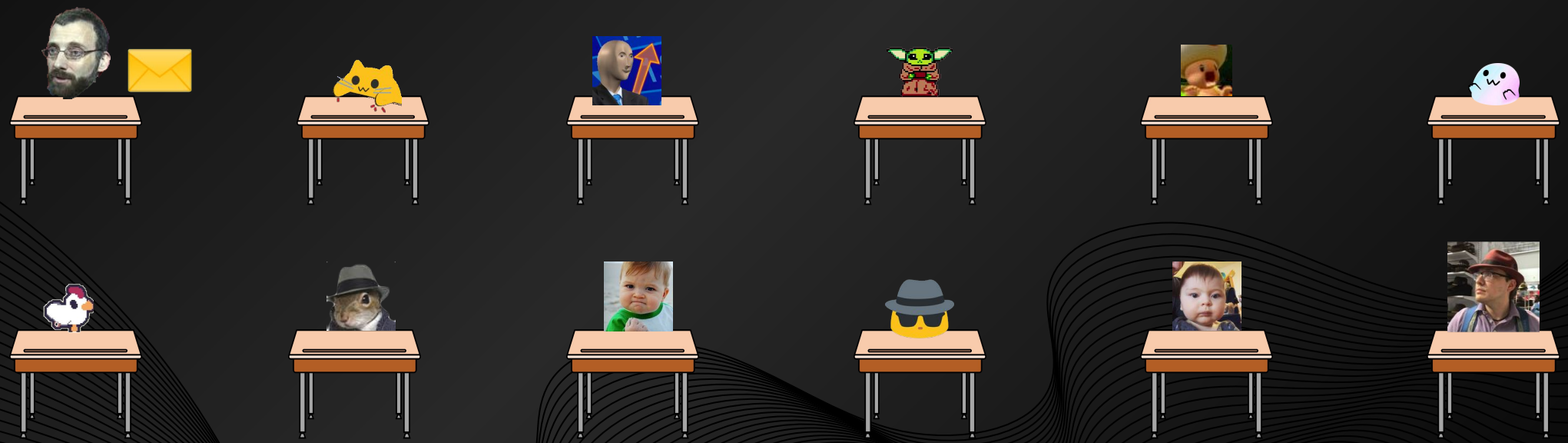
Simple Decryption Methods

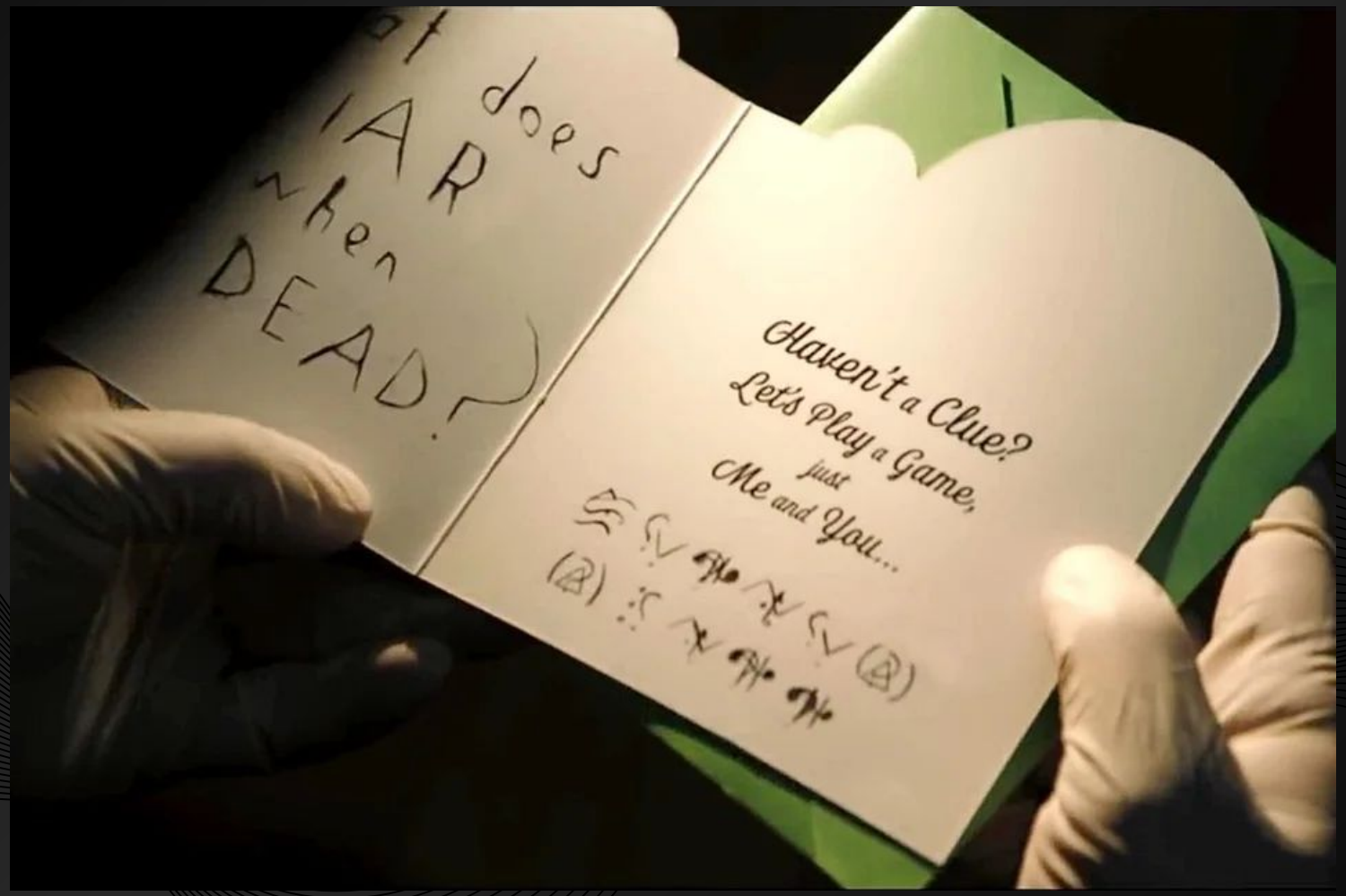
Jiyoon Kim, Eduardo Leite, Tiffany Wong

WWYD?

Mike wants to pass a super secret message to JonAlf across the room.
How can he keep the message confidential?



The Batman (2022)

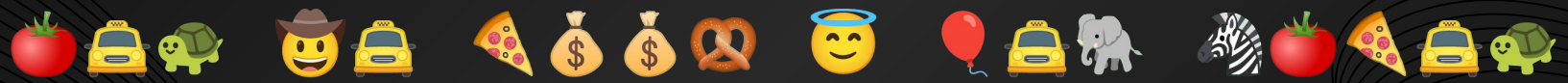


Solve the riddle ?

Student: Sorry, teacher. My dog ate my homework.

Teacher: Your dog ate your computer science homework?

Student:



KEY												
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
	💰	🏰	🏁	👍	🐢	🍕	🎲	🎅	🐘	🏆		🦐

Breakout Room Activity

~5 mins

Given the clues, try to crack the cipher!
When we regroup...

- What strategies did you use to deduce certain letters?
- Can you guess what the punchline is?

Solution

Student: Sorry, teacher. My dog ate my homework.

Teacher: Your dog ate your computer science homework?

Student:

🍅🚕🐢 🤠🚕 🍕💰💰🥨 😇 🎈🚕🐘 🦓🍅🍕🚕🐢

yes he took a few bytes

KEY												
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
🚀	💰	🏰	🏁	👍	🐢	🍕	🎲	🎅	🐘	🏆	🍅	🦐

Substitution Cipher

In a Substitution cipher, any character of plain text is substituted by some other character or symbol.

Mono-Alphabetic Substitution
Text: abcdefghijklmnopqrstuvwxyz Key: fcpevqkzgmtrayonujdlwhbxsi Cipher: fcpevqkzgmtrayonujdlwhbxsi
Text: substitutioncipher Key: fcpevqkzgmtrayonujdlwhbxsi Cipher: dwcdlglwlgoypgnzvj

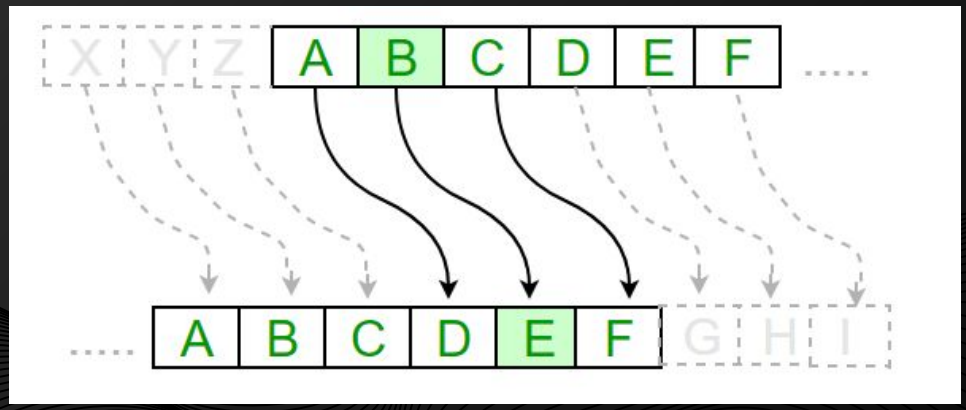
Symbols Substitution
Text: abcdefghijklmnopqrstuvwxyz Key: 12345678910!@#$%^&*()_=+-*/ Cipher: 12345678910!@#$%^&*()_=+-*/
Text: substitutioncipher Key: 12345678910!@#$%^&*()_=+-*/ Cipher: *_2*(9(_(9#@39%85&

Caesar Cipher

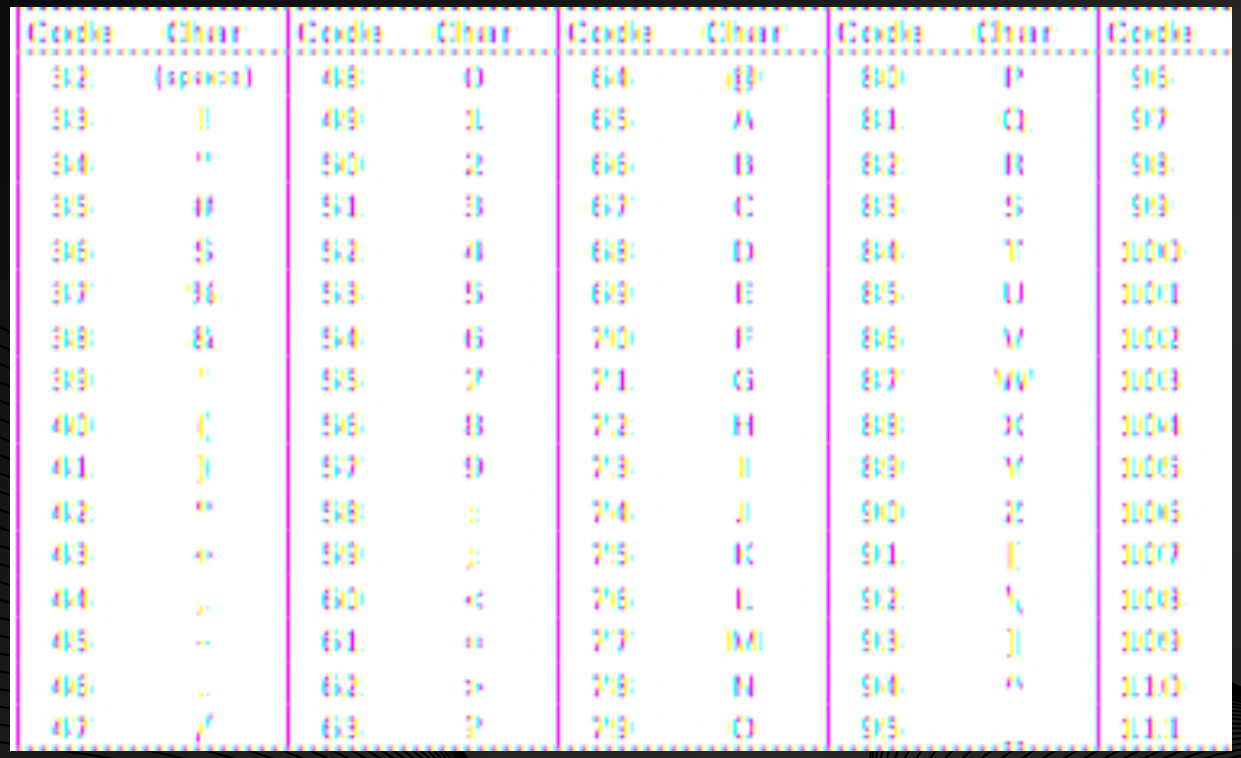
Each letter of a given text is replaced by a letter some fixed number of positions down the alphabet.

Text: ABCDEF
Shift: 4
Cipher: DEFGHI

Text: CAESARCIPHERdemo
Shift: 4
Cipher: GEIWEVGMTLIVhiqs

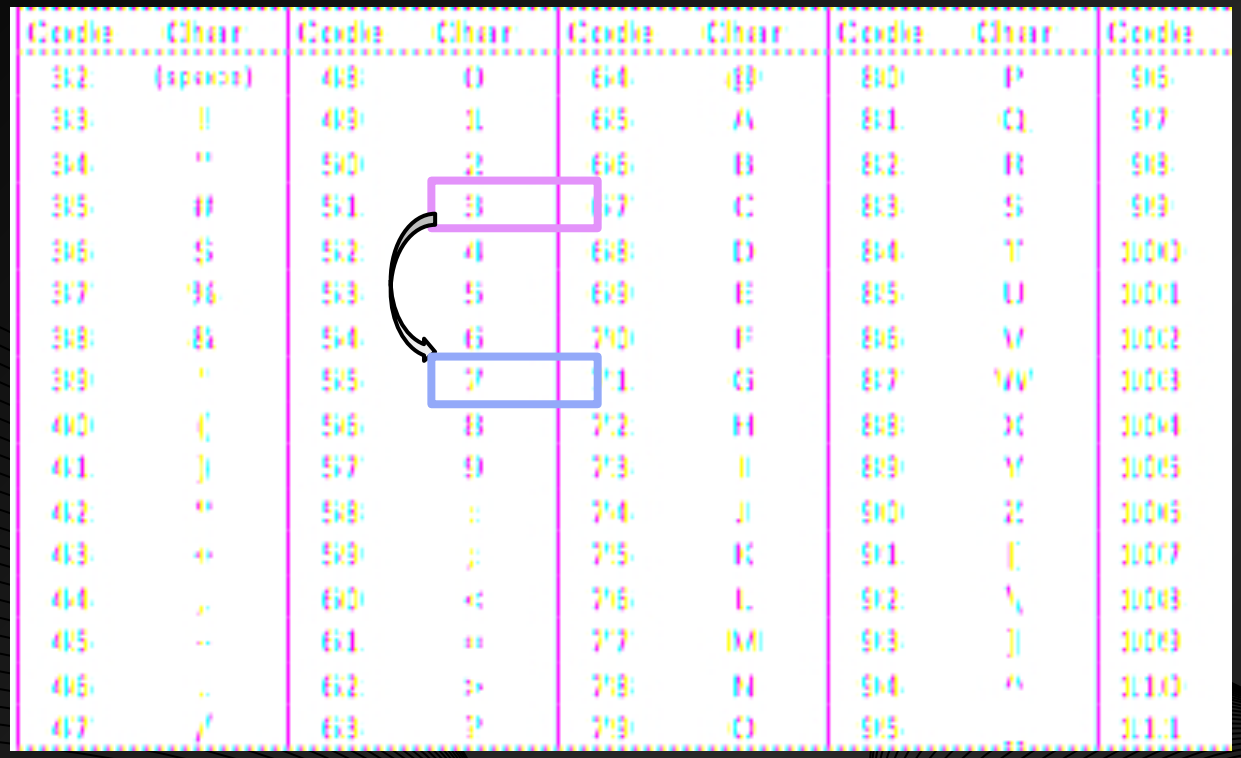


Coding the Caesar Cipher



CAESARCIPHERdemo with shift of 4

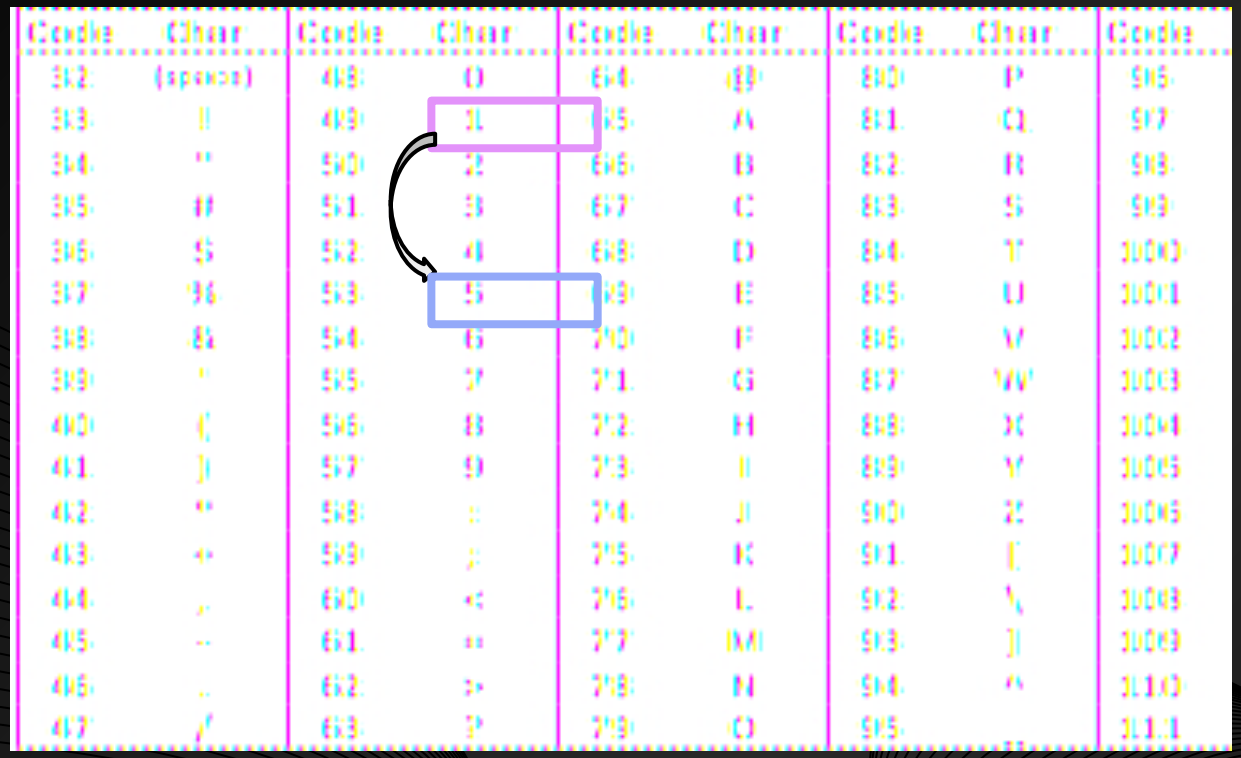
Coding the Caesar Cipher



CAESARCIPHERdemo with shift of 4

C + 4 → 67 + 4 → 71 → G

Coding the Caesar Cipher



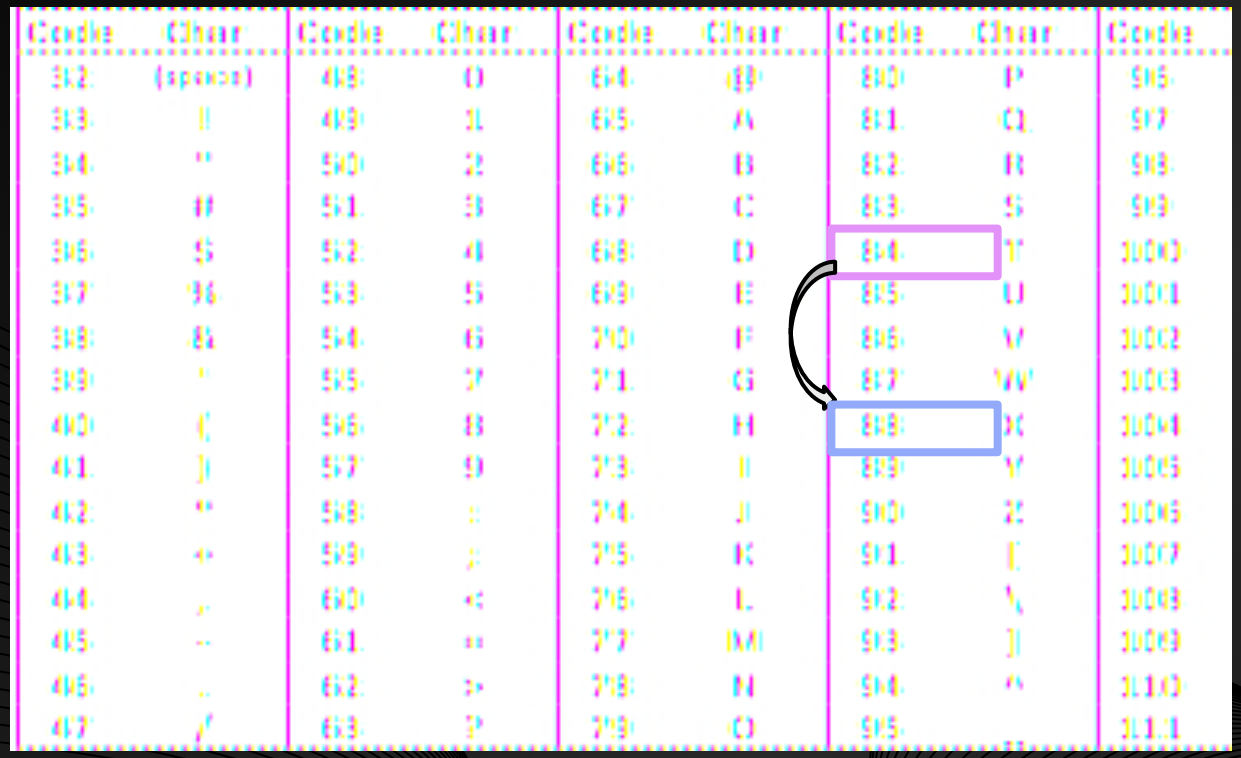
CAESARCIPHERdemo with shift of 4

C + 4 → 67 + 4 → 71 → G

A + 4 → 65 + 4 → 69 → E

...

Coding the Caesar Cipher



CAESARCIPHERdemo with shift of 4

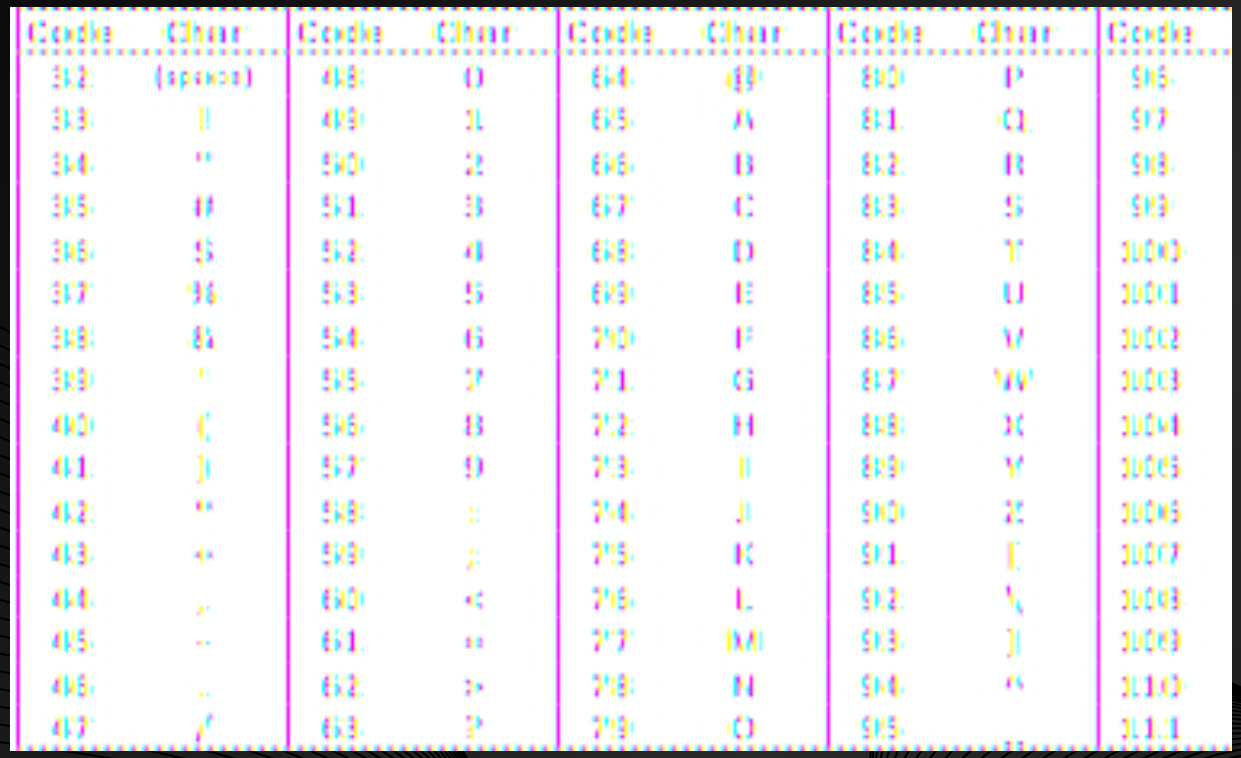
C + 4 → 67 + 4 → 71 → G

A + 4 → 65 + 4 → 69 → E

...

d + 4 → 100 + 4 → 104 → h

Coding the Caesar Cipher



CAESARCIPHERdemo with shift of 4

C + 4 → 67 + 4 → 71 → G

A + 4 → 65 + 4 → 69 → E

…

d + 4 → 100 + 4 → 104 → h

…

GEIWEVGMTLIVhiqs

Coding the Caesar Cipher

Breakout Room Activity

~5 mins

In groups...

1. **Decide:** What is capital letter “Z” shifted by 4?
2. **Discuss:**
   - What does a shift of 30 look like?
   - What does a shift of -4 look like?

If time permits:

3. **Brainstorm:** How can we code the Caesar Cipher?
   - What control structures (conditionals/loops) will we need?
   - What functions will be useful?

Let’s look at the code together when we regroup!

Vigenere Cipher

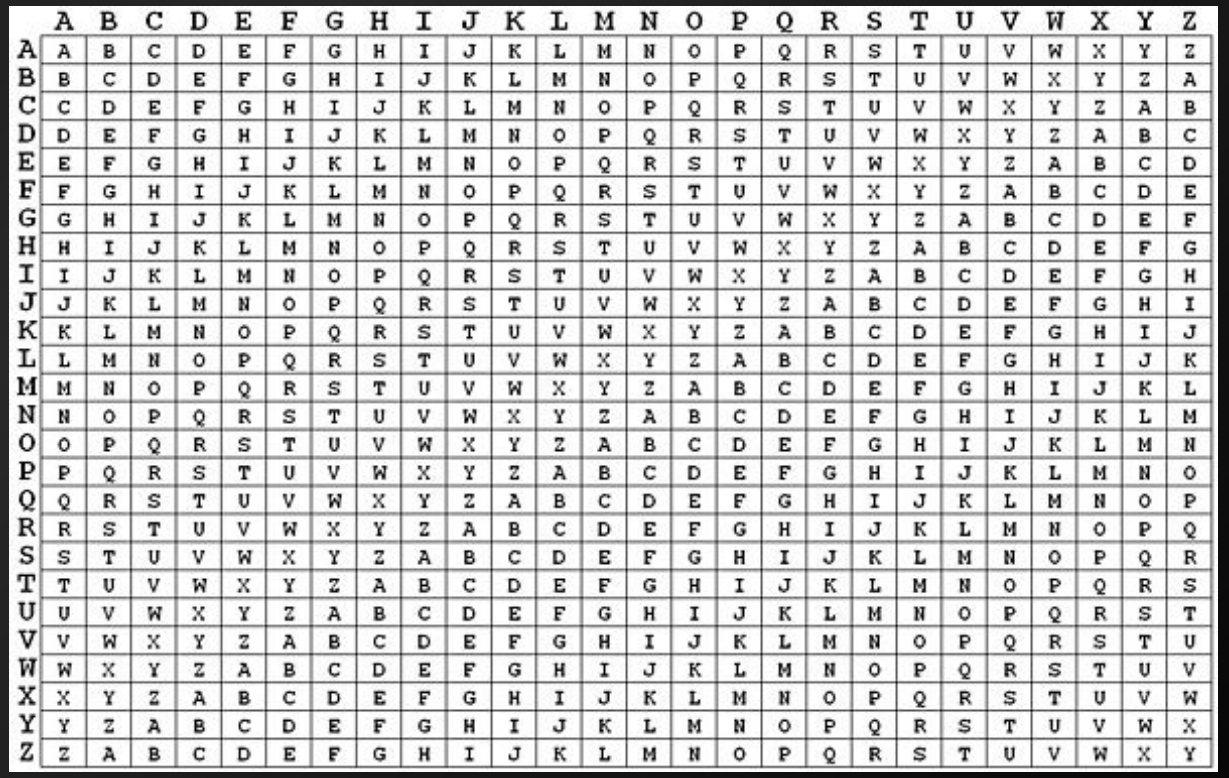
- First described in 1553 by Giovan Battista Bellaso but popularized in 1586 by Blaise de Vigenère
- Enigma Machine
  - Nazi encoding machine that also utilizes a polyalphabetic cipher
  - Uses a 3 rotors and 1 reflector
  - Famously decoded by Alan Turing during WW2

Overview

A vigenere cipher is a **polyalphabetic cipher** which is like a multiple Caesar ciphers.

- **Plaintext**: the message you wish to encode
- **Key**: a secret word/phrase that you will use to encode

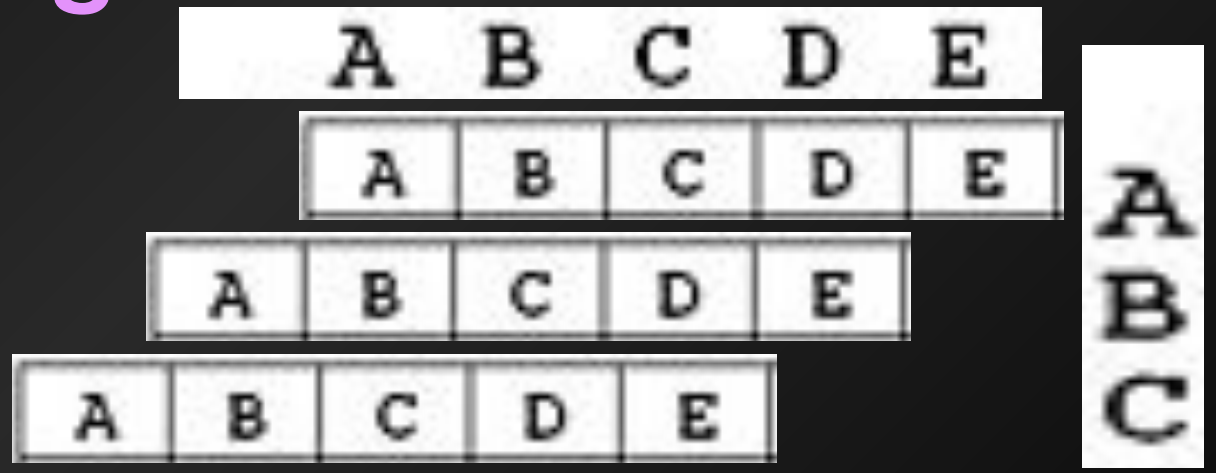
Depending on your key, the shift of the “caesar cipher” will change



	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

So how does encoding work?

Encoded letters are shifted from their original space depending on the key letter.



If your key letter is ‘A’, the encoded letter is shifted **forward 0**.

If your key letter is ‘B’ the encoded letter is shifted **forward 1**

If your key letter is ‘C’, the encoded letter is shifted **forward 2**

Example

Plain text: JED DEFIED DAD

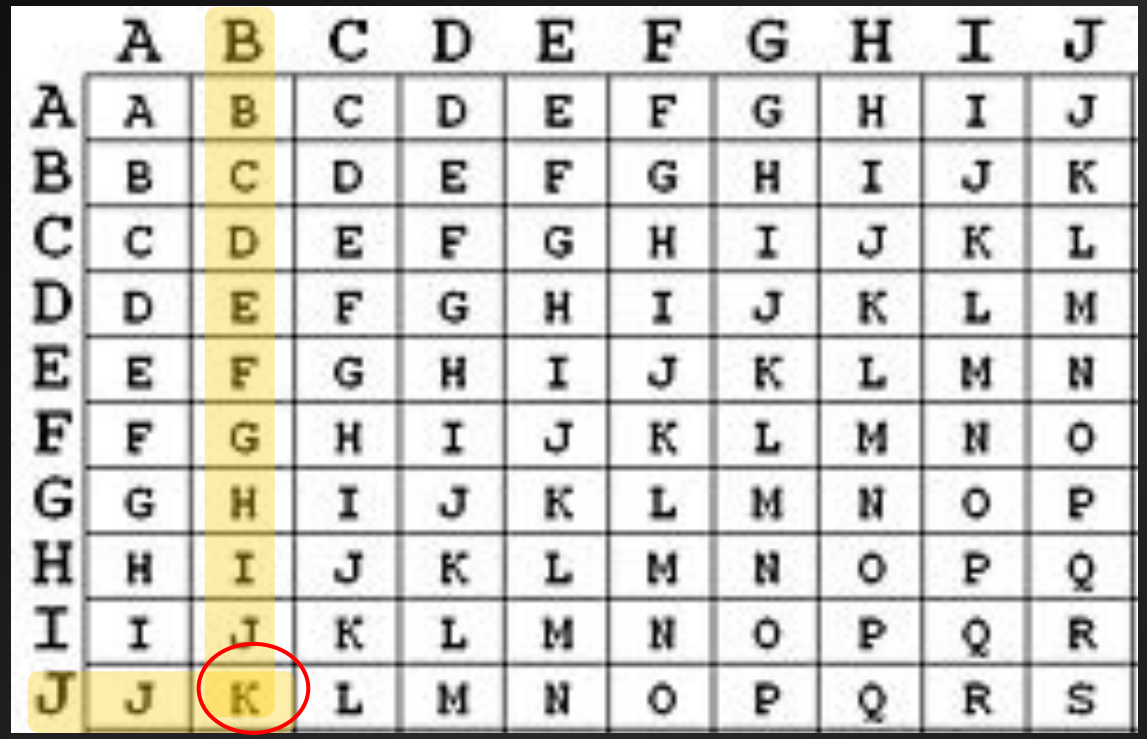
Key: BED

Plain text	J	E	D	D	E	F	I	E	D	D	A	D
Key	B	E	D	B	E	D	B	E	D	B	E	D

Key will repeat for the length of the plain text

Example

Plain text	J	E	D	D	E	F	I	E	D	D	A	D
Key	B	E	D	B	E	D	B	E	D	B	E	D
Encoded	K											



	A	B	C	D	E	F	G	H	I	J
A	A	B	C	D	E	F	G	H	I	J
B	B	C	D	E	F	G	H	I	J	K
C	C	D	E	F	G	H	I	J	K	L
D	D	E	F	G	H	I	J	K	L	M
E	E	F	G	H	I	J	K	L	M	N
F	F	G	H	I	J	K	L	M	N	O
G	G	H	I	J	K	L	M	N	O	P
H	H	I	J	K	L	M	N	O	P	Q
I	I	J	K	L	M	N	O	P	Q	R
J	J	K	L	M	N	O	P	Q	R	S

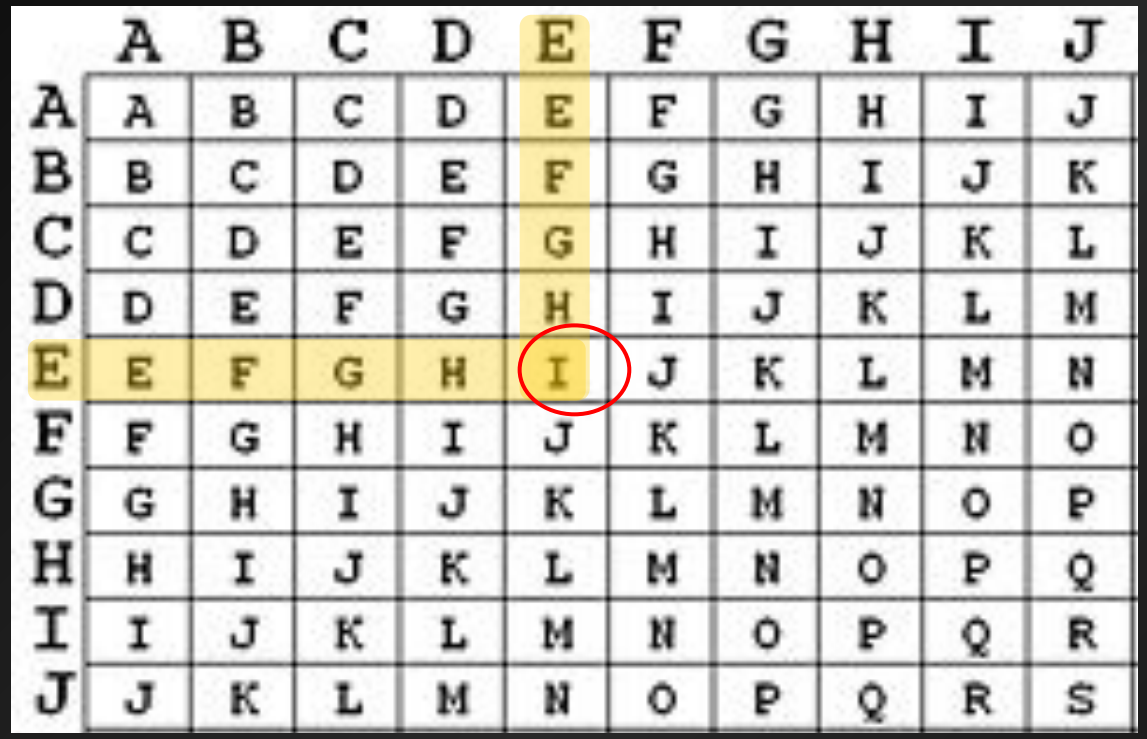
J and B are partners!

B → shift of 1
E → shift of 4
D → shift of 3

J will be encoded as the letter “B” letters ahead or 1 letter ahead

Example

Plain text	J	E	D	D	E	F	I	E	D	D	A	D
Key	B	E	D	B	E	D	B	E	D	B	E	D
Encoded	K	I										



	A	B	C	D	E	F	G	H	I	J
A	A	B	C	D	E	F	G	H	I	J
B	B	C	D	E	F	G	H	I	J	K
C	C	D	E	F	G	H	I	J	K	L
D	D	E	F	G	H	I	J	K	L	M
E	E	F	G	H	I	J	K	L	M	N
F	F	G	H	I	J	K	L	M	N	O
G	G	H	I	J	K	L	M	N	O	P
H	H	I	J	K	L	M	N	O	P	Q
I	I	J	K	L	M	N	O	P	Q	R
J	J	K	L	M	N	O	P	Q	R	S

E and E are partners!

B → shift of 1

E → shift of 4

D → shift of 3

E will be encoded as the letter “E” letters ahead or 4 letters ahead

Example

Plain text	J	E	D	D	E	F	I	E	D	D	A	D
Key	B	E	D	B	E	D	B	E	D	B	E	D
Encoded	K	I	G									

	A	B	C	D	E	F	G	H	I	J
A	A	B	C	D	E	F	G	H	I	J
B	B	C	D	E	F	G	H	I	J	K
C	C	D	E	F	G	H	I	J	K	L
D	D	E	F	G	H	I	J	K	L	M
E	E	F	G	H	I	J	K	L	M	N
F	F	G	H	I	J	K	L	M	N	O
G	G	H	I	J	K	L	M	N	O	P
H	H	I	J	K	L	M	N	O	P	Q
I	I	J	K	L	M	N	O	P	Q	R
J	J	K	L	M	N	O	P	Q	R	S

D and D are partners!

B → shift of 1

E → shift of 4

D → shift of 3

D will be encoded as the letter “D” letters ahead or 3 letters ahead

Example

Plain text	J	E	D	D	E	F	I	E	D	D	A	D
Key	B	E	D	B	E	D	B	E	D	B	E	D
Encoded	K	I	G	E								

	A	B	C	D	E	F	G	H	I	J
A	A	B	C	D	E	F	G	H	I	J
B	B	C	D	E	F	G	H	I	J	K
C	C	D	E	F	G	H	I	J	K	L
D	D	E	F	G	H	I	J	K	L	M
E	E	F	G	H	I	J	K	L	M	N
F	F	G	H	I	J	K	L	M	N	O
G	G	H	I	J	K	L	M	N	O	P
H	H	I	J	K	L	M	N	O	P	Q
I	I	J	K	L	M	N	O	P	Q	R
J	J	K	L	M	N	O	P	Q	R	S

D and B are partners!

B → shift of 1

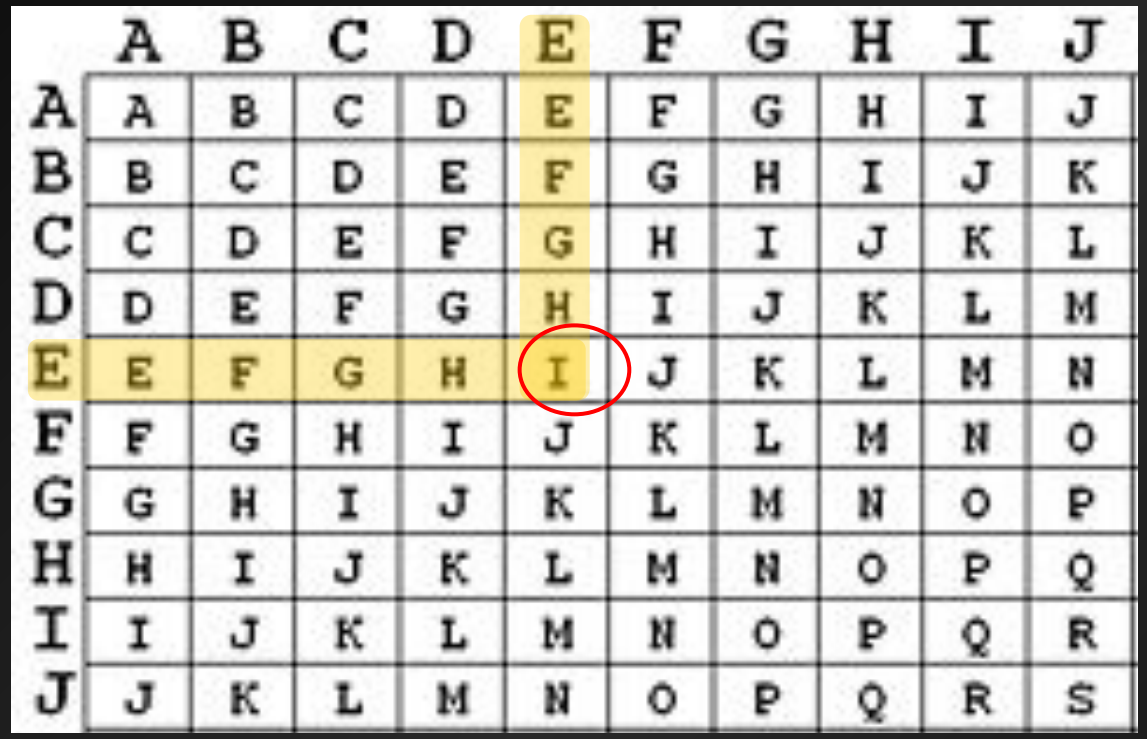
E → shift of 4

D → shift of 3

D will be encoded as the letter “B” letters ahead or 1 letter ahead

Example

Plain text	J	E	D	D	E	F	I	E	D	D	A	D
Key	B	E	D	B	E	D	B	E	D	B	E	D
Encoded	K	I	G	E	I							



	A	B	C	D	E	F	G	H	I	J
A	A	B	C	D	E	F	G	H	I	J
B	B	C	D	E	F	G	H	I	J	K
C	C	D	E	F	G	H	I	J	K	L
D	D	E	F	G	H	I	J	K	L	M
E	E	F	G	H	I	J	K	L	M	N
F	F	G	H	I	J	K	L	M	N	O
G	G	H	I	J	K	L	M	N	O	P
H	H	I	J	K	L	M	N	O	P	Q
I	I	J	K	L	M	N	O	P	Q	R
J	J	K	L	M	N	O	P	Q	R	S

E and E are partners!

B → shift of 1

E → shift of 4

D → shift of 3

E will be encoded as the letter “E” letters ahead or 4 letters ahead

Comment-along segment

Please find all code for this class in this repo:

- https://github.com/hunter-teacher-cert/work-topics-jkimbxv/tree/master/cipher/classResources

Async Work

Complete the encrypt function in the Caesar Cipher starter code from class. Add code to encrypt lowercase letters as well.

- Uppercase ‘Z’ shifted by 1 should be uppercase ‘A.’
- Lowercase ‘z’ shifted by 1 should be lowercase ‘a.’

Find starter code from class in repo on Slide 23 in bellpepper.py.

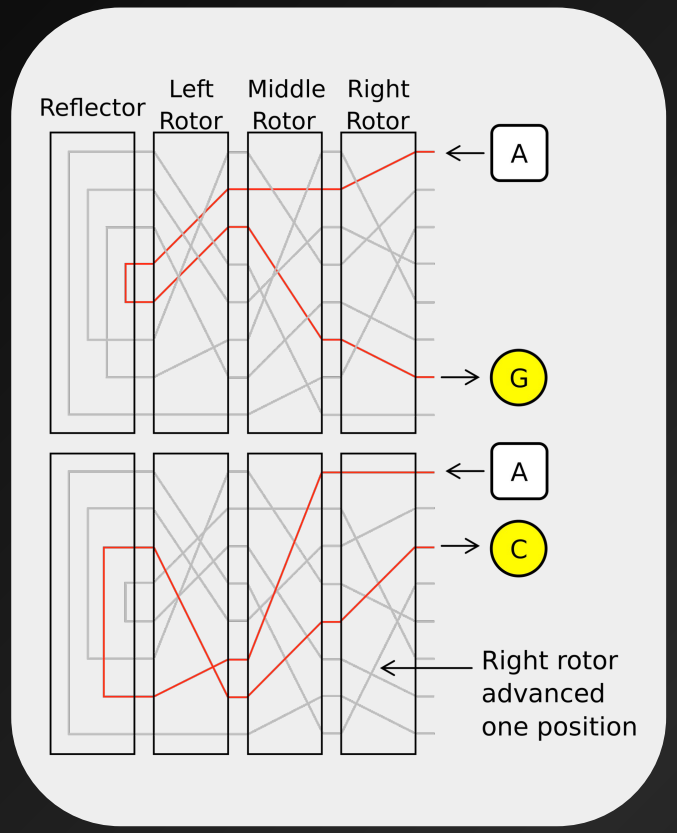
Homework

Bell Pepper (🔥)	Jalapeno (🔥🔥)	Habanero (🔥🔥🔥)
Write the decryption function of a caesar cipher from the starter code given in class	Write a decryption function for a vigenere cipher with knowing the key	The enigma machine is a rotor based encryption machine that simulates 6 vigenere ciphers. Using the resources on the next slide, recreate the enigma machine by code.

Please place your homework in the **cipher** folder of your github repo with your selected difficulty level as the title. Ex: If I do the bell pepper assignment, I'd name it **bellpepper.py**.

Habanero (Extra Spicy) Homework

The enigma machine is a rotor based encryption machine that simulates 6 vigenere ciphers. Take a look at the flowchart below and recreate the enigma machine by code.



Sources

https://www.geeksforgeeks.org/

https://www.tutorialspoint.com/