

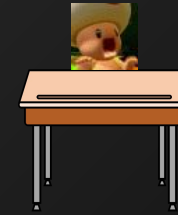
Simple Decryption Methods

Jiyeon Kim, Eduardo Leite, Tiffany Wong

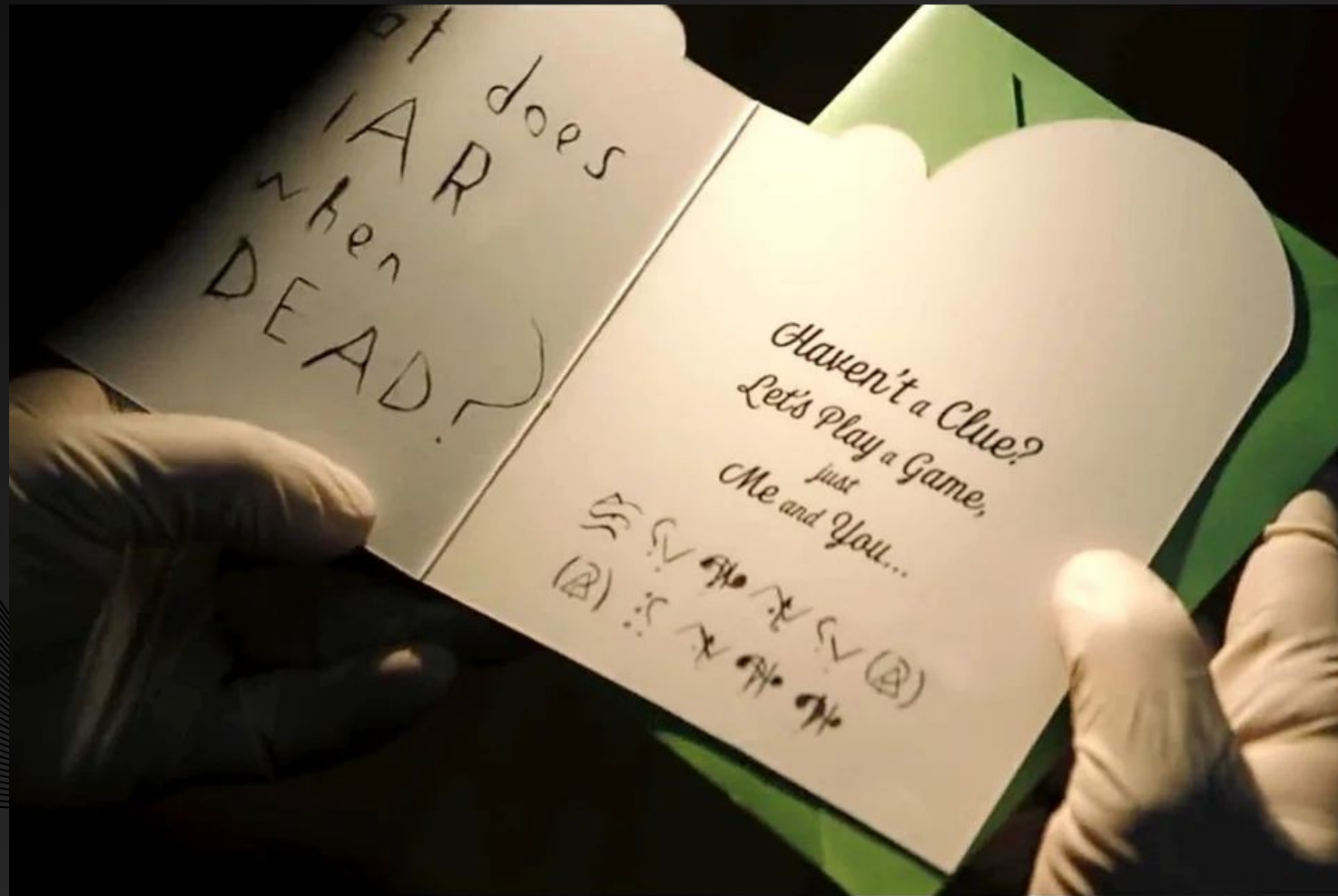


WWYD?

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: fcpevqkzgmtrayonujdlwhbksi

Cipher:

fcpevqkzgmtrayonujdlwhbksi

Text: substitutioncipher

Key: fcpevqkzgmtrayonujdlwhbksi

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

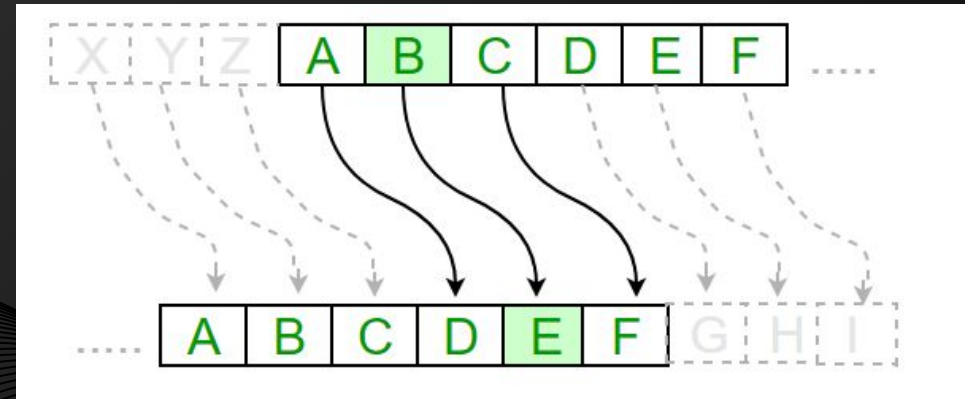
Shift: 4

Cipher: DEFGHI

Text: CAESARCIPHERdemo

Shift: 4

Cipher: GEIWEVGMTLIVhiqs



Coding the Caesar Cipher

CAESARCIPHERdemo with shift of 4

Code	Char	Code	Char	Code	Char	Code	Char	Code
302	(space)	408	0	604	(@)	800	P	906
303	!	409	1	605	A	801	Q	907
304	"	500	2	606	B	802	R	908
305	#	501	3	607	C	803	S	909
306	\$	502	4	608	D	804	T	1000
307	%	503	5	609	E	805	U	1001
308	&	504	6	700	F	806	V	1002
309	'	505	7	701	G	807	W	1003
400	(506	8	702	H	808	X	1004
401)	507	9	703	I	809	Y	1005
402	*	508	:	704	J	900	Z	1006
403	+	509	;	705	K	901	[1007
404	,	600	<	706	L	902	\	1008
405	-	601	=	707	M	903]	1009
406	.	602	>	708	N	904	^	1100
407	/	603	?	709	O	905	_	1101

Coding the Caesar Cipher

Code	Char	Code	Char	Code	Char	Code	Char	Code	Char
312	(space)	48	0	64	@	80	P	96	
313	!	49	1	65	A	81	Q	97	
314	"	50	2	66	B	82	R	98	
315	#	51	3	67	C	83	S	99	
316	\$	52	4	68	D	84	T	100	0
317	%	53	5	69	E	85	U	100	1
318	&	54	6	70	F	86	V	100	2
319	'	55	7	71	G	87	W	100	3
400	(56	8	72	H	88	X	100	4
401)	57	9	73	I	89	Y	100	5
402	*	58	:	74	J	90	Z	100	6
403	+	59	;	75	K	91	[100	7
404	,	60	<	76	L	92	\	100	8
405	-	61	=	77	M	93]	100	9
406	.	62	>	78	N	94	^	110	0
407	/	63	?	79	O	95	_	111	1

CAESARCIPHERdemo with shift of 4

$C + 4 \rightarrow 67 + 4 \rightarrow 71 \rightarrow G$

Coding the Caesar Cipher

Code	Char	Code	Char	Code	Char	Code	Char	Code	Char
32	(space)	48	0	64	@	80	P	96	
33	!	49	1	65	A	81	Q	97	
34	"	50	2	66	B	82	R	98	
35	#	51	3	67	C	83	S	99	
36	\$	52	4	68	D	84	T	100	
37	%	53	5	69	E	85	U	101	
38	&	54	6	70	F	86	V	102	
39	'	55	7	71	G	87	W	103	
40	(56	8	72	H	88	X	104	
41)	57	9	73	I	89	Y	105	
42	*	58	:	74	J	90	Z	106	
43	+	59	;	75	K	91	[107	
44	,	60	<	76	L	92	\	108	
45	-	61	=	77	M	93]	109	
46	.	62	>	78	N	94	^	110	
47	/	63	?	79	O	95	_	111	

CAESARCIPHERdemo with shift of 4

$C + 4 \rightarrow 67 + 4 \rightarrow 71 \rightarrow G$

$A + 4 \rightarrow 65 + 4 \rightarrow 69 \rightarrow E$

...

Coding the Caesar Cipher

Code	Char	Code	Char	Code	Char	Code	Char	Code	Char
32	(space)	48	0	64	@	80	P	96	
33	!	49	1	65	A	81	Q	97	
34	"	50	2	66	B	82	R	98	
35	#	51	3	67	C	83	S	99	
36	\$	52	4	68	D	84	T	100	0
37	%	53	5	69	E	85	U	100	1
38	&	54	6	70	F	86	V	100	2
39	'	55	7	71	G	87	W	100	3
40	(56	8	72	H	88	X	100	4
41)	57	9	73	I	89	Y	100	5
42	*	58	:	74	J	90	Z	100	6
43	+	59	;	75	K	91	[100	7
44	,	60	<	76	L	92	\	100	8
45	-	61	=	77	M	93]	100	9
46	.	62	>	78	N	94	^	110	0
47	/	63	?	79	O	95	_	110	1

CAESARCIPHERdemo with shift of 4

$C + 4 \rightarrow 67 + 4 \rightarrow 71 \rightarrow G$

$A + 4 \rightarrow 65 + 4 \rightarrow 69 \rightarrow E$

...

$d + 4 \rightarrow 100 + 4 \rightarrow 104 \rightarrow h$

Coding the Caesar Cipher

Code	Char	Code	Char	Code	Char	Code	Char	Code
312	(space)	48	0	64	@	80	P	96
313	!	49	1	65	A	81	Q	97
314	"	50	2	66	B	82	R	98
315	#	51	3	67	C	83	S	99
316	\$	52	4	68	D	84	T	100
317	%	53	5	69	E	85	U	101
318	&	54	6	70	F	86	V	102
319	'	55	7	71	G	87	W	103
400	(56	8	72	H	88	X	104
401)	57	9	73	I	89	Y	105
402	*	58	:	74	J	90	Z	106
403	+	59	;	75	K	91	[107
404	,	60	<	76	L	92	\	108
405	-	61	=	77	M	93]	109
406	.	62	>	78	N	94	^	110
407	/	63	?	79	O	95	_	111

CAESARCIPHERdemo with shift of 4

$C + 4 \rightarrow 67 + 4 \rightarrow 71 \rightarrow G$

$A + 4 \rightarrow 65 + 4 \rightarrow 69 \rightarrow E$

...

$d + 4 \rightarrow 100 + 4 \rightarrow 104 \rightarrow h$

...

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 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

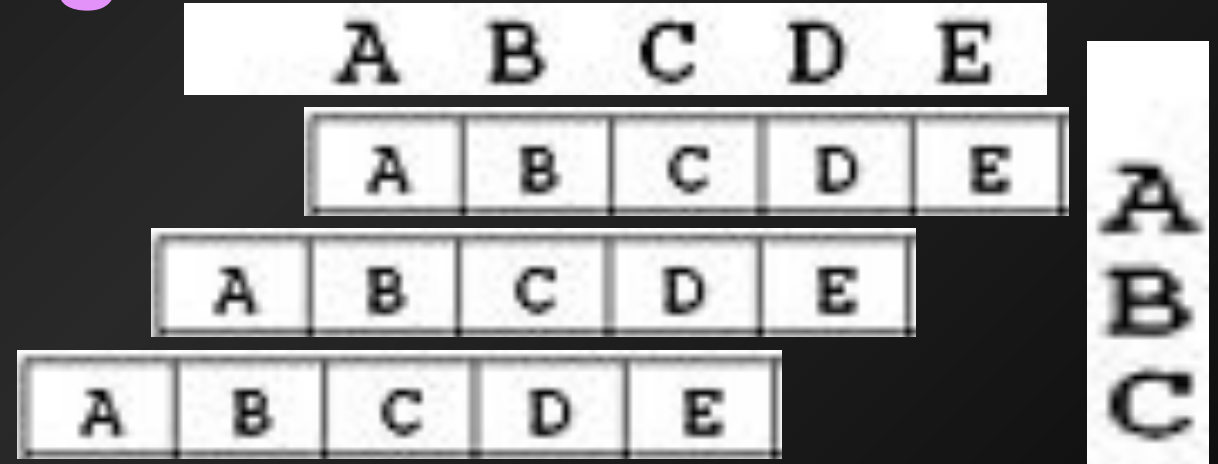
So how does encoding work?

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/class>
Resources

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.

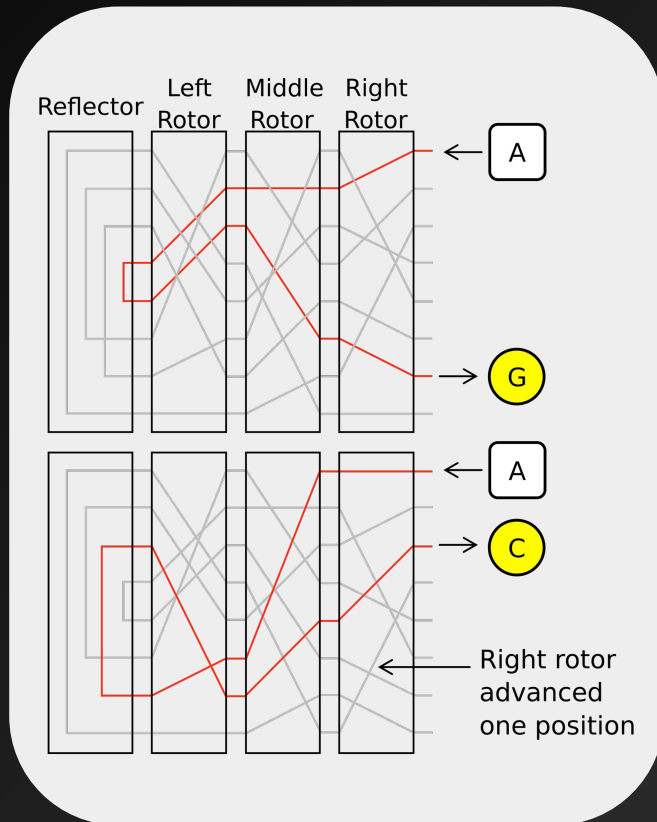
Homework

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/>