Please mute your microphones.
You may keep your video on if you wish.
We will begin shortly.

Thank you.

FYS

Encryption and Decryption

Computer Science / Mathematics / Cybersecurity

Materials

Paper

Pen/Pencil

That’s it! :)

It’s been a week since you saw the mysterious initials “C.C” in the park. At this point, it seems like an unsolvable mystery. Who is this person?

But one day, you bring in the mail
and notice an unmarked envelope.
You open it and find a letter.

F.F. MXVW PHDQW
FDHVDU FLSKHU!

FYS

Let’s Think:

Have you ever tried to write a secret message to a friend using a special code? Did anyone ever break this code?

What is encryption?

- The process of making a message unreadable to people who you don’t want to see it, but readable to the person you want to see it.
- There are many cases where data is being shared and we don’t want this data to be publicly understandable.

Let's Think:

Can you think of a reason why a message would need to be encrypted?

Uses of Encryption

- If you’re messaging your friend private information and don’t want other people to see it (WhatsApp/iMessage)
- If you’re buying something online and have to enter your credit card number, and don’t want other people to access that information.

FYS

Let's Think:

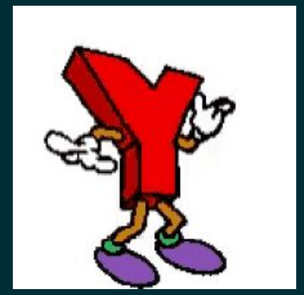
Do you know of any encryption methods?

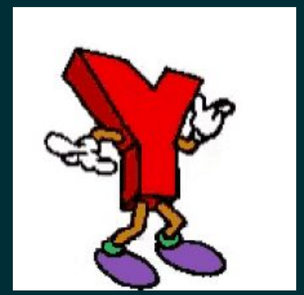
Caesar Cipher

- The **Caesar Cipher** is an ancient secret code named after **Julius Caesar**, a famous Roman leader who lived a long time ago.
- Around 2,000 years ago, Julius Caesar used this special code to send **secret messages** during wars, so his enemies couldn't understand his plans.

Caesar Cipher Cont’d

- If you want to send a message, **each letter** in the message has to be **moved a certain number** of places **down the alphabet** to create the secret code. For example, "A" might become "D," and "B" becomes "E."
- It's **not very secure** because there are only a few ways to change the code, so people can guess it easily (and we’ll show you how!)





Caesar Cipher Cont’d

- You shift each letter in the message the same number of letters in the alphabet
- For example, **“hello”** with a **shift of 3** would be **“khoor.”**

0	h	e	l	l	o
1	i	f	m	m	p
2	j	g	n	n	q
3	k	h	o	o	r

Let’s practice! If we want to do a shift of 3...

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

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

Now with this code, let’s go between encrypting and decrypting!

Scientist -> VFLHQWLVW

DGYHQWXUH -> ??????

Practice problems! (Still with a shift of 3)

Encrypting

CIPHER -> ???

SUMMER -> ???

LAVA LAMP -> ???

Decrypting

RREOHFN -> ???

FDQGB -> ???

SKRQH -> ???

Great job! Can you try **encrypting** your name with a shift of 7?

First, let’s make a new alphabet to make things easier.

If we did it correctly, this is what our new alphabet should look like.

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
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

So, “NIKKI” with a shift of 7 is “UPRRP”! What’s yours?

Now that we've learned the Caesar Cipher, we can figure out what this means! We're not going to tell you the shift number. Can you decipher it?

F.F. MXVW PHDQW
FDHVDU FLSKHU!

FYS

Let’s Think:

Thousands of years after Julius Caesar, we don’t use the Caesar Cipher much anymore. Can you think why?

Why isn’t the Caesar Cipher secure?

- Sometimes, you can figure out key using certain clues. In our secret message, you could guess the shift was 3 because you knew F.F. was going to decrypt to C.C.
- Even if you don’t know the key, you can just try all 25 different combinations until you find a readable word. This is known as a **brute-force attack**.
- It might sound like this would take long to do, but it’s really easy using a computer.

Questions?

Great job! Now, let's move on to some reflection questions.

Reflection Questions

1. *Why do you think encrypting and decrypting a message is important in the world?*
2. *Can you think of other ways people might encrypt messages?*
3. *What was your favorite part of this activity?*

See you all next week!

Visit our website, **futureforyoungscientists.org**.

If you have any photos from this week, please share these with us by email (futureforyoungscientists@gmail.com) or Facebook, as we would like to be able to share everyone's experience.