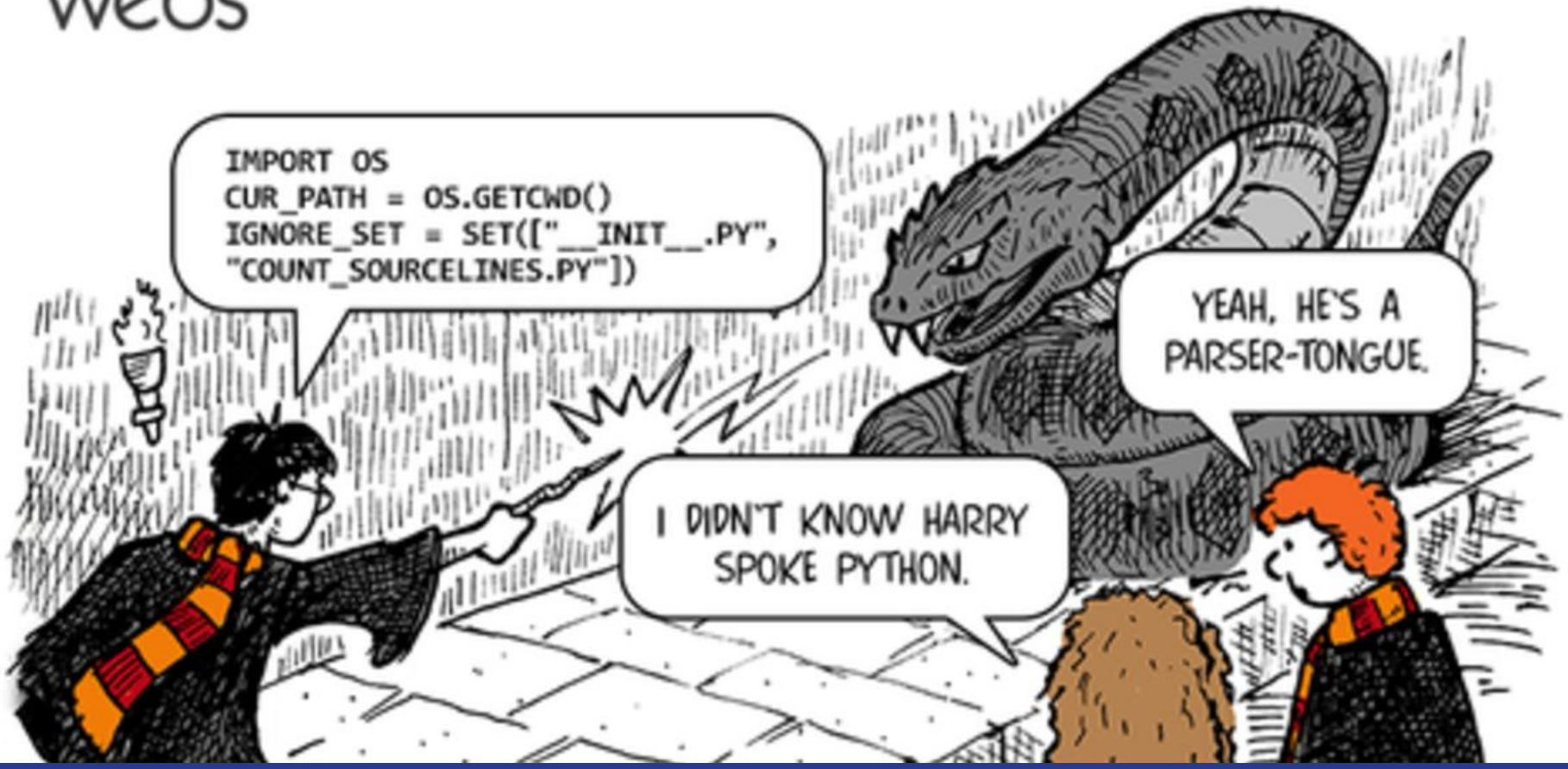
Cyber Security

Brainstorm:

What are examples of valuable data?

webs


IMPORT OS
CUR_PATH = OS.GETCWD()
IGNORE_SET = SET(["__INIT__.PY",
"COUNT_SOURCELINES.PY"])
I DIDN'T KNOW HARRY SPOKE PYTHON.
YEAH, HE'S A PARSER-TONGUE.

Financial Gains

- You information worth money.
- Single Credit Card Number: $4-15
- Single Credit Card: $12 -30
- “Fullz” :
  - Full name, address, phone, email, birthday, SSN, bank account and routing number and etc.
- Online bank accounts: under $300

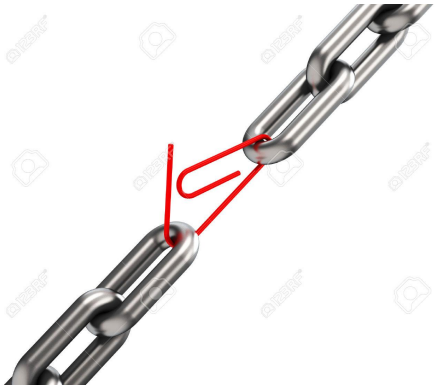

A SMALL LOAN
OF A MILLION
DOLLARS
memegenerato


CUSTOMER
DATA
gg74947355 www.gograph.com

Security Principles

Security Mindset

- “There are no secure systems, only degrees of insecurity.” -Shamir
  - Adversary only needs one weak link to break through
  - Defenders must defend all the links
- **Think like an adversary**
- Do not trust anything ! (not even your own code)
- No security through obscurity
  - We always assume that the attacker knows all the mechanisms



Security Principles

When protecting data, ask yourself if you have the following:

- **Confidentiality:**

- **Integrity:**
- **Availability:**

Security Principles

When protecting data, ask yourself if you have the following:

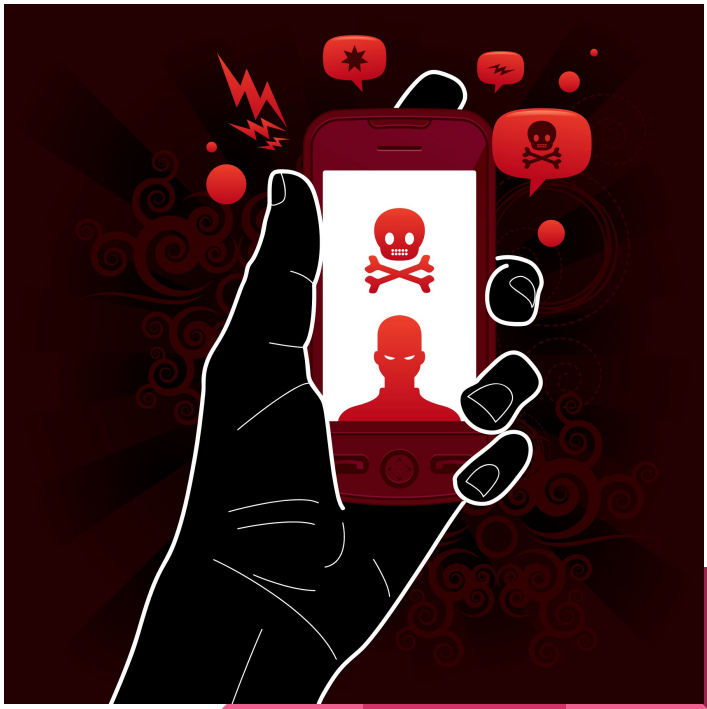
- **Confidentiality:** Is the data only known by authorized users?
- **Integrity:** Is the data from a legitimate source?
- **Availability:** Can authorized users get access to the data?

What/who are we defending against?

Your role is to **defend** a system or service against an **adversary** or **attacker**.

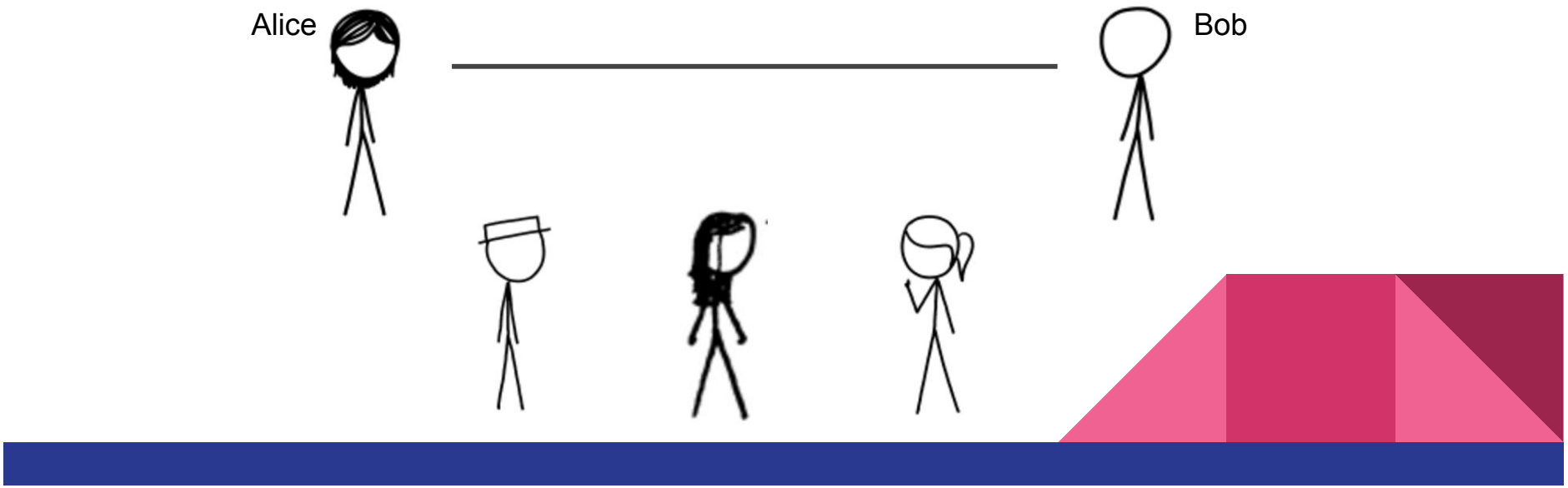
But in order to know what to do, you must put yourself in the role of the attacker. What are their means? What aspects of the network or data do they have access to? What are their goals?

Writing down what your adversaries can do called making a **threat model**.



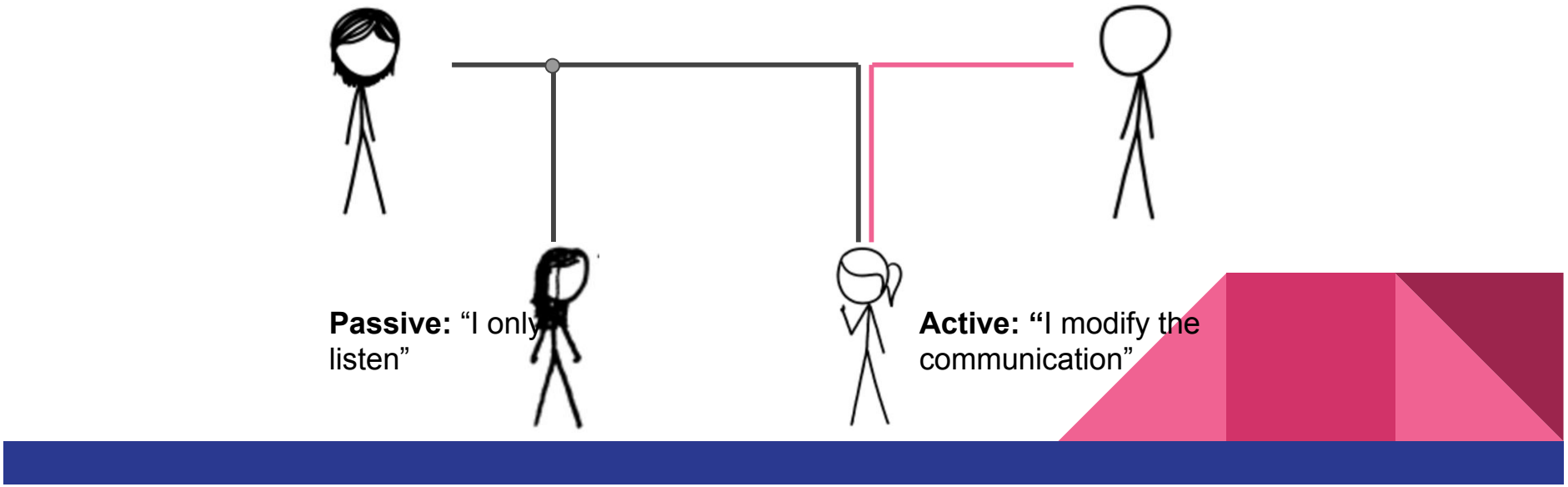
Threat Models

Alice and Bob want to communicate in the presence of **adversaries**. What can the adversaries do?



Threat Models

passive vs **active** adversaries - a passive adversary will only eavesdrop on communication, never alter it. An active adversary may maliciously change the content of web communication.



Passive or Active

Copying your friends homework

Changing your friend’s profile picture on Facebook

Trying to log on your friends account by guessing their passwords

Go to your teacher’s office and look for the answer key for the next exam.

Come up with your own scenarios.

Attack categories/goals

What are some things attackers might want to do?

Remember CIA: confidentiality, integrity, availability

Are they active or passive?

Attack categories

Eavesdropping -

Exfiltration -

Spoofing -

Tampering -

Denial-of-service attack (DOS) -

Attack categories

Eavesdropping - listening to a private conversation (violates **confidentiality**)

Exfiltration - stealing secret data (violates **confidentiality**)

Spoofing - creating a fake message that looks real (violates **integrity**)

Tampering - alter an existing message maliciously (violates **integrity**)

Denial-of-service attack (DOS) - prevent legitimate use of a service (e.g. by flooding a server; violates **availability**)

Confidentiality

- If you want to tell your friend a secret, but you know someone is eavesdropping, what would you do?

Cryptography

Crypto-

Cryptology

Cryptography

Cryptanalysis

Cryptosystem

Crypto

Crypto- latin root for “hidden” or “secret”

Cryptology - Study and practice of securing communication and data in the presence of **adversaries**, usually by making codes

Cryptography - Writing/making codes

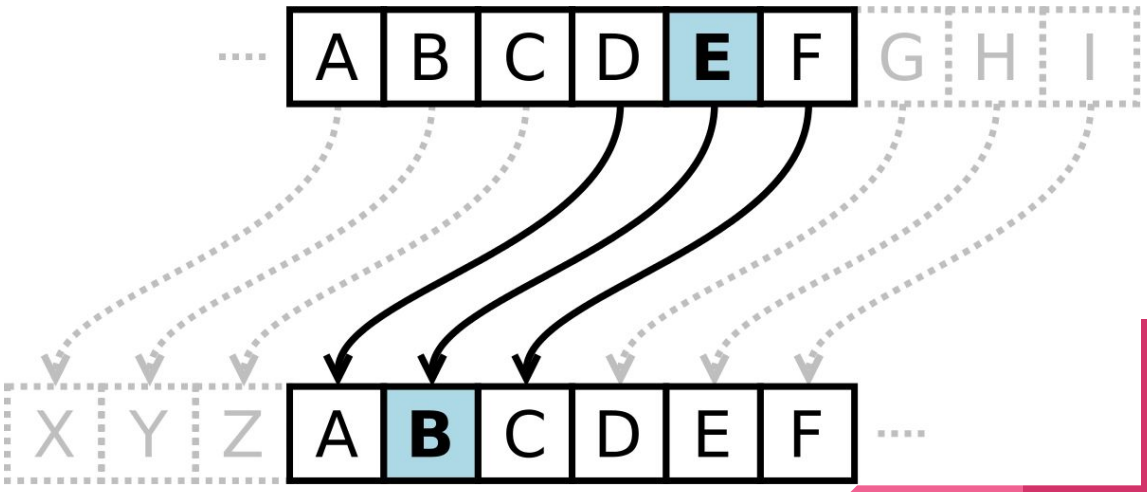
Cryptanalysis - Breaking/cracking codes

Cryptosystem - A method for **encrypting** and **decrypting messages** using **keys**

Crypto - Any or all of these

Caesar Shift

- One of the oldest example of cryptography
- Shifts all the letter by the key(a number or a letter)

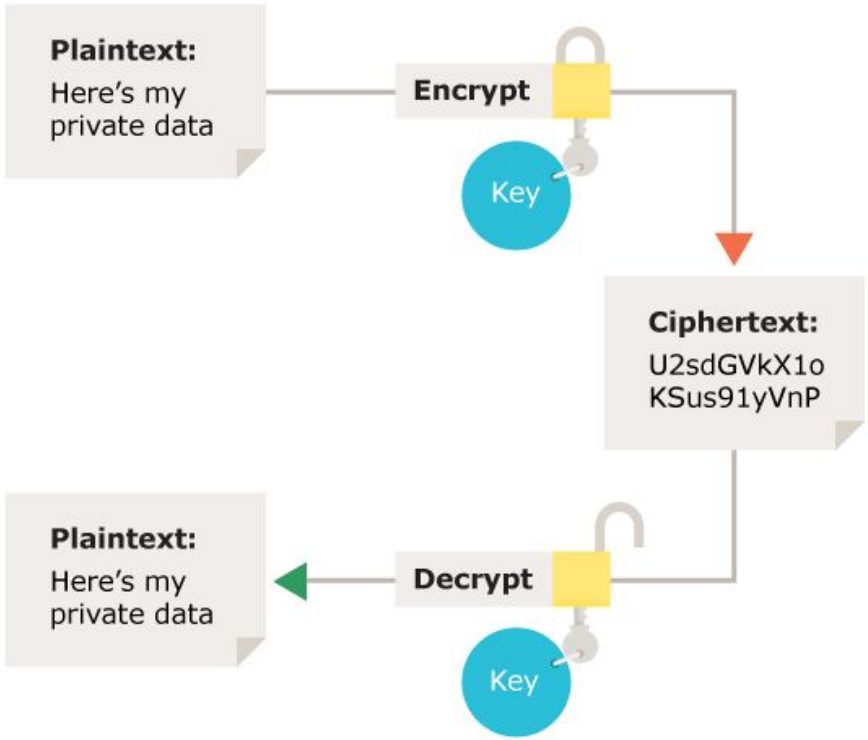


Exercise: Build your own cryptosystem

- Cryptosystem: A system of encrypting and decrypting a message
- Cut out one set of Alphabet and tape it around the cup **Counterclockwise**
- Then pick a partner and put the two cups together.

Caesar Shift

- Plaintext:
- Keys:
-
- Ciphertext:
- Encryption:
- Decryption:

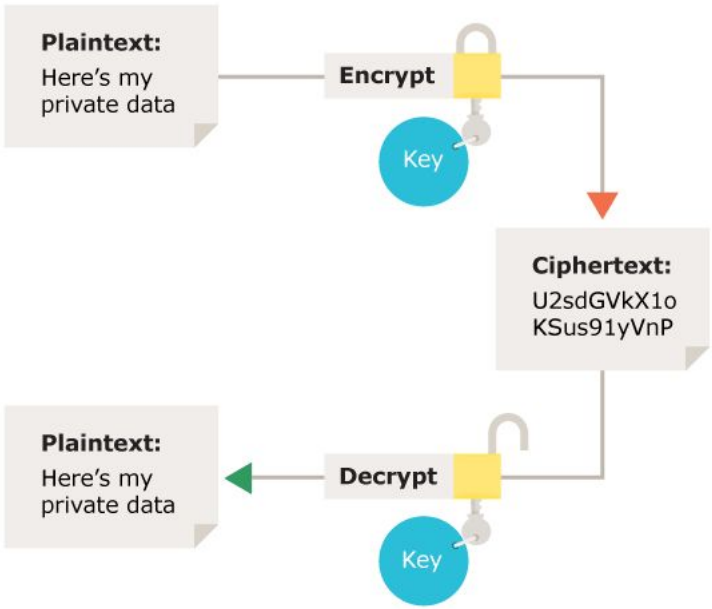


Caesar Shift Cryptosystem

- Plaintext: sequence of letter (A to Z)
- Ciphertext: sequence of letters (A to Z)
- Encryption: Look from left to right on your cup
  - (message + key) % 26
- Decryption: Look from right to left on your cup
  - (26 + ciphertext - key) % 26
- Keys: numbers from 0 to 25, or alphabets from A to Z

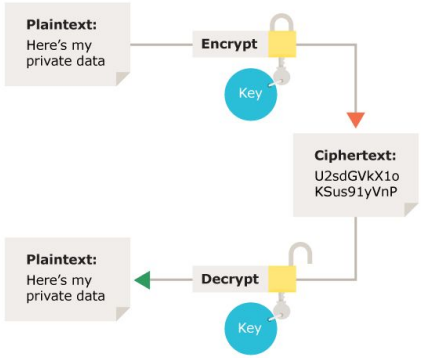
Cryptosystem

- Plaintext:
- Ciphertext:
- Encryption:
- Decryption:



Cryptosystem

- Plaintext: The message that you want to send.
- Ciphertext: coded message
- Encryption: A function that encode a message. (Plaintext to ciphertext)
- Decryption: A function that decodes a message. (ciphertext to plaintext)
- Key: How to encrypt and decrypt a message



What are some problems with the Caesar Cipher?

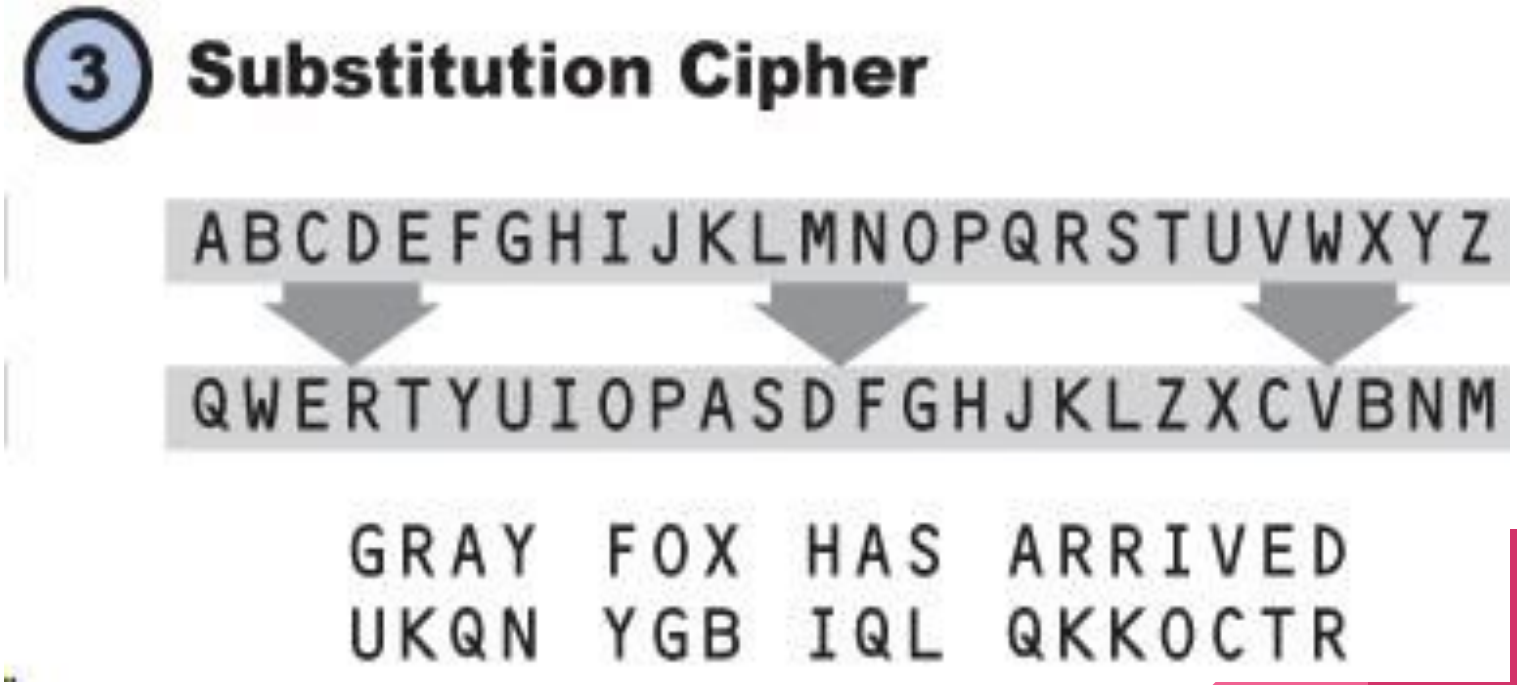
What are some problems with the Caesar Cipher?

Only 26 possibilities for keys - makes it very easy for an adversary to just try them all

In its current form, can only work with messages made of letters (no special characters!)

Is there a cipher that have more keys?

Substitution Cipher



Substitution Cup Activity

- Cut out another set of Alphabet.
- Cut out each of the letters and put it in the cup.
- Draw one letters out at a time and fill it on a blank column.
- Now tape the new set of letters to another cup.

Why is it safer than Caesar Shift

Why is it safer than Caesar shift

Way more keys than Caesar, safer from brute forcing attacks

Key space is 26! .

Jefferson Wheel Cipher

Jefferson Wheel Cup Activity

We will now give you a number.

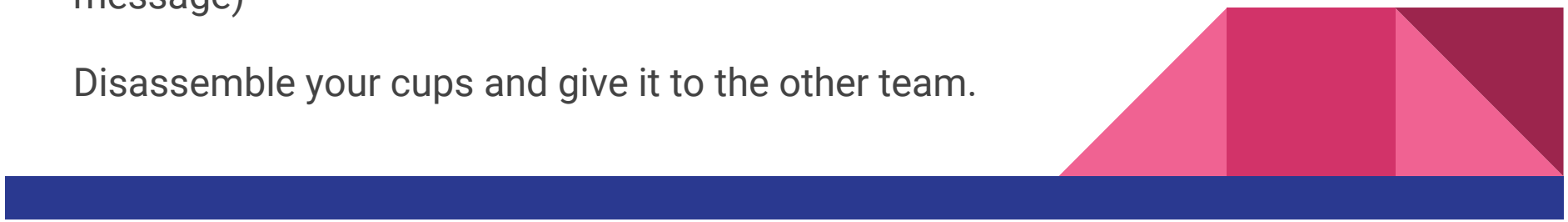
Split the whole class into 2 teams.

Assemble your cup with random alphabets on them (remember the orders)

Come up with your message and spin the cups till you get it

Write down the order of the cups and a random row of letters (not the one with the message)

Disassemble your cups and give it to the other team.



Jefferson Cup activities

How many keys do you think this cipher has?

Symmetric Encryption

Keys are the same, but encryption and decryption might be different.

Now Let’s do some coding

Implement you own Caesar Cipher Encryption and Decryption