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

Thank you.

FYS

Public Key Cryptography

Computer Science / Mathematics / Cybersecurity

Materials

Paper

Pen/Pencil

That’s it! :)

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 encoding data so that third parties are prevented from seeing certain data, while specific parties are able to see it.
- There are many cases where data is being transmitted and we don’t want this data to be publicly visible.

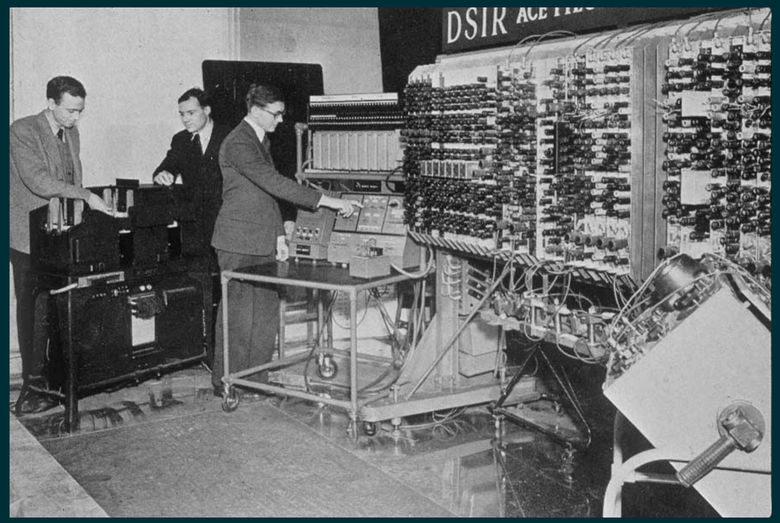
FYS

Let's Think:

Can you think of a scenario where a message would need to be encrypted?

Uses of Encryption

- Wartime communication: Enigma during WWII
- Messages: WhatsApp, iMessage, Telegram, etc.
- Websites, banking apps, shopping apps, and anything else that we don’t want unknown third parties to see



FYS

Let's Think:

Do you know of any encryption methods?

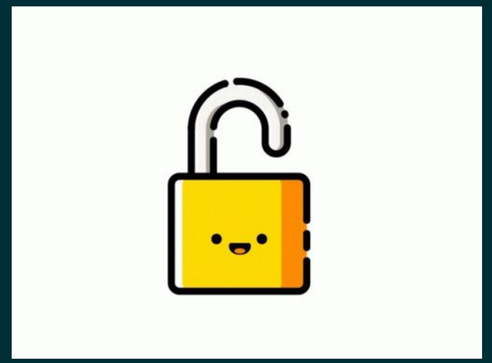
Caesar Cipher

- Used by **Julius Caesar** to securely communicate with his military
- 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.”**
- It’s not obvious what “khoor” means, but you could easily (especially with a computer) shift each letter 25 times without knowing the key, to get the answer.

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

Public-Key Cryptography

- Let’s pretend everyone buys a lock, writes their name on it, and puts them all open on the same table for others to use. You’re all going to keep your own key. If I want to send you a secure message, I put it in a box, pick up your padlock, lock the box and send it to you.
- Even if it falls into the wrong hands, no-one else can unlock it!



Now, let’s dive into a specific example of Public Key Cryptography:

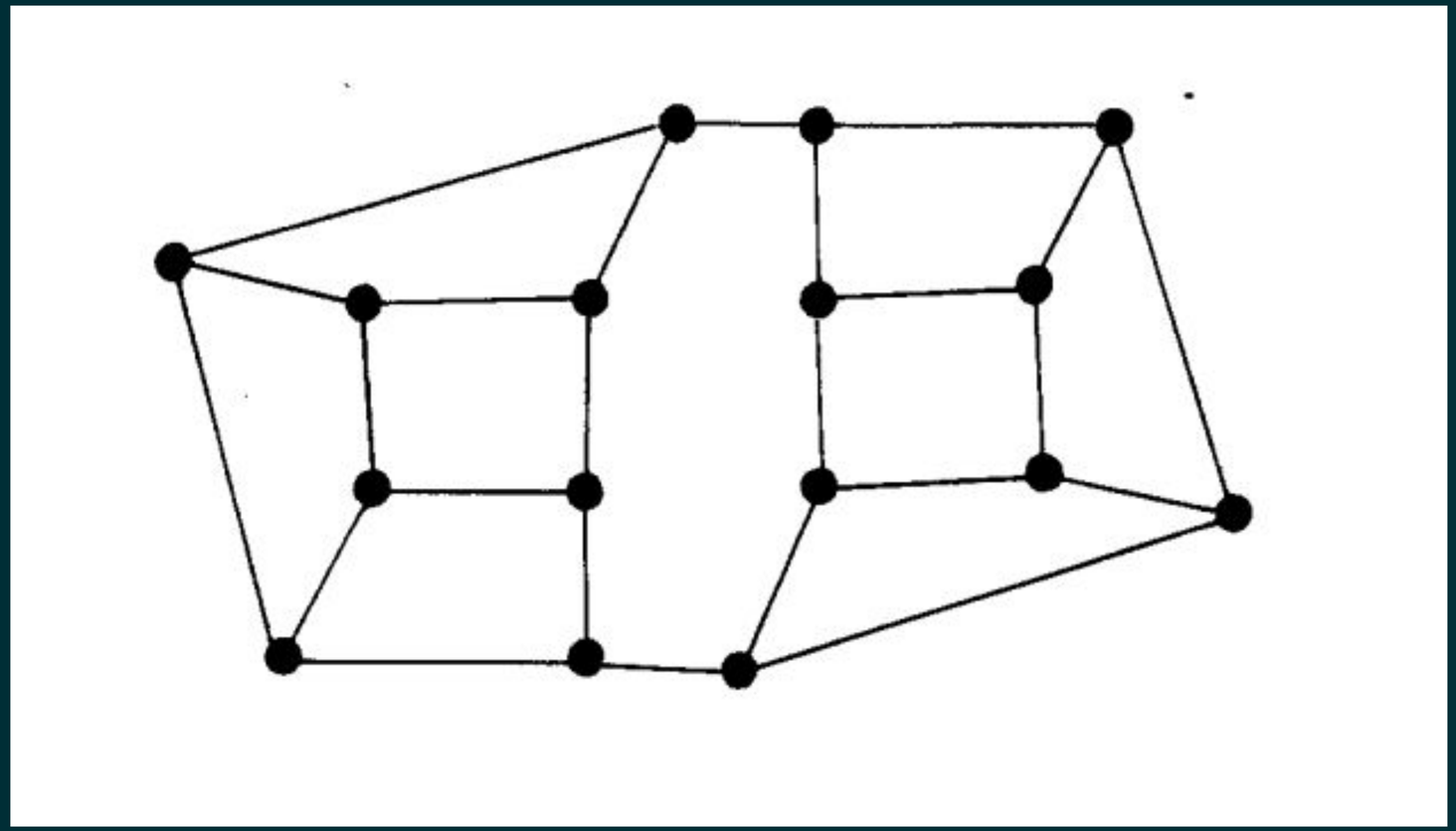
Perfect Code Cryptosystem

Questions?

Bob is going to have a public lock. This will be accessible to everyone so they can use it to encrypt a message, but if anyone tries to decrypt it, they won’t be able to because they don't have the key.

So, to send Bob a message, we will encrypt our message with Bob’s public lock.

Bob’s Public Lock (copy this down onto paper)

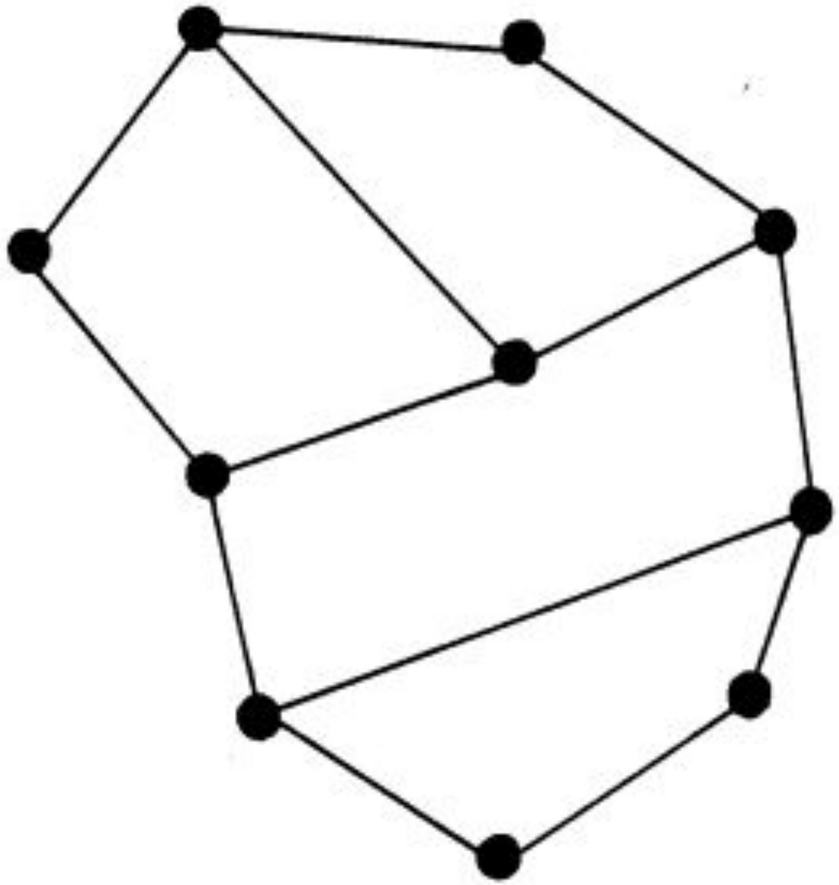


Procedure

1. *Now, pick a number. Place random numbers at each vertex, so that all of the numbers add up to the first number you chose. After, just double check that all of the numbers add up to your secret number. Don't tell anyone the number!*
2. *To lock it, choose any vertex look at it and its 3 neighbors, and add all 4 numbers together. Then write this number in a different color / in parenthesis under the vertex. Repeat for each vertex. Make sure you add correctly!*
3. *Now, show us the graph. We will determine your number using the private key.*

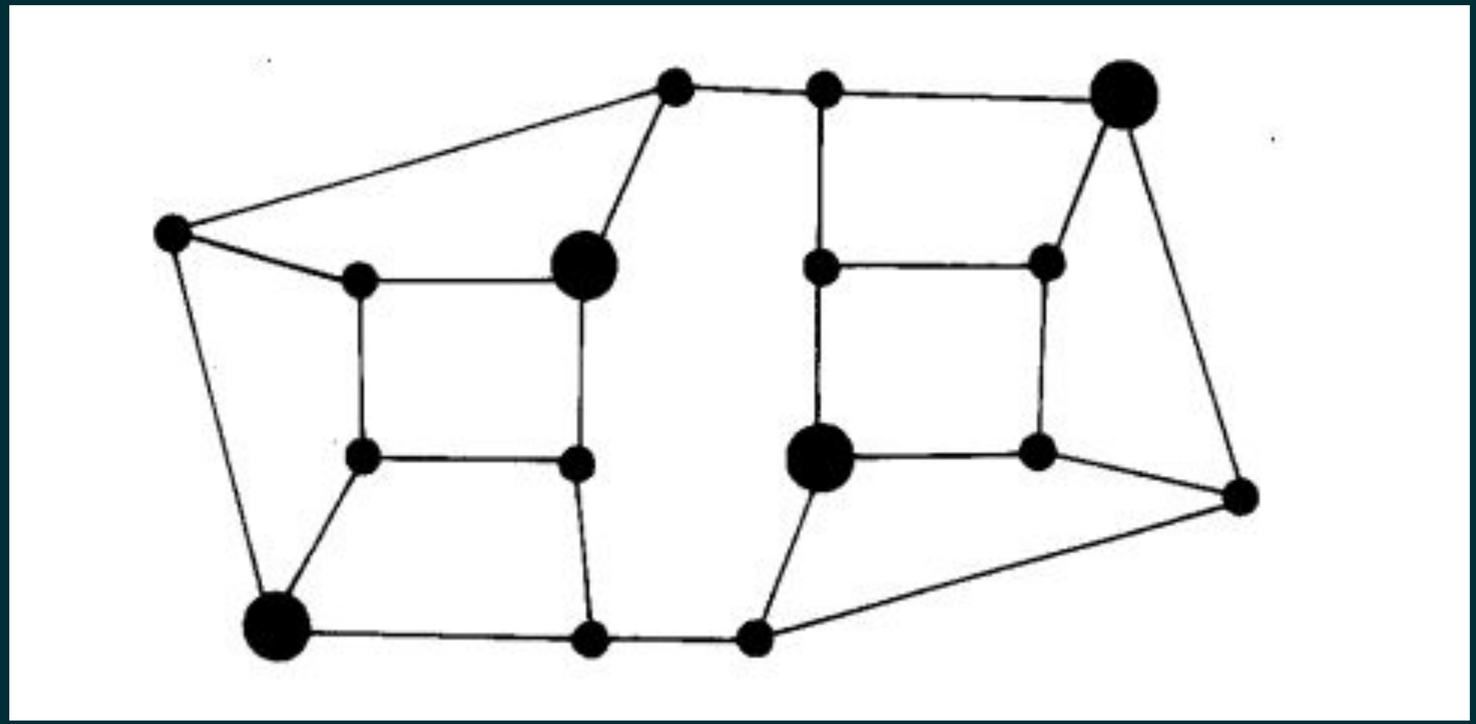
Let’s do that again
with a different map!
This time, you can do it
on your own.

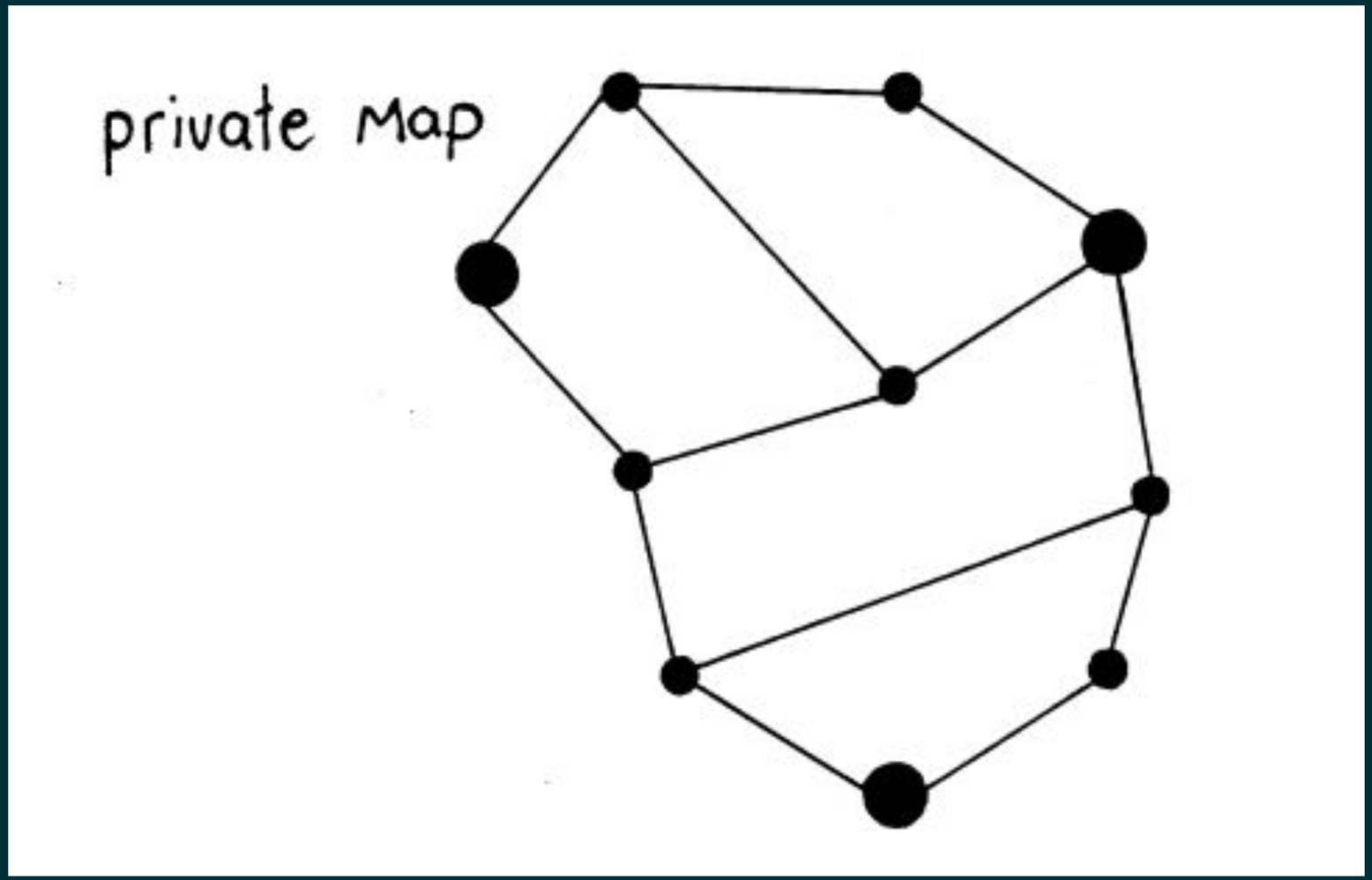
public Map



How did we figure out your number?

Bob’s Key

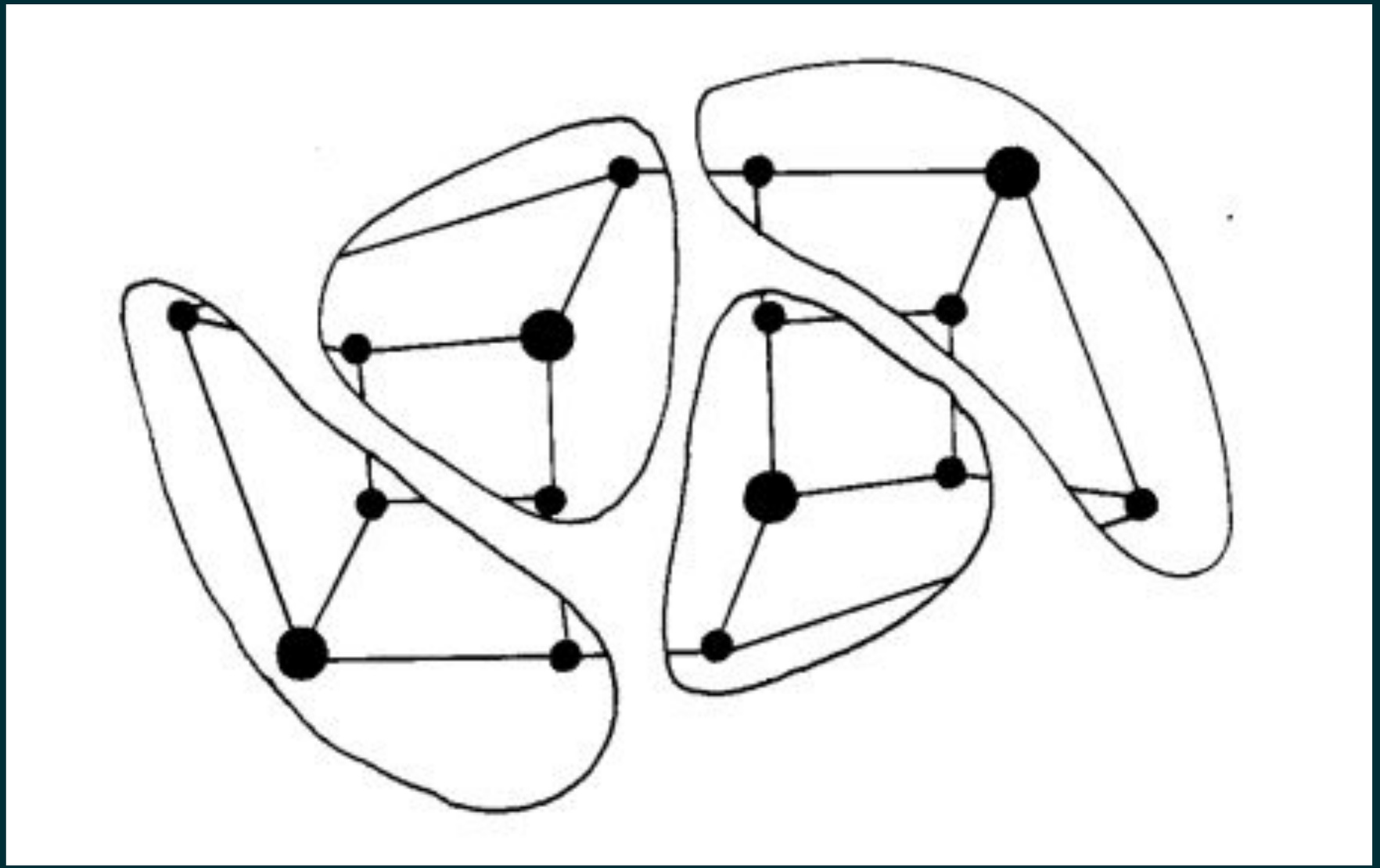



private map

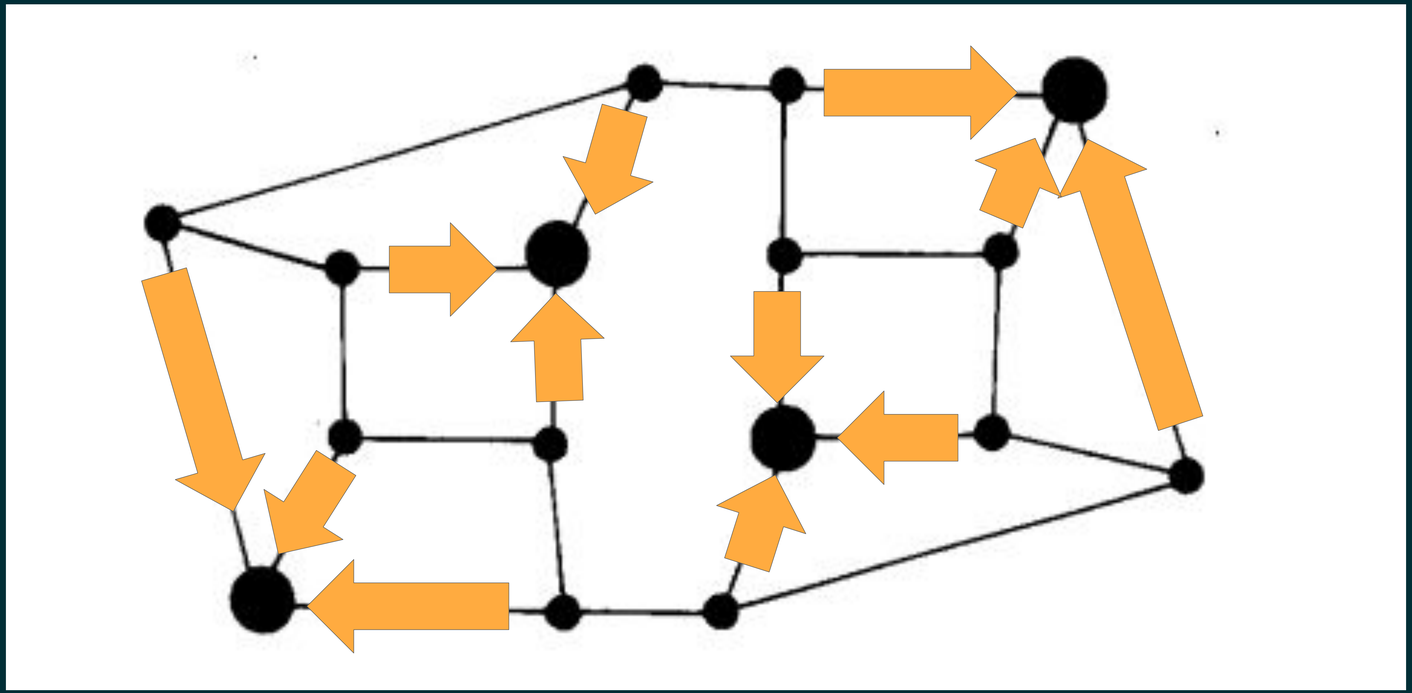
FYS

Let's Think:

Why do you think these particular vertices are special?



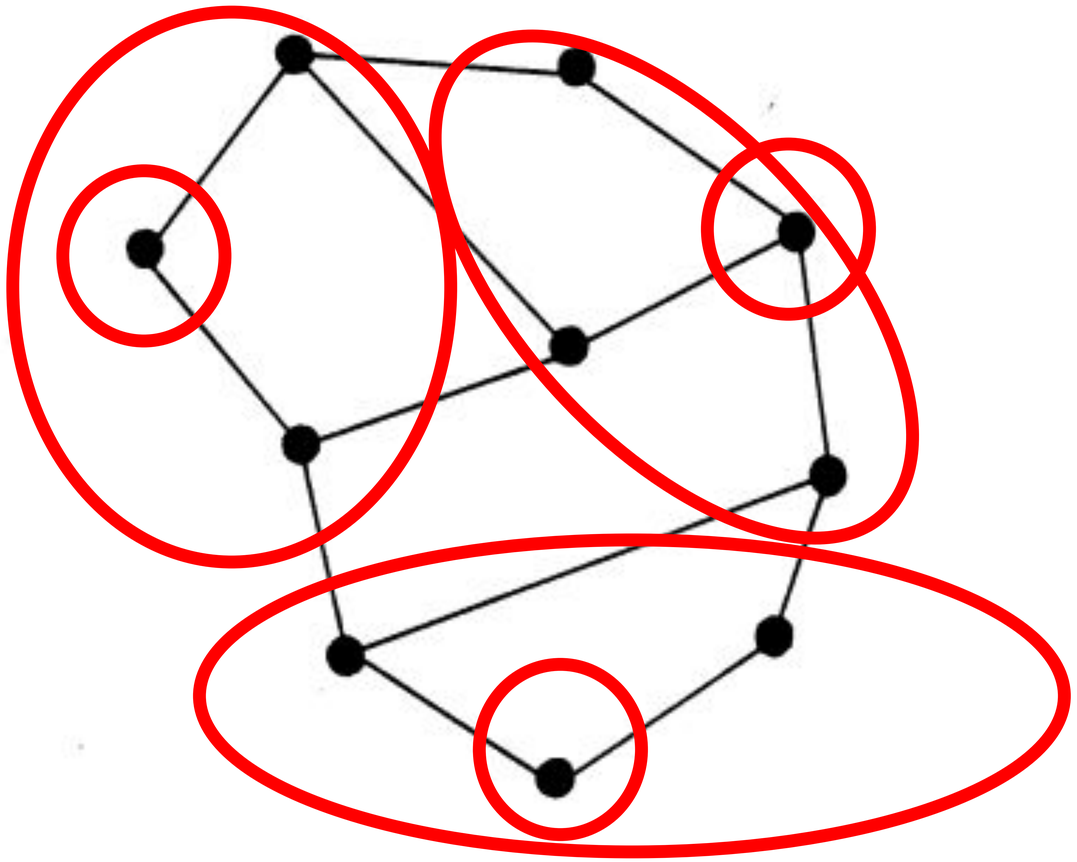
With the unlocked graph, we can get to our original number by adding up all the vertices.
By locking it, we added each vertex to its neighborhood.
So in the locked graph, the sum of the bold vertices is the sum of all of the vertices in the unlocked graph.



Questions?

Let’s try finding the private key in our second example!

public Map



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

Reflection Questions

1. *What is the purpose of using two keys (public key and private key) in public key cryptography? How does this make communication more secure?*
2. *Why do you think Cryptography might be important in the real world?*
3. *What was your message?*

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.