Ethical Student Hackers

Cryptography

The Legal Bit

- The skills taught in these sessions allow identification and exploitation of security vulnerabilities in systems. We strive to give you a place to practice legally, and can point you to other places to practice. These skills should not be used on systems where you do not have explicit permission from the owner of the system. It is VERY easy to end up in breach of relevant laws, and we can accept no responsibility for anything you do with the skills learnt here.

- If we have reason to believe that you are utilising these skills against systems where you are not authorised you will be banned from our events, and if necessary the relevant authorities will be alerted.

- Remember, if you have any doubts as to if something is legal or authorised, just don't do it until you are able to confirm you are allowed to.

Code of Conduct

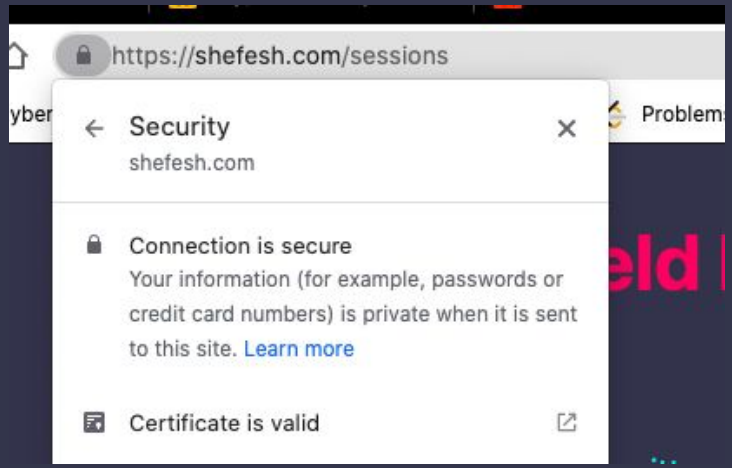
- Before proceeding past this point you must read and agree to our Code of Conduct - this is a requirement from the University for us to operate as a society.
- If you have any doubts or need anything clarified, please ask a member of the committee.
- Breaching the Code of Conduct = immediate ejection and further consequences.
- Code of Conduct can be found at https://shefesh.com/downloads/SESH%20Code%20of%20Conduct.pdf

What is Cryptography?

Cryptography is the science of keeping information secret and secure.

It involves transforming plain text into cipher text, which is unreadable to anyone who does not have the key to decrypt it. Cryptography is important because it helps protect our sensitive information, like credit card details and personal data, from hackers and cybercriminals.

Cryptography is used everywhere in everyday life.



Types of Cryptography

The development of Cryptography can be divided into 2 types:

- Classical cryptography
  - Substitution
  - Transposition

- Modern Cryptography
  - Symmetric key cryptography
  - Public key cryptography

Message: JAM**ESB**ONDNEEDSBACKUP
Code: J**E**ONDAUA**S**NESCPM**B**DEBK

J	**E**	O	N	D	A	U
A	**S**	N	E	S	C	P
M	**B**	D	E	B	K	

Practical on Classical Cryptography

This word below has been encrypted with the Caesar cipher using a shift of 7, decode the word and see what it says in plaintext:

zolmlzo

This word has been encrypted using a transposition cipher with key:“zebra”. By drawing a grid, work out the encrypted word:

CP EEK LLR TY BHA

Symmetric Key Cryptography

Symmetric key cryptography uses the same key to encrypt and decrypt the message.

Examples of symmetric key cryptography:

- Advanced Encryption Standard (AES)
- Data Encryption Standard (DES)

AES works by dividing the plaintext data into fixed-size blocks, and then encrypting each block separately using a key.

DES works by dividing the plaintext data into 64-bit blocks and then encrypting each block separately using a key. The key used is 56 bits long.

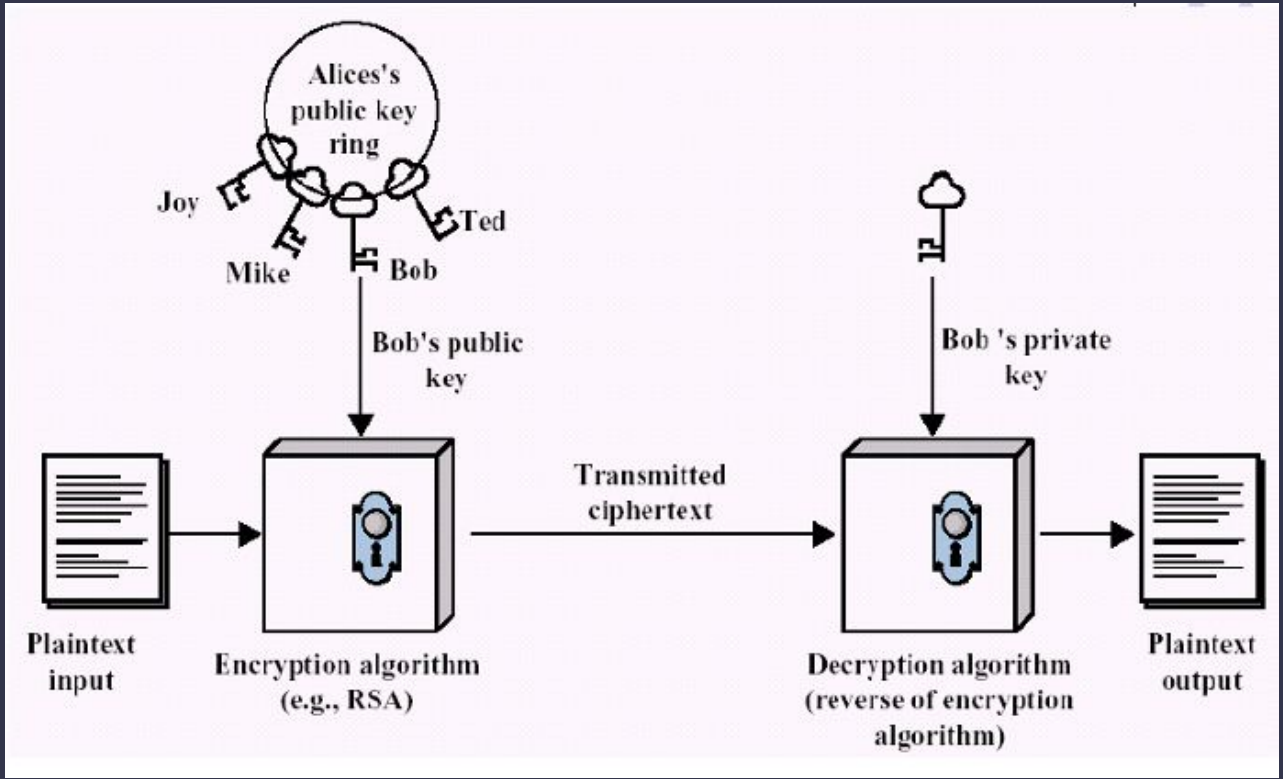
Public Key Cryptography

Public key cryptography uses two different keys for encryption and decryption. (Can also be known as asymmetric cryptography).

Examples of public key cryptography:

- RSA
- Elliptic Curve Cryptography (ECC)

How Public Key Cryptography Works



RSA

RSA works by using large prime numbers and modular arithmetic.

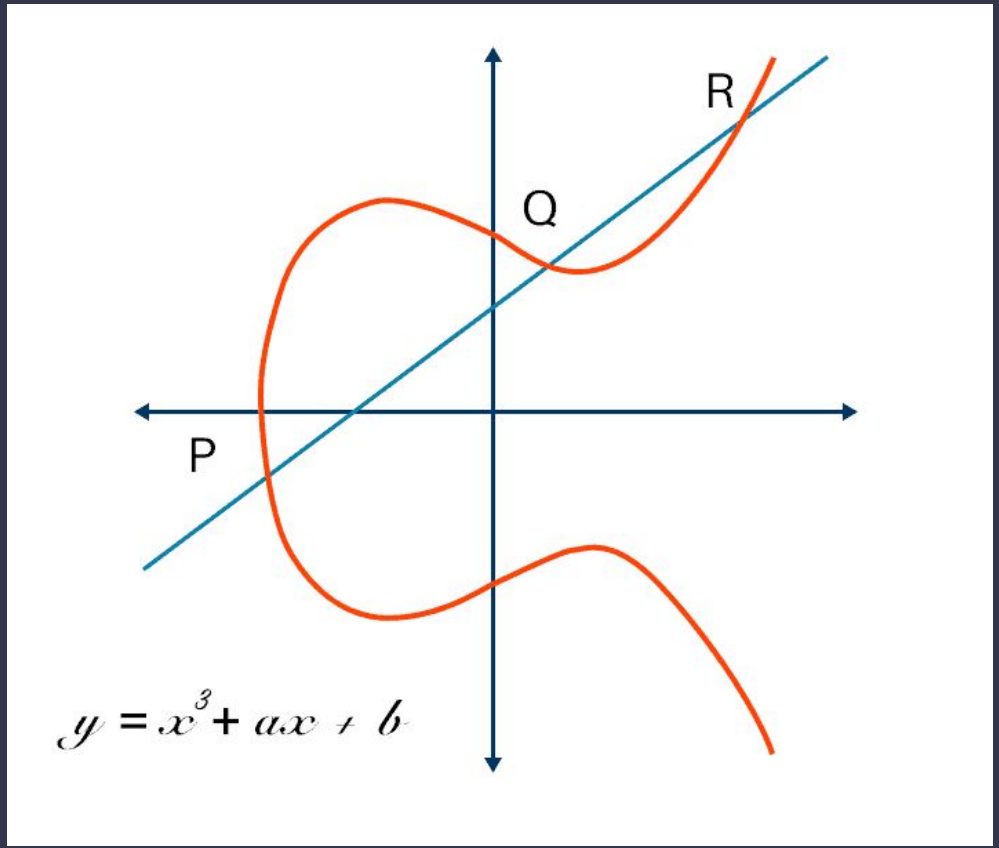
1. The person who wants to receive encrypted data generates a key pair.
2. The sender uses the recipient's public key to encrypt the data.
3. The recipient uses their private key to decrypt the data.
4. The keys are generated using two large prime numbers, p and q. These numbers are kept secret by the key owner.
5. The owner uses p and q to generate a modulus, n = p x q.
6. The owner then chooses a number, e, that is relatively prime to (p-1) x (q-1), which means that e has no common factors with (p-1) x (q-1).
7. The owner then computes a number, d, that is the multiplicative inverse of e modulo (p-1) x (q-1).
8. The public key is the pair (n, e), and the private key is the pair (n, d).
9. The encryption algorithm works by raising the plaintext message to the power of e modulo n.
10. The decryption algorithm works by raising the encrypted message to the power of d modulo n.

Elliptic Curve Cryptography

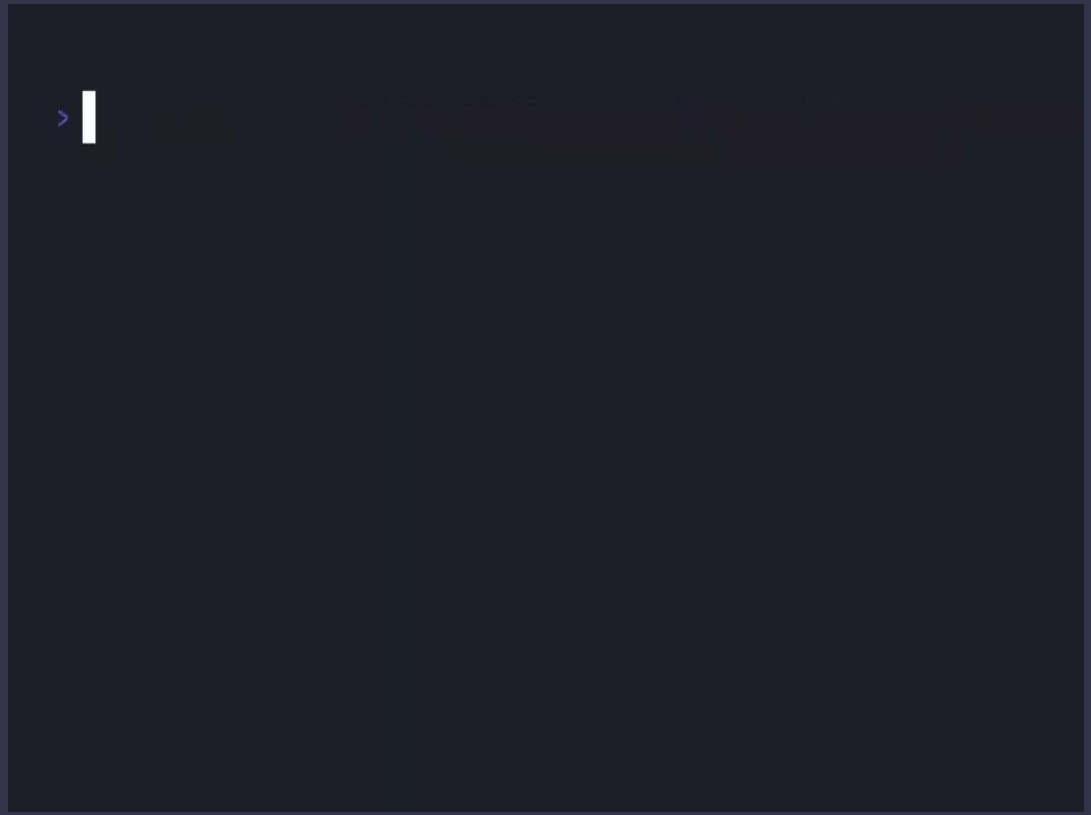
Elliptic Curve Cryptography (ECC) is a type of public key cryptography that is based on the mathematics of elliptic curves.

1. The person who wants to receive encrypted data generates a key pair
2. The sender uses the recipient's public key, which is a point on the elliptic curve, to encrypt the data.
3. The recipient uses their private key, which is a scalar value, to decrypt the data.
4. The keys are generated using a random starting point on the elliptic curve, called the base point.
5. The owner chooses a random number, called the private key, which is a scalar value. This scalar value is multiplied by the base point on the elliptic curve, resulting in a point on the curve. This point is the public key.
6. The encryption algorithm works by multiplying the plaintext message by the recipient's public key, which is a point on the elliptic curve.
7. The decryption algorithm works by multiplying the encrypted message by the recipient's private key, which is a scalar value.

Elliptic Curve Cryptography



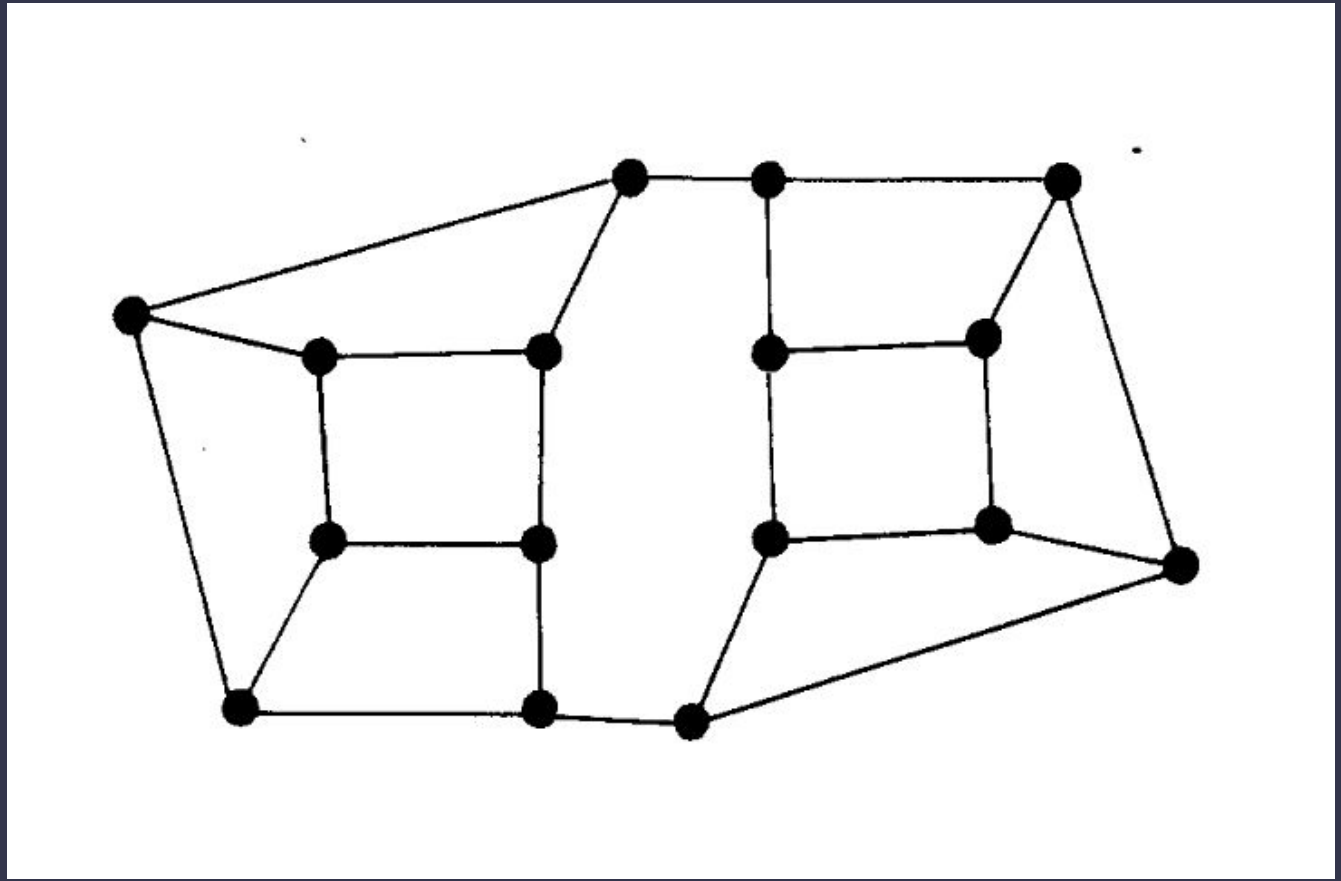
Practicals on Public Key Cryptography



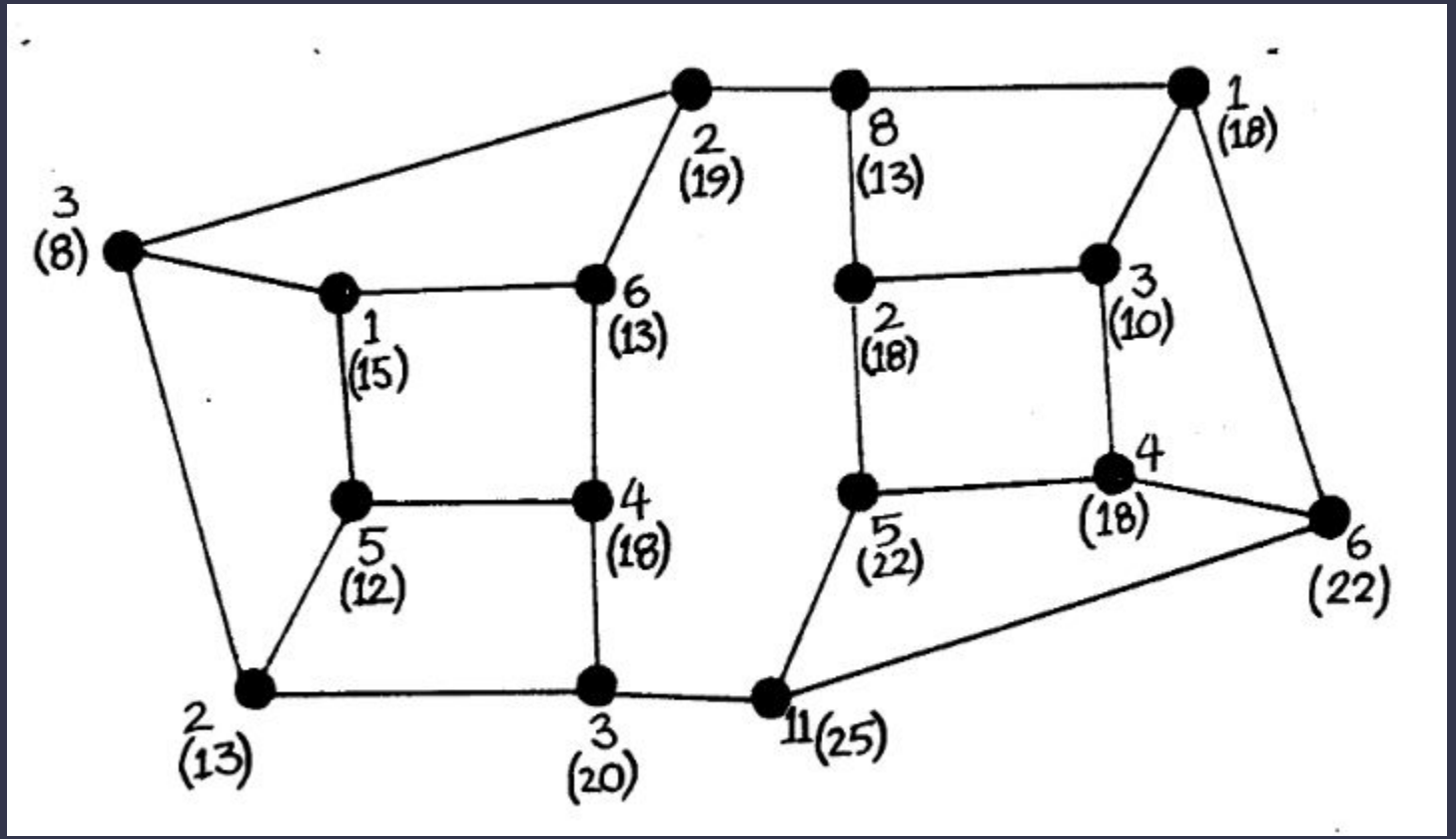
[Click me for GIF](), if the video doesn't work

Practical from: https://classic.csunplugged.org/activities/public-key-encryption/
The book: "Computer Science Unplugged" ©Bell, Witten, and Fellows, 199

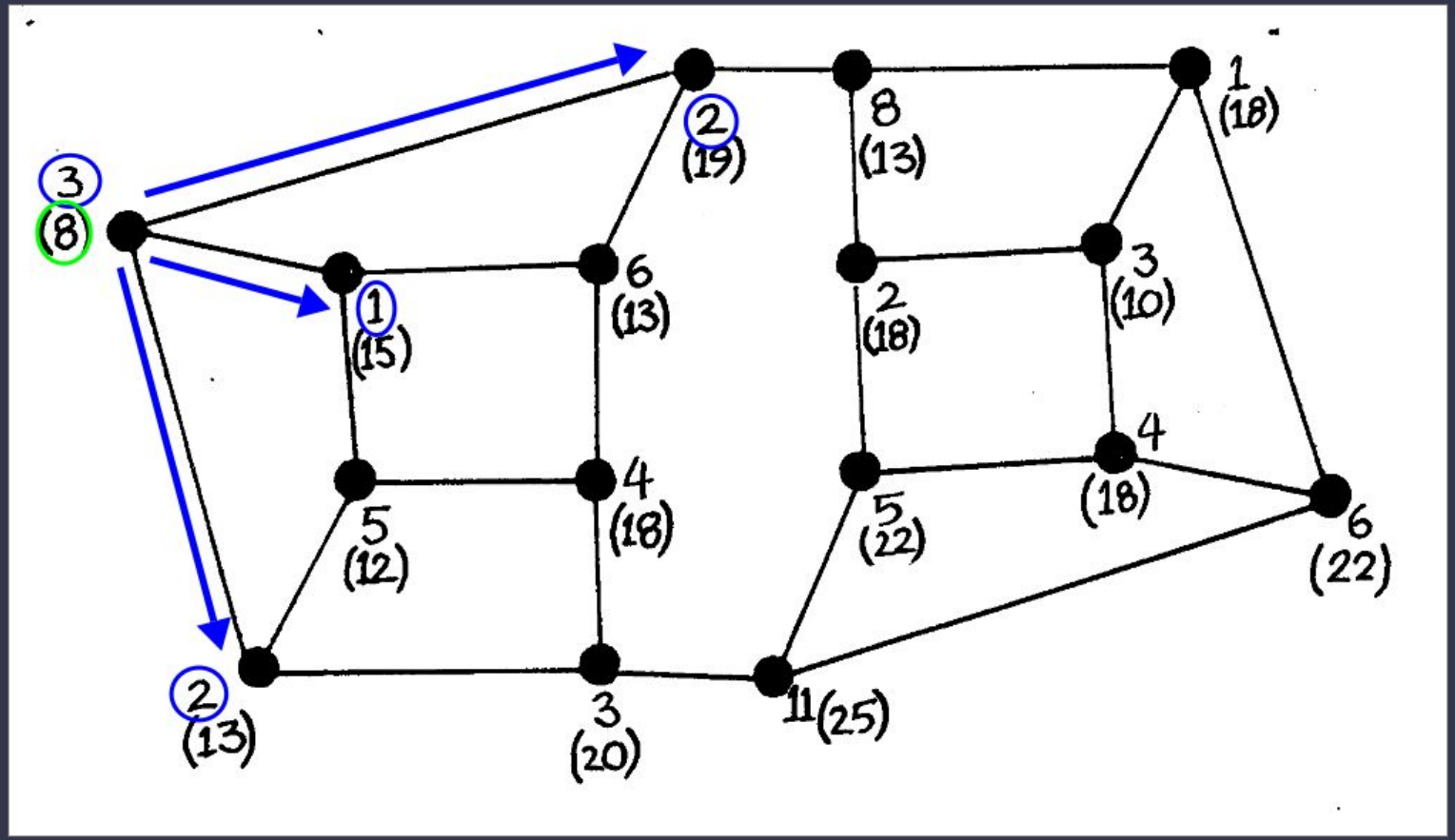
Demo: Bill's public map



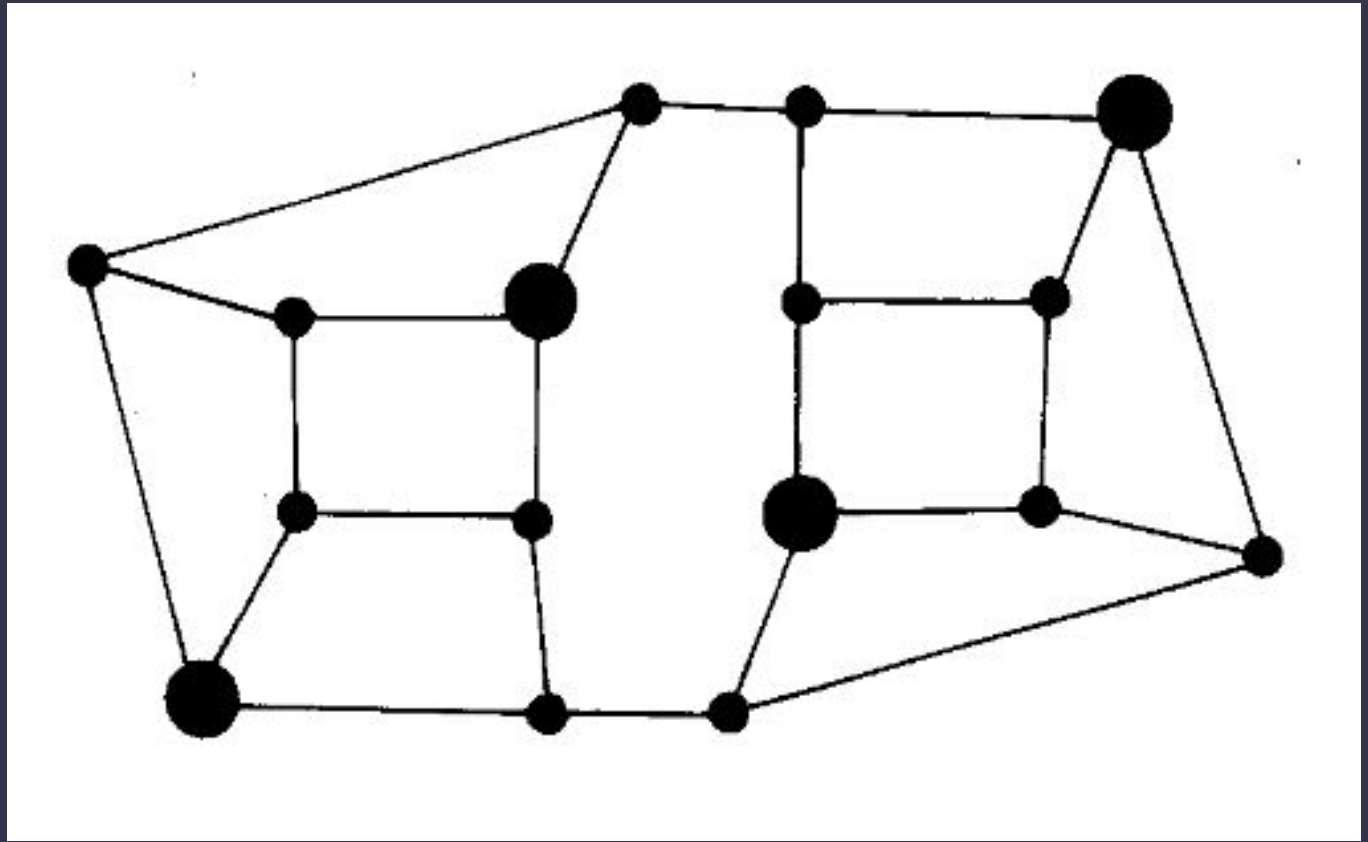
66



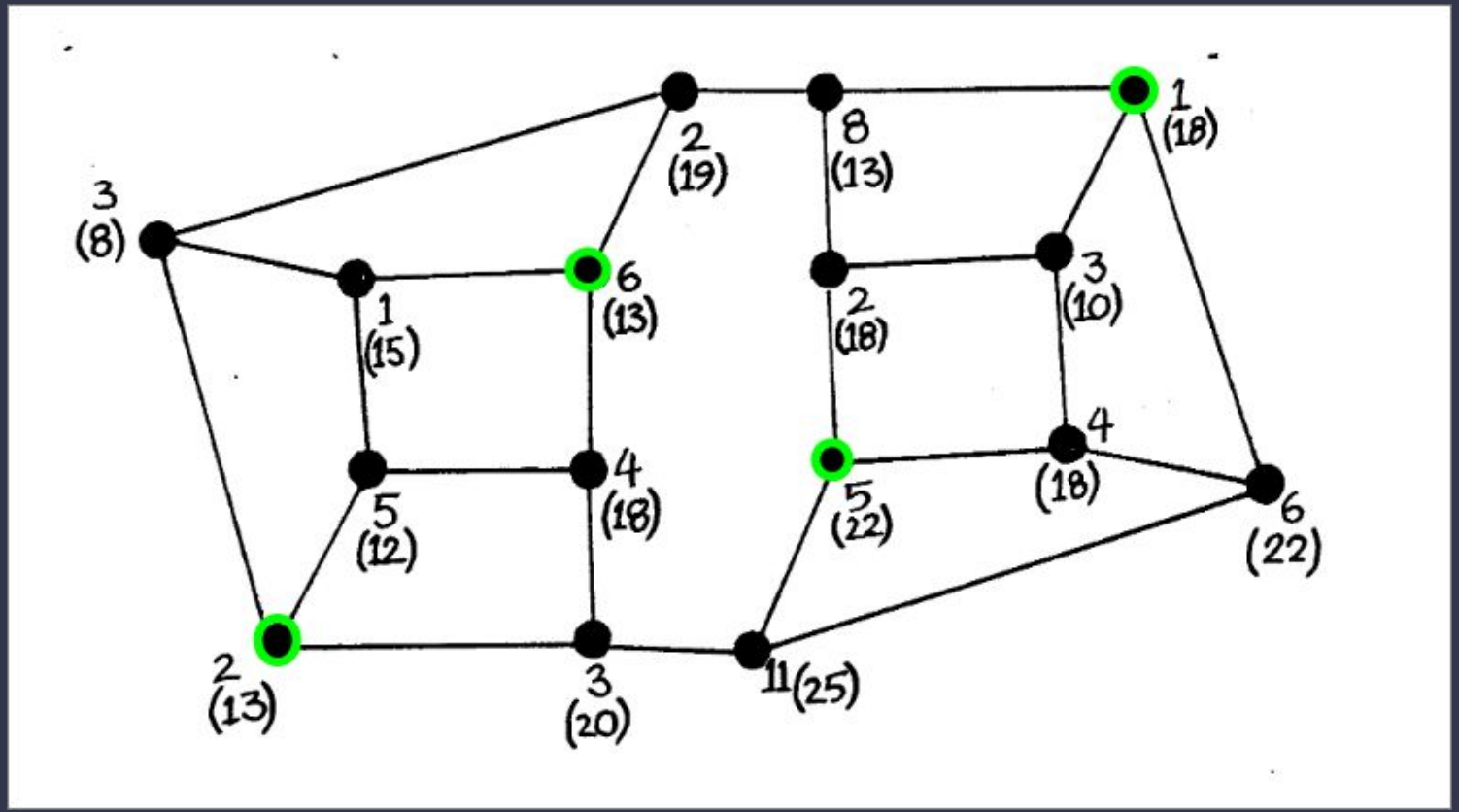
66



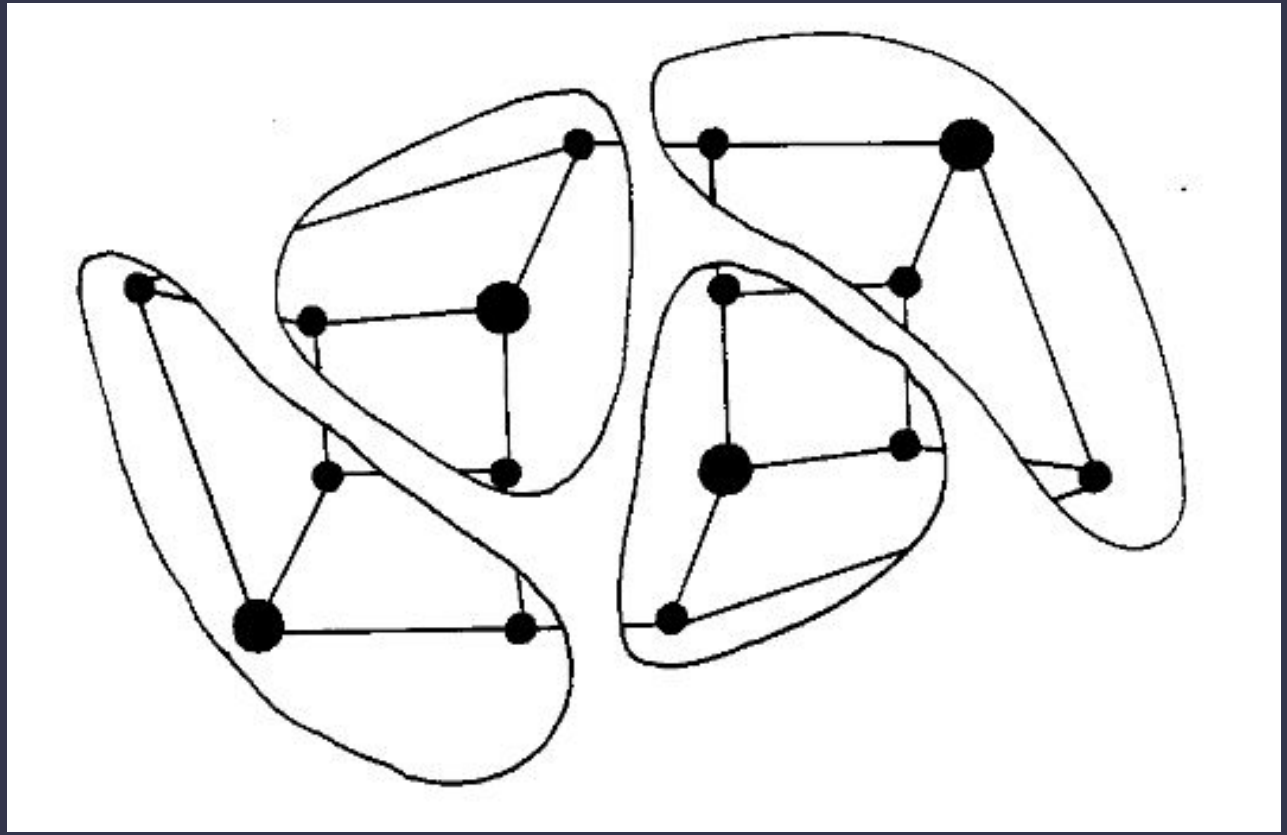
Demo: Bill's private map



Demo: Bill's private map



How it works



Practicals on Public Key Cryptography

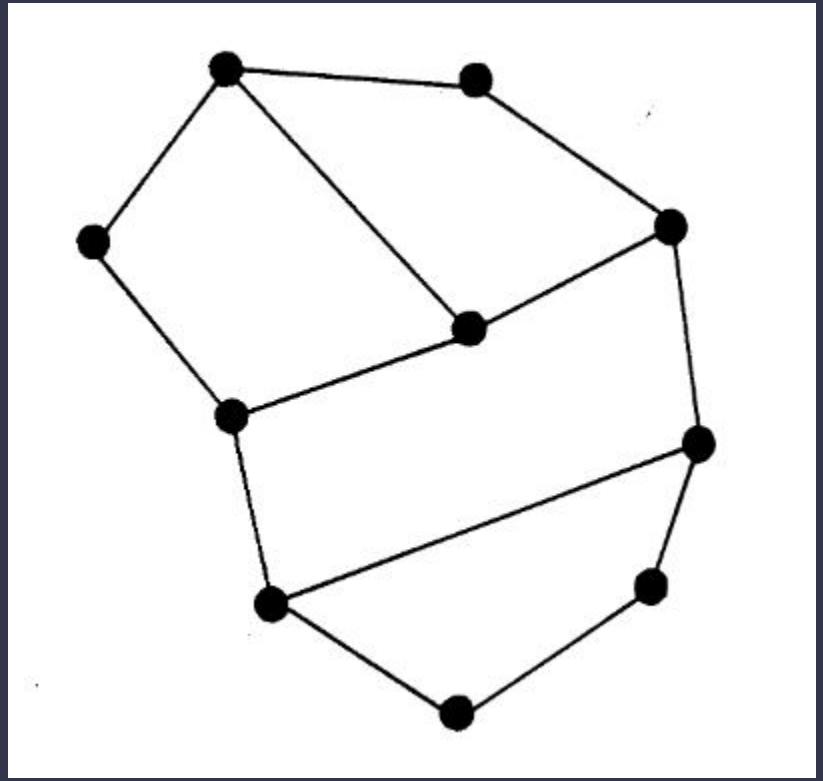
Instructions:

1) Decide which number Amy's going to send. Can be any number, but choose between 20-60 for simplicity.
2) Now on the public map, assign numbers to each "dot" such that the sum of all dots will be equal to the chosen number.
3) Now for each dot, assign it a new number in brackets, or on a fresh map such that it is the sum of all the "dots" it is connected to and itself.
4) Now remove the original number, and only keep the number in the brackets. This is our encrypted map/message.
5) Try and give it a different team and see if they can figure out your original number!

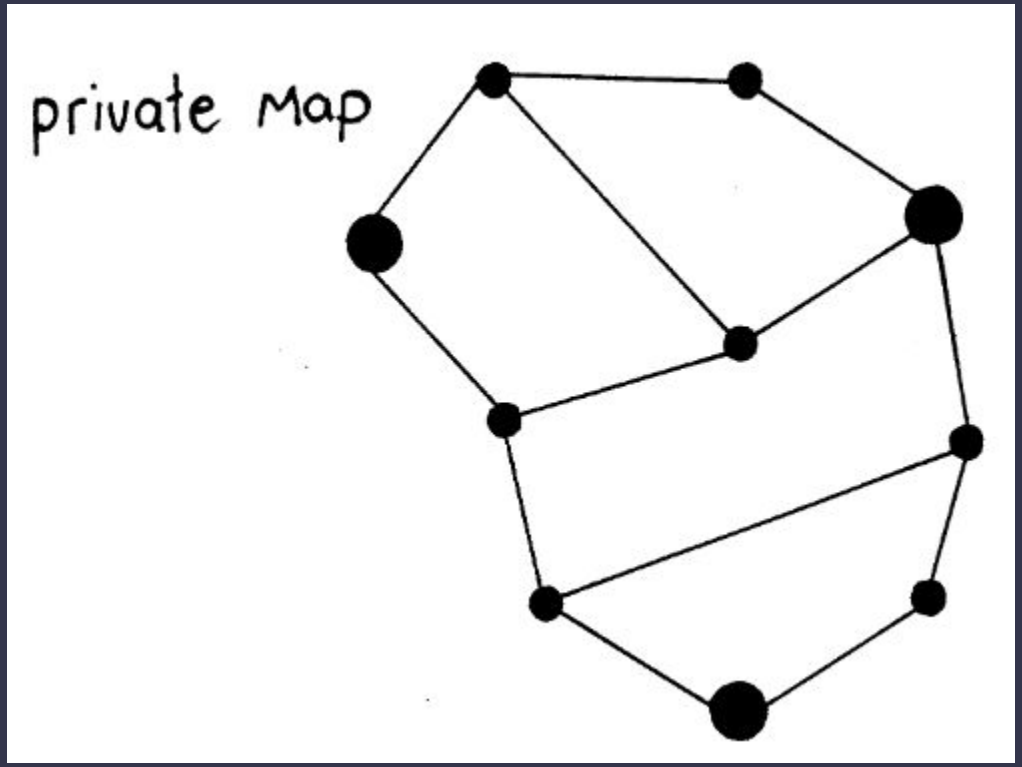
With the size of our map, it would be possible to brute force it, but by increasing the number of intersection of our nodes to 100, it would be unbreakable!

Practical from: https://classic.csunplugged.org/activities/public-key-encryption/
The book: "Computer Science Unplugged" ©Bell, Witten, and Fellows, 199

Practical: public map



Practical: public map



Useful links

Here are some links if you would like to learn more about anything I've covered today:

Videos:
RSA-129 by Numberphile - https://youtu.be/YQw124CtvO0
The Elliptic Curve by Computerphile - https://youtu.be/NF1pwjL9-DE
Also Computerphiles video discussing backdoors of the Elliptic Curve if you're interested - https://youtu.be/nybVFJVXbww

Websites:
Elliptic Curve - https://cryptohack.org/challenges/ecc/
RSA - https://cryptohack.org/challenges/ecc/

Upcoming Sessions

What's up next?
www.shefesh.com/sessions

12/03 - Bletchley Park

13/03 - Hardware

...

Hoodies are available (see discord or SU website)

Thanks for coming!

www.shefesh.com