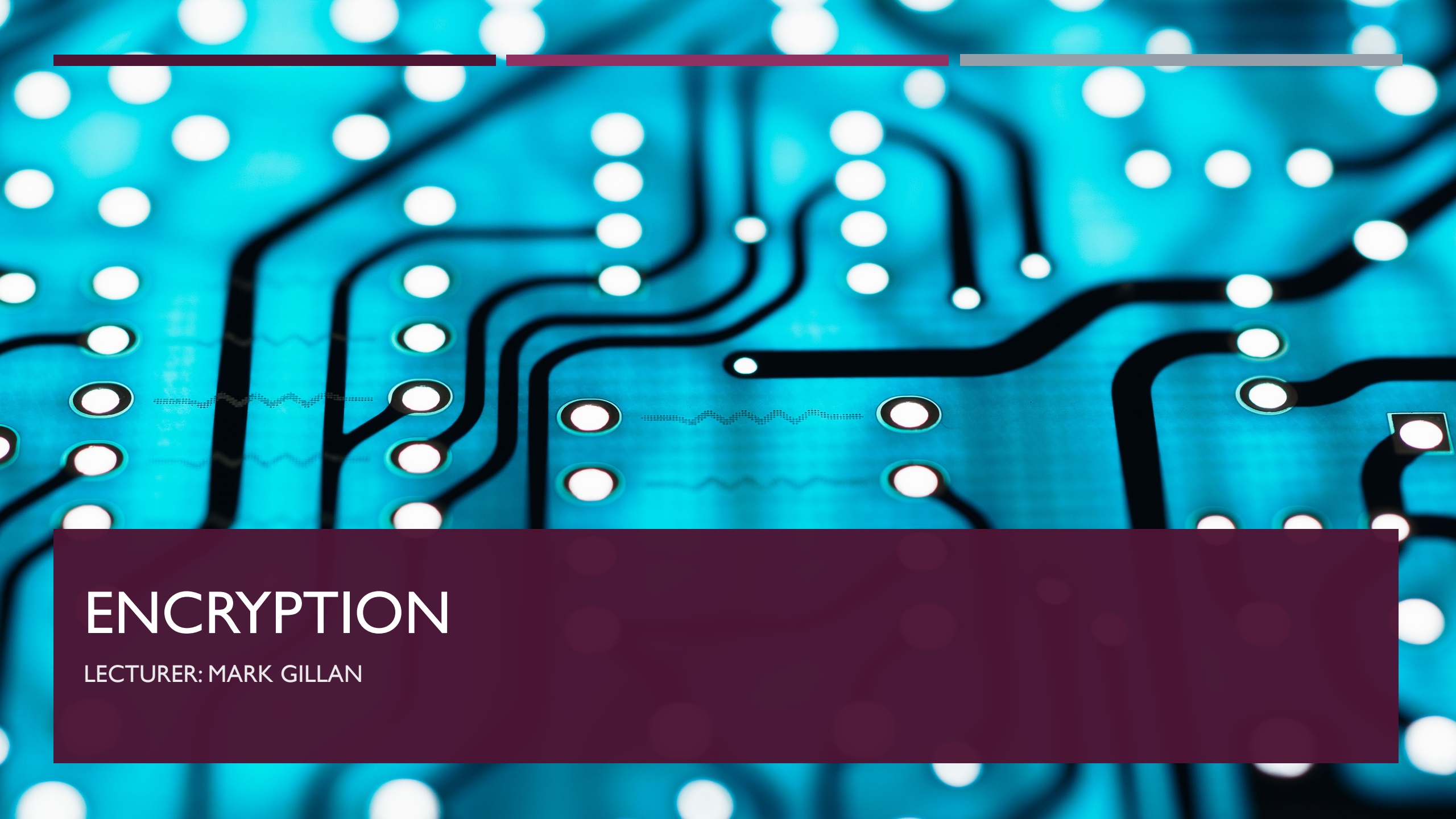


ENCRYPTION

LECTURER: MARK GILLAN

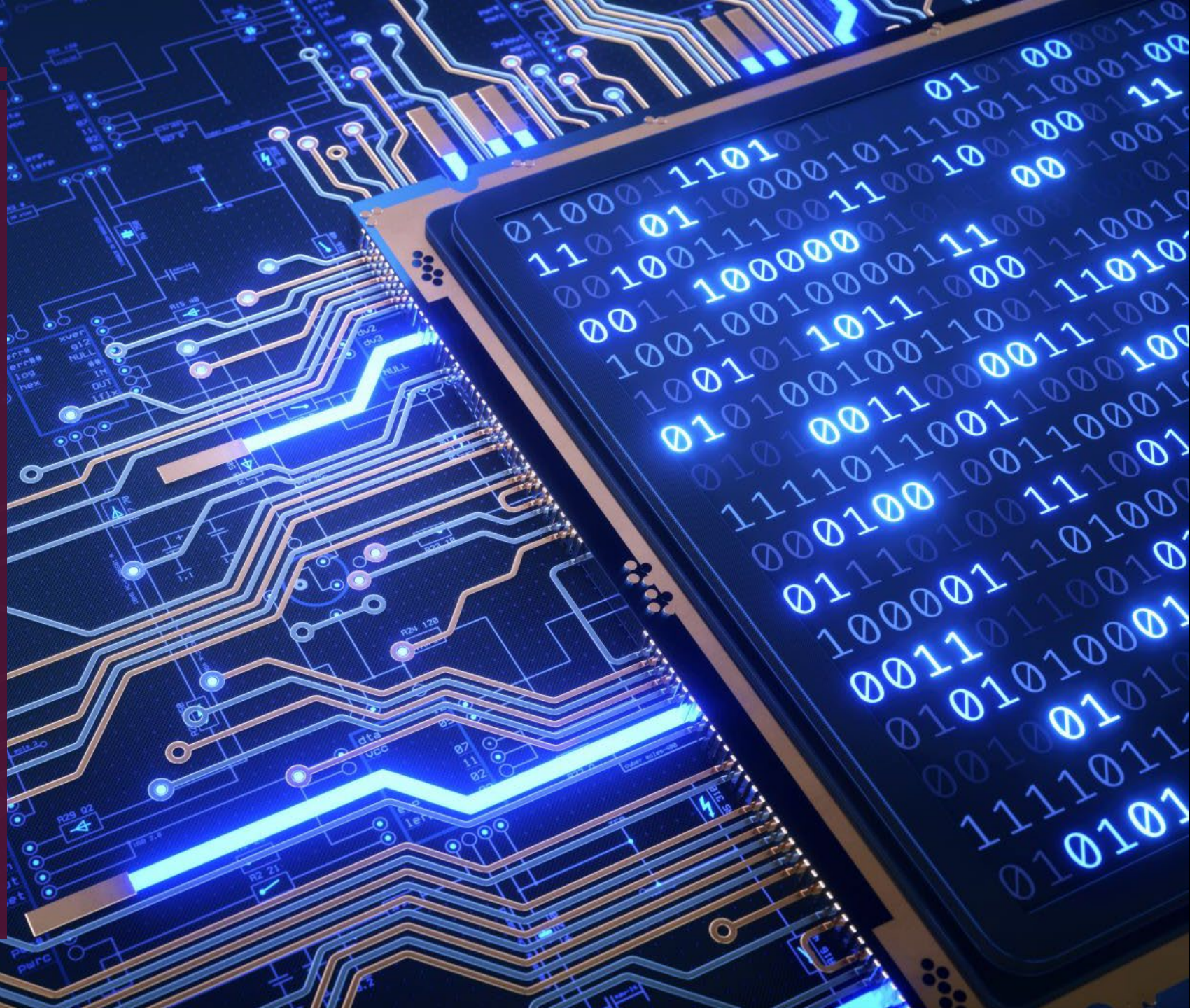
ENCRYPTION

Encryption refers to the process of converting a piece of plaintext into an encoded version that is unreadable to the human eye. The message's recipient on the other side requires a decryption key, which can then be used to decode the message back to plaintext.

Encryption is an extremely important technology for securing data. Particularly for data that is being transmitted over a network like the internet.

THIS LESSON YOU WILL LEARN ABOUT:

- The purposes of encryption used on data at rest.
- The purposes of encryption used on data in transit.



ENCRYPTION OF DATA AT REST

DATA AT REST

- By “data at rest” we’re referring to data that is stored on your computer. Data at rest is usually encrypted using symmetric encryption. This means that the same key is used to encrypt and decrypt the data.
- There are many different examples of encryption being used on data at rest. For example …

SAFE PASSWORD STORAGE

- Websites like Facebook require us to choose a password which they will store on their servers. If the website's servers are hacked, they could gain access to all the user details, including the password.
- This would be a disaster as most people use the same password on multiple websites which would mean an attacker could access masses of confidential data.
- This is why stored passwords should always be encrypted. This way if a hacker accesses the website's server, they will only have the encrypted password, which means they won't be able to use it.

DIGITAL RIGHTS MANAGEMENT (DRM)

- Digital rights management refers to a technology which attempts to control access to copyrighted material. DRM often uses encryption to protect copyright material in this way.
- So, for example, a movie may be encrypted, and the end user will require a decryption key in order to watch the movie. This might be provided through online authentication, or by being built-in to your Blue-Ray player

FILE, FOLDER & DISC ENCRYPTION

- Encrypting files, folders and discs is sometimes used where greater security is needed.
- For example, if you're storing confidential data, such as financial records, on a shared computer, the device could be used by people who shouldn't have access to that financial data. We, therefore, need some way of preventing others from accessing that data on the device.
- We do this by encrypting specific areas of our computer so that the other users of the computer system will not be able to access them.

FURTHER THOUGHT

If stored passwords are encrypted, how can the password we enter to log in be compared to ensure we've entered it correctly?

ENCRYPTION OF DATA IN TRANSIT

DATA IN TRANSIT

- Data in transit is data that is being transmitted between two devices over a network. Data in transit is usually encrypted using asymmetric encryption. This means that a different key is used to encrypt and decrypt the data.
- There are many different technologies we use when encrypting data when being communicated over a network. We'll look at some of these …

BUILT INTO DEVICES

- Many devices, particularly mobile devices like smartphones and tablets, come with built-in encryption. This encrypts our data on our mobile devices, including messages we send. This provides great security for our device which is needed as we store and send so much confidential data on them nowadays.
- This has been a big story in recent years with the FBI wanting Apple to decrypt data, including messages, stored on the iPhone of the perpetrators of a terrorist attack.

THE ONION ROUTER (TOR)

- TOR is a method for individuals to use the internet with anonymity. TOR encrypts the data multiple times, which then passes it through multiple relay servers which each remove a layer of encryption. Once each layer is removed the original data can then be passed onto the destination.
- The amount of encryption and relaying of data to slowly remove it makes finding the original source of data impossible (without exploiting some other vulnerability) so users are completely anonymous, hence why it is used and associated with some very nefarious uses of the web.

VIRTUAL PRIVATE NETWORK (VPN)

- A VPN creates a secure connection over a public network (the internet) through the use of encryption. This works by connecting to a VPN server, where the data between your computer and that VPN will be encrypted using asymmetric encryption technology such as IPsec or SSL.
- VPNs are commonly used by businesses to allow users to access the businesses local area network securely while away from the office. The business will have a VPN server that you can connect to and then that VPN server will have a connection to the company's LAN.

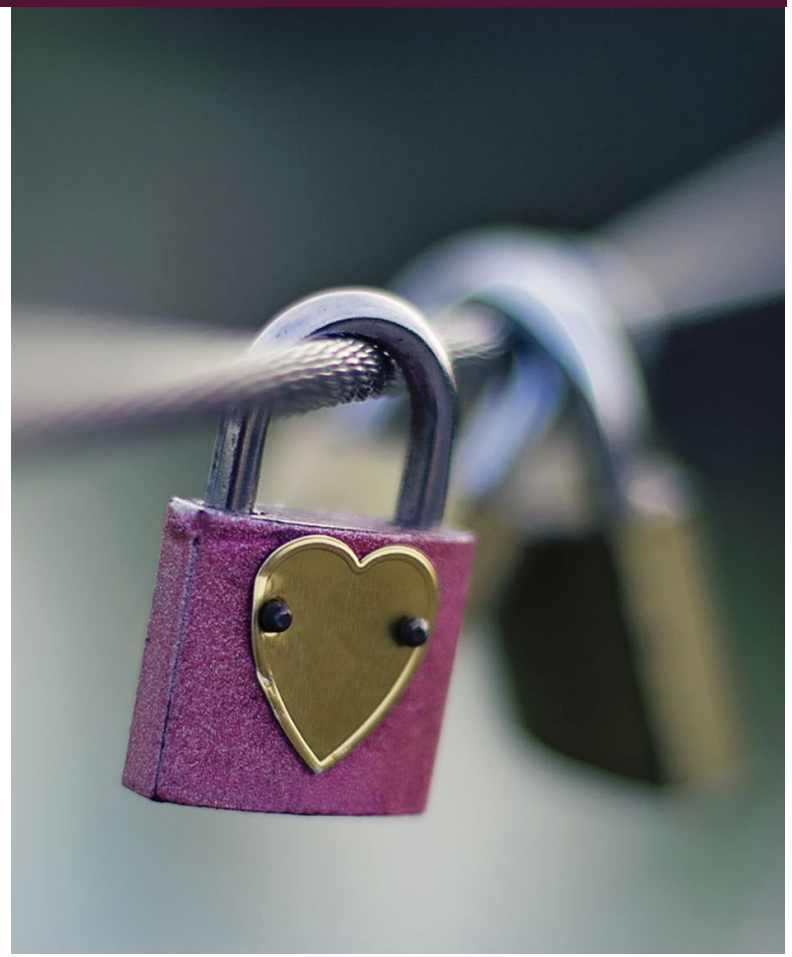
DIGITAL CERTIFICATES & CERTIFICATE AUTHORITIES

- A digital certificate (or public key certificate) is an electronic document that verifies that the sender of a message over a network is who they say they are. It also provides the information the recipient requires in order to encrypt a response (i.e. the senders public key).

- A certificate authority issues digital certificates to organisations. When a browser receives a digital certificate, it will verify the identity of the certificate sender with the CA, so they know the data they're sending is going to the correct destination.

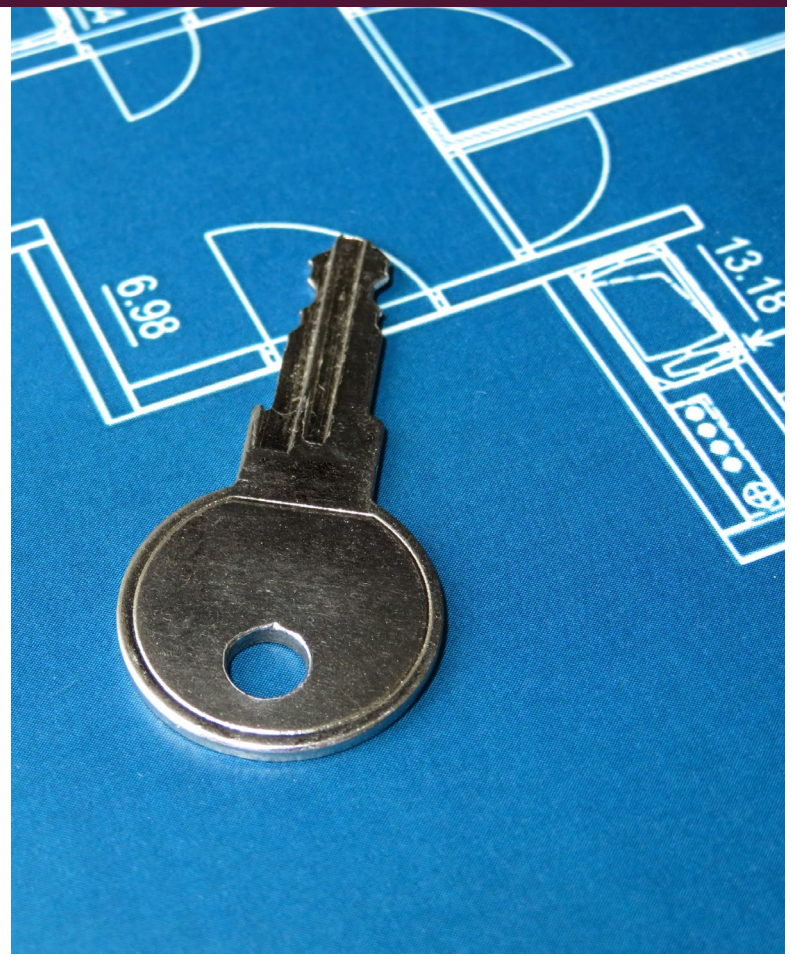
HYPER TEXT TRANSFER PROTOCOL SECURE (HTTPS)

- HTTPS is communication protocol that uses TLS or SSL encryption to securely transmit data through a web page.
- For example, when purchasing an item online we enter our card details into a web form. If the website uses HTTPS then the data we submit will be encrypted and so if a malicious user intercepted the data while it is transmitting to the web server, it would be completely unreadable.
- Without this technology, if the data was intercepted it could be read and used to steal money from us.



PUBLIC/PRIVATE KEYS

- When using encryption on data during transit, a different key is used to encrypt the data as that which is used to decrypt the data. These two keys are known as the public and private keys.
- Data that we are sending will be encrypted using the recipients public key. The sender will have access to that key because it is "public" and so anyone can access it. Usually, it is shared through the digital certificate.
- The recipient can then decrypt the message with their private key. This is not shared with anyone and is kept securely on the server.
- The public key cannot be used to decrypt the message, only the private key can.



FURTHER THOUGHT

- Why do we not use symmetric encryption when transmitting data? Keep in mind this means the same key is used to encrypt the data is used to decrypt it.

LESSON SUMMARY

- Stored passwords on servers are encrypted to protect against hackers who might gain access to user data.
- DRM uses encryption to restrict access to copyright content. You need a key to decrypt the content in order to access it.
- Files, folders and discs can be encrypted to ensure data stored on a shared computer is still secure.
- Encryption can be built into devices, especially mobile devices, so that data stored on them and transmitted in messaging apps are secure.
- TOR provides anonymous browsing through using multiple layers of encryption which are removed one-by-one as it moves between relays.
- VPNs provide a secure connection over the internet. You have an encrypted connection to a VPN server, then the data can be passed on in plaintext.
- Digital certificates authenticate the sender of a message and provide the public key for a response to be encrypted. Certificate authorities will issue certificates and verify the owner.
- HTTPS is a secure protocol that is used in web pages so users can send data to a web server that is secured through TLS or SSL encryption.
- In asymmetric encryption, we use a public key to encrypt data and a private key to decrypt it.