Security Precautions

Security Precautions

There are a number of security risks to computers, the data that they store and the data that is sent across the internet.

These risks include viruses, cyber attacks, and unauthorised malicious access to computer networks. Unauthorised access can be gained by hacking, or via social engineering such as phishing.

The video on the next slide explains these risks.

Security Risks

Watch this video to learn about the risks that are faced online.

Security Precautions

There are precautions that you can take to protect your computer or network from these risks. At National 5 you need to know about two precautions:

- Firewalls
- Encryption of data

Encryption

Encryption protects data even if it is accessed by a malicious or unauthorised entity. Data needs to be encrypted in two states:

- **in transit** (while it is being sent across the internet)
- **at rest** (while it is being stored in databases or data warehouses)

Data in Transit

We saw that the internet is public, and that packets are sent from router to router with no pre-determined path – it is possible that unauthorised entities can intercept and have access to the data.

We have to make sure that data cannot be read and understood by anyone other than the intended recipient.

Data at Rest

Hackers will often gain access to computer systems with the intention of stealing data from databases or data warehouses.

Data should be encrypted so that even if hackers steal the data, they cannot read and understand it, or sell it for profit.

How Does Encryption Work?

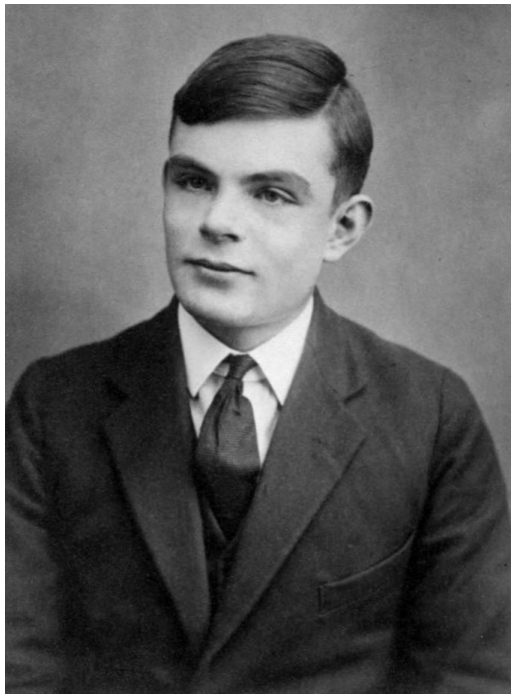
Watch this video up to 5:45 to see how encryption works.

Encryption Through History

Encryption has been used throughout history, particularly to keep military strategies secret. The Caesar's Cipher was named after Julius Caesar and is the method he supposedly used to send instructions to his army.

During World War II, the German military used encryption for the same purpose, using the Enigma machine to encrypt communications.

Alan Turing and his team worked to break Enigma and helped the allied forces to victory.



Types of Encryption

There are two types of encryption:

- Symmetric encryption
- Asymmetric encryption

These encryption techniques use a **key** to scramble the data and create **ciphertext**, which looks like nonsense and is impossible to understand.

There is some incredibly complex maths involved in encryption, which you are not expected to know for National 5.

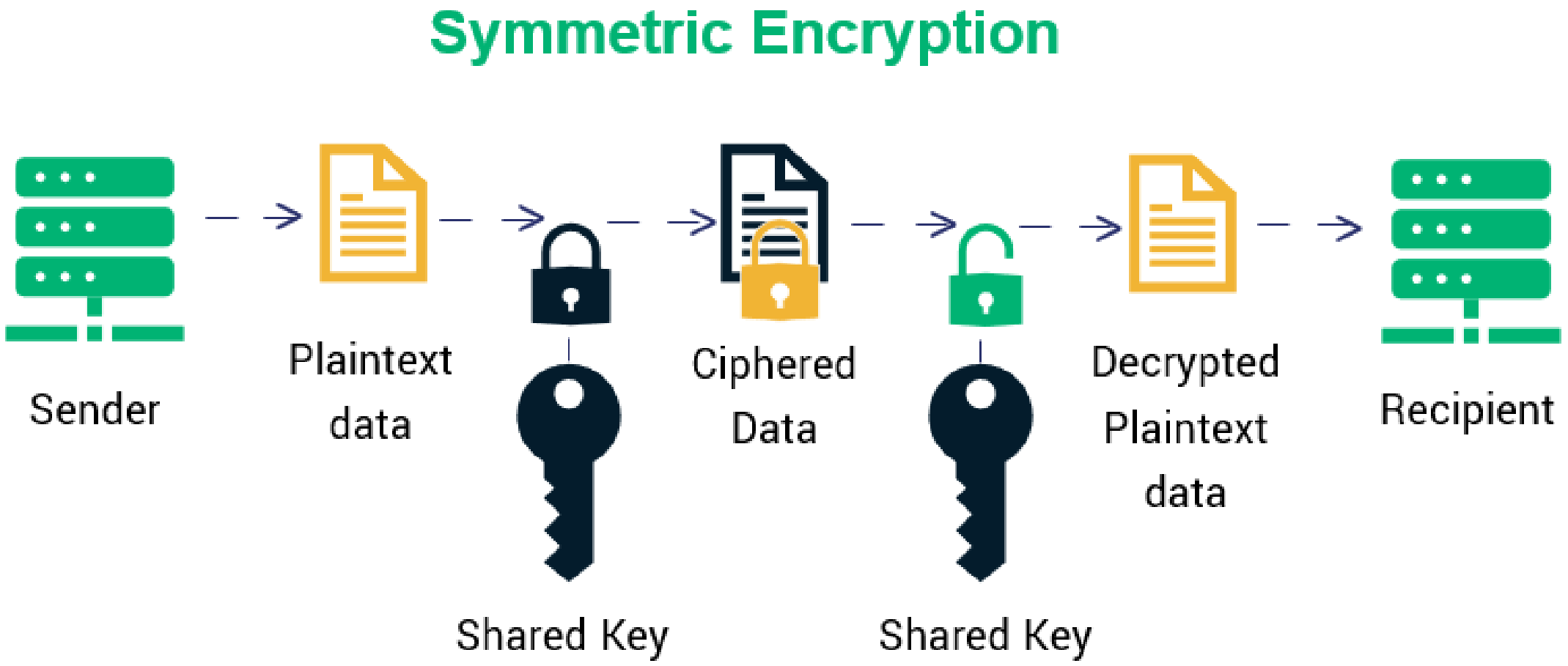
Symmetric Encryption

Symmetric encryption is when a **single, secret, shared key** is used to encrypt and decrypt data.

The two entities that are communicating must exchange the key, but it can be difficult to keep the key secret when it's being sent across the internet, so symmetric encryption is usually only used to keep **data secure at rest**.

Symmetric encryption is faster and more efficient than asymmetric encryption, so it is usually used for **encrypting large amounts of data**, e.g. databases.

Symmetric Encryption



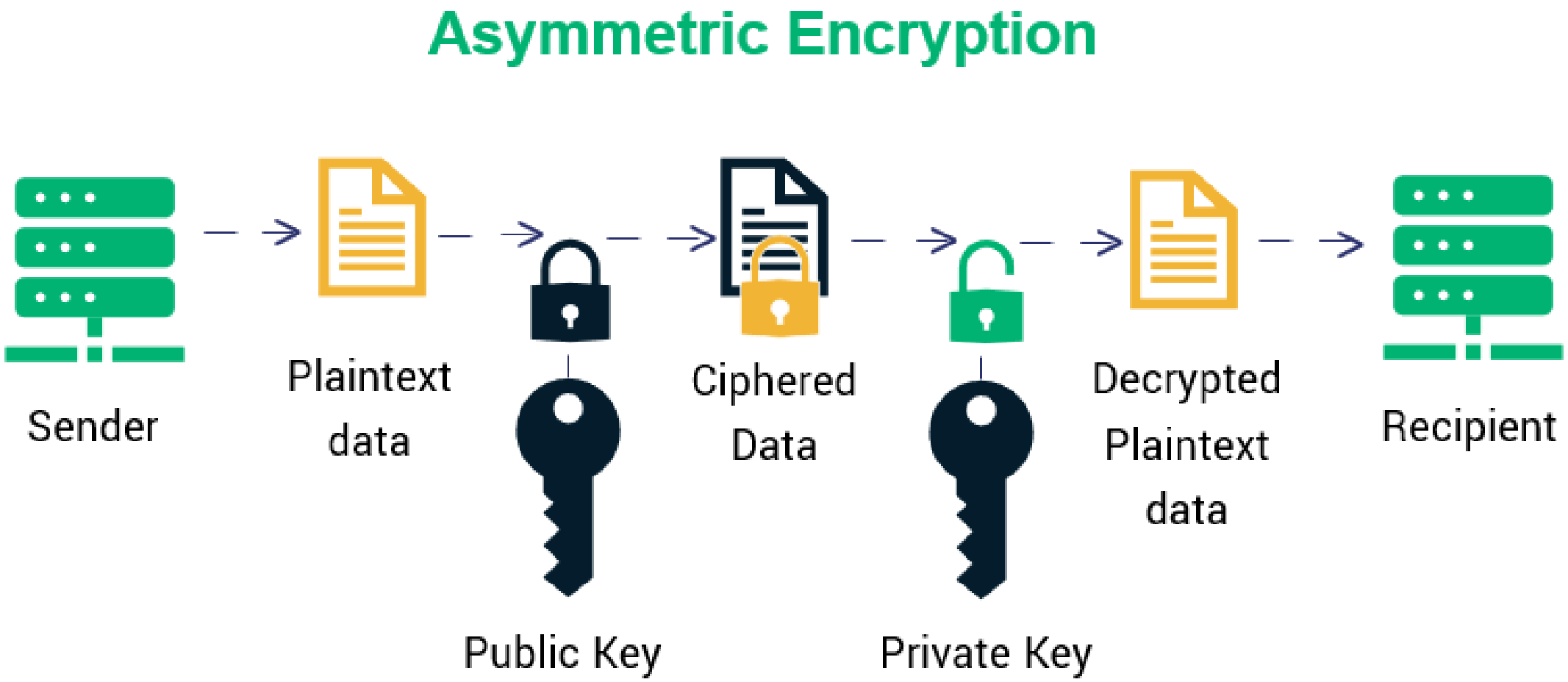
Asymmetric Encryption

Asymmetric encryption uses a **public key** **to encrypt data** and a separate, secret, **private key** **is used to decrypt**.

There is no need to exchange a secret key, so asymmetric encryption is considered much more secure and is usually used to keep **data secure in transit**.

Asymmetric decryption is a slow process compared to symmetric cryptography, so it is used for **encrypting smaller amounts of data**, e.g. IP packets.

Asymmetric Encryption



How is Your Data Protected?

Your data is regularly encrypted when you use the internet.

Whenever you see https or a padlock in the address bar of your browser, your details are encrypted before they are sent – you should check for this before you enter any personal data or bank details.

Your messages are often encrypted so that only the intended recipient can read them – this means that Facebook cannot read your WhatsApp messages.