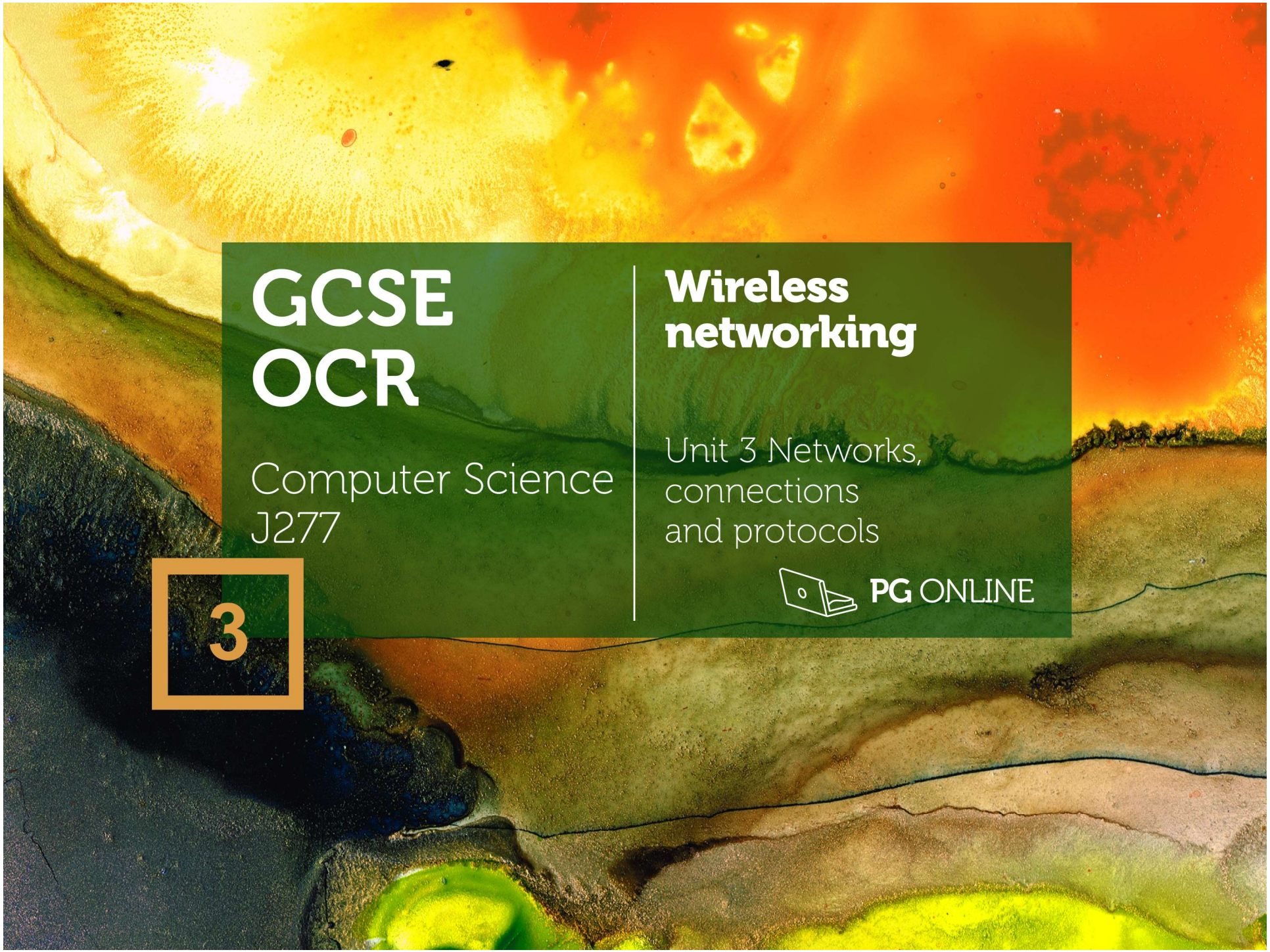

GCSE
OCR
Computer Science
J277
3
Wireless networking
Unit 3 Networks, connections and protocols
PG ONLINE

Objectives

- Understand wireless modes of connection, including:
  - Wi-Fi
  - Bluetooth
- Explain the need for Wireless Access Points to create wireless hotspots
- Understand how encryption is used to secure data across network connections

Starter

- How are wireless technologies used by people and electronic devices today?
  - Name at least **six** different products they are used in

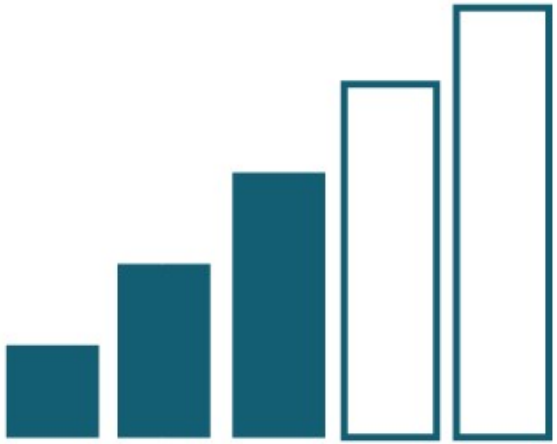
Starter

Answers

- Wi-Fi
  - Laptops, some desktops, tablets, smartphones, many IoT devices such as smart speakers and smart lights
- Bluetooth
  - Wireless headphones, connecting phones to car entertainment systems, keyboards

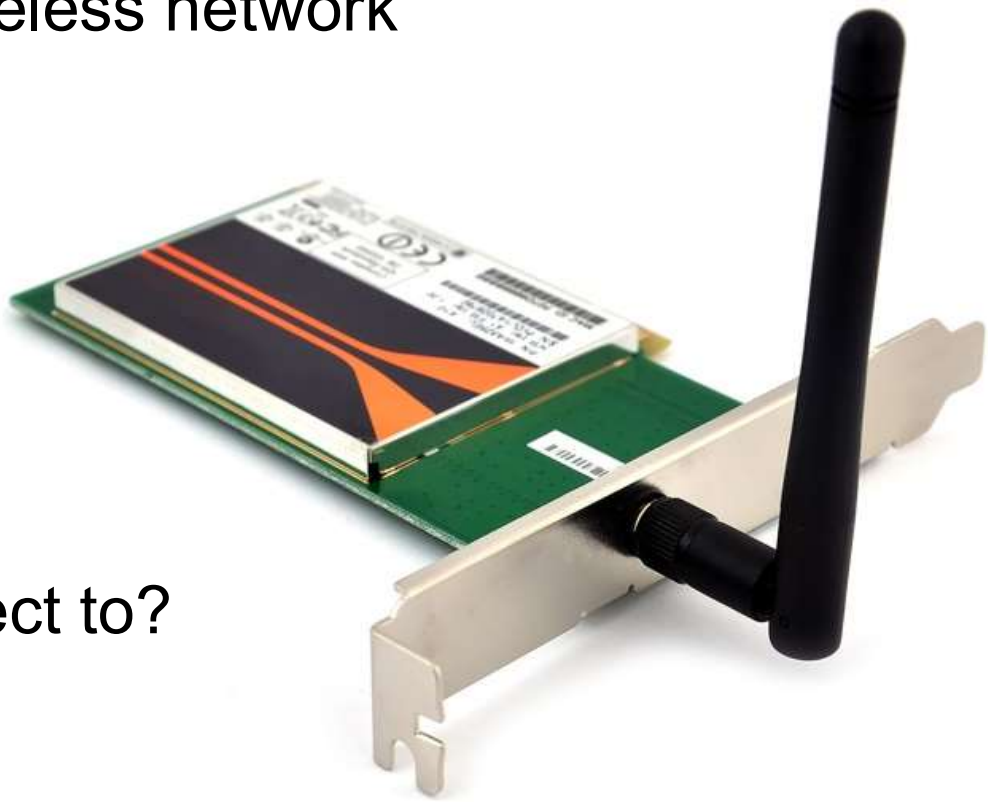
Wireless transmission

- Commonly uses radio waves for communication
- Susceptible to interference from objects and other nearby electronic or radio devices
    - How does your wireless signal strength vary throughout your own home or school?



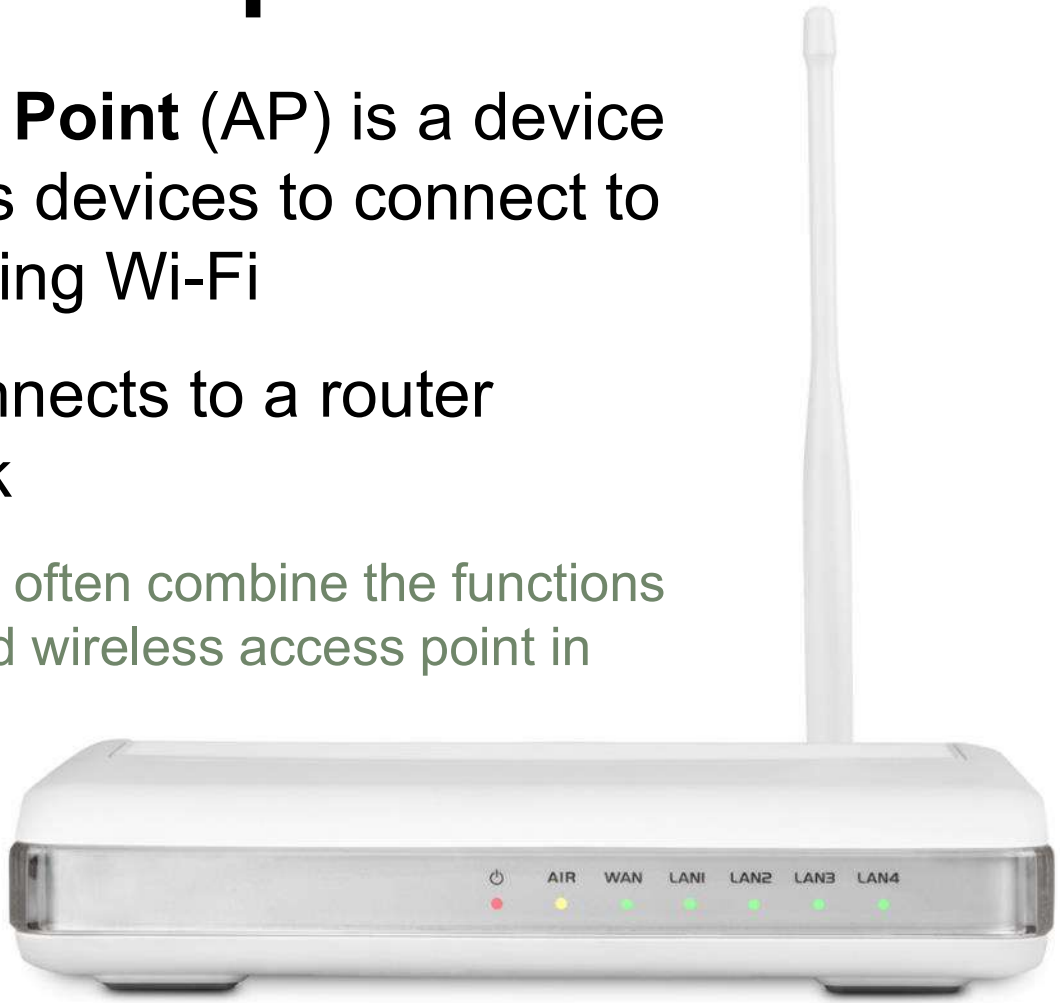
Wireless NICs

- Built into every networked device capable of connecting to a wireless network
- These include:
  - PCs
  - Smart phones
  - Wireless speakers
- What does a wireless NIC connect to?



Wireless access point

- A wireless **Access Point** (AP) is a device that allows wireless devices to connect to a wired network using Wi-Fi
- The AP usually connects to a router via a wired network
  - Home Wi-Fi routers often combine the functions of switch, router and wireless access point in one box



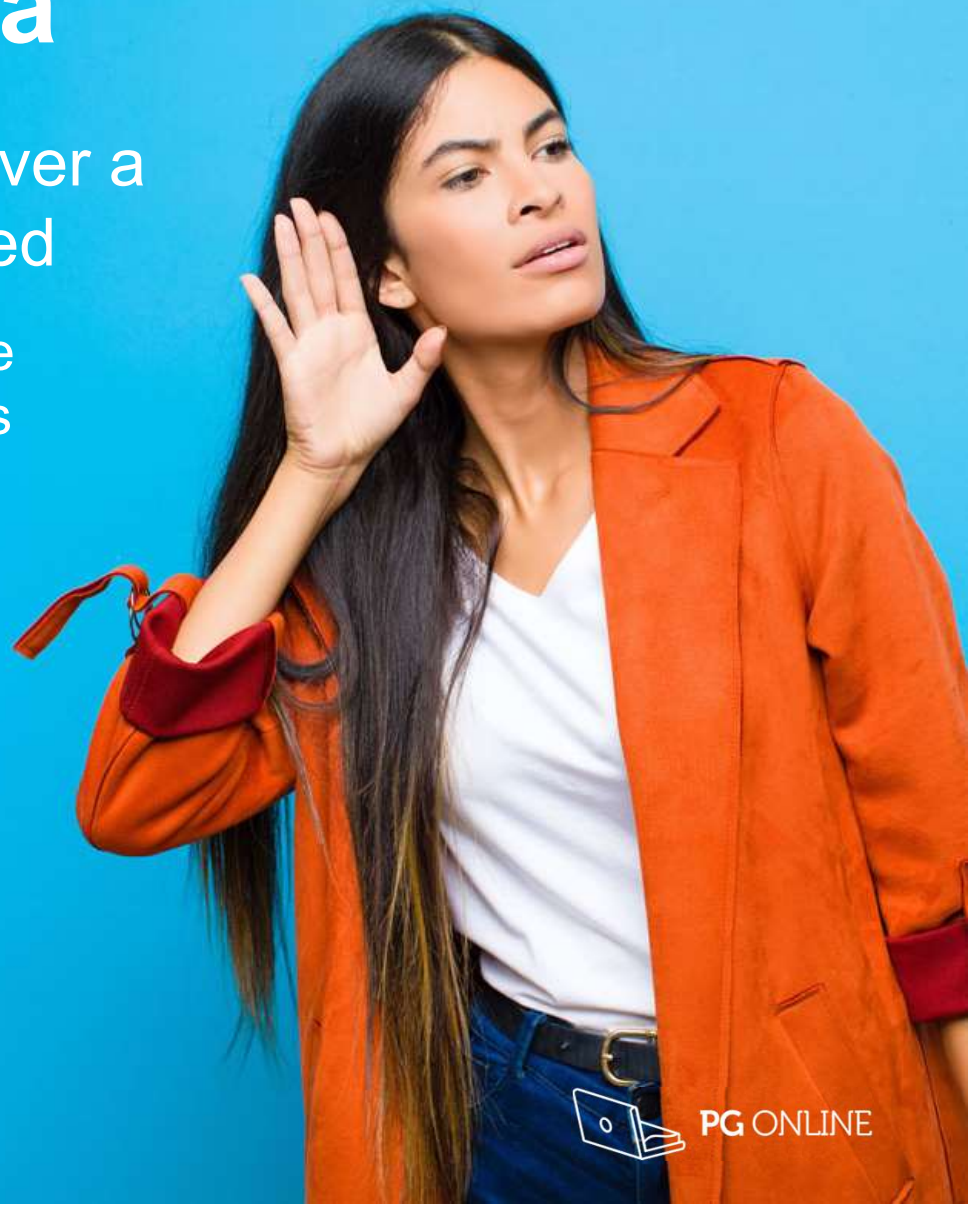
802.11 standards

- 802.11b/g/n uses the 2.4GHz frequency
- 802.11a/n/ac uses the 5GHz frequency

	Advantages	Disadvantages
2.4GHz	Greater range and coverage	More interference from other devices as this is a crowded frequency
5GHz	Less crowded space with 23 non-overlapping channels with higher data transmission rates	Less able to penetrate through walls

Intercepting data

- Data that is transmitted over a network can be intercepted
  - Any intercepted data can be read and understood unless measures are taken to prevent it from being interpreted
  - These measures are known as encryption



Worksheet 3

- Complete **Task 1** on **Worksheet 3**

Encryption

- Encryption is the encoding of data so that it can no longer be easily understood
- A simple shift cipher might encode "*Box345*" as follows:

"Box345" → Encryption algorithm  → "Dqz567"

Encryption terminology

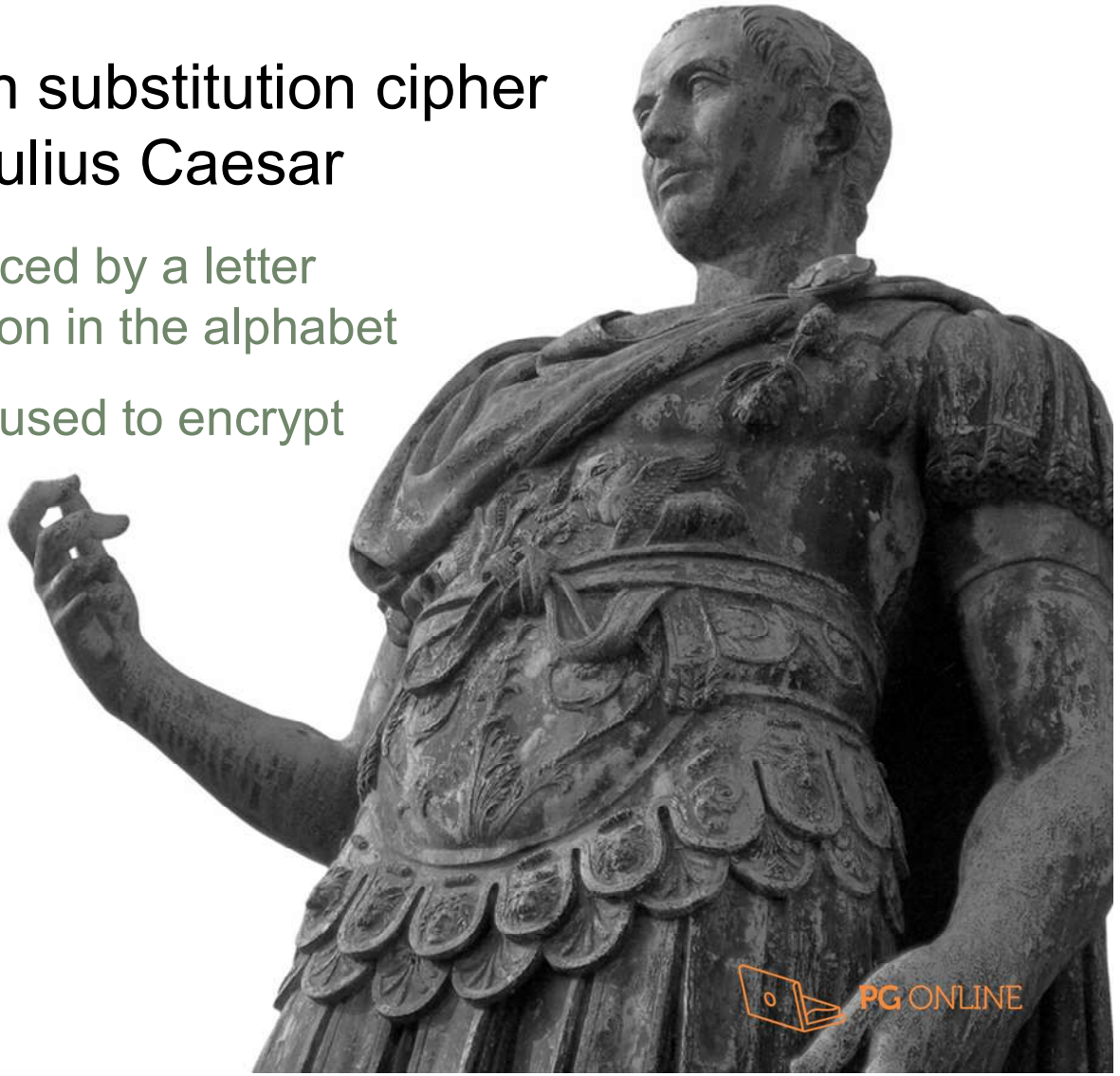
- Plaintext: the original message to be encrypted
- Ciphertext: the encrypted message
- Encryption: the process of converting plaintext into ciphertext
- Key: a sequence of numbers used to encrypt or decrypt, often data using a mathematical formula
- Encryption algorithm: the formula for encrypting the plaintext
  - Two inputs: **plaintext** and a **secret key**

Encryption techniques

- Private key (Symmetric encryption)
  - A single key is used to encrypt and decrypt a message and must be given to the recipient of your message to decrypt the data
- Public key (Asymmetric encryption)
  - Two keys are used - one (public key) to encrypt and the other (private key) to decrypt data
  - This is more secure as it means that you never have to send or reveal your decryption key

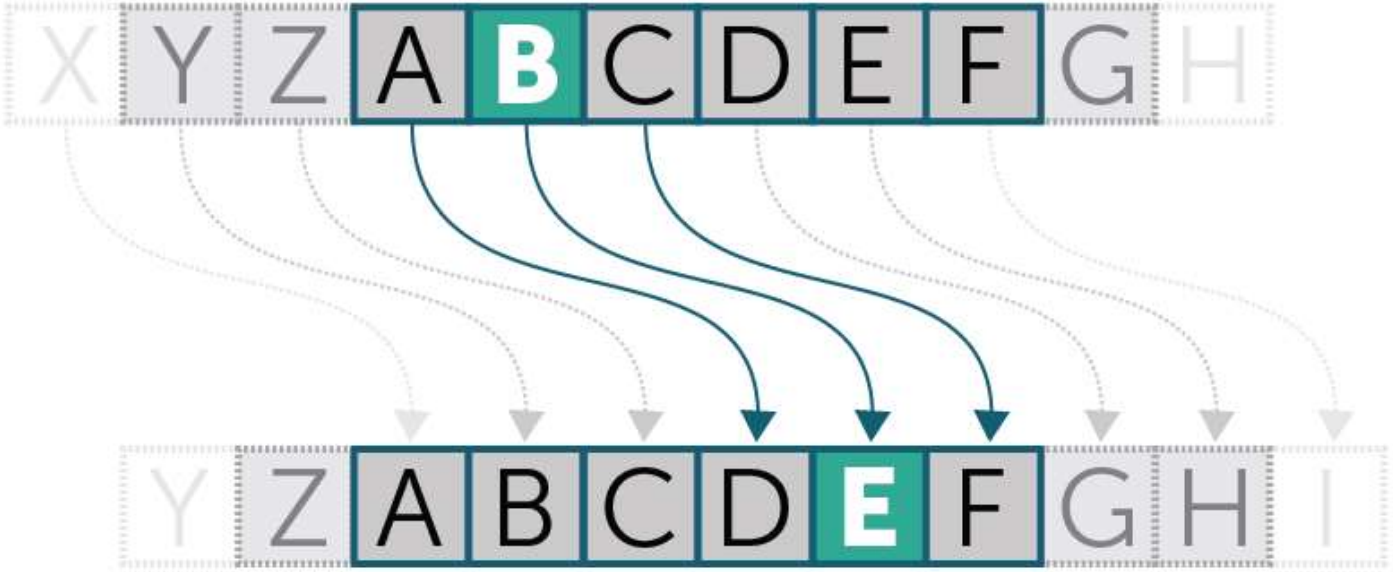
Caesar shift cipher

- The earliest known substitution cipher was invented by Julius Caesar
  - Each letter is replaced by a letter *n* positions further on in the alphabet
  - *n* is the key and is used to encrypt and decrypt the message
  - This is an example of **symmetric encryption**



Caesar cipher

- The Caesar cipher is most basic type of encryption and the most insecure
- Letters of the alphabet are shifted by a given number



Deciphering the code

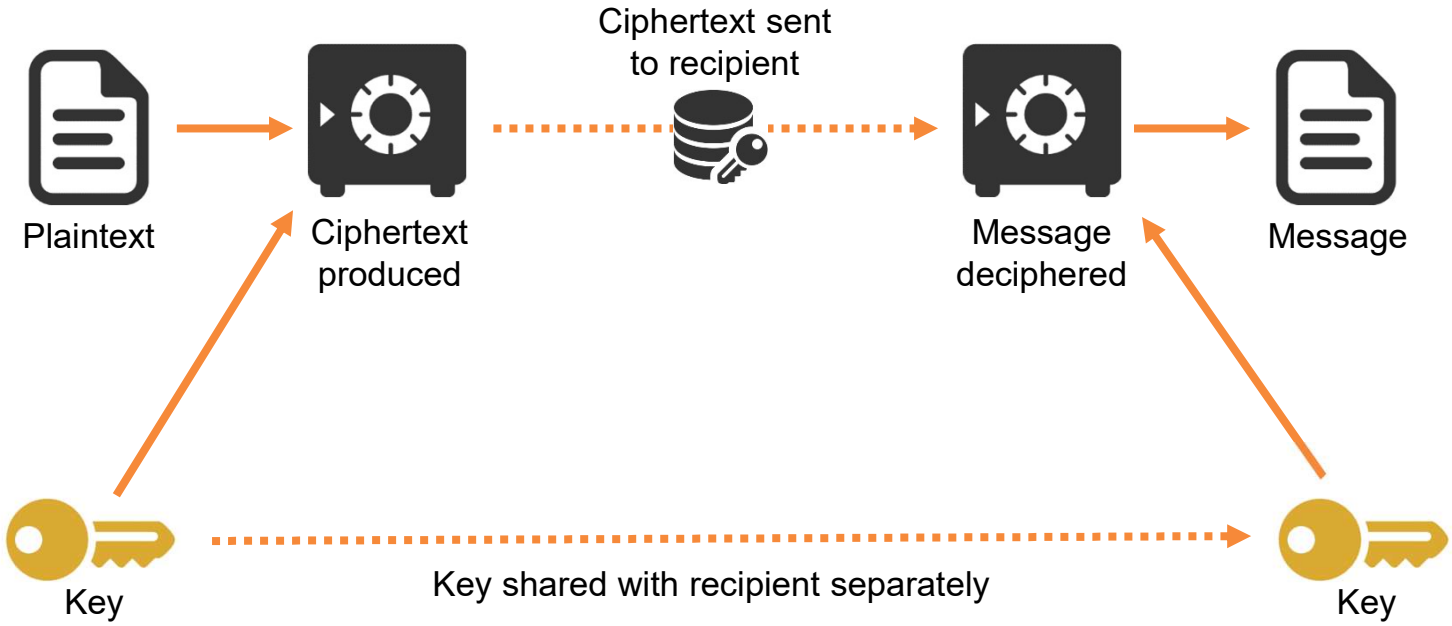
- **Key** = **Shift → 3**
- Decode "**DWWDFN DW GDZQ**"

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
↓														
D	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**

- Using a different key, crack the code for '**PCRPCYR**'

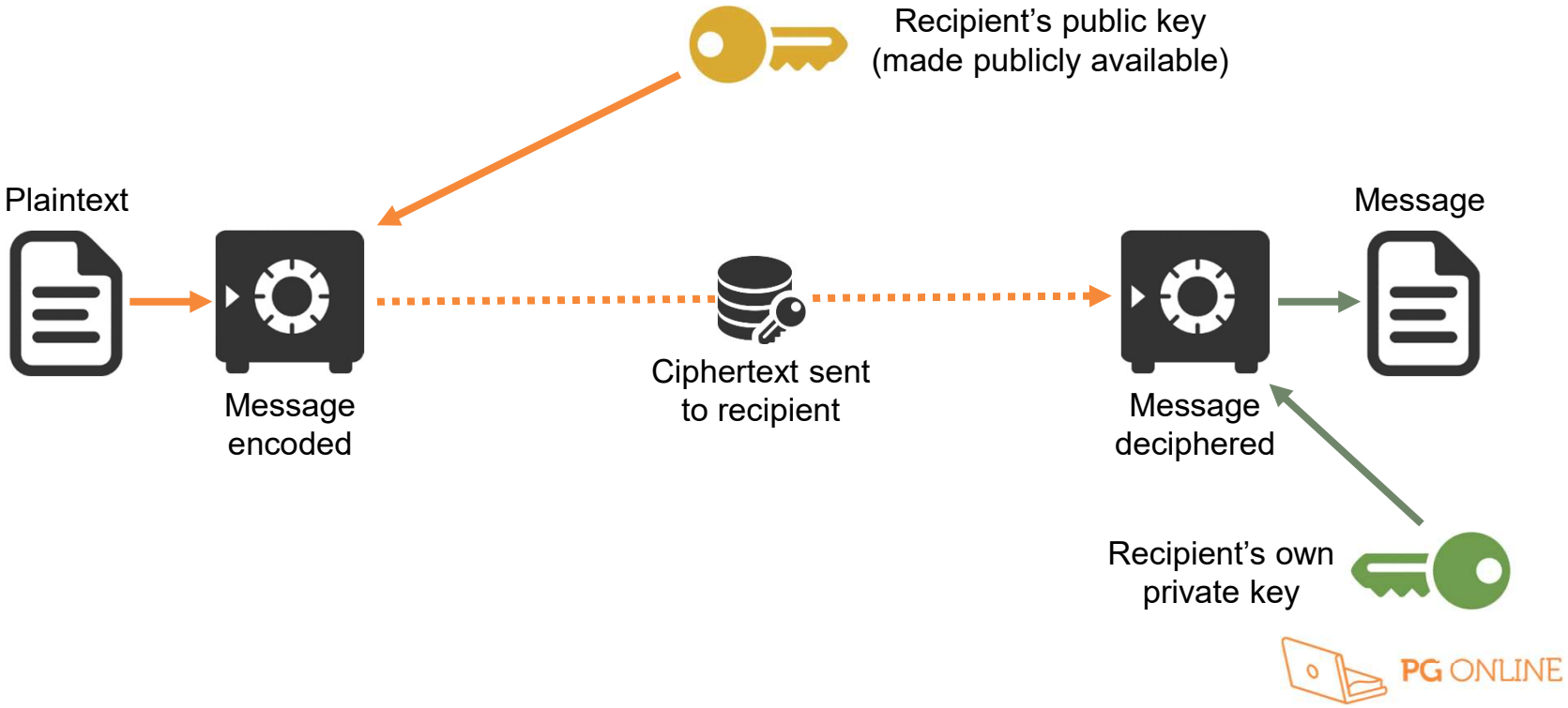
Symmetric encryption

- Same key used to encrypt and decrypt a message



Public key (Asymmetric) encryption

- Two keys are used: a public key known to everyone for encrypting and a private key for decrypting



Encryption in networks

- Wi-Fi is particularly vulnerable to eavesdroppers as the signal can be listened to from a distance
- Wired connections such as Ethernet and fibre optic are also vulnerable
    - What methods of encryption are used when using wireless networks?

Wireless encryption standards

- The most common wireless security standards are:
  - WEP (Wired Equivalent Privacy) and
  - WPA (Wi-Fi Protected Access)
- The WEP method of encryption is older and can be cracked in seconds
  - As such this standard should no longer be used to protect your home router
  - Instead you should use WPA or preferably the newer WPA2 encryption methods
- HTTPS should be used for websites as it encrypts data sent to and received from the site

Strong and weak encryption

- These terms are relative, but:
  - Encryption can be considered to be ‘strong’ when the useful lifetime of the encrypted data is less than the time taken to break the code
  - With weak encryption, the code may be broken in time to use the information, but it wouldn’t be worth the effort trying

Worksheet 3

- Complete **Task 2** on **Worksheet 3**

Plenary

- Discuss in a pair or threes how you use, or could use wireless networks and network security in your home, school and life. Make sure to use the following words at least once:

  - Wireless
  - Wi-Fi
  - Bluetooth
  - Wireless Access Point
  - Encryption
  - WEP
  - WPA / WPA2
  - HTTPS
  - Router
  - Switch

Plenary

Answers

- Possible answer:
  - We use a wireless router at home. This contains a switch, router and modem all in one box. All our mobile devices connect to the wireless access point with Wi-Fi. It is encrypted with WPA2. We don't use WEP as it is insecure. Where possible we try to connect to websites using HTTPS as this makes all data transmitted secure. Our TV and soundbar are connected to the box using Ethernet cables. Bluetooth is used to connect our headphone to smartphones.

Copyright

Licence agreement