# AQA Computer Science A-Level

## 4.9.3 The Internet

Concise Notes

**Specification:**

**4.9.3.1 The Internet and how it works:**

Understand the structure of the Internet.

Understand the role of packet switching and routers.

Know the main components of a packet.

Define:

- router
- gateway

Consider where and why they are used.

Explain how routing is achieved across the Internet.

Describe the term 'uniform resource locator' (URL) in the context of internetworking.

Explain the terms ‘fully qualified domain name’ (FQDN), ‘domain name’ and ‘IP address’.

Describe how domain names are organised.

Understand the purpose and function of the domain service and its reliance on the Domain

Name Server (DNS) system.

Explain the service provided by Internet registries and why they are needed.

**4.9.3.2 Internet security:**

Understand how a firewall works (packet filtering, proxy server, stateful inspection).

Explain symmetric and asymmetric (private/public key) encryption and key exchange.

Explain how digital certificates and digital signatures are obtained and used.

Discuss worms, trojans and viruses, and the vulnerabilities that they exploit.

Discuss how improved code quality, monitoring and protection can be used to address worms, trojans and viruses.

# The structure of the Internet

- The Internet is defined as:
  - a network of interconnected computer networks
  - which uses an end-to-end communication protocol
- The Internet is mostly a wired network
- Underwater cables connect different continents

Internet service providers

- Companies that provide their customers with access to the Internet
- The largest are national companies and are referred to as national internet service providers
- National ISPs provide internet access to smaller regional and local ISPs
- Homes and businesses can buy access to the Internet from local ISPs

# Packet switching and routers

Packets

- Containers in which data is transmitted over networks
- Labelled with addresses for their sender and recipient
- Contain information intended for the recipient

Packet switched networks

- Networks in which data is sent in packets
- One message is frequently split into multiple packets, each of which is sent to its recipient via the best possible route
- Packets are reassembled with other packets that form part of the same message by their recipient
- Packets usually have to pass through a number of routers before reaching their destination
- Packets' recipient addresses are used by routers to determine where to send them
- Every time that a packet passes through a router, a hop is said to occur
- Each packet can only pass through a finite number of hops
- A packet's time to live (or TTL) is a number that indicates how many hops the packet can partake in and is reduced by one with each hop
- When a packet's TTL expires, the packet is dropped
- The recipient will notice a missing packet and request that the sender transmits the missing packet again

The primary components of a packet

| Component of packet | Purpose |
|---|---|
| Sender's address | Identifies where the packet was sent from |
| Receiver's address | Identifies the packet's intended recipient |
| Packet contents | Where the packet holds the data that is being transferred |
| Time to live (TTL) | Holds the number of hops a packet can go through before being dropped |
| Sequence number | Contains the number of packets in a message and identifies a packet's position in relation to others |

Routers and gateways

- Routers and gateways connect different networks
- Routers send packets to their recipient via the fastest possible route
- Routers hold tables with information relating to the fastest routes to certain devices
- Where two networks use different protocols, packets must be modified by a gateway so as to conform to both protocols
- Gateways strip away most of the packet's details, leaving just the packet's content
- The gateway then gives packets new sender and receiver addresses which comply to the new protocol

# Uniform resource locators

- Addresses assigned to files on the Internet
- Different protocols can be used in URLs to access different types of files in different ways

`https://www.bbc.co.uk/news/technology/index.html`

| Part of URL | Purpose |
|---|---|
| `https://` | The protocol being used to access a file |
| `www` | Subdomain for world wide web |
| `bbc.co.uk` | Domain |
| `/news` | Directory of the file being requested |
| `/technology` | Subdirectory of the file being requested |
| `/index` | Name of the file being requested |
| `.html` | The file's extension |

- There is a wide variety of top level domains (TLDs) available for use
- While `.com` is the most frequently used, TLDs like `.org` and `.net` are also common

Domain names

- Identify an organisation or individual on the Internet
- Use alphanumeric characters making them easy for humans to remember

Fully qualified domain names

- A domain that specifies an exact resource and can be interpreted in only one way
- An FQDN will always include the server's host name

`https://bbc.co.uk/news/index.html` FQDN ✗

`https://www.bbc.co.uk/news/index.html` FQDN ✓

IP Addresses

- IP stands for internet protocol
- Assigned to every computer on the Internet and every device that communicates on a network
- Not easy for humans to remember, which is why domain names are used
- Domain names map to IP addresses, meaning they are essentially a human-friendly representation of an IP address

## The domain name server (DNS) system

- Domain names have a direct relationship with IP addresses
- A domain name server is used to translate domain names into their corresponding IP addresses
- A domain name server stores a table of domain names and their corresponding IP address
- If a domain name server does not have a record of a requested domain, the request will be passed to another domain name server
- Some very small and rarely visited websites will require numerous changes of servers before a record can be found

| DNS Table | |
|---|---|
| **Domain Name** | **IP address** |
| turing.me | 41.47.142.208 |
| lovelace.com | 16.57.142.88 |
| babbage.net | 84.88.49.3 |

## Internet registries

- Organisations responsible for the allocation of IP addresses
- There are only five in operation, each serving a different geographical area
- An important part of an internet registry's work is to protect the world's depleting pool of unallocated IP addresses
- When a new IP address is requested, an internet registry will first look for a previously allocated IP address that has become unused rather than allocate a brand new IP address straight away

# Internet security

## Firewalls

- Sit between a device and the Internet
- Regulate the packets that pass through them
- Can be either software or hardware
- Work as a proxy server which can perform both packet filtering and stateful inspection

### Packet filtering

- Firewalls use packet filtering to accept and block packets based on their source IP address or the protocol that they are using
- A network's administrator can specify particular IP addresses or protocols to block or use automatic filtering software that can block suspicious packets

### Stateful inspection

- Stateful inspection actually examines the contents of a packet before deciding whether to allow it through the firewall
- Some firewalls keep a record of current connections in a network, allowing them to filter out packets that aren't related to activity on the network

### Proxy servers

- Servers that sit between a public network and a private network
- Manage every packet that passes between the two networks
- Firewalls can be said to act as proxy servers when they control the movement of packets between public and private networks
- When a device in a private network sends a packet through a firewall and into a public network, the packet's "sender" address is that of the firewall, rather than the device's private IP address
- This provides some degree of anonymity to devices on private networks as their private address is never sent beyond the private network

# Symmetric and asymmetric encryption and key exchange

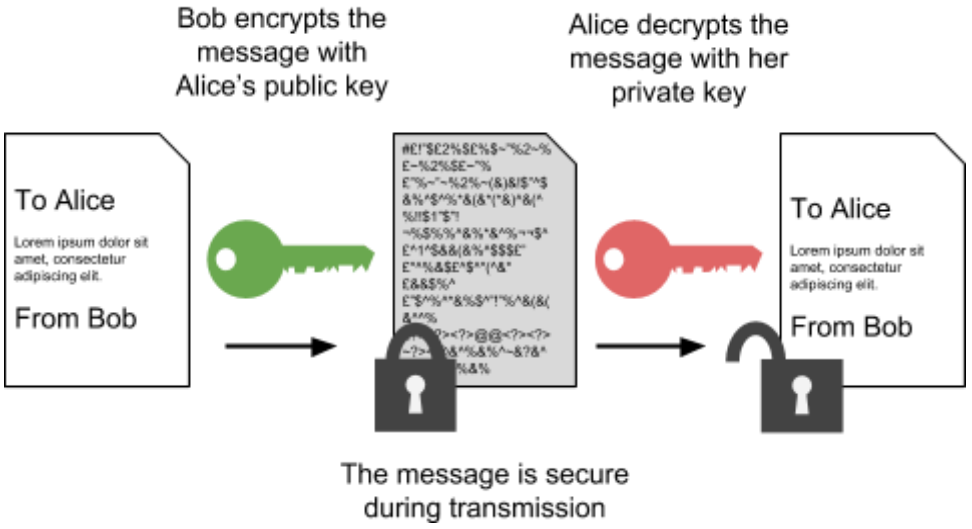
- Encryption is used when information is to be transmitted securely over a network

Symmetric encryption

- Both the sender and receiver share the same private key
- This key is used to both encrypt and decrypt data sent between the two parties
- Before sending any information, the sender and receiver must participate in a key exchange
- If the key is exchanged over a network, it is vulnerable to interception
- This is a major floor in symmetric encryption that asymmetric encryption overcomes

Asymmetric encryption

- Each device has a pair of mathematically related keys
- One key is kept secret (the private key) and the other shared on the Internet (the public key)
- When a message is encrypted with a public key, only the corresponding private key can decrypt it and vice versa




- Before a message is sent, it is encrypted by the sender using the recipient's public key
- The message can only be decrypted by the corresponding private key, the recipient's private key
- Only the recipient has access to this key, so the recipient is the only person who can decrypt the message

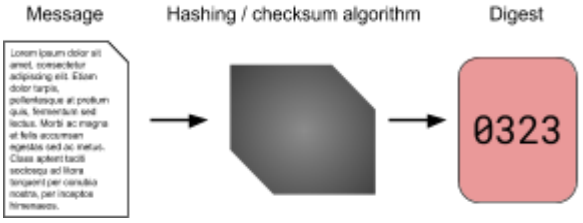
# Digital certificates & digital signatures

Digital signatures

Can be used alongside asymmetric encryption to verify the sender of a message

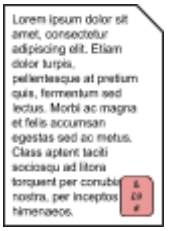
Also verify that a message has not been tampered with or corrupted during transmission

1. A digest of the message is created



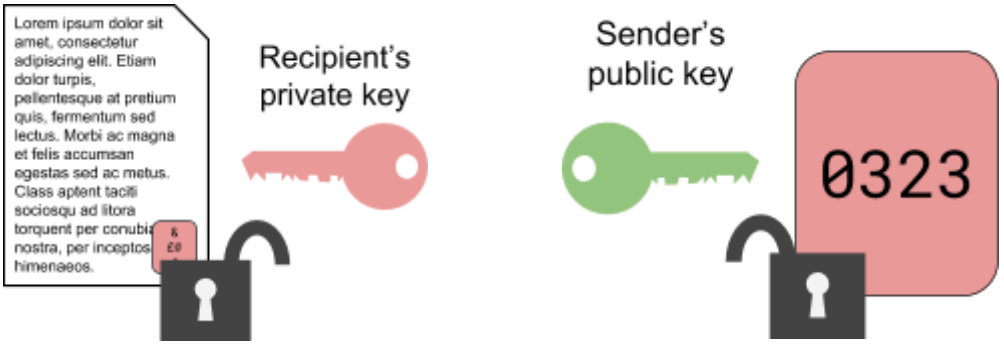

2. This digest is encrypted with the sender's private key


3. The encrypted digest is appended to the message



4. The message and appended digest are encrypted with the recipient's public key


- When the recipient receives the message, they:
  - decrypt the message using their private key
  - decrypt the digest using the sender's public key
  - carry out the same digest algorithm on the message
  - check whether their result matches the now decrypted digest



Digital certificates

- Verify ownership of a key pair used in asymmetric encryption
- Can be used to check that a fake key pair isn't being used by an imposter
- Issued by certificate authorities, these files contain:
    - a serial number
    - the owner's name
    - an expiry date
    - the owner's public key
    - the certificate authority's digital signature

## Worms, trojans and viruses

- Types of malware that can infect computers

Worms

- Pieces of malicious software that can self-replicate between computers
- Either within a network or by users downloading and running a malicious file

Trojans

- A type of malware that is disguised as a benign file
- Users can be tricked into opening this file
- Often spread as email attachments or downloaded from malicious websites

Viruses

- Require a host file in which to reside
- These files are typically executable files
- Can lie dormant in a computer until their host file is opened or run
- Can spread between computers over a private network, the Internet or even through the use of physical media

Preventing malware

- It is difficult to avoid malware completely
- There are a number of precautions that can be taken in order to protect computers from malicious software
    - Malware often exploit bugs in code that enable them to take hold of a computer system so good code quality is an important factor in preventing malware
    - Install antivirus software
    - In organisations, employees can be trained about the risks of opening suspicious email attachments