1	**1**	**Mark is AO1 (knowledge)** How to pass the key (from the sender) to the receiver; **A.** key must be sent along with the data **NE.** key must be exchanged, without a reference to the receiver Without it being intercepted / securely; **A.** the key can be intercepted if/when it is <u>transmitted</u>	**2**

1	2	**All marks AO1 (understanding)** B's private key is used to decrypt the message (and signature); **R.** more than one key referenced The message is rehashed // a new message digest/hash is calculated from the message; A's public key is used to decrypt the digital signature (to produce the received message digest); If received message digest and recalculated message digest match / if both hashes match then the sender can be authenticated / B knows that A sent the message; **A.** if recalculated hash matches digital signature then B knows A sent message, if third mark point not awarded. **NE.** if hashes match then B knows message has not been tampered with **A.** data for message **A.** checksum, hash, digest as synonyms **A.** encrypted hash/encrypted digest for signature	**4**

2	**1**	**4 marks for AO1 (understanding)** Block/allow (traffic on) specific ports // block specified protocols; Block/allow (traffic from) specific IP addresses; **A.** Domain names as BOD **NE.** Block access to certain websites **R.** MAC addresses Block/allow certain types of packet; **A.** Examples eg pings/echo requests **NE.** Block specific programs connecting to Internet Firewall maintains information about current connections and only allows packets relevant to these connections through; **NE.** Just the name “stateful inspection” Act as a proxy server // all traffic to Internet must go via firewall // stops computers on the Internet directly accessing devices on the LAN; Identify unusual behaviour from a host // example of unusual behaviour eg sending an unusually large amount of data; Rules are written to specify conditions under which to block/allow; If none of the first three marks scheme points awarded then a mark can be awarded for: Examine the contents of the packet header and allow/block based on rules; **NE.** Just the name “packet filtering” **Max 4**	**4**

Question			Marks
3	1	**1 mark AO1 (knowledge) and 2 marks AO1 (understanding)** **Purpose (1 mark – AO1 knowledge):** Translates/converts/maps Fully Qualified Domain Names / FQDNs into IP addresses; **A.** domain names **R.** Uniform Resource Locators / URLs **How it works (2 marks – AO1 understanding):** • DNS / Domain Name Server(s) stores a database/table of FQDNs and corresponding IP addresses **A.** FQDN looked up in table **A.** domain names **DPT** Uniform Resource Locators / URLs • DNS is a distributed database of mappings • (Individual) mappings are only known by some DNS servers • DNS servers are organised into a hierarchy **A.** hierarchy given by example **R.** description of how domain names themselves are organised • If one DNS server cannot resolve a lookup the query will be passed to another (DNS server) • DNS servers support load distribution by returning one IP address from a list	**3**

Qu	Pt	Marking guidance	Total marks
4	**1**	**All marks AO1 (knowledge)** Port number(s); **A.** destination port number and source port number as separate marks **A.** "port" as **BOD** Sequence number; **A.** packet number Time to live; **A.** TTL, maximum hop count Packet size/length; **A.** size Type of service; **A.** priority Protocol identifier; **A.** "protocol" as **BOD** Packet identifier/ID number; IP version; Options/Padding; Flags; Window size value; Fragment offset // header length; **A.** Total number of packets in message **NE.** Total number of packets **A.** Acknowledgement number **Only mark first two responses** **Max 2**	**2**

Qu	Pt	Marking guidance	Total marks
4	2	**All marks AO1 (understanding)** Connects two networks together; **NE.** Connects a network to the Internet **Note:** Must be explicitly stated to award mark, not implied from other points Router determines which outgoing link to send packet along // determines which router/host/node to send packet to next; **NE.** Router determines where to send packet next **NE.** Router determines next hop **R.** Responses which suggest a router always sends the packet to the final destination Router uses most efficient/shortest/cheapest/best path to the destination; Router (monitors the network and) updates routes/routing table to reflect congestion/failure/network changes; **A.** Congestion management as **BOD** Router modifies the (MAC/hardware) addresses for the next hop // router modifies the (MAC/hardware) addresses to get to the next router; **R.** IP addresses **A.** To remove packets that have no time to live // have reached the maximum hop count **Max 2**	**2**

Qu	Pt	Marking guidance	Total marks
05	1	**Mark is AO1 (understanding)** Each resource is represented by a URL; Entering a URL causes the server to (use CRUD to) retrieve (the relevant) data; **A.** Used to carry out a search **A.** To access a database/resource/dataset URLs are sent between the client and the server using HTTP; **Max 1**	1

Qu	Pt	Marking guidance	Total marks
6	1	**Mark is AO1 (understanding)** Protocol conversion;	1

<table>
<tr><th>Qu</th><th>Pt</th><th>Marking guidance</th><th>Total marks</th></tr>
<tr><td>6</td><td>2</td><td>

All marks AO1 (understanding)

<table>
<tr><th>Level</th><th>Description</th><th>Mark Range</th></tr>
<tr><td>3</td><td>The description is comprehensive and covers both transmission and reception. At least three of the keys to use for particular processes have been correctly identified. Whilst there may be some omissions, any errors are minor.</td><td>5–6</td></tr>
<tr><td>2</td><td>A significant amount of the process has been described but there may be some misunderstandings and/or omissions. At least two of the keys to use for particular processes have been correctly identified. The description might cover only transmission or reception.</td><td>3–4</td></tr>
<tr><td>1</td><td>A few relevant points have been made but the description contains significant omissions or misunderstandings.</td><td>1–2</td></tr>
</table>

<u>Guidance – Indicative Content</u>

Transmission

- A message digest/(hash) value is calculated from the message contents.
- The message digest/(hash) value is encrypted using A's private key.
- The encrypted message digest/(hash) value is known as the digital signature.
- The digital signature (**A.** hash) is appended to the message.
- The message (and signature) are encrypted using B's public key.

Note: Signature can be appended to message before or after encryption with B's public key takes place.

Reception

- B's private key is used to decrypt the message (and signature).
- The message is rehashed // a new message digest/hash is calculated from the message.
- A's public key is used to decrypt the digital signature (to produce the received message digest).
- If received message digest and recalculated message digest match/if both hashes match then the sender can be authenticated/then B knows that A sent the message.
  A. If recalculated hash matches digital signature then B knows A sent message, if third point not awarded.
  NE. If hashes match then B knows message has not been tampered with

A. "data" for message
A. "checksum", "hash", "digest" as synonyms
A. "encrypted hash" or "encrypted digest" for signature
R. More than one key referenced for any process that involves just one key

</td><td>6</td></tr>
</table>

Qu	Pt	Marking guidance	Total marks
7		**All marks AO1 (understanding)** **Monitoring** Firewall could block packets from sources / computers known to be high-risk // could block packets not part of a current communication (stateful inspection); **A.** firewall could filter/monitor data entering network **A.** firewall could block packets containing malicious data Proxy server could receive/check downloaded files; Spam filters can block emails from suspicious sources // spam filters can block emails that contain suspicious content // block pop-ups to prevent users clicking on potentially harmful links // have a system that enables the reporting of spam emails // block download of attachments from outside organisation / untrusted sources // block download of attachments based on file type / executables; Web filters can check websites against a list of websites known for having content that might contain/spread a virus; Digital certificates can be used to verify the source of a downloaded file; Digital signature / checksum can be used to verify that a file has not been changed // that a file came from a known source; **Protection** Enable automatic update of applications / OS to patch code vulnerabilities; **A.** keep software up to date **R.** automatic update of anti-virus software Use a virtual machine to execute programs // use a sandbox when executing programs (**A.** opening files); Set access rights to minimise risk of viruses being able to access / modify sensitive / important data / files; Disable execution of macros in documents (from outside sources); Restrict execution of software from unverified sources // restrict execution of unauthorised software; Encrypt files so that data cannot be extracted from them; Backup data and keep offline / away from computer so it can be recovered; **NE.** "backup" without explaining that this could be used to recover data or expanding on how backups should be made Disable the use of external drives / removable media; **A**. disable USB ports Use a computer with the Harvard architecture to prevent data being executed as code; Use a MAC address allow list so that only known devices can join a network; (Enforce) strong passwords / biometric access would make it harder for a hacker to access a computer <u>to install a virus</u>; **Code Quality** Ensure code does not allow buffer overflow / overrun // ensure code prevents programs writing to memory locations not allocated to them; Test software for security issues / vulnerabilities; Carry out a code review so the code is independently checked by another programmer / other programmers;	**4**

		Use code analysis software to identify flaws / measure code quality; Only use / load up Internet services / libraries from the Internet if required // use the latest version of libraries // use libraries that are known to have been thoroughly tested // use libraries from trusted sources; **Note:** Question requires a description. Naming methods eg “backup”, “firewall” without describing how they would be used is not enough to award a mark. **Max 4**	

Qu	Pt	Marking guidance	Total marks
8	1	**Mark is AO2 (analyse)** **1 mark**: Both protocol and domain name correct. **Protocol:** HTTP // Hypertext Transfer Protocol **R.** HTTPS **Domain name:** `loveapug.org.uk` **NE.** `www.loveapug.org.uk` **I**. minor misspellings in domain name, case	**1**

Qu	Pt	Marking guidance	Total marks
8	2	**All marks AO1 (knowledge)** **1 mark**: Hierarchical organisation **A.** names of two parts of domain stated eg top/first-level domain and second-level domain **NE.** split into parts **TO.** hierarchical used in incorrect context eg hierarchical organisation of DNS servers **1 mark**: Expansion / example of hierarchical organisation: • example of top-level domain that is identified as being a top-level domain eg com, org, uk, fr • example of second-level domain that is identified as being a second-level domain eg ac, co **A.** ac.uk, co.uk or similar • domains can have subdomains created for them • example of subdomain for a domain, eg pastpapers.aqa.org.uk for aqa.org.uk **Note:** Do not award second mark if part of a URL that is not part of the domain name is referenced eg the protocol or the name of the file on the server.	**2**

Qu	Pt	Marking guidance	Total marks
8	3	**1 mark AO1 (knowledge) and 1 mark AO1 (understanding)** **Service (1 mark – knowledge)**: Registering domains to people / organisations / companies // storing domain names and who owns them; **Why needed (Max 1 mark – understanding)**: To enter domain name (to IP address mappings) into the DNS system; To ensure that domain names are unique; To ensure domain names not used by more than one person / organisation / company; **A.** "website" for person / organisation / company **NE.** domain names could not be used // all addressing would need to be done using IP addresses	**2**