1.3 Exchanging Data: Databases, Networks and Web Technologies: 1-hour Pack

OCR H446 · Calculators not allowed · about 60 minutes

Total Marks

Name: _____ Date: ____ / ____ / _____

Answer ALL questions. Show all your working.

1 A retailer's website uses HTTPS to protect data sent between a customer's browser and the web server.

(a) Distinguish between symmetric encryption and asymmetric encryption. **(3)**

(b) Explain why HTTPS uses asymmetric encryption only to establish a shared secret key at the start of the connection, and then switches to symmetric encryption for the rest of the session. **(3)**

(c) A simple Caesar cipher shifts every letter of the plaintext forward by 3 places in the alphabet (wrapping Z back to C). Encrypt the plaintext NETWORK using this cipher. **(2)**

(d) State one weakness of the Caesar cipher as a method of encryption. **(1)**

(Total for Question 1 is 9 marks)

© Revision Library | revisionlibrary.co.uk

2 A bank's database processes transactions using the ACID properties.

(a) State what each of the four letters in ACID stands for, giving a brief description of each property. **(4)**

(b) Priya Sharma and her partner share a joint bank account with a balance of £500. Both attempt to withdraw £300 at almost the same time from different cash machines. Explain, using this example, how the Isolation property prevents an incorrect final balance being recorded. **(3)**

(c) Explain why record locking is used in transaction processing systems. **(2)**

(Total for Question 2 is 9 marks)

---

3 Search engines allow users to find relevant web pages within a fraction of a second.

(a) Explain how a search engine uses a crawler and an index to respond quickly to a search query. **(4)**

(b) Explain how the PageRank algorithm uses backlinks to help rank web pages, illustrating your answer with an example. **(4)**

(Total for Question 3 is 8 marks)

© Revision Library | revisionlibrary.co.uk

4 Discuss the range of technologies and techniques an online retailer should employ to keep customers' payment data secure, both while it is being transmitted and while it is being stored, evaluating how effective each is.

(Total for Question 4 is 8 marks)

© Revision Library | revisionlibrary.co.uk

5 Data sent between an office in Manchester and a branch office in Glasgow is broken into packets, which can arrive out of order because they may take different routes across the network.

(a) State one field found in a packet header that allows the receiving device to reassemble the data in the correct order. **(1)**

(b) An array packets[0 TO n-1] holds packet records that have arrived out of order, where each record has a field seqNum. Write an algorithm, using the OCR Exam Reference Language, that sorts the packets array into ascending order of seqNum using an insertion sort. **(6)**

(c) Three packets arrive with seqNum values 3, 1, 2 (in that array order). Complete a trace table for the algorithm from part (b) as it sorts this array, showing the value of i, current, j and the full array contents after each outer loop iteration. **(4)**

(Total for Question 5 is 11 marks)

---

6 A device on a home network has IPv4 address 192.168.1.14 and MAC address 00-1A-2B-3C-4D-5E. The device sends a request to a web server on the internet.

(a) Convert the IPv4 address 192.168.1.14 to its full binary representation, showing each octet. **(4)**

(b) Explain the difference between how the MAC address and the IP address are used to deliver the device's data across the internet to the web server. **(4)**

(c) Explain the function of a router in forwarding this data toward the web server. **(3)**

(Total for Question 6 is 11 marks)

© Revision Library | revisionlibrary.co.uk

Mark scheme · 1.3 Exchanging Data: Databases, Networks and Web Technologies: 1-hour Pack

Question 1

(a) Symmetric encryption uses the same single key to encrypt and decrypt the data (oe) **B1**

(a) Asymmetric encryption uses a mathematically linked key pair (a public key and a private key); data encrypted with one key can only be decrypted with the other (oe) **B1**

(a) Comparative point, e.g. symmetric is faster but requires the key to be shared securely in advance, whereas asymmetric avoids that key-distribution problem but is slower (oe) **B1**

(a) Answer: Symmetric: one shared key for both encryption and decryption, fast but must be distributed securely. Asymmetric: a public/private key pair, slower, but removes the need to share a secret key in advance.

(b) States that asymmetric encryption is computationally expensive/slow, particularly for large amounts of data (oe) **M1**

(b) States that symmetric encryption is much faster and better suited to encrypting the bulk of the session's data (oe) **A1**

(b) Explains that asymmetric encryption is instead used briefly to securely exchange the symmetric session key, solving the key-distribution problem without the ongoing performance cost (oe) **A1**

(b) Answer: Asymmetric encryption is slow for large volumes of data, so it is used only to safely exchange a symmetric session key; the fast symmetric algorithm then encrypts the rest of the session, combining the security of asymmetric key exchange with the speed of symmetric encryption.

(c) Shows a shift of 3 applied consistently to each letter **M1**

(c) Fully correct ciphertext cao: QHWZRUN **A1**

(c) Answer: QHWZRUN

(d) Only 25 possible shifts/keys exist, so it can be broken quickly by brute force, or it is vulnerable to frequency analysis (oe) **B1**

(d) Answer: There are only 25 possible shift values, so the cipher can be broken almost instantly by trying every shift (brute force) or by frequency analysis.

Question 2

(a) Atomicity: a transaction is treated as a single indivisible unit that either completes fully or is rolled back entirely (oe) **B1**

(a) Consistency: a transaction takes the database from one valid state to another, obeying all defined rules/constraints (oe) **B1**

(a) Isolation: concurrently executing transactions do not interfere with one another, behaving as if run sequentially (oe) **B1**

(a) Durability: once a transaction is committed, its changes are permanent, even if the system subsequently fails (oe) **B1**

(a) Answer: Atomicity - all or nothing. Consistency - database moves between valid states. Isolation - concurrent transactions do not interfere. Durability - committed changes survive failure.

(b) Identifies the problem: without isolation, both transactions could read the original balance (500) before either writes back, so one withdrawal's update could be lost/overwritten (a lost update) **M1**

(b) Explains that Isolation ensures the transactions are processed as if one happens completely before the other (serially), e.g. via locking the record during the first transaction **A1**

(b) Explains that the second transaction then reads the updated balance (200) left by the first, correctly declining/processing based on the true remaining balance, so both withdrawals are reflected correctly **A1**

(b) Answer: Without isolation both machines could read the 500 balance and each write back 200, losing one withdrawal. Isolation locks the record so the second transaction must wait and reads the already-updated balance (200), giving a correct final result.

(c) Prevents two transactions from modifying the same record at the same time, avoiding data inconsistency/lost updates (oe) **B1**

(c) States that the lock is released once the transaction has committed or been rolled back, allowing other transactions to proceed (oe) **B1**

(c) Answer: Record locking stops two transactions updating the same record simultaneously, preventing lost updates; the lock is released once the transaction commits or rolls back so others can then access the record.

© Revision Library | revisionlibrary.co.uk

Question 3

(a) Describes a crawler as a program that automatically follows hyperlinks between pages to discover content across the web (oe) **B1**

(a) Describes the index as a data structure storing keywords/terms mapped to the pages they appear in (oe) **B1**

(a) States that the index is built up in advance from the pages the crawler visits **B1**

(a) Explains that this allows the search engine to search the prebuilt index rather than the entire live web at query time, giving a fast response (oe) **B1**

(a) Answer: A crawler automatically follows links to discover web pages, and the content found is used to build an index mapping keywords to pages. When a query is made, the search engine searches this prebuilt index rather than the live web, giving a near-instant response.

(b) States that PageRank counts the number of backlinks (links from other pages) pointing to a page (oe) **B1**

(b) States that a link from a page with a higher rank/quality contributes more to the score than a link from a low-ranked page, so quality matters as well as quantity (oe) **B1**

(b) States that pages with a higher resulting score are ranked/displayed higher in the search results (oe) **B1**

(b) Valid illustrative example, e.g. a recipe page linked to from a well-established site such as BBC Good Food would rank higher than an identical recipe page linked to only from one small personal blog (oe) **B1**

(b) Answer: PageRank scores a page by counting backlinks, weighting links from higher-ranked pages more heavily than links from low-ranked pages, and pages with a higher score are shown higher in results; for example, a recipe page linked from BBC Good Food would outrank an identical page linked only from a small personal blog.

Question 4

Level 3 A detailed and coherent discussion covering a range of relevant technologies for both data in transit and data at rest (e.g. TLS/HTTPS, hashing and salting of stored data, tokenisation, firewalls, two-factor authentication). The candidate evaluates the effectiveness and/or limitations of the measures discussed, recognising that a combination of techniques (defence in depth) is needed. Technical terminology is used accurately and the answer is well structured throughout. **6-8**

Level 2 A reasonable discussion of some relevant technologies covering transit and/or storage, with some evaluation of effectiveness, but the range or depth is limited, coverage is one-sided (e.g. transit only), or there are minor inaccuracies. Some relevant technical terminology is used. **3-5**

Level 1 Limited, mostly descriptive or list-like points are made, with little or no evaluation of effectiveness. The answer may contain inaccuracies and lacks coherent structure. **1-2**

Level 0 No creditable response, or the response does not address the question. **0**

Indicative content:

- TLS (HTTPS) encrypts data sent between the customer's browser and the server, preventing eavesdropping/interception in transit.
- Asymmetric encryption is used during the TLS handshake to securely exchange a symmetric session key, which then encrypts the bulk of the transmitted data.
- Passwords should be stored using a hash function (ideally with a salt) rather than in plaintext, so that even if the database is stolen, the original passwords are not directly readable.
- A salt prevents attackers from using precomputed rainbow tables to reverse common hashed passwords.
- Card/payment data at rest should be encrypted, and full card numbers are often replaced with tokens (tokenisation) so the retailer never stores the real, usable card number.
- Firewalls and intrusion detection systems help prevent unauthorised access to the servers/database that hold customer data.
- Two-factor authentication adds an extra barrier against an attacker who has obtained a password.
- Evaluation: TLS protects data only in transit, not once it is stored, so it must be combined with storage-level protection; hashing without a salt is vulnerable to rainbow table attacks; no single technique is sufficient on its own, so a combination (defence in depth) gives the strongest overall protection; measures such as PCI DSS compliance and regular security audits help ensure these technologies are implemented and maintained correctly.

© Revision Library | revisionlibrary.co.uk

Question 5

(a) Sequence number (accept packet/fragment number) **B1**

(a) Answer: Sequence number

(b) Any correct logic, ignore minor syntax: outer loop correctly iterates through the array starting from the second element (index 1) to the last element **M1**

(b) Current element is stored in a variable before it is potentially overwritten **M1**

(b) Inner loop/comparison correctly compares seqNum of the stored element against seqNum of preceding elements **M1**

(b) Preceding elements with a greater seqNum are correctly shifted one place to the right **M1**

(b) The stored current element is correctly inserted at the resulting empty position **M1**

(b) Complete, logically correct algorithm that sorts the whole array into ascending order of seqNum for any valid input, using correct array index bounds **A1**

(b) Answer:

```
PROCEDURE SortPackets(packets, n)
  FOR i <- 1 TO n - 1
    current <- packets[i]
    j <- i - 1
    WHILE j >= 0 AND packets[j].seqNum > current.seqN
      packets[j + 1] <- packets[j]
      j <- j - 1
    ENDWHILE
    packets[j + 1] <- current
  NEXT i
ENDPROCEDURE
```

(c) Correct row for i = 1: current = 1, array shifts to [3, 3, 2] mid-pass then current inserted at index 0, giving array [1, 3, 2] **M1**

(c) Correct value of j shown ending at -1 for the i = 1 pass **A1**

(c) Correct row for i = 2: current = 2, packets[1] (value 3) shifts right, j ends at 0, current inserted at index 1, giving array [1, 2, 3] **M1**

(c) Final array fully correct and in ascending order cao: [1, 2, 3] **A1**

(c) Answer: i=1: current=1, j finishes at -1, array becomes [1,3,2]. i=2: current=2, j finishes at 0, array becomes [1,2,3]. Final sorted array: [1,2,3]

Question 6

(a) 192 correctly converted to 11000000, cao **B1**

(a) 168 correctly converted to 10101000, cao **B1**

(a) 1 correctly converted to 00000001, cao **B1**

(a) 14 correctly converted to 00001110, cao **B1**

(a) Answer: 11000000.10101000.00000001.00001110

(b) States that the MAC address is a fixed/physical address built into the network interface (NIC) and does not change (oe) **B1**

(b) States that the MAC address is used to deliver data to the correct device on the same local network/link (data link layer) (oe) **B1**

(b) States that the IP address is a logical address that can be reassigned (e.g. by a router/DHCP) and identifies the network as well as the device (oe) **B1**

(b) States that the IP address is used to route the data across different networks toward its destination (network layer), with the MAC address changing at each hop while the IP address stays the same (oe) **B1**

(b) Answer: The MAC address is a fixed, hardware address used only for delivery within the local network. The IP address is a logical, changeable address used by routers to direct the data across different networks all the way to the destination.

(c) States that the router examines the destination IP address of each packet (oe) **M1**

(c) States that it uses a routing table to determine the best next hop toward the destination network (oe) **A1**

(c) Explains that this allows the router to connect and forward data between different networks (e.g. from the home LAN onto the wider internet/WAN) (oe) **A1**

(c) Answer: The router reads the destination IP address of each packet, consults its routing table to find the best next hop, and forwards the packet on toward the destination network, connecting the home LAN to the wider internet.

© Revision Library | revisionlibrary.co.uk