Week 15

A-Level Computer Science

Homework bundle for this week

本周作业合集

exercises.lol

Contents 目录

Topic 6 quiz 2

Exercise sheet 6.1 5

Past-paper questions 6.1 10

Exercise sheet 6.2 16

Past-paper questions 6.2 23

6. Security, privacy and data integrity

Starter Quiz · 课前小测

A-Level Computer Science Name: _____ Score: _____

1. Which best describes data ”integrity”?
   - ☐ the data is accurate and complete (not corrupted)
   - ☐ only authorised people can access the data
   - ☐ a person controls who sees their personal data
   - ☐ the data is encrypted
2. A firewall mainly:
   - ☐ filters network traffic by rules, blocking unwanted connections
   - ☐ encrypts the hard disk
   - ☐ scans files for viruses
   - ☐ backs up data off-site
3. Checking that a month entered is between 1 and 12 is a:
   - ☐ range check
   - ☐ presence check
   - ☐ format check
   - ☐ check digit
4. How does a worm differ from a virus?
   - ☐ a worm spreads over networks by itself, with no user action
   - ☐ a worm needs the user to run an infected program
   - ☐ a worm cannot copy itself
   - ☐ a worm only shows adverts
5. The best defence against data being intercepted in transit is to:
   - ☐ encrypt it (e.g. with HTTPS or a VPN)
   - ☐ use a longer password
   - ☐ install antivirus
   - ☐ add a CAPTCHA
6. Malware that encrypts your files and demands payment for the key is called _____.

7. Symmetric encryption uses one shared key, while asymmetric encryption uses a public key to encrypt and a private key to decrypt.

   ☐ True ☐ False

8. Privacy is about a person controlling who sees their personal data, while security is about stopping unauthorised access.

   ☐ True ☐ False

9. Verification proves the data was copied or entered without change — but not that the value is factually correct.

   ☐ True ☐ False

10. An extra digit computed from the others to catch a mistyped number (as on ISBNs and card numbers) is a _____ digit.

    _____

6. Security, privacy and data integrity

Answers · 答案

A-Level Computer Science

1. **the data is accurate and complete (not corrupted)**

   Integrity = accurate and complete. Security = blocking unauthorised access; privacy = control over personal data.

2. **filters network traffic by rules, blocking unwanted connections**

   A firewall controls which network traffic is allowed in or out, by a set of rules.

3. **range check**

   A range check confirms a value lies within sensible limits.

4. **a worm spreads over networks by itself, with no user action**

   A worm self-propagates across networks without user action; a virus needs an infected program to be run.

5. **encrypt it (e.g. with HTTPS or a VPN)**

   Encrypted data intercepted in transit is useless without the key. Authentication and antivirus address different threats.

6. **ransomware**

   Ransomware encrypts the victim's files and demands a ransom for the decryption key.

7. **True**

   That public/private split is what lets asymmetric encryption solve the problem of sharing a key safely.

8. **True**

   They overlap but differ: security blocks intruders; privacy is control over personal data; integrity is about accuracy.

9. **True**

   Double entry / checksums prove the data arrived unchanged; only a human or a cross-check can confirm it is actually true.

10. **check**

    A check digit is recomputed from the rest and compared, catching most single-digit and transposition errors.

A-LEVEL COMPUTER SCIENCE • EXERCISE SHEET

6.1 Data Security

Name: _____ Class: _____ Date: _____ **Total: 36 marks**

KEY WORDS security 安全 • integrity 完整性 • phishing 网络钓鱼 • data security 数据安全 • privacy 隐私

Objective

Build the skills to answer exam questions on **data security** 数据安全 — the difference between security, privacy and integrity; the threats from networks; and the measures that protect a system.

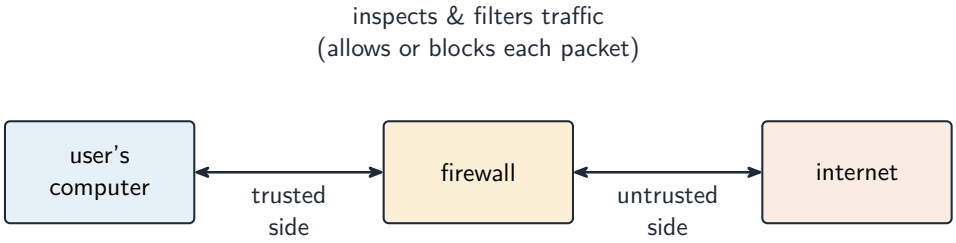
You must be able to:

- explain the difference between **security**, **privacy** 隐私 and **integrity** 完整性
- describe the **threats** to data and systems posed by networks and the internet
- describe **security measures** for a standalone PC and for a networked system

1 Worked examples

Study these first. Each one shows the method for a question type used later — follow the steps and you can do the Practice and Exam-style questions yourself.

■ Three different ideas



A firewall is a core data-security control at the network edge

Term	Means	Example failure
security	protect data from **unauthorised** access/change	a hacker reads the file
privacy	a person controls **who sees** their personal data	data shared without consent
integrity	data stays **accurate and complete**	a typo corrupts a record

All three are needed — a file can be secure but still have a typo (no integrity), or accurate but readable by anyone (no privacy).

Threats from the internet

Threat	What it does
virus / worm	self-copying malware (a worm spreads over the network alone)
Trojan horse	looks useful but hides malicious code
ransomware	encrypts your files and demands payment
spyware	secretly records keystrokes / passwords
phishing	fake emails/sites trick users into giving credentials
pharming 域名欺骗	redirects a user to a fake site **even when they type the correct address**
denial of service	floods a server so real users can't connect
brute-force attack	tries many passwords until one works

Security measures

- **standalone PC:** strong password; up-to-date antivirus; software updates; **backup**; **encryption**; locked screen.
- **networked system:** all of the above **plus** a **firewall** 防火墙, per-user **permissions**, central account management and **audit logs**.

2 Practice

Now apply the methods above.

2.1 State the difference between data **security** and data **privacy**. [2]

2.2 Name the type of malware that **encrypts a user's files and demands payment**. [1]

2.3 State **two** security measures suitable for a standalone PC. [2]

2.4 State what a **firewall** does. [1]

3 Exam-style questions

3.1 Explain the difference between **security**, **privacy** and **integrity**, giving an example of each. [3]

3.2 Describe **two** threats posed by connecting a computer to the internet, and give a measure that reduces each. [4]

3.3 (a) State what **phishing** is. [1]

(b) State one way a user can reduce the risk of falling for a phishing attack. [1]

3.4 Explain how a **firewall** and **user permissions** together help protect a networked system. [3]

3.5 State **one** difference between **phishing** and **pharming**. [2]

3.6 A bank sends confidential statements to its customers over the internet.

(a) **Describe** how the bank uses **asymmetric encryption** so that only the intended customer can read a statement. [3]

(b) The statement also carries a **digital signature**. **Describe** how the signature is created by the bank and checked by the customer, and **state** what it proves. [5]

(c) A **checksum** is sent with the file as well. **Explain** what a checksum detects that a digital signature does not need to, and **state** why a checksum alone would not be enough for security. [3]

(d) A customer's computer is infected by **malware** that records keystrokes. **Name** this type of malware and **describe** two measures that would reduce the risk. [3]

(e) The bank also protects its own network with a **firewall**. **Describe** two things a firewall does. [2]

Solutions

2.1 Security = protecting data from unauthorised access/change; privacy = the individual's right to control **who sees** their personal data.

2.2 Ransomware.

2.3 Any two of: strong password; up-to-date antivirus; software updates; backups; encryption; locked screen.

2.4 It monitors and controls traffic between a trusted network and an untrusted one (the internet), blocking unauthorised connections.

3.1 Security = protection from unauthorised access (e.g. a hacker); privacy = controlling who sees personal data (e.g. consent); integrity = data being accurate/complete (e.g. not corrupted by a typo).

3.2 Any two threats, each with a measure, e.g.: malware → antivirus + updates; phishing → user training / don't click unknown links. *(Other valid pairs accepted.)*

3.3 (a) Fake emails or websites that trick the user into giving away credentials/personal data.
(b) e.g. check the sender / don't click links in unexpected emails / type the address yourself.

3.4 The firewall blocks unauthorised connections from outside; user permissions limit what each account can access inside, so even a logged-in user (or attacker) can only reach what they are allowed to.

3.5 Phishing tricks the user into clicking a fake link / giving details themselves; pharming **redirects** the user to a fake site automatically even when they type the correct web address.

3.6 (a) The customer has a key pair and publishes the **public** key. The bank encrypts the statement with that public key. Only the customer's **private** key can decrypt it, and the customer never shares it, so nobody else can read the statement.
(b) The bank puts the statement through a **hashing algorithm** to produce a digest, then encrypts that digest with the **bank's private key** — that is the signature. The customer decrypts the signature with the **bank's public key** to recover the digest and hashes the received statement themselves. If the two digests match, the statement came from the bank and has not been altered.
(c) A checksum detects **accidental corruption** in transmission — dropped or flipped bits. It is not enough for security because an attacker who alters the file can simply recompute the checksum; a signature cannot be forged that way, because the attacker does not have the bank's private key.
(d) A **keylogger**, a form of spyware. Any two: keep antivirus software installed and up to date; do not open attachments or install software from unknown sources; use two-factor authentication so a stolen password alone is useless; use an on-screen keyboard or a password manager for sensitive entry.
(e) Any two: it **inspects** incoming and outgoing traffic against a set of rules and blocks whatever fails them; it maintains a blacklist or whitelist of addresses and ports; it can block traffic to unauthorised applications and log attempted intrusions.

7 A banker stores personal data on their work computer.

(a) The banker needs to transfer confidential data across the internet.

Identify and describe **one** method of restricting the risks posed by an unauthorised person intercepting the data whilst it is being transferred across the internet.

Method .....

Description .....

.....

.....

.....

.....

[3]

(b) The banker receives confidential data across the internet. The data includes a digital signature.

Explain how a digital signature can make sure the data has **not** been changed during transmission.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

[5]

(c) The data that is transferred can also be verified using a checksum.

Explain how data can be verified using a checksum.

.....

.....

.....

.....

.....

..... [3]

5 A bank allows customers to access their accounts using an application that they can download onto a device such as a smartphone.

(a) The system that allows customers to access their accounts using the application is a client-server model.

Describe the roles of the different devices in this model.

.....

.....

.....

.....

.....

.....

.....

..... [4]

(b) The bank wants to protect the integrity of its data while transferring the data to other banks. Parity check is one example of data verification.

Complete the description of parity check when Computer A is transmitting data to Computer B.

Computer A and Computer B agree on whether to use ..... parity. Computer A divides the data into groups of ..... . The number of 1s in each group is counted. If the agreed parity is ..... and the group has an even number of 1s, a parity bit of 1 is appended, otherwise a parity bit of 0 is appended.

In a parity ..... check the bytes are grouped together, for example in a grid. The number of 1s in each column (bit position) is counted. A bit is assigned to each column to make the column match the parity. These parity bits are transmitted with the data as a parity ..... .

[5]

(c) The bank also needs to keep its customers' data private and secure.

(i) The bank's network has a firewall.

Explain how a firewall can help protect the customers' data.

.....

.....

.....

.....

.....

.....

.....

..... [3]

(ii) Customers need to use biometric authentication to access their accounts.
One biometric authentication method is facial recognition.

Facial recognition uses Artificial Intelligence (AI).

Describe how AI is used in facial recognition.

.....

.....

.....

.....

.....

.....

.....

..... [4]

3 An assessment board scans exam papers and stores the digitised papers on a server. Exam markers download the digitised papers to mark. The exam markers then upload the mark for each paper.

(a) The assessment board needs to make sure the data stored on the server is secure.

(i) Authentication methods can help to protect the server against hackers.

Identify **one other** security measure that helps to protect the server from hackers.

Describe how the security measure works.

Security measure .....

Description .....

.....

.....

.....

[3]

(ii) Identify **one** security measure that helps to protect the data when it is being transmitted to its destination. Describe how the security measure works.

Security measure .....

Description .....

.....

.....

.....

[3]

(b) The exam markers use software that operates as a thin-client to mark the exam papers.

Complete the table by identifying **two** characteristics of a thin-client.

Describe how each characteristic will be used in this software.

	Thin-client characteristic	**Description of use in this software**
1	.....	.....
	.....	.....
	.....	.....
	.....	.....
2	.....	.....
	.....	.....
	.....	.....
	.....	.....

[4]

(c) Data transmitted on the internet passes through multiple different systems.

(i) Describe the role of routers in the transmission of data through the internet.

.....

.....

.....

..... [2]

(ii) Describe the role of the PSTN (Public Switched Telephone Network) in the transmission of data through the internet.

.....

.....

.....

..... [2]

A-LEVEL COMPUTER SCIENCE • EXERCISE SHEET

6.2 Data Integrity

Name: _____ Class: _____ Date: _____ **Total: 34 marks**

KEY WORDS verification 核对 • validation 验证 • check digit 校验位 • data integrity 完整性 • checksum 校验和

Objective

Build the skills to answer exam questions on **data integrity** 完整性 — how **validation** and **verification** protect it, and the methods used for each.

You must be able to:

- explain how **validation** 验证 and **verification** 核对 protect data integrity
- describe and use methods of **validation**
- describe and use methods of **verification** during data entry and data transfer

1 Worked examples

Study these first. Each one shows the method for a question type used later — follow the steps and you can do the Practice and Exam-style questions yourself.

■ Validation vs verification

- **Validation** asks *"is this data sensible?"* — automatic checks before storing.
- **Verification** asks *"was this data copied/entered correctly?"* — confirms it was not changed.

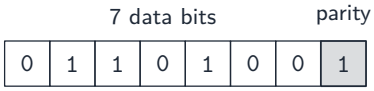
Use both: validation catches nonsense; verification catches copying errors. Neither proves the data is *factually* correct (a sensible, correctly-typed value can still be wrong).

■ Validation methods

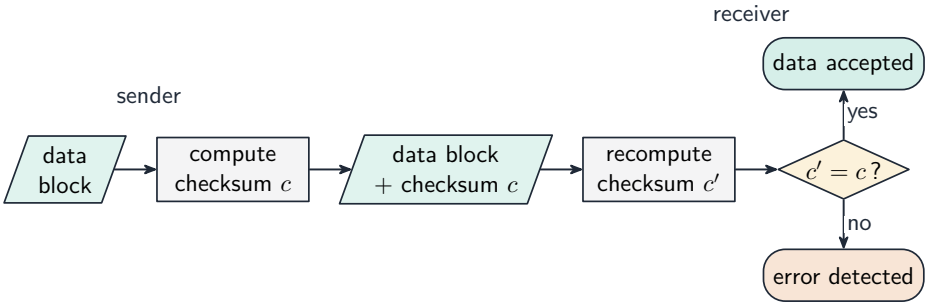
Check	Rejects...	Example
range	values outside limits	a month not in 1–12
length	wrong number of characters	a 5-digit phone number
type / character	wrong kind of data	a letter in an age field
format	wrong pattern	an email with no `@`
presence	empty required fields	a blank surname
check digit	mistyped long numbers	a wrong ISBN / card number

Verification methods

- **On entry: double entry** (type it twice and compare, like a new password) or a visual check.
- **On transfer** (bits can flip): a **parity check** adds a bit so the number of 1s is even (or odd); the receiver re-counts.



data has three 1s; for **even parity** the parity bit is **1** (four 1s in total)



worked example – checksum = (sum of bytes) mod 256

1 sum of all bytes: $X = 1185$

2 $X \div 256 = 4.629$, round down: $Y = 4$

3 $Z = Y \times 256 = 1024$

4 checksum $= X - Z = 1185 - 1024 = 161$

A checksum is the other main data-integrity check

A **checksum** sends a summary value the receiver recomputes and compares.

Check digit

A **check digit** is an extra digit added to the end of a long number (ISBN, barcode, card number) so that a mistyped digit can be spotted.

Worked example (modulo 11). For the digits `4 2 1 3`, multiply each by a weight (here 5, 4, 3, 2) and add: $4{\times}5 + 2{\times}4 + 1{\times}3 + 3{\times}2 = 37$. The check digit is chosen so the grand total — with the check digit itself weighted 1 — is a **multiple of 11**: $37 + c \equiv 0 \pmod{11}$, so $c = 7$. The full number is `42137`.

To **verify** a number, repeat the weighted sum including the check digit; if the total is a multiple of 11, the number is probably correct.

2 Practice

Now apply the methods above.

2.1 State the difference between **validation** and **verification**. [2]

2.2 Name the validation check for each: (a) a month must be 1–12 (b) an email must contain `@`. [2]

2.3 Describe how **double-entry** verification works. [1]

2.4 A byte uses **even parity**. The seven data bits are `1011001`. State the parity bit. [1]

3 Exam-style questions

3.1 Describe **three** validation checks, giving an example of each. [3]

3.2 Explain why validation **cannot guarantee** that stored data is correct. [2]

3.3 (a) Describe how a **parity check** detects an error during transmission. [2]

(b) State one limitation of a parity check. [1]

3.4 A new user sets a password by typing it into two boxes. State which technique this is and what it checks. [2]

3.5 A 4-digit code `5 1 3 2` uses a modulo-11 check digit. Each digit is multiplied by a weight (5, 4, 3, 2) and the check digit (weight 1) makes the total a multiple of 11. Calculate the **check digit**. Show your working. [3]

3.6 A membership number is a five-digit integer. When a number is typed in, the system checks it before use.

(a) **Draw one line** from each method to say whether it is used during **data entry** or during **data transfer**. [2]

method	**used during**
double entry	data entry
parity check	
visual check	data transfer
checksum	

(b) **State** the difference between **validation** and **verification**. [2]

(c) The number `41623` is typed as `14623` — the **first two digits** were transposed. **State** which single check would catch this, and **explain** why a **range check** would not. [3]

(d) A **check digit** is added to make a six-digit number. **Describe** how a check digit is calculated and used. [3]

(e) **Write** pseudocode for a function `Generate(Original)` that takes a five-digit integer and returns it with a check digit appended, where the check digit is the sum of the five digits modulo 10. [5]

Solutions

2.1 Validation checks the data is **sensible** (against rules) before storing; verification checks the data was **entered/transferred correctly** (not changed).

2.2 (a) **range** check. (b) **format** check.

2.3 The data (e.g. password) is entered **twice** and the two copies are compared; if they differ, there was a typing error.

2.4 `1011001` has **four** 1s (already even), so the parity bit is **0**.

3.1 Any three with examples, e.g.: range (month 1–12); length (a 6-character code); type (digits only in a phone field); format (email contains `@`); presence (required field not blank).

3.2 Validation only checks the data is the right **format/range**; a value can be sensible and correctly formatted yet **factually wrong** (e.g. "Bob" instead of "Bib"), which validation cannot detect.

3.3 (a) A parity bit makes the number of 1s even (or odd) when sent; the receiver recounts the 1s; if the count no longer matches, a bit was flipped — an error is detected.
(b) It misses an **even number** of flipped bits (e.g. two), which leave the parity unchanged.

3.4 Double-entry verification; it checks the two typed copies match, catching a typing error before the password is saved.

3.5 Weighted sum $= 5\times5 + 1\times4 + 3\times3 + 2\times2 = 25 + 4 + 9 + 4 = 42$; $42 \bmod 11 = 9$, so the check digit $= 11 - 9 = 2$. Check: $42 + 2 = 44 = 4 \times 11$.

3.6 (a) **Data entry**: double entry and visual check. **Data transfer**: parity check and checksum.
(b) **Validation** is an automatic check that data is **reasonable** — the right type, in range, the right format. **Verification** checks that data has been **copied or transmitted accurately**, that it matches the source.
(c) A **check digit**, because transposing two digits changes the weighted sum and so changes the digit that should follow. A range check passes both values: 14623 and 41623 are each five-digit numbers within the allowed range, so nothing about the range is violated.
(d) The check digit is calculated from the other digits by a fixed rule — often a weighted sum reduced modulo a number — and appended to them. Whenever the number is entered or received, the rule is applied again to the leading digits and the result compared with the digit that was carried; a mismatch means an error.
(e)

```
FUNCTION Generate(Original : INTEGER) RETURNS INTEGER
    DECLARE Total, Temp, CheckDigit : INTEGER
    Total ← 0
    Temp ← Original
    WHILE Temp > 0
        Total ← Total + (Temp MOD 10)
        Temp ← Temp DIV 10
    ENDWHILE
    CheckDigit ← Total MOD 10
    RETURN Original * 10 + CheckDigit
ENDFUNCTION
```

1 Draw **one** line from each verification method to indicate whether it is used during data transfer or data entry.

Verification Method	Use
Parity byte check	
Checksum	Data transfer
Visual check	
Parity block check	Data entry

[2]

6 Students are learning about a simple check digit method for data validation. In this method, a single check digit is appended to the end of an original number to give a new number.

The students are studying a method which:

- calculates the sum of all the digits in the original number
- uses integer division to calculate the remainder when the sum is divided by 10
- uses the remainder as the check digit
- appends the check digit to the original number, creating the new number.

For example:

original number	4162
sum of all digits	4 + 1 + 6 + 2 = 13
remainder when the sum is divided by 10 using integer division	3
new number	41623

The method described can be used to detect single-digit errors. For example, if the new number is incorrectly input as 41633, then the check digit does not match and the input will be rejected.

(a) An incorrect attempt was made to enter 41623. The **first two** digits were entered incorrectly; the **last three** digits were entered correctly.

When this number was tested, the check digit was found to be correct and the input was accepted.

Identify an example of the incorrect attempt to enter 41623 and explain why this number would **not** be rejected.

Number .....

Explanation .....

.....

[2]

(b) A module `Generate()` will take an integer value representing an original number and return an integer value representing a new number which includes the check digit.

The original number is always at least three digits in length.

Write pseudocode for the module `Generate()`

Assume that the parameter is valid.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

..... [7]