NAME DATE STARTED TARGET END DATE

GCE A LEVEL — COMPUTER SCIENCE UNIT 4 QUESTION PACK

1500U40-1 · 2015 spec Unit 4 Topic 5 · A2 unit, first sat 2017, 100 marks, 2h paper

REVISE.wales

COMPUTER SCIENCE — UNIT 4 · Security, Cryptography & Cyber-Attacks

Topic 4.5 — Symmetric / asymmetric encryption, biometrics, BYOD, phishing, penetration testing and access control

Comparing single-key (symmetric) and double-key (asymmetric) cryptography, identifying security issues with shared keys, describing biometric authentication, the risks of BYOD policies, common cyber-attack vectors (phishing, malware), the purpose of penetration testing, and how ID / smart-card and biometric systems control physical access.

2015 specification · current

Estimated time for entire question pack: ~2 h 18 min

Derived from the Unit 4 pace of ~1.5 min/mark, padded for written-prose answers (92 marks over 11 questions).

*You are advised to **not** attempt to complete all of this in one sitting.*

ABOUT THIS QUESTION PACK

This is a **comprehensive topic question pack**, not a single mock paper. It contains every question from the WJEC A2 Unit 4 papers (Summer 2017 – Summer 2024, COVID gap) that maps onto Topic 4.5 of the 2015 specification.

Questions are ordered by source paper date.

INSTRUCTIONS

Use black ink or black ball-point pen. Show all working. A calculator is allowed where useful.

For Examiner's use only

Q	Source	Max	Mark
1	S17 Q8	9	
2	S17 Q9	7	
3	S17 Q12	11	
4	S18 Q8	10	
5	S18 Q10	12	
6	S19 Q10	11	

Q	Source	Max	Mark
7	S22 Q7	4	
8	S22 Q8	5	
9	S22 Q13	7	
10	S22 Q14	8	
11	S23 Q13	8	
Total		**92**	

Security, Cryptography & Cyber-Attacks — what the spec asks

WJEC GCE A Level Computer Science (from 2015) · Unit 4: Computer Architecture, Data, Communication & Applications · Topic 4.5.

Symmetric (single-key) encryption

- Same key encrypts and decrypts — both parties must already share it.
- Fast — suitable for bulk data (AES, ChaCha20).
- Problem: securely distributing the key to the other party.
- If one key is leaked, all past and future messages are compromised.

Asymmetric (double-key) encryption

- Two mathematically-linked keys: **public** (shared) and **private** (secret).
- Encrypt with the recipient's public key → only their private key can decrypt.
- Sign with your private key → anyone with your public key can verify authenticity.
- Slower; in practice used to exchange a symmetric session key (TLS handshake).

Biometric authentication

- Unique biological / behavioural traits: fingerprint, iris, face, voice, typing rhythm.
- Hard to forge; can't be forgotten.
- Privacy concerns: biometrics can't be changed if leaked.
- Used in phones, border control, secure access to labs and labs/data centres.

Cyber-attack vectors

- Phishing: social engineering email to harvest credentials.
- Malware: viruses, worms, trojans, ransomware, spyware.
- Denial of service: flood resources to make service unavailable.
- Insider threats: legitimate users abusing access.

Penetration testing

- Authorised simulated attack to find vulnerabilities before attackers do.
- Black-box (no info), grey-box (some info), white-box (full info).
- Stages: recon, scanning, exploitation, privilege escalation, reporting.
- Output: report with severities, recommended fixes, retest schedule.

BYOD & access control

- BYOD: personal devices on company networks — lower hardware cost, but device variety / loss / leak risks.
- MDM / containers separate work data from personal apps.
- ID cards / smart cards: physical access control; can be combined with PIN.
- Multi-factor: something you know + have + are.

Crib sheet »

Security, Cryptography & Cyber-Attacks in one page

Quick-reference notes — revisit before each question.

Symmetric vs asymmetric

Sym: 1 key, fast, key-distribution problem.
Asym: public + private, slow, solves distribution.
TLS: asym to exchange a sym session key.

Biometric basics

Bio: fingerprint, iris, face, voice, gait.
Can't be forgotten; hard to forge.
Can't be reset if leaked.

Phishing red flags

Urgency / fear / authority appeals.
Mismatched display name vs domain.
Generic greeting, spelling errors.
Links to look-alike domains.

Pen-test stages

Recon → Scan → Exploit → Escalate → Report.
Box colour = info given (black / grey / white).
Always with written authorisation.

Access control layers

Something you know (password / PIN).
Something you have (card / phone / token).
Something you are (biometric).
Combine = MFA.

BYOD risks

Mixed personal/business data.
Lost / stolen device.
Inconsistent patching.
Mitigations: MDM, containers, VPN.

7. *(a)* When scheduling, name and describe the **three** basic states of a process. [6]

(b) Interrupts cause the operating system to respond to system events. Give **two** examples of common interrupts. [2]

(c) Describe a single buffer and a double buffer. Explain the role of a single buffer and a double buffer. Explain why double buffering is usually preferred. [5]

8. Cryptography uses asymmetric or symmetric encryption methods.

Symmetric encryption methods use a single key which encrypts and decrypts data. Asymmetric encryption methods use a public key for encryption and a private key for data decryption.

(a) Describe the advantages of asymmetric encryption and the advantages of symmetric encryption. [4]

(b) The Boolean operation XOR is often used in cryptography.

In the 8 bit ASCII character set, the characters OK! are represented by the following binary numbers.

$O = 01001111_2$
$K = 01001011_2$
$! = 00100001_2$

Use XOR to encrypt the string OK! with the 8 bit binary key 11110011_2 [3]

(c) Describe **two** deficiencies of the key used in question 8*(b)*. [2]

9. A company with a large office building operates a “Bring Your Own Device to Work” (BYOD) scheme allowing employees to use personal devices (e.g. tablet or laptop) on the company’s network.

(a) Describe the hardware necessary to connect a device to the company’s network wirelessly and provide an Internet connection. [3]

(b) Identify and describe **two** network applications that could be used by an employee with a connected device. [4]

7. *(a)* When scheduling, name and describe the **three** basic states of a process. [6]

(b) Interrupts cause the operating system to respond to system events. Give **two** examples of common interrupts. [2]

(c) Describe a single buffer and a double buffer. Explain the role of a single buffer and a double buffer. Explain why double buffering is usually preferred. [5]

8. Cryptography uses asymmetric or symmetric encryption methods.

Symmetric encryption methods use a single key which encrypts and decrypts data. Asymmetric encryption methods use a public key for encryption and a private key for data decryption.

(a) Describe the advantages of asymmetric encryption and the advantages of symmetric encryption. [4]

(b) The Boolean operation XOR is often used in cryptography.

In the 8 bit ASCII character set, the characters OK! are represented by the following binary numbers.

$O = 01001111_2$
$K = 01001011_2$
$! = 00100001_2$

Use XOR to encrypt the string OK! with the 8 bit binary key 11110011_2 [3]

(c) Describe **two** deficiencies of the key used in question 8*(b)*. [2]

9. A company with a large office building operates a “Bring Your Own Device to Work” (BYOD) scheme allowing employees to use personal devices (e.g. tablet or laptop) on the company’s network.

(a) Describe the hardware necessary to connect a device to the company’s network wirelessly and provide an Internet connection. [3]

(b) Identify and describe **two** network applications that could be used by an employee with a connected device. [4]

10. Expert systems are widely used by organisations for a variety of purposes. Describe the benefits to an organisation of using an expert system. [8]

11. Explain the use of multi-level indexes and draw a diagram to demonstrate the operation of a three-level index. [6]

12. Khan's Pharmaceuticals currently uses an ID card system to control employee access to its premises. This has proved problematical with employees swapping cards and the company now wishes to use a voice print recognition system in its place.

Describe how this system would operate and explain the benefits and drawbacks associated with a biometric system used for this purpose. [11]

END OF PAPER

10. Expert systems are widely used by organisations for a variety of purposes. Describe the benefits to an organisation of using an expert system. [8]

11. Explain the use of multi-level indexes and draw a diagram to demonstrate the operation of a three-level index. [6]

12. Khan's Pharmaceuticals currently uses an ID card system to control employee access to its premises. This has proved problematical with employees swapping cards and the company now wishes to use a voice print recognition system in its place.

Describe how this system would operate and explain the benefits and drawbacks associated with a biometric system used for this purpose. [11]

END OF PAPER

8. *(a)* (i) State a security problem that may arise if a single key (symmetric) encryption method is used. [1]

(ii) An asymmetric encryption method makes use of a private and public key pair. Explain how these could be used in the safe transfer of data over the internet. [3]

(b) A method of encrypting text is the Caesar cypher. Each letter is moved forward in the alphabet by a fixed number of places using modulo 26 arithmetic. For example, using a shift of 5 places, W becomes B.

State why messages using the Caesar cypher can be decrypted easily by an unauthorised person. [1]

(c) Two members of staff in a law firm decide to exchange a confidential message over the Internet using a stream cypher method:

- Letters in the original message are shifted forward by a specified number of positions in the alphabet using modulo 26 arithmetic, but each character in the message is moved forward by a different number of letters.
- The shifts for the first two letters in the message have been agreed:

  shift[1] = 4

  shift[2] = 3
- The letter shifts for each following letter in the message are calculated with the formula:

  shift[N+2] = shift[N] + 2 times shift[N+1]

  where N = (position of the letter in the message) –2

  In this way, for the third letter,

  shift[3] = shift[1] + 2 x shift[2] = 4 + (2 x 3) = 10
- Modulo 26 arithmetic is again used. For example, a shift calculated as 30 places would become a shift of (30-26) = 4 places.

(i) Calculate the letter shifts for the characters in the fourth and fifth positions. [2]

(ii) Encrypt the word ZEN using this cypher. [3]

9. A large and complex computing task needs to be carried out. Programmers consider two possible solutions:

- using parallel processing on a large computer
- using distributed processing on smaller computers.

(a) Explain what is meant by parallel processing and distributed processing. [4]

(b) Discuss the factors that the programmers might consider when making a choice between parallel processing and distributed processing. [4]

10. *(a)* Explain what is meant by the term biometric data. [2]

(b) Describe **two** examples of biometric data. [2]

(c) Explain using an example how biometric data can permit access to a secure area or system. [4]

(d) Explain why there may be objections to the use of biometric data. [4]

11. Large organisations use database management systems.

Explain what is meant by a database management system and discuss the tasks carried out by the Information Technology staff who operate the database management system. [10]

END OF PAPER

8. Define the term **data mining** and describe how three different organisations might use data mining. [8]

9. Describe four data validation techniques. [4]

10. *(a)* Describe the types of malicious software which might be transferred to computers and the delivery mechanisms, and the steps that can be taken to protect against these. [6]

(b) Computer data may be at its highest security risk during transfer from one location to another. Outline the risks that exist at this time, and how they can be minimised. [4]

11. A city is developing a new light railway system to connect the city centre to the surrounding suburbs. The system will use driverless trains, and several computer centres will control different areas of the network.

(a) Give examples of input and output which might be required by control systems on board the trains. [3]

(b) The system will be safety critical. Explain what is meant by a safety critical system, describing measures that are involved in ensuring safety. [5]

12. Describe the operation of a mainframe computer using a multi-programming, multi-user operating system. [7]

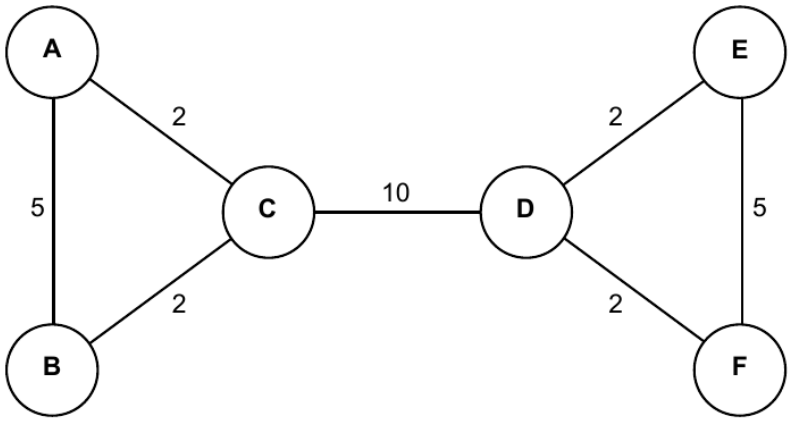
13. Explain what is meant by distributed processing, and describe how this will operate using an example that you have studied. [6]

END OF PAPER

6. In a certain computer network the protocol used to determine lowest cost routes is based on transfer rates and delays. Transfer rates are based on bandwidth of network links. Delays represent the overhead arising from the time taken for a router to process, queue and transmit a data packet.

The total route cost is calculated as the cost of each link multiplied by the total of the delay factors of each intermediate router visited.

This is a diagram of the network. The delay at each intermediate router = 1.2.



(a) Calculate the lowest cost route from router A to router F. [2]

(b) (i) A new link of bandwidth cost = 14 is to be added from B to F. Re-calculate the lowest cost route from router A to router F. [2]

(ii) The link from router C to router D is then upgraded to a network cost of 5. Describe the effect the upgrade will have on overall network costs. [2]

7. Phishing is the most common cyber-attack vector.

(a) Explain what is meant by the term 'cyber-attack vector'. [2]

(b) Describe **two** other cyber-attack vectors. [4]

8. Penetration testing is an important aspect of computer security.

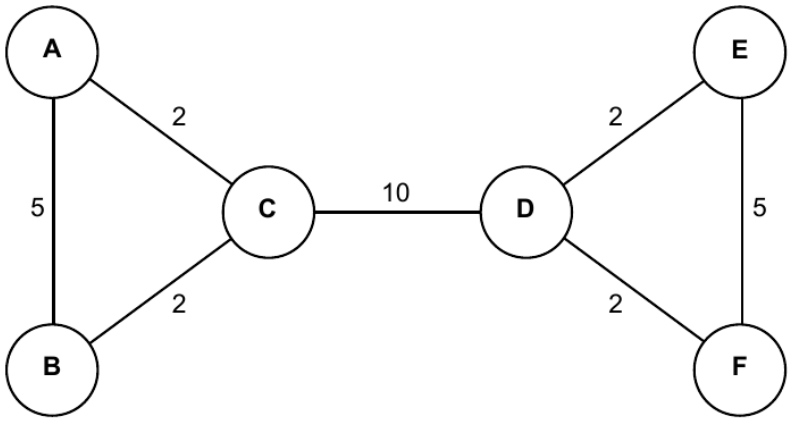
(a) State what is meant by the term penetration testing. [1]

(b) Describe **three** penetration testing strategies. [6]

6. In a certain computer network the protocol used to determine lowest cost routes is based on transfer rates and delays. Transfer rates are based on bandwidth of network links. Delays represent the overhead arising from the time taken for a router to process, queue and transmit a data packet.

The total route cost is calculated as the cost of each link multiplied by the total of the delay factors of each intermediate router visited.

This is a diagram of the network. The delay at each intermediate router = 1.2.



(a) Calculate the lowest cost route from router A to router F. [2]

(b) (i) A new link of bandwidth cost = 14 is to be added from B to F. Re-calculate the lowest cost route from router A to router F. [2]

(ii) The link from router C to router D is then upgraded to a network cost of 5. Describe the effect the upgrade will have on overall network costs. [2]

7. Phishing is the most common cyber-attack vector.

(a) Explain what is meant by the term 'cyber-attack vector'. [2]

(b) Describe **two** other cyber-attack vectors. [4]

8. Penetration testing is an important aspect of computer security.

(a) State what is meant by the term penetration testing. [1]

(b) Describe **three** penetration testing strategies. [6]

9. A community craft group that sells jewellery to the general public is creating a database to manage its sales.

This is a design for a database table it intends to use:

Customer (customerID, surname, orderDate, itemNo, orderQuantity)

(a) Write an SQL command that will create this table using appropriate data types and sizes. [4]

The Customer table is then populated with the following data:

customerID	surname	orderDate	itemNo	orderQuantity
C00001	Heald	01/06/2021	CT00016	3
C00002	Munden	03/06/2021	CT00017	6
C00001	Heald	08/06/2021	CT00014	4

An Item table has already been created in the database and contains this data:

itemNo	stockLevel	itemName	price
CT00011	7	Bracelet	101
CT00014	11	Necklace	123
CT00016	4	Ring	81
CT00017	12	Necklace	80

(b) Write an SQL command to add this record to the Item table. [2]

CT00111	13	Earrings	97

(c) Write an SQL command to change the price of itemNo CT00016 to 93. [1]

10. (a) Describe what is meant by the term relational database. [2]

(b) Describe the advantages of database normalisation. [4]

A health care company is creating a relational database to manage its dental surgeries located in different towns across Wales.

Each dental surgery employs **dentists** who will only work in that **surgery**. **Patients** will be registered with one of the dentists and will only be treated by that dentist. Patients will book **appointments** to see their dentist.

(c) Produce an entity relationship diagram for the system described. [3]

(d) Design a database structure in third normal form for the system. [3]

11. The increase in speed due to parallel processing can be calculated as:

$$\frac{1}{S + \frac{P}{N}}$$

where P = parallel fraction, N = number of processors and S = serial fraction. (S = 1 – P)

(a) Calculate the increase in speed due to parallel processing using 10 processors and the increase in speed of doing the same task using 1000 processors, where the parallel fraction P is equal to:

- 0.5 for 10 and 1000 processors
- 0.9 for 10 and 1000 processors [4]

(b) Discuss the effect that increasing the parallel fraction of the task will have on the speed due to parallel processing. [3]

12. Describe the advantages of using a distributed database. [4]

13. Cryptography may be based on symmetric or asymmetric algorithms. Describe the advantages of using asymmetric encryption. [6]

14. A local hospital needs to ensure that access to its medical laboratories is restricted to authorised personnel. It is considering using biometric technologies to identify and restrict access to authorised personnel only.

Describe the biometric options available to the hospital and explain the main benefits and drawbacks of biometric security technologies. [9]

END OF PAPER

10. (a) Describe what is meant by the term relational database. [2]

(b) Describe the advantages of database normalisation. [4]

A health care company is creating a relational database to manage its dental surgeries located in different towns across Wales.

Each dental surgery employs **dentists** who will only work in that **surgery**. **Patients** will be registered with one of the dentists and will only be treated by that dentist. Patients will book **appointments** to see their dentist.

(c) Produce an entity relationship diagram for the system described. [3]

(d) Design a database structure in third normal form for the system. [3]

11. The increase in speed due to parallel processing can be calculated as:

$$\frac{1}{S + \frac{P}{N}}$$

where P = parallel fraction, N = number of processors and S = serial fraction. (S = 1 – P)

(a) Calculate the increase in speed due to parallel processing using 10 processors and the increase in speed of doing the same task using 1000 processors, where the parallel fraction P is equal to:

- 0.5 for 10 and 1000 processors
- 0.9 for 10 and 1000 processors [4]

(b) Discuss the effect that increasing the parallel fraction of the task will have on the speed due to parallel processing. [3]

12. Describe the advantages of using a distributed database. [4]

13. Cryptography may be based on symmetric or asymmetric algorithms. Describe the advantages of using asymmetric encryption. [6]

14. A local hospital needs to ensure that access to its medical laboratories is restricted to authorised personnel. It is considering using biometric technologies to identify and restrict access to authorised personnel only.

Describe the biometric options available to the hospital and explain the main benefits and drawbacks of biometric security technologies. [9]

END OF PAPER

12. (a) Explain what is meant by a distributed system and describe what will be distributed in the system. [2]

(b) A car manufacturer has a number of dealerships across the UK. Car owners take their cars for servicing each year to a convenient dealership. Records are kept of servicing, any faults found, and replacement parts fitted.

Explain the advantages to the company of implementing a distributed database system across its dealerships compared with using a single centralised database. [4]

13. (a) Explain the advantages and disadvantages of single key (symmetric) encryption compared with double key (asymmetric) encryption, giving an example, for each method, of a situation where that method would be the most suitable. [6]

(b) Text is stored in 8-bit binary ASCII format, with numeric codes representing each character:

A = 65_{10} $0100\ 0001_2$

B = 66_{10} $0100\ 0010_2$

C = 67_{10} $0100\ 0011_2$

The text is encrypted using a sequential XOR method:

- The first character is encrypted by XOR with the key value $0110\ 1010_2$
- The second character is encrypted by XOR with the encrypted value of the first character
- The third character is encrypted by XOR with the encrypted value of the second character

Using this algorithm, encrypt the word CAB. [3]

14. (a) Identify **two** hardware devices required to make a wireless connection to a network. [2]

(b) State **two** protocols used for wireless digital communication. [2]

(c) Describe **one** disadvantage of using a public wireless network. [2]

15. Information and advice on medical and health issues are readily available to the public through the internet, including online expert systems. Discuss the possible effects of using the internet for this purpose on health professionals and the wider community. [9]

END OF PAPER

END OF QUESTION PACK

11 questions · 92 marks · ~2 h 18 min
Source: WJEC A2 Computer Science Unit 4 (1500U40-1), Summer 2017–2024, COVID gap
Curated for WJEC Computer Science 2015 spec A2 Unit 4 — Topic 5 (4.5)