Cambridge International A Level

Cambridge International Examinations
Cambridge International Advanced Level

CANDIDATE NAME

CENTRE NUMBER

CANDIDATE NUMBER

8788782541

COMPUTER SCIENCE **9608/31**

Paper 3 Advanced Theory **May/June 2016**

1 hour 30 minutes

Candidates answer on the Question Paper.

No Additional Materials are required.

No calculators allowed.

READ THESE INSTRUCTIONS FIRST

Write your Centre number, candidate number and name in the spaces at the top of this page.
Write in dark blue or black pen.
You may use an HB pencil for any diagrams, graphs or rough working.
Do not use staples, paper clips, glue or correction fluid.
DO **NOT** WRITE IN ANY BARCODES.

Answer **all** questions.
No marks will be awarded for using brand names of software packages or hardware.

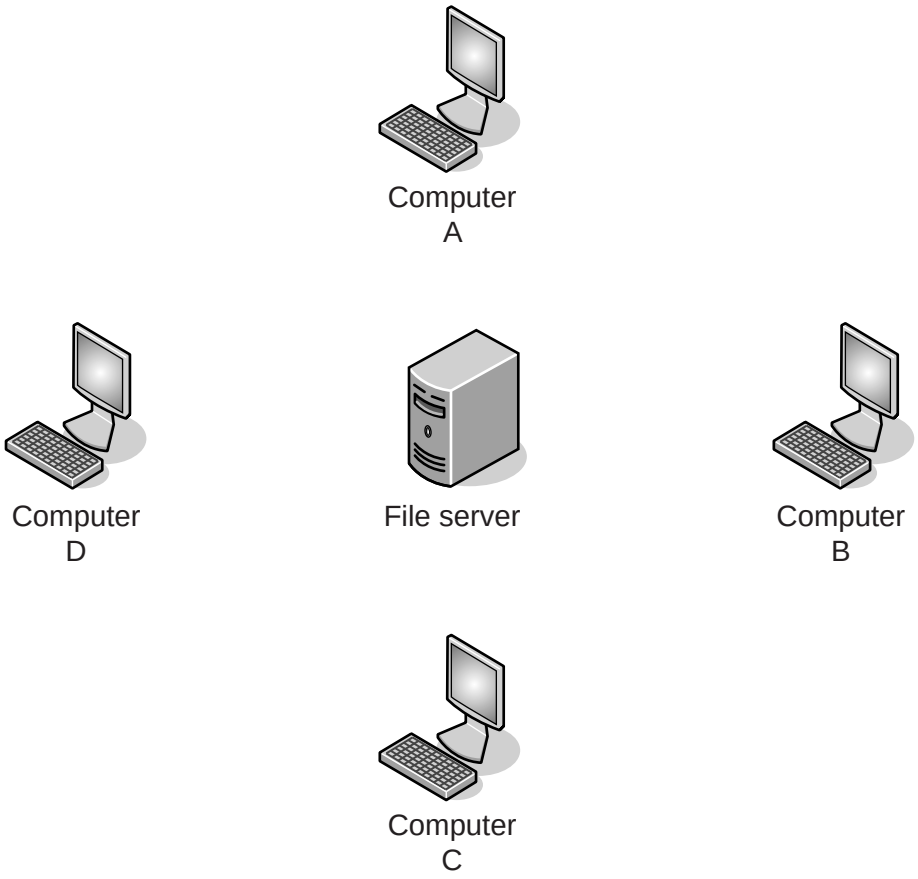
At the end of the examination, fasten all your work securely together.
The number of marks is given in brackets [ ] at the end of each question or part question.

The maximum number of marks is 75.

DC (NH/AR) 115894/3
© UCLES 2016

1 A Local Area Network (LAN) consists of four computers and one server. The LAN uses a bus topology.

(a) Complete the diagram below to show how the computers and the File server could be connected.



[2]

(b) Computer C sends a data packet to Computer A.

Three statements are given below.

Tick (✓) to show whether each statement is true or false.

Statement	True	False
Computer C uses the IP address of Computer A to indicate that the packet is for Computer A.		
Computer B can read the packet sent from Computer C to Computer A.		
The File server routes the packet to Computer A.		

[3]

© UCLES 2016

(c) Computer A starts transmitting a packet to Computer C. At exactly the same time, the File server starts transmitting a packet to Computer D. This causes a problem.

(i) State the name given to this problem.

.....

.....[1]

(ii) Give **three** steps taken by both Computer A and the File server to allow them to transmit their packets successfully.

Step 1 .....

.....

Step 2 .....

.....

Step 3 .....

.....[3]

(d) Adding a switch to the LAN changes its topology. Explain how the use of a switch removes the problem identified in **part (c)(i)**.

.....

.....

.....

.....

.....

.....

.....

.....[4]

© UCLES 2016

2 Digital certificates are used in Internet communications. A Certificate Authority (CA) is responsible for issuing digital certificates.

(a) Name **three** data items present in a digital certificate.

1 .....

2 .....

3 .....[3]

(b) The method of issuing a digital certificate is as follows:

1 A user starts an application for a digital certificate using their computer. On this computer a key pair is generated. This key pair consists of a public key and an associated private key.

2 The user submits the application to the CA. The generated ..... **(i)** ..... key and other application data are sent. The key and data are encrypted using the CA's ..... **(ii)** ..... key.

3 The CA creates a digital document containing all necessary data items and signs it using the CA's ..... **(iii)** ..... key.

4 The CA sends the digital certificate to the individual.

In the above method there are three missing words. Each missing word is either 'public' or 'private'.

State the correct word. Justify your choice.

(i) .....

Justification .....

.....[2]

(ii) .....

Justification .....

.....[2]

(iii) .....

Justification .....

.....[2]

© UCLES 2016

(c) Alexa sends an email to Beena.

Alexa's email program:

- produces a message digest (hash)
- uses Alexa's private key to encrypt the message digest
- adds the encrypted message digest to the plain text of her message
- encrypts the whole message with Beena's public key
- sends the encrypted message with a copy of Alexa's digital certificate

Beena's email program decrypts the encrypted message using her private key.

(i) State the name given to the encrypted message digest.

.....[1]

(ii) Explain how Beena can be sure that she has received a message that is authentic (not corrupted or tampered with) and that it came from Alexa.

.....

.....

.....

.....[2]

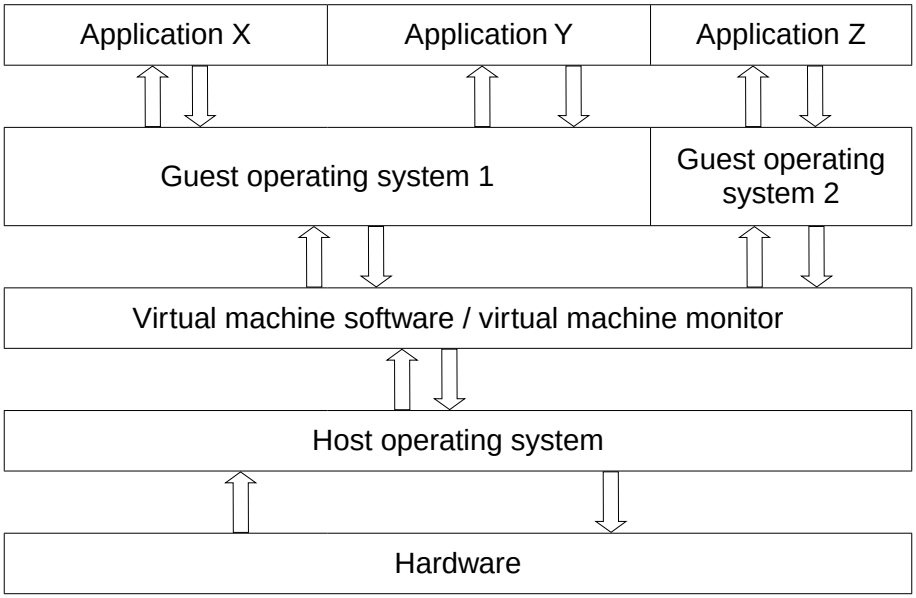
(iii) Name **two** uses where encrypted message digests are advisable.

1 .....

2 .....[2]

© UCLES 2016

3 **(a)** The following diagram shows how applications X, Y and Z can run on a virtual machine system.



(i) The virtual machine software undertakes many tasks.

Describe **two** of these tasks.

Task 1 .....

.....

Task 2 .....

.....[2]

(ii) Explain the difference between a **guest operating system** and a **host operating system**.

.....

.....

.....

.....[2]

(b) A company uses a computer as a web server. The manufacturer will no longer support the computer's operating system (OS) in six months' time. The company will then need to decide on a replacement OS.

The company is also considering changing the web server software when the OS is changed.

Whenever any changes are made, it is important that the web server service is not disrupted.

In developing these changes, the company could use virtual machines.

(i) Describe **two** possible uses of virtual machines by the company.

Use 1 .....

.....

.....

.....

Use 2 .....

.....

.....

.....[4]

The web server often has to handle many simultaneous requests.

(ii) The company uses a virtual machine to test possible solutions to the changes that they will need to make.

Explain **one** limitation of this approach.

.....

.....

.....

.....[2]

4 **(a)** Three file organisation methods and two file access methods are shown below.

Draw lines to link each file organisation method to its appropriate file access method or methods.

File organisation method	File access method
serial	direct
sequential	sequential
random	

[4]

(b) A bank has a very large number of customers. The bank stores data for each customer. This includes:

- unique customer number
- personal data (name, address, telephone number)
- transactions

The bank computer system makes use of three files:

- A – a file that stores customer personal data. This file is used at the end of each month for the production of the monthly statement.
- B – a file that stores encrypted personal identification numbers (PINs) for customer bank cards. This file is accessed when the customer attempts to withdraw cash at a cash machine (ATM).
- C – a file that stores all customer transaction records for the current month. Every time the customer makes a transaction, a new record is created.

For each of the files A, B and C, state an appropriate method of organisation. Justify your choice.

(i) File A organisation .....

Justification .....

.....

.....

.....[3]

(ii) File B organisation .....

Justification .....

.....

.....

.....[3]

(iii) File C organisation .....

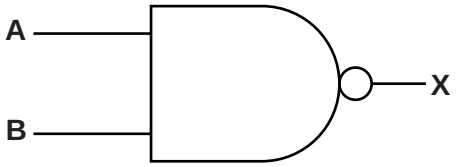
Justification .....

.....

.....

.....[3]

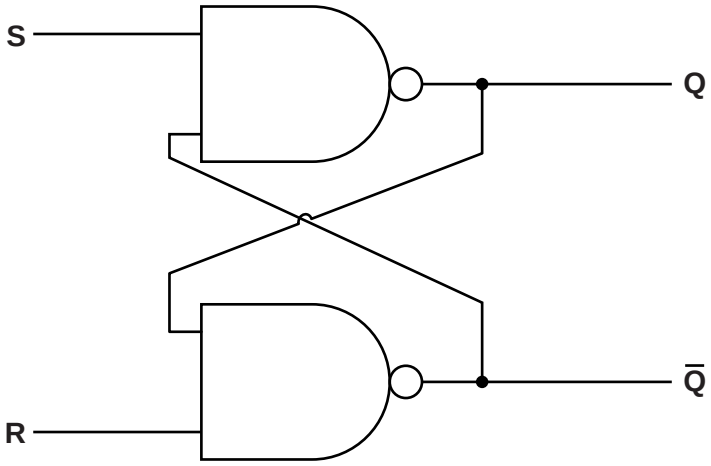
5 **(a)** Complete the truth table for this NAND gate:



A	B	X
0	0	
0	1	
1	0	
1	1	

[1]

A SR flip-flop is constructed using two NAND gates.



(b) **(i)** Complete the truth table for the SR flip-flop.

	S	R	Q	$\bar{Q}$
Initially	1	0	0	1
R changed to 1	1	1		
S changed to 0	0	1		
S changed to 1	1	1		
S and R changed to 0	0	0		

[4]

(ii) One of the combinations in the truth table should not be allowed to occur.

State the values of S and R that should not be allowed. Justify your choice.

S = ... R = ...

.....

.....

.....

.....[3]

© UCLES 2016

Another type of flip-flop is the JK flip-flop.

(c) (i) Give one extra input present in the JK flip-flop.

.....

.....[1]

(ii) Give **one** advantage of the JK flip-flop.

.....

.....[1]

(d) Describe the role of flip-flops in a computer.

.....

.....

.....

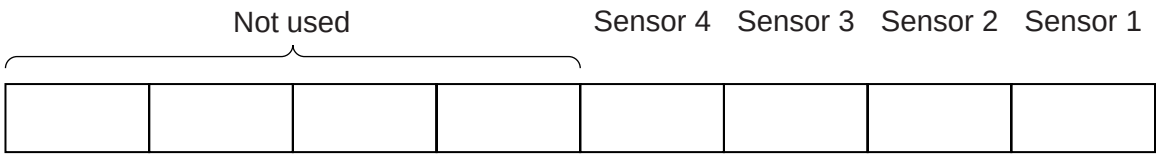
.....[2]

6 An intruder detection system for a large house has four sensors. An 8-bit memory location stores the output from each sensor in its own bit position.

The bit value for each sensor shows:

- 1 – the sensor has been triggered
- 0 – the sensor has not been triggered

The bit positions are used as follows:



The output from the intruder detection system is a loud alarm.

(a) (i) State the name of the type of system to which intruder detection systems belong.

.....[1]

(ii) Justify your answer to **part (i)**.

.....

.....[1]

(b) Name **two** sensors that could be used in this intruder detection system. Give a reason for your choice.

Sensor 1 .....

Reason .....

.....

Sensor 2 .....

Reason .....

.....[4]

The intruder system is set up so that the alarm will only sound if two or more sensors have been triggered.
An assembly language program has been written to process the contents of the memory location.

The table shows part of the instruction set for the processor used.

Instruction		Explanation
Op code	Operand	
LDD	<address>	Direct addressing. Load the contents of the given address to ACC
STO	<address>	Store the contents of ACC at the given address
INC	<register>	Add 1 to the contents of the register (ACC or IX)
ADD	<address>	Add the contents of the given address to the contents of ACC
AND	<address>	Bitwise AND operation of the contents of ACC with the contents of <address>
CMP	#n	Compare the contents of ACC with the number n
JMP	<address>	Jump to the given address
JPE	<address>	Following a compare instruction, jump to <address> if the compare was True
JGT	<address>	Following a compare instruction, jump to <address> if the content of ACC is greater than the number used in the compare instruction
END		End the program and return to the operating system

© UCLES 2016

[Turn over

(c) Part of the assembly code is:

	Op code	Operand
SENSORS:		B00001010
COUNT:		0
VALUE:		1
LOOP:	LDD	SENSORS
	AND	VALUE
	CMP	#0
	JPE	ZERO
	LDD	COUNT
	INC	ACC
	STO	COUNT
ZERO:	LDD	VALUE
	CMP	#8
	JPE	EXIT
	ADD	VALUE
	STO	VALUE
	JMP	LOOP
EXIT:	LDD	COUNT
TEST:	CMP	…
	JGT	ALARM

© UCLES 2016

(i) Dry run the assembly language code. Start at `LOOP` and finish when `EXIT` is reached.

BITREG	COUNT	VALUE	ACC
B00001010	0	1	

[4]

(ii) The operand for the instruction labelled `TEST` is missing.

State the missing operand.

.....[1]

(iii) The intruder detection system is improved and now has eight sensors.

One instruction in the assembly language code will need to be amended.

Identify this instruction .....

Write the amended instruction .....[2]

© UCLES 2016

BLANK PAGE

Permission to reproduce items where third-party owned material protected by copyright is included has been sought and cleared where possible. Every reasonable effort has been made by the publisher (UCLES) to trace copyright holders, but if any items requiring clearance have unwittingly been included, the publisher will be pleased to make amends at the earliest possible opportunity.

To avoid the issue of disclosure of answer-related information to candidates, all copyright acknowledgements are reproduced online in the Cambridge International Examinations Copyright Acknowledgements Booklet. This is produced for each series of examinations and is freely available to download at www.cie.org.uk after the live examination series.

Cambridge International Examinations is part of the Cambridge Assessment Group. Cambridge Assessment is the brand name of University of Cambridge Local Examinations Syndicate (UCLES), which is itself a department of the University of Cambridge.