2024 EXAMINATIONS

Part II

COMPUTING AND COMMUNICATIONS

Available Time **[2 Hours]**

Recommended Completion Time **[2 Hours]**

SCC.363 Security and Risk

*Candidates are asked to answer **THREE** questions from **FOUR**; each question is worth a total of 20 marks.*

Total pages: 7

Question 1

1a. Briefly explain the following terms and for each provide one example of a technique that implements it:

i. mandatory access control policy; **[2 marks]**
ii. message authentication code; **[2 marks]**
iii. anonymity; **[2 marks]**
iv. least privilege; **[2 marks]**
v. non-repudiation. **[2 marks]**

1b. A key exchange protocol is described in the following steps. Identify an attack the protocol is vulnerable to and add additional steps and/or amend the existing ones to explain in detail your attack.

STEP 1: A and B share a prime number q and integer α
STEP 2: A generates private key PRA and computes public key PUA = α^(PRA) mod q
STEP 3: B generates private key PRB and computes public key PUB = α^(PRB) mod q
STEP 4: A sends PUA to B and B calculates K = PUA^(PRB) mod q
STEP 5: B sends PUB to A and A calculates K = PUB^(PRA) mod q

[6 marks]

1c. Consider the following mandatory access control policy that implements the Bell-LaPadula model by applying the simple security and the *-property rules:

Classification: Restricted < Confidential < Secret < Top Secret

SUBJECTS = {user1, user2, user3}
OBJECTS = {file1, file2, file3}
OPERATIONS = {read, write, read/write}

Clearance level: {user1, Confidential}, {user2, Secret}, {user3, Top Secret}
Objects classification: {file1, Confidential}, {file2, Secret}, {file3, Top Secret}

What operations are permitted for user2 on file1 and why? **[2 marks]**
What operations are permitted for user1 on file3 and why? **[2 marks]**

[20 marks]

Question 2

2a. Briefly explain the following terms, and for each provide one example of a technique that implements it:

i.	dynamic packet filtering;	**[2 marks]**
ii.	buffer overflow;	**[2 marks]**
iii.	data integrity.	**[2 marks]**

2b. Figure 1 shows an AES mode. Consider the scenario where an adversary knows any pair of plaintext Pi and ciphertext Ci, where index *i* is a positive integer.

i.	Explain what attack may be possible and why.	**[4 marks]**
ii.	Provide a detailed explanation (steps) of the possible attack.	**[4 marks]**

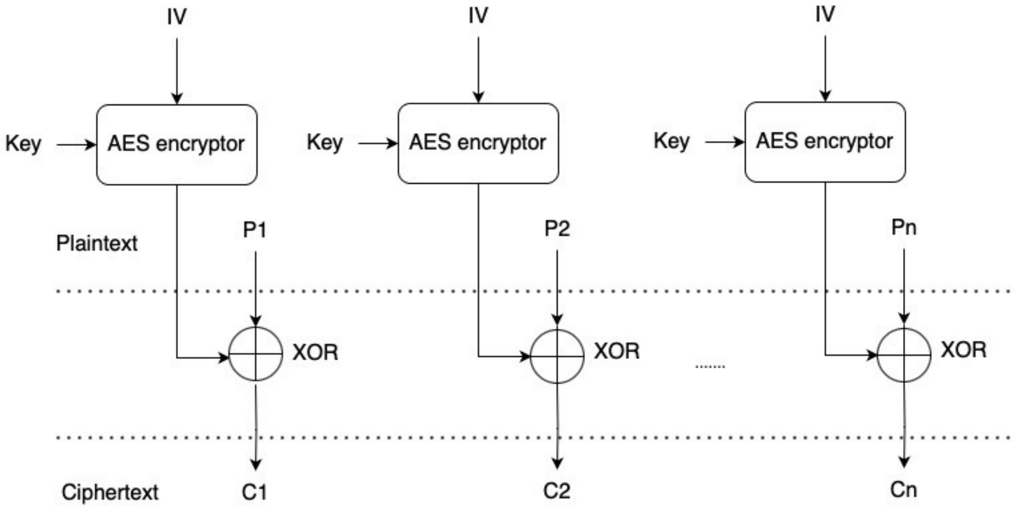

Figure 1 - An AES mode.

2c. Consider the following Role-Based Access Control (RBAC) policy:

USERS = {Alice, Bob, Charlie}
ROLES = {Admin, Manager, Employee}
OPS = {Read, Write, Delete}
OBS = {Files, Documents, Emails}
PRMS = OPS x OBS

A double-headed arrow "←→" is used to define an assignment between elements of the sets. E.g. {u1} ←→ {r1} reads: user u1 is assigned to role r1.
A single-headed arrow "→" is used to define a role hierarchy. E.g. {r1} → {r2} reads: role r1 inherits role r2.

Question *2* continues on next page

The relationships between the sets are defined as follows:
{Alice} ←→ {Admin}
{Bob} ←→ {Manager}
{Charlie} ←→ {Employee}

Role Hierarchies:
{Admin} → {Manager}
{Manager} → {Employee}

Additional assignments are as follows:
{Admin} ←→ {{Read, Files}, {Write, Documents}, {Delete, Emails}}
{Manager} ←→ {{Read, Documents}, {Write, Emails}, {Delete, Files}}
{Employee} ←→ {{Read, Files}, {Write, Documents}}

Given this RBAC policy, answer the following questions:

i. Which permissions are accessible by Alice? **[1 mark]**

ii. Which permissions are accessible by Bob? **[1 mark]**

iii. Which permissions are accessible by Charlie? **[1 mark]**

iv. Amend the RBAC policy to introduce a new role, Supervisor, that inherits permissions from both Manager and Employee roles. Describe the role assignments and hierarchy changes necessary to accommodate this addition. **[1 mark]**

v. Is the hierarchy {Employee} → {Admin} a valid relationship and why. **[1 mark]**

vi. If we set {Alice} ←→ {Manager}, explain what will change in the list of permissions for Alice and why. **[1 mark]**

[20 marks]

Question 3

3.a The CIA triad is a respected model designed to guide policies for information security within an organisation.

i. Provide the three principles that the three letters CIA stand for and provide a definition for each of them.

[3 marks]

ii. A message is transmitted from Alice to Bob. For each of the CIA properties, provide one possible technique that Alice and Bob can use to achieve that property.

[3 marks]

3.b The Plan Do Check Act Cycle (also known as the Deming Cycle) provides a simple concept to understand what information security management is. Provide the objective of each of th e four phases.

[4 marks]

3.c Explain the key sources of uncertainty in risk management.

[4 marks]

3.d Ideas from economics can help us understand cyber security issues in a broader context.

i. Use an example to describe the concept of lock in cost (Not restricted to cyber security examples).

[2 marks]

ii. Use the concepts of hidden information and hidden action to explain potential reasons for the phenomenon that sometimes users who have purchased powerful antivirus products suffer more from virus attacks.

[2 marks]

iii. Briefly explain why so much online information is free and zero is a fair price.

[2 marks]

[20 marks]

Question 4

4.a Assume that X, Y and Z are three independent discrete random variables. Their distributions are provided by the following three tables.

xi	1	4	8	15	20
P(X=xi)	0.20	0.25	0.15	0.36	0.04

yi	-5	-3	0	3	6
P(Y=yi)	0.30	0.11	0.16	0.25	0.18

zi	-1	0	2	6	8
P(Z=zi)	0.05	0.15	0.20	0.33	0.27

i. Find the standard deviation of the random variable T = 2X+4Y+6Z.

[4 marks]

ii. Find the probability that Y is strictly larger than Z.

[2 marks]

iii. Find the probability that X+Y lies in the range of [0, 10].

[2 marks]

4.b Suppose a cybersecurity analyst is tasked with assessing the risk of a potential data breach in a company's network. The analyst knows that 5% of all emails received by the company contain malicious attachments. Additionally, the company's email filtering system is 95% effective at correctly identifying and blocking emails with malicious attachments, but it also incorrectly flags 3% of legitimate emails as malicious. Now, if the analyst receives an alert from the email filtering system indicating that an email has been flagged as containing a malicious attachment, what is the probability that the email actually contains a malicious attachment?

[5 marks]

4.c A cybersecurity firm needs to allocate limited resources effectively to mitigate cybersecurity risks across multiple client networks. The firm must optimize resource allocation to minimize the overall cybersecurity risk while staying within budget constraints.

Question *4* continues on next page

Consider the following scenario:

The cybersecurity firm offers four primary services to its clients: network monitoring, vulnerability assessments, intrusion detection, and incident response. Each service requires a certain amount of resources, including financial cost, manpower and software licenses, and contributes differently to reducing cybersecurity risk.

Network monitoring: Requires £3000, 5 manpower resources and 10 software licenses. It reduces cybersecurity risk by 20 units.

Vulnerability assessments: Requires £5000, 8 manpower resources and 15 software licenses. It reduces cybersecurity risk by 30 units.

Intrusion detection: Requires £9000, 10 manpower resources and 20 software licenses. It reduces cybersecurity risk by 40 units.

Incident response: Requires £11000, 12 manpower resources and 25 software licenses. It reduces cybersecurity risk by 50 units.

The firm has a total budget of £100000, 300 available manpower resources in total, and 1000 available software licenses in total. Also notice that the allocation of resources cannot be negative.

Develop a linear optimization model to help the cybersecurity firm allocate resources effectively and minimize cybersecurity risk. Express the formulation in the following canonical form

$$\begin{aligned} \max_{x} \quad & c^T x \\ \text{s.t.} \quad & Ax \leq b. \end{aligned}$$

Identify the parameters c, A, and b, but do not solve the problem.

[5 marks]

ii. Now the firm wants to investigate whether it should include a new service, firewalls and network segmentation. This service incurs £10000, 15 manpower resources and 22 software licenses, and it reduces cybersecurity risk by 35. Help the firm determine whether it should include this new service. Justify your answer.

[2 marks]

[20 marks]

--- End of Paper ---