2022 EXAMINATIONS

Lancaster University

Part II

COMPUTING AND COMMUNICATIONS – On-line Assessment [120 Minutes]

SCC.363 Security and Risk

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

[Please turn over]

Question 1

1.a Alice wants to send a message to Bob. The security requirements for their communication require integrity and authentication of the data origin. Confidentiality is not a requirement. What function(s) can be used to achieve this and how?

[4 marks]

1.b In asymmetric cryptosystems, a pair of keys is generated, i.e., a public key and a private key.

i. What do we achieve when we share our private key with another person?

[1 mark]

ii. What do we achieve when we encrypt with our public key?

[1 mark]

iii. What do we achieve when we encrypt with our private key?

[1 mark]

1.c Digital signatures offer authentication, integrity and non-repudiation. Extend the digital signatures scheme to also offer confidentiality. Describe how your scheme may achieve this.

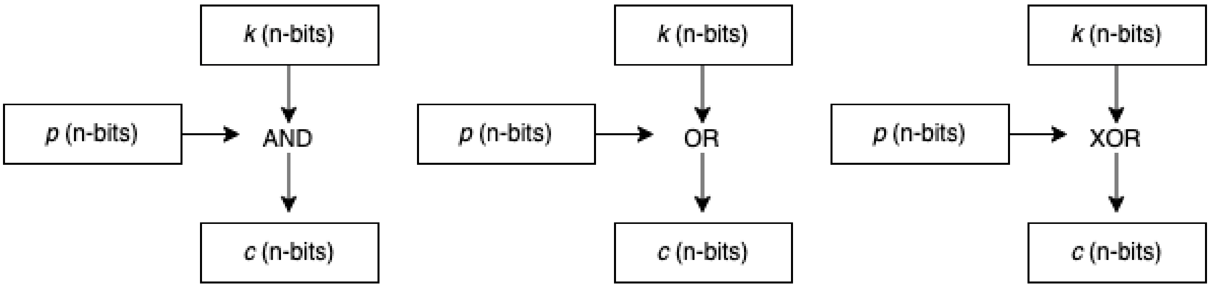
[6 marks]

1.d Answer the following questions:

i. Consider the standard ASCII character set. Each character is represented by an integer value in the range of [0, 127]. Define a function for use in a cipher that will uniquely map each character to another character in the same range of values. The function should be of the form $f(x) = (\mathrm{a} * \mathrm{x} + \mathrm{b})\ mod\ c$, where $a, b, c \in \mathbb{Z}$ and $x \in [0,127]$. Explain your selection of a, b, c.

[4 marks]

ii. Let *p* and *k* be plaintext and keystream, respectively. Explain which of the following logical operations are secure to use in a stream cipher for producing a n-bit ciphertext *c*?



[3 marks]

[Please turn over] **Total 20 marks**

Question 2

2.a Which access control model would you use in the following situations:

i. In a system where confidentiality is the top priority? Justify your answer and provide an example policy supported by such a model.

[4 marks]

ii. In a system that operates in a dynamic environment where its subjects and objects are distributed? Justify your answer and provide an example policy supported by such a model.

[4 marks]

2.b In the following access control matrix, list two *capabilities,* and two *access control lists*.

		files				
		cat	cp	echo	prg1	prg2
users	root	rwx	rwx	rwx	-	-
	alice	xr	xr	x	rwx	-
	bob	xr	xr	x	-	rwx

r: Read; w: Write; x: eXecute

[4 marks]

2.c In Role-Based Access Control (RBAC), why would you require:

i. A static separation of duty constraint between two or more roles.

[2 marks]

ii. A dynamic separation of duty constraint between two or more roles.

[2 marks]

2.d You are given the following sets of an RBAC model:

USERS = {u1, u2, u3}, ROLES = {r1, r2, r3}, OPS = {op1, op2, op3}, OBS = {ob1, ob2, ob3} and

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 Continues on Next Page ---
[Please turn over]

Consider the following RBAC policy:

{r1} ↔ {{op1, ob1}, {op1, ob2}, {op1, ob3}}

{r2} ↔ {{op2, ob1}, {op2, ob2}, {op2, ob3}}

{r3} ↔ {{op3, ob1}, {op3, ob2}, {op3, ob3}}

{r3} → {r1}

{u2} ↔ {r3}

{u3} ↔ {r1}

Answer the following questions:

i. Which permissions are accessible by {u1}?

[1 mark]

ii. Which permissions are accessible by {u2}?

[1 mark]

ii. Which permissions are accessible by {u3}?

[1 mark]

iv. Amend the RBAC policy by introducing a new role that will subsequently have access to all permissions via an appropriate role hierarchy using the existing roles.

[1 mark]

Total 20 marks

[Please turn over]

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. To protect information security, a digital signature is generated and transmitted along with the message. In addition, the combination of the message and a digital signature is transmitted over five communication links between Alice and Bob. Identify one or more principles of the CIA triad which are considered in the above protection mechanism and briefly state how they are achieved.

[4 marks]

iii. Provide a definition for non-repudiation.

[1 mark]

3.b **Strategic, tactical and operational** are three primary planning types for risk management.

i. Briefly state why risk management needs to be planned for cyber security.

[3 marks]

ii. Provide a definition for each of the three primary planning types for risk management.

[3 marks]

3.c The **Plan Do Check Act** Cycle (also known as the Deming Cycle) provides a simple concept to unde rstand what information security management is. Provide the objective of each of the four phases.

[4 marks]

3.d Briefly state the relationship between compliance and security.

[2 marks]

Total 20 marks

[Please turn over]

Question 4
4.a The four key ingredients necessary to conduct an attack on a socio-technical system are **Vulnerability, Exploit, Payload and Action**. Provide a definition for each of them.

[4 marks]

4.b Risk can be defined as the effect of uncertainty on security objectives in a socio-technical system.

i. Provide a definition for the terms effect and uncertainty.

[2 marks]

ii. Explain the four key sources of uncertainty.

[4 marks]

iii. Risk Treatment is a process used to modify identified risks. Define the four types of risk treatment.

[4 marks]

4.c There are three prototype cases for system reliability, **total effort, weakest link, and best short**.

i. Explain each of the three prototype cases.

[3 marks]

ii. Provide an example for each of the three prototype cases.

[3 marks]

Total 20 marks

--- End of Paper ---