Candidate Number

G6077

THE UNIVERSITY OF SUSSEX

BSc FINAL YEAR EXAMINATION
MComp THIRD YEAR EXAMINATION
January 2019 (A1)

Introduction to Computer Security

Assessment Period: January 2019 (A1)

DO NOT TURN OVER UNTIL INSTRUCTED TO BY THE LEAD INVIGILATOR

Candidates should answer TWO questions out of THREE.
If all three questions are attempted only the first two answers will be marked.

The time allowed is TWO hours.

Each question is worth 50 marks.

At the end of the examination the question paper and any answer books/answer sheets, used or unused, will be collected from you before you leave the examination room.

1.

a) Identify and explain which of the three principles of information security, CIA (*Confidentiality*, *Integrity* and *Authentication*/*Availability*), were compromised for the cyber-attack on LinkedIn in light of the reported description below:

> The social networking website LinkedIn was hacked on June 5, 2012, and passwords for nearly 6.5 million user accounts were stolen by cybercriminals. Owners of the hacked accounts were no longer able to access their accounts, and the website repeatedly encouraged its users to change their passwords after the incident. Vicente Silveira, the director of LinkedIn, confirmed, on behalf of the company, that the website was hacked in its official blog. He also said that the holders of the compromised accounts would find their passwords were no longer valid on the website.

[15 marks]

b) Explain and compare *unconditionally* and *computationally secure cipher*. Provide examples to illustrate your answer. [10 marks]

c) Decrypt the ciphertext given below using the given formula and alphabet index:

Ciphertext: phhw ph diwhu wkh wrjd

Formula: p = d (3, c) mod 26

a	b	c	d	e	f	g	h	i	j	k	l	m	n
0	1	2	3	4	5	6	7	8	9	10	11	12	13

o	p	q	r	s	t	u	v	w	x	y	z
14	15	16	17	18	19	20	21	22	23	24	25

[10 marks]

d) Describe Diffie-Hellman protocol for Bob and Alice who agreed on two values 5 and 7. Bob's random value is 3 and Alice's random value is 4. [15 marks]

2.

a) Using the Playfair cipher, perform the following tasks. Show all your working.

i) Encrypt the plaintext *learning* using key *Monday*
ii) Decrypt the ciphertext *kokfry* using key *monarchy*

[14 marks]

b) Using the Hill cipher, encrypt and decrypt the plaintext *hell*. Show all your working.

Plaintext: *hell*
Key:

3 7
5 12

a	b	c	d	e	f	g	h	i	j	k	l	m	n
0	1	2	3	4	5	6	7	8	9	10	11	12	13

o	p	q	r	s	t	u	v	w	x	y	z
14	15	16	17	18	19	20	21	22	23	24	25

[14 marks]

c) Describe *self-synchronising* and *non-self-synchronising* ciphers through an example.

[10 marks]

d) Suppose the following table is a sample of how a company is storing their clients' login details in their database. What risks would you identify and what would you advise to minimise those risks?

Username	**Password**
Jonny1	123Abc$
Neeli	£HelloDear

[12 marks]

/Turn over

3.

a) How is a *collision attack* different from *pre-image attack*?

[5 marks]

b) You are recommending a networking solution for an organisation that is based in several locations, and needs to exchange data securely between those locations and also with its mobile sales team. Which of the following would be the most practical option and why?

i) Encryption
ii) VPNs
iii) LANs

[10 marks]

c) What is the role of *cryptographic hash* in blockchain?

[10 marks]

d) Suppose a student creates a software program that allows him to access a teacher's computer. He is not authorised to access that computer. Has the student committed any criminal offence? Explain your answer and describe UK laws and regulations that are relevant to such a situation.

[15 marks]

e) Suppose you want to set up a secure wifi network. Which of the following security protocols would you use and why?

i) WEP
ii) WPA2

[10 marks]

End of paper