University of Colombo, Sri Lanka

UCSC *University of Colombo School of Computing*

BACHELOR OF SCIENCE IN COMPUTER SCIENCE

Second Year Examination — Semester II— UCSC AY19 [held in March/April/May 2023]

SCS 2214 — Information System Security

(2 Hours)

Answer All Questions

Number of Pages = 14 Number of Questions = 4

To be completed by the candidate

Index Number								

Important Instructions to candidates:

- Students should answer in the medium of English language only using the space provided in this question paper.
- Note that questions appear on both sides of the paper. If a page or a part of this question paper is not printed, please inform the supervisor immediately.
- Write your index number CLEARLY on each and every page of this Question paper.
- This paper consists of 4 questions in14 pages (including the Cover Page).
- Answer ALL questions.
- Programmable Calculators and any electronic device capable of storing and retrieving text including electronic dictionaries, smart watches and mobile phones are not allowed.
- Non-Programmable calculators are allowed
- Do not tear off any part of this answer book. Under no circumstances may this book, used or unused, be removed from the Examination Hall by a candidate

To be completed by the examiners

1	
2	
3	
4	
Total	

Index Number								

1. (a). Explain the main difference between **unconditional** security and **computational** security.

[5 marks]

(b). What is meant by a one-way hash function ? List three(3) fundamental requirements for a Hash Function.

[6 marks]

Index Number

(c). Explain the concept of the **birthday paradox** with regards to hash functions.

[6 marks]

(d). Block ciphers usually process 64-bit or 128-bit blocks at a time by using a block cipher operational mode. Cipher Block Chaining (CBC) mode and Counter mode (CTR) are such operational modes.

i. Briefly explain the reason for using a random IV in CBC mode encryption.

[2 marks]

Index Number □□□□□□□□

ii. Briefly explain the reason for using a nonce in CTR mode encryption.

[2 marks]

iii. Briefly describe two (2) differences between Cipher Block Chaining (CBC) mode and Counter mode (CTR) encryption.

[4 marks]

Index Number

2. (a). Determine the Greatest Common Divisor (GCD) of 18 and 300.

[3 marks]

(b). Suppose we want to use the Diffie-Hellman Key Agreement protocol between two parties, A and B, and we have chosen the integer g=5 and the integer n=11. If A generates the private key x=7 and B generates the private key y=5, calculate the session key k between A and B.

[5 marks]

Index Number □□□□□□□□

(c). Suppose we want to use the Elliptic Curve (EC) Diffie-Hellman Key Agreement protocol between two end points, A and B, and we have chosen the following parameters.

Curve $Y^2=X^3+2X+2$
G=(5,1)
n=19

(Note: G = (5,1), 2G=(6,3), 3G=(10,6), 4G=(3,1), 5G=(9,16), 6G=(16,13),7G=(0,6), 8G=(13,7), 9G=(7,6), 10G=(7,11))

i. If A generates the private key p=2, what is the ECC public key of A?

[3 marks]

ii. If B generates the private key q=3, what is the ECC public key of B?

[3 marks]

iii. Calculate the session key k between A and B.

[3 marks]

Index Number □□□□□□□□

(d). Suppose we want to use the RSA algorithm between two end points, A and B, and we have chosen (e,n) = (7,33) as public key of A and (d,n)=(3,33) as private key of A.

i. A has a message M=5 to be sent to B. What is the signature S of message M?

[4 marks]

ii. B encrypts the message M=3 before it transmits to A. What is the cipher text of message M?

[4 marks]

Index Number

3. (a). Explain the difference between a Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP) in terms of

   i. what they provide, and

   ii. how they are issued.

[6 marks]

(b). Define the terms Digital Cash and Digital Currency.

[5 marks]

Index Number | | | | | | | |

(c). Describe the consensus algorithm of the Bitcoin network.

[7 marks]

(d). Briefly explain how PGP provides confidentially, integrity, authenticity and non-repudiation security services by using an appropriate diagram.

[7 marks]

Index Number □□□□□□□□

4. (a). Kerberos is a protocol that is used to authenticate both clients and services in an open (insecure) network.

i. Following is a vulnerable network authentication protocol you learned in class which can be used to authenticate users to network services.

Once per user login session:

$C \Rightarrow AS : ID_C || ID_{tgs}$

$AS \Rightarrow C : E(K_c, Ticket_{tgs})$

Once per type of service:

$C \Rightarrow TGS : ID_C || ID_V || Ticket_{tgs}$

$TGS \Rightarrow C : Ticket_v$

Once per type of service:

$C \Rightarrow V : ID_C || Ticket_v$

Abbriviations:

$C = client$

$AS = Authentication\,Server$

$TGS = Ticket\,Granting\,Service$

$V = User\,requested\,service.\,e.g.\,FTP$

$E = Denotes\,encryption$

$ID_c = Identity\,of\,client,\ should\,understand\,ID_v,\ ID_{tgs}\,similarly$

$K_c = Key\,of\,client,\ should\,understand\,K_{tgs},\ K_v\,similarly$

$AD_c = IP\,address\,of\,client$

$TS_1 = A\,timestamp,\ should\,understand\,TS_2\,similarly$

$Ticket_{tgs} = E(K_{tgs}, [ID_C || AD_C || ID_{tgs} || TS_1 || Lifetime_1])$

$Ticket_v = E(K_v, [ID_C || AD_C || ID_v || TS_2 || Lifetime_2])$

Index Number

A. List **two (02)** vulnerabilities of the given protocol.

B. Describe **one (01)** of the vulnerabilities listed in (A), and

C. Explain how the described vulnerability can be mitigated.

[12 marks]

ii. "*Kerberos protocol require the time of each component to be synchronized to work* ". Is the above statement **true** or **false**? Explain your response.

[5 marks]

(b). i. "*Data Leakage Prevention (DLP) is not very effective if Deep Packet Inspection (DPI) feature is not enabled in the firewall appliance*"
Is the above statement **true** or **false**? Explain your response.

[5 marks]

Index Number								

ii. "*Packet filtering firewall is a passive network device*".
Is the above statement **true** or **false**? Explain your response.

[3 marks]

****