請勿攜去
Not to be taken away

香港中文大學
The Chinese University of Hong Kong

二零二零至二一年度下學期科目考試
Course Examination 2nd Term, 2020-21

科目編號及名稱
Course Code & Title : IERG4130 Introduction to Cyber Security

時間　　　　　　　小時　　　　　分鐘
Time allowed : 2 hours 0 minutes

學號　　　　　　　座號
Student I.D. No. : ………………………… Seat No. : …………………

Instructions:

(1) Please write down all your answers to the answer book. Please remember to also write down your name and student ID on the answer book.
(2) For those who take online exam, please write down your answers on papers prepared by yourself, then uploading photos of all answer sheets at the end of the exam.
(3) You need to answer all questions.

Part I. Multiple choices.

Note: Each question may have one or more correct answers. Please choose all of them out to get the full marks of four points. Any missed one(s) will lead to two points, and any wrong one(s) will lead to zero points.

Multiple-Choice questions

not to be provided.

P.1 – P.2

Multiple-Choice questions

not to be provided.

P.1 – P.2

Part II: True or False

True-False questions

not to be provided.

P.2 – P.3

True-False questions

not to be provided.

P.2 – P.3

Part III: Short Questions

Note: Please answer each of the question concisely and accurately. Different questions may carry different points.

1. (5') Please calculate: 7^{17} mod 23

2. Please write down the relevant security principle for following practices: (2'x4)

A. Use AES instead of home-crafted encryption algorithm

B. Install both Anti-virus software and a Firewall on a Windows computer

C. Run Apache Web server under a dedicated user account instead of *root* account

D. Turning down unused network services (like network sharing, etc.)

3. Why SHA512 is more secure than SHA256? Is there any potential limitation of SHA512? (3’+3’)

4. What is the fundamental reason for SQL injection? What is the most effective way to defense SQL injection? (3’+3’)

5. How the origin of a web page is defined? Does a CSRF attack violate the Same Origin Policy enforced by browsers? Why? (3’+1’+4’)

6. On UNIX-like systems, password is not saved in plaintext to avoid possible leakage. Instead, it will be saved in hashed form together with a *salt*. What is the purpose of that “salt”? (4’)

7. What is the difference between Authentication and Authorization? (4’)

8. In RSA, e is a part of public key. Please answer following questions:

(a) Can e be an even number? Why or why not? (1’+5’)

(b) Is it a good idea to choose 23 as the value of e? Why or why not? (1’+4’)

9. Fingerprint is a common way for user authentication. Could you list two possible limitations of this method? (3’+7’)

- End -