請勿攜去
Not to be taken away

香 港 中 文 大 學
The Chinese University of Hong Kong

二 0 一七至一八年度下學期科目考試
Course Examination 2nd Term, 2017-18

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

時間 Time allowed : 2 小時 hours 0 分鐘 minutes

學號 Student I.D. No. : .....

座號 Seat No. : .....

SPECIAL NOTES:

1. **Write student ID and seat number on BOTH question paper and answer book**
2. **Each student can take ONLY ONE double-sided A4 cheat sheet**
3. **Please answer ALL questions.**
4. **Put your answers on ANSWER BOOK**

<u>Section I: Multiple Choices</u> [Each question carries 5 points. You are required to select out ALL correct answers. Any wrong choice will lead to ZERO points, and any missing choice will lead to only 2 points]

Multiple Choice Questions
Not to be provided
P.1 - P.2

Section II: True or False **[For each statement, please first indicate whether it is true or false. For false statement, please also explain why. Wrong answer or wrong explanations will get zero points. Correct answer without any explanations will get 2 points. Each has 5 points]**

True or False Questions
Not to be provided
P.2 - P.3

Section III: Short questions **[Please answer all of the following questions in a concise and succinct way. Questions may carry different points.]**

1. What is the meaning of security principle "least privilege"? Could you give one real world example that follows this principle? [3' + 4']

2. Assume the key length is equal to k in a vigenere cipher, and then what is the complexity for a brute force attack to it (i.e., the size of searching space for the encryption key)? [3']

3. Please write down the corresponding purpose for each of the following operations (e.g., sign a document, protect secrete message, or does not make sense): (3'+3'+3'+3')
   A. Alice decrypt a cipher text received from Bob using Bob's public key
   B. Alice encrypt a plain text with her own public key
   C. Alice encrypt a plain text using Bob's public key
   D. Alice encrypt a plain text using her own private key

4. Answer following questions related to Diffie-Hellman protocol (2'+3'+5')
   A. What is the purpose of Diffie-Hellman Key Exchange protocols?
   B. Does it have any limitation?
   C. Why does it have such a limitation?

5. Please calculate the answers for 9^{25} mod 35? [8', you need to give the detailed procedure in order to get full 8 points, otherwise zero point]

6. Answer following questions related to Hash functions and X.509 certificate (4'+4')
   A. If adversaries want to generate a fake X.509 certificate which has different contents but the same digital signature as the genuine one, what kind of attack they want to launch? (Hints: birthday attack or some type of preimage attack?)
   B. What is the attacking complexity (i.e., size of searching space) for SHA256 in order to find a collision (i.e., two different messages with same 256-bit of hash value) by brute force?

7. Please answer following questions related to Same Origin Policy in Web security.
   A. How is the same origin defined in browsers? (3')
   B. Following is a piece of code extracted from the Web page from URL http://www.abc.com/index.html . Will the file "a.js" have the same origin as www.abc.com or www.xyz.com ? (3')

   <script type="text/javascript" src=http://www.xyz.com/a.js>

8. Answer following questions about code injection attacks.
   A. What is the fundamental reason for Code injection attack? (5')
   B. To defend against code injection attack, we can perform input validation based on either white-list or black-list techniques. Which one do you think is more secure? Why? (1' +4')

9. For the program given below, could you identify a possible vulnerability? Please also explain why. (5'+5')

```
1. #include <stdio.h>
2. #include <stdlib.h>
3. int *matvec(int **A, int *x, int n) {
4.   int i, j;
5.   int *y = malloc(n*sizeof(int));
6.   for (i=0; i<n; i++)
7.     for (j=0; j<n; j++)
8.        y[i] += A[i][j] * x[j];
9.   return y;
10.}
```

10. Answer following questions related to authentication and password. (11')

    A. Why do we need two-factor authentication in some situations? (2')

    B. Besides the bank card + password example introduced in our lecture, could you give us another example of two-factor authentication? (2')

    C. What is the purpose of using "salt" when saving hashed value of password? (3')

    D. What is the potential limitation of fingerprint based authentication methods? (4')

- End -