Beijing-Dublin International College

SEMESTER I FINAL EXAMINATION - 2017/2018

School of Computer Science & Informatics

COMP3020J Information Security for Internet

HEAD OF SCHOOL NAME: Prof. Pádraig Cunningham

MODULE COORDINATOR NAME*: Dr. Anca D. Jurcut

Time Allowed: 90 minutes

Instructions for Candidates

The distribution of marks in the right margin shown as a percentage gives an indication of the relative importance of each part of the question.

BJUT Student ID: ________________ **UCD Student ID:** ________________

I have read and clearly understand the Examination Rules of both Beijing University of Technology and University College Dublin. I am aware of the Punishment for Violating the Rules of Beijing University of Technology and/or University College Dublin. I hereby promise to abide by the relevant rules and regulations by not giving or receiving any help during the exam. If caught violating the rules, I accept the punishment thereof.

Honesty Pledge： ____ **(Signature)**

Instructions for Invigilators

Non-programmable calculators are permitted.

Obtained score

QUESTION 1

a. Define each of the fundamental challenges in information security known as the CIA triangle.

[5 marks]

b. Discuss one real-world example of a buffer overflow that was exploited as part of a successful attack.

[5 marks]

c. Give a real-world example where Kerckhoffs' Principle has been violated. Did this cause any security problems?

[5 marks]

d. Nonces and timestamps are both used in security protocols to prevent freshness (replay) attacks.

i) Give one significant advantage of a nonce over a timestamp.

ii) Give one significant advantage of a timestamp over a nonce.

[10 marks]

e. What is a hash function in cryptography? Give an example of hash function. Briefly describe the five properties a hash function must provide.

[10 marks]

f. What is the difference between the authentication problem and the identification problem with respect to biometrics? Which is inherently easier, authentication or identification?

[5 marks]

g. How and why does a digital signature provide non-repudiation?

[5 marks]

h. Explain the difference between symmetric and asymmetric encryption.

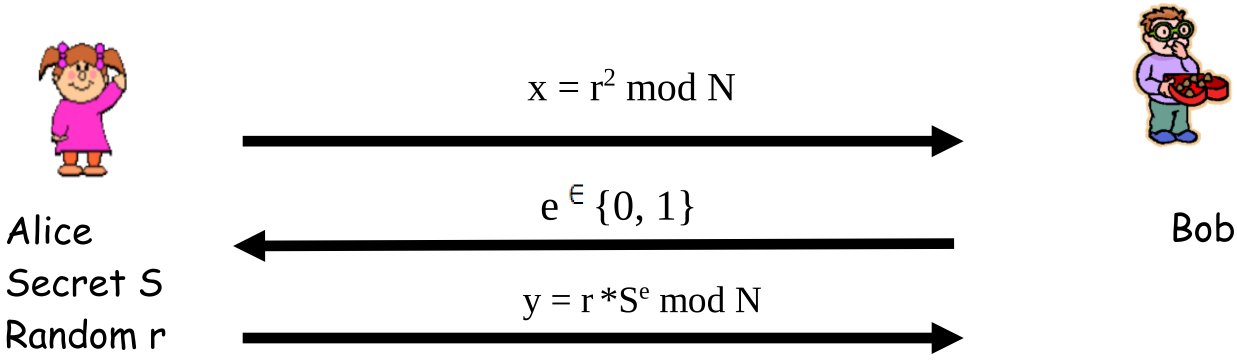
[5 marks]

[Total 50 marks]

Obtained score

QUESTION 2

a. The Fiat-Shamir zero knowledge protocol is illustrated below. Suppose that N = 63 and Alice's secret is S=13.



i) What is v?

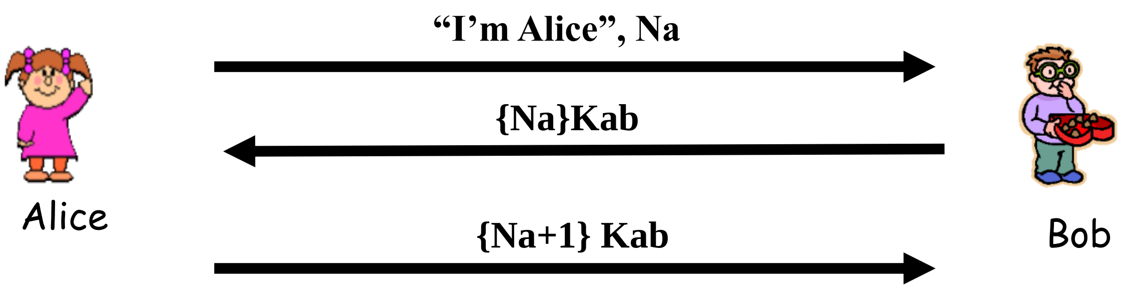
ii) If Alice chooses r =10, what does Alice send in the first message?

iii) Suppose Alice chooses r = 10 and Bob sends e = 0 in message two. What does Alice send in the third message?

iv) Suppose Alice chooses r = 10 and Bob sends e = 1 in message two. What does Alice send in the third message?

[20 marks]

b. Consider the following mutual authentication protocol, where *Kab* is a shared symmetric key.



Give two different attacks that Trudy can use to convince Bob that she is Alice.

[10 marks]

[Total 30 marks]

Obtained score

QUESTION 3

a. What is a botnet? Give a known example.

[5 marks]

b. Consider the following protocol for adding money to a debit card.

(i) User inserts debit card into debit card machine.

(ii) Debit card machine determines current value of card (in dollars), which is stored in variable *x*.

(iii) User inserts dollars into debit card machine and the value of the inserted dollars is stored in variable *y*.

(iv) User presses enter button on debit card machine.

(v) Debit card machine writes value of *x* + *y* dollars to debit card and ejects card.

This particular protocol has a race condition.

(1) What is the race condition in this protocol?

[5 marks]

(2) Describe a possible attack that exploits the race condition.

[5 marks]

(3) How could you change the protocol to eliminate the race condition, or at least make it more difficult to exploit?

[5 marks]

[Total 20 marks]