Beijing-Dublin International College

SEMESTER I FINAL EXAMINATION - 2016/2017

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.

[10 marks]

b. Give a concrete example where availability is the overriding concern.

[5 marks]

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

[5 marks]

d. Give the definition of a Feistel Cipher and justify if DES and AES are (or not) a Feistel Cipher. Why is the Tiny Encryption Algorithm (TEA) "almost" a Feistel Cipher?

[10 marks]

e. Suppose that you know a MAC value *X* and the key *K* that was used to compute the MAC, but you do not know the original message. Show that you can construct a message *M* that also has its MAC equal to *X*. Note that we are assuming that you know the key *K* and the same key is used for both MAC computations.

[10 marks]

f. Define non-repudiation in the context of cryptography.

[5 marks]

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

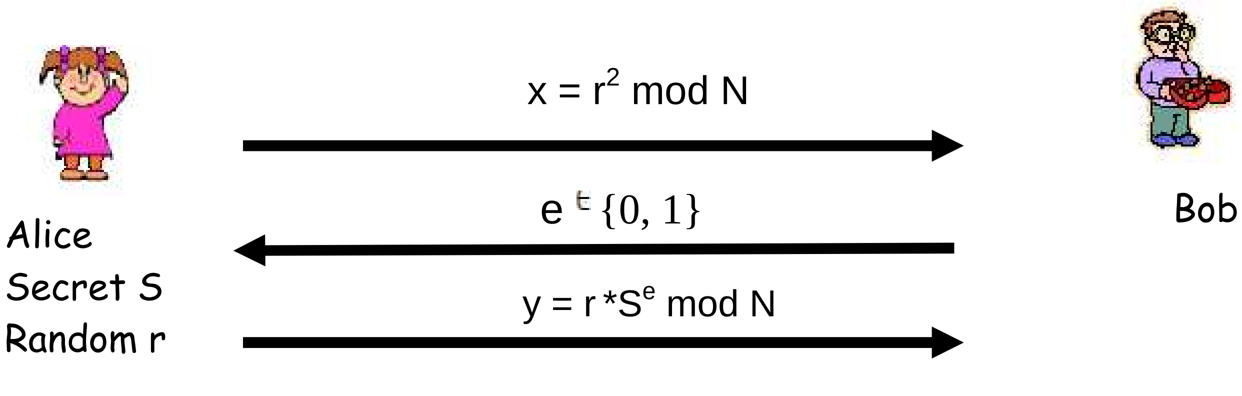
[5 marks]

[Total 50 marks]

Obtained score

QUESTION 2

a. The Fiat-Shamir zero knowledge protocol is illustrated below. Suppose that N = 55 and Alice’s secret is S=9.



i) What is v?

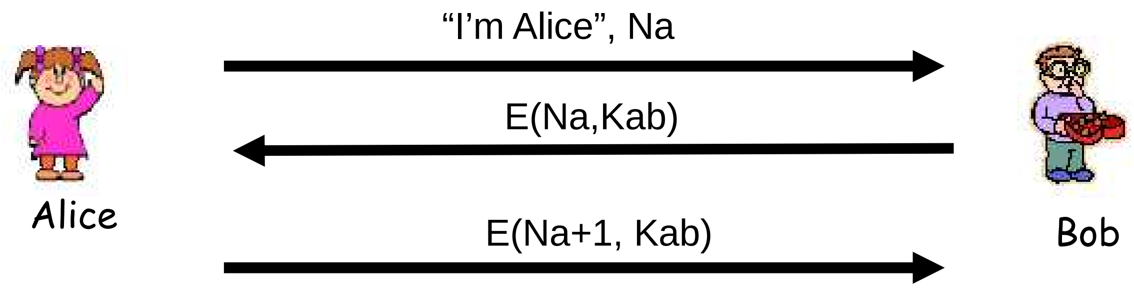
ii) If Alice chooses r =10, what does Alice send in the first message?

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 validation error and how can such an error lead to a security flaw?

[5 marks]

b. What is a virus? What is a worm? Explain the differences between the two terms and give examples of known viruses and worms.

[5 marks]

c. Explain how an integer overflow works, in contrast to the stack-based buffer overflow.

[10 marks]

[Total 20 marks]