Beijing-Dublin International College

SEMESTER I FINAL EXAMINATION - 2018/2019

Faculty of Information Technology

COMP3031J Security and Privacy

NAME OF THE HEAD OF SCHOOL: Junfei Qiao
NAME OF THE MODULE COORDINATOR: Jingsha He
OTHER EXAMINER NAME:

Time Allowed: 90 minutes

Instructions for Candidates

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.
No rough-work paper is to be provided for candidates.

Obtained score

Question 1 (20 points)

1. State the most important property that distinguishes symmetric cryptography from asymmetric cryptography in real applications. (5 points)
2. Some hash or message digest functions or algorithms, such as MD5 and SHA, are also considered by some people as encryption algorithms. Do you agree? Please justify your answer. (5 points)
3. Public key based cryptography offers the functionality of both confidentiality and integrity while secret key based cryptography can only do confidentiality. Please explain the main reason that has kept secret key based cryptography from becoming obsolete. (5 points)
4. Design a solution that uses public key based cryptography to form a digital signature for message M in which hash function should also be used. (5 points)

Obtained score

Question 2 (20 points)

1. State the purpose of key exchange. (5 points)
2. Describe a procedure that uses public key based cryptography for key exchange. (5 points)
3. What is the most important information that should go into a certificate constructed based on public key based cryptography? Why is the certificate mechanism capable of countering man-in-the-middle-attack that happens during the distribution of public keys? (10 points)

Obtained score

Question 3 (20 points).

1. What are the three main issues of information security? Please explain each of them. (5 points)
2. State the most important property of information protection in confidentiality models in terms of the flow of information. (5 points)
3. In the Bell-LaPadula model, is a subject with clearance level L_S allowed to read from an object with classification level L_O when $L_S \leq L_O$? Is the same subject allowed to write into the same object? (5 points)
4. Describe the concept of role-based access control (RBAC) and explain why RBAC would generally reduce the granularity of access control. (5 points)

Obtained score

Question 4 (20 points)

1. Security of password-based authentication can be approached from the directions of system design, user password selection and authentication management strategy. Describe what can be done following the above three approaches to improve the security of authentication. (5 points)
2. Describe the single purpose of network single sign-on (SSO). (5 points)
3. Authentication succeeds when user supplied authentication information matches system stored complementary information through direct comparison. Describe how in Kerberos the two pieces of information are matched for successful authentication. (10 points)

Obtained score

Question 5 (20 points)

1. Name and describe the two strategies of implementing access control based on the access control matrix model. (5 points)
2. Describe the default access rule for optimizing access control lists. (5 points)
3. Given the following group membership setup and the access control list (ACL) in the Windows environment, determine the access rights for Bob, Alice, John, Thomas and Peter for access to file c:\document. (10 points)
   (1) Manager = {Peter};
   (2) Engineer = {Bob, Alice, Peter};
   (3) Staff = {John, Thomas};
   (4) ACL(c:\document)={(Manager,{own}),(Engineer,{read,write}),(Staff,{read}),(John,{no access})}.