**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.

**Question 1 (20 points)**

**Obtained score**

1. State the most important property that distinguishes symmetric cryptography from asymmetric cryptography in real applications. (5 points)

**Symmetric cryptography uses a shared key when encryption and decryption, but asymmetric uses a pair of keys which is public key and private key to encrypt and decrypt information, that means if encryption with public key than decryption with private key, and if encryption with private key then decryption with public key.**

1. 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)

**I do not agree with this idea. Although they can be used to encrypt password and that is why some people consider them as encryption algorithms, but in fact hash functions or message digest functions are one way functions which means they can not come back to the origin values using hash values. So after encrypt the information with these algorithms, it can not decrypt the information with the same hash functions.**

1. 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)

**Because the secret key based cryptography is more efficient than public key based cryptography which has a time consuming encryption. So we can use public key based cryptography to ensure the integrity of information that is using private key to encrypt the information and then use secret key based cryptography to ensure the confidentiality and improve the efficiency.**

1. 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)

**For Generation(Bob):**

1. **At first, message M is pass through a hash function and then get hash value h.**
2. **Then h is encrypted with the private key of Bob and the cipher text s is sent to Alice.**

**For Verification(Alice):**

**1. Alice receive the cipher text s, so he decrypt the s with Bob’s public key and get a hash value h’.**

**2. Then Alice compare the h and h’ to determine if the signature is valid or not.**

# Question 2 (20 points)

**Obtained score**

1. State the purpose of key exchange. (5 points)

**The purpose of key exchange is to establish a session key for the two communicating parties which can ensure the security using session key.**

1. Describe a procedure that uses public key based cryptography for key exchange. (5 points)

**Note: Alice who generate the session key, Bob who retrieve the session key.**

**A simple procedure:**

1. **Alice encrypted a session key with the private key of Bob.**
2. **Bob received the cipher text and decrypt with public key of Bob and get the session key**

**A more complex procedure:**

1. **Alice encrypted a session key with the private key of Bob and use public key of Bob to encrypt the cipher text again. And then sent to Bob**
2. **Bob receive the cipher text and decrypt with private key of Bob and then decrypt with public key of Alice to get the session key.**
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)

**The public key of corresponding entity should be the most important information in a certificate and it also includes identity information of corresponding entity. Because certificate is issued by a trusted third party usually called certificate authentication(CA) and is encrypted by private key of CA, only the entity has the public key can decrypt the certificate and verify the identity. But without the private key of CA, anyone else can not modify the information of certificate.**

# Question 3 (20 points).

**Obtained score**

1. What are the three main issues of information security? Please explain each of them. (5 points)
   1. **Confidentiality: The secrecy and privacy information such as your personal information will be read by unauthorized entity, and they may publish in the network to defame you.**
   2. **Integrity: The information is modified by unauthorized entity, so you get wrong information.**
   3. **Availability: The information is not available for you due the inhibition of access to the information such as DoS(denial of service), so you can’t get what you what.**
2. State the most important property of information protection in confidentiality models in terms of the flow of information. (5 points)

**Information can only flow upwards that is information can flow from one object to another if and only if the second object dominates the first.**

1. In the Bell-LaPadula model, is a subject with clearance level LS allowed to read from an object with classification level LO when LS≤LO? Is the same subject allowed to write into the same object? (5 points)

**The subject with level Ls can not read from an object with level Lo but it can write into the same object.**

1. Describe the concept of role-based access control (RBAC) and explain why RBAC would generally reduce the granularity of access control. (5 points)

**In RBAC, subjects may be grouped together or classified into different categories, and the permission is assigned on roles not users, it reduced the number of permissions granted, and reduced the complexity of authority management, so there is less granularity in access control.**

# Question 4 (20 points)

**Obtained score**

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. **In the directions of system design, for example, we can assume that the system will disconnect after a specified number of failed attempts**
3. **Select a strong password, for example, include at least one digit, at least one letter, at least one punctuation character, and at least one control characters.**
4. **In authentication management strategy, we can choose a strong complementary function to store complementary information such as one way hash function with salt.**
5. Describe the single purpose of network single sign-on (SSO). (5 points)
6. **The single sign-on tries to achieve that user only needs to log in once with the Authentication Server (AS) and Ticket-Granting Server(TS) issues tickets to the user to access the application servers.**

**2. So the user can log in any application servers which is connected to the AS with the tickets issued by TS and the log in process is actually transparent to the user.**

1. 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)

**In Kerberos protocol, the Authentication Server(AS) shares a secret key with each and every user and Ticket-Granting Server(TS), and TS shares a secret key with each and every of applications servers S1,...,Sn. User Alice want to enjoy some application provided by application server S, and the authentication process between S and Alice is:**

1. **At first Alice need to log in the AS with authentication information(may use passwords or fingerprints), and get a secret key k(Alice,TS) of Alice and TS encrypted with k(Alice, AS) and a ticket which denoted as T(Alice, TS) to log in TS .**
2. **Then Alice sends the identity of S, an authenticator A(Alice, TS) which includes the identity of Alice and a timestamp, T(Alice, TS) which is from AS.**
3. **TS authenticate the identity of Alice and returns the identity of Alice, session key k(Alice, S) encrypted with secrete key between Alice and TS, and a ticket T(Alice, S) encrypted with the secret key between TS and S, and T(Alice, S) includes the identity of Alice, Alice’s address , valid time and session key K(Alice, S).**
4. **Finally, Alice sends to S with A(Alice, S) generated by Alice encrypted with secret key between Alice and S which includes the identity of Alice and T(Alice, S) from TS, and S can check these two piece of information to give the authentication to Alice.**

# Question 5 (20 points)

**Obtained score**

1. Name and describe the two strategies of implementing access control based on the access control matrix model. (5 points)

**1. Access Control Lists(ACLs): break the access control matrix by the columns and assign the permissions of subject to corresponding objects, for instance, acl(File)={(Bob, own)}**

**2. Abbreviation of Access Control Lists: similar to ACLs, but subjects may be grouped together or may be classified into different categories.**

**3. Capabilities: break the access control matrix by the rows and each subject has a capability list with the permission of corresponding objects, for instance, cap(Bob)={(File, {own})}.**

1. Describe the default access rule for optimizing access control lists. (5 points)

**Access requests from a subject to access an object is denied if the subject doesn’t appear in the ACL for the object, so the default access rule for blank part in matrix is no access, and it can save a lot of space without storing the blank entries in ACLs.**

1. 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})}.

**Bob, Alice: read and write**

**John: no access**

**Thomas: read**

**Peter: own, read, write.**