RMIT UNIVERSITY

School of Science

COSC2536/2537 Security in Computing and Information Technology

Exercise

	Assessment Type: Individual exercise; no group work. Submit online via Canvas→Assignments→Exercise. Marks awarded for meeting requirements as closely as possible. Clarifications/updates may be made via announcements/relevant discussion forums.
	Due date: Week 12, Thursday the 15th October 2020 5:00 pm Deadlines will not be advanced, but they may be extended. Please check Canvas→Syllabus or via Canvas→Assignments→Assignment 3 for the most up to date information. As this is a major assignment in which you demonstrate your understanding, a university standard late penalty of 10% per each working day applies for up to 5 working days late, unless special consideration has been granted.
	Weighting: 20 marks (Contributes 20% of the total Grade)

1. Overview

You must follow the special instructions below:

- Answer all of the questions.
- You must fulfil the requirements in the questions.
- Upload your solution as a single PDF or Word document in CANVAS.
- DO NOT put the PDF/DOC file within the ZIP file.

2. Assessment Criteria

This assessment will determine your ability to:

- Follow requirements provided in this document and in the lessons.
- Independently solve a problem by using cryptography and cryptanalysis concepts taught over the last 10 weeks from first to tenth weeks of the course.
- Meeting deadlines.

3. Learning Outcomes

This assessment is relevant to the following Learning Outcomes:

1. CLO 1: explain the functioning of security services in computing environments and the security issues in networked applications.
2. CLO 2: discuss various types of data integrity and confidentiality mechanisms including public key cryptography.

3. CLO 3: describe basic system security mechanisms and protocols, such as those used in operating systems, file systems and computer networks.
4. CLO 4: analyse the overarching importance of IT security in areas such as networking, databases, operating systems, and web systems.
5. CLO 5: apply privacy principles in basic practical settings in IT environments.
6. CLO 6: analyse and evaluate the security of computing and IT systems on a practical level and privacy related issues in computing.

4. Assessment details

Please ensure that you have read **Section 1** to **3** of this document before going further. Assessment details (i.e. question Q1 to Q4) are provided in the **next page**.

Answer all of the following questions

Total marks: 20 (Contributes 20% of the total Grade)

Q1. Encryption using Public-Key Cryptography (Marks: 2+4 = 6)

Say, Alice wants to send a secret message ***(M)*** to Bob using Public-Key Cryptography Algorithm. That is, Alice is the sender and Bob is the receiver. Assume that Alice considers your student number as the secret message M. For example, if your student number is "S123456", the secret message is: ***M = 123456***. Bob generates public and private keys and sends the public key to Alice for encryption.

Answer the following questions:

a) Consider that Alice and Bob are using **RSA Public-Key Cryptography Algorithm**. With proper description, show detailed steps of key generation, encryption, and decryption process. Bob uses parameter **p = 3919** and **q = 2789.**

   i. Choose a small public key parameter **(*e = 7*)** on behalf of Bob and show detailed steps to compute Bob's **public-key** and **private-key?**

   ii. How would Alice encrypt message ***M* = <*your student number without 'S'*>** and produce the ciphertext ***C***?

   iii. How would Bob decrypt the encrypted message ***C***?

b) Consider that Alice and Bob are using **ElGamal Public-Key Cryptography Algorithm**. Show detailed steps of key generation, encryption, and decryption process. Bob uses parameter **p = 4000159, g = 56,** and **x = 1634.**

   i. Show detailed steps to compute Bob's **public-key** and **private-key?**

   ii. Alice chooses a random number ***r = 2317***. How would Alice encrypt message ***M* = <*your student number without 'S'*>** and produce the ciphertext ***C***?

   iii. How would Bob decrypt the encrypted message ***C***?

Q2. Digital Signature using Public-Key Cryptography (Marks: 2)

Say, Alice wants to send a signed message to Bob using **RSA Public-Key Cryptography Algorithm based digital signature**. That is, Alice is the signer and Bob is the verifier. The digital signature is a pair ***(M, S)*** where ***M*** is the message and ***S*** is the digital signature. Assume that Alice considers your student number as the message ***(M)***. For example, if your student number is "S123456", the message is: ***M = 123456***. Alice generates public and private keys and sends the public key to Bob for verification.

With proper description, show detailed steps of key generation, signing, and verification process. Alice uses parameter **p = 4373** and **q = 3407.**

   i. Choose a small public key parameter **(*e = 19*)** on behalf of Alice and show detailed steps to compute Alice's **public-key** and **private-key?**

   ii. How would Alice sign the message ***M* = <*your student number without 'S'*>** and produce the signature ***S***?

   iii. How would Bob verify the signature ***S***?

Q3. Privacy-Preserving Computation using Public-Key Cryptography (Marks: 3+5 = 8)

Say, Alice wants to multiply two numbers (M1 and M2) and send the result to Bob. That is, Alice is the sender and Bob is the receiver. However, Alice does not have the computation power to multiply two numbers. Therefore, she decides to send both numbers to a cloud server. Though the cloud server has the computation power, it cannot be trusted. As a result, Alice relies on the ***Homomorphic properties of Public-Key Cryptography Schemes***. Alice encrypts both numbers before sending them to the cloud. The cloud performs multiplication on encrypted numbers and sends the encrypted result to Bob.
Assume that Alice considers the last digit of your student number as the first number ***(M1)*** and the second last digit as the second number ***(M2)***. For example, if your student number is "S123456", the numbers are: ***M1 = 6*** and ***M2 = 5***. Bob generates public and private keys and sends the public key to Alice for the encryption and to cloud for the homomorphic multiplication.

Answer the following questions:

a) Consider that Alice and Bob are using **RSA Public-Key Cryptography Algorithm**. With proper description, show detailed steps of key generation, encryption, homomorphic multiplication, and decryption process. Bob uses parameter ***p* = 79** and ***q* = 83.**

   i. Choose a small public key parameter ***(e = 19)*** on behalf of Bob and show detailed steps to compute Bob's **public-key** and **private-key?**

   ii. How would Alice encrypt numbers ***M1=<****last digit of your student number***>** and ***M2=<****second last digit of your student number***>**? What would Alice send to the cloud?

   iii. How would the cloud perform homomorphic multiplication? What encrypted result would the cloud send to Bob?

   iv. How would Bob decrypt the encrypted result?

b) Consider that Alice and Bob are using **ElGamal Public-Key Cryptography Algorithm**. Show detailed steps of key generation, encryption, homomorphic multiplication, and decryption process. Bob uses parameter ***p* = 5081, g = 93,** and ***x* = 106.**

   i. Show detailed steps to compute Bob's **public-key**?

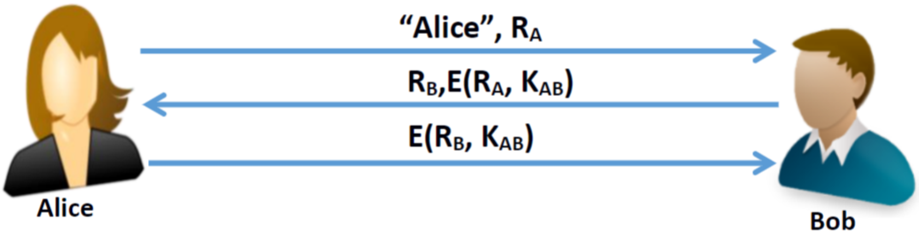
   ii. Alice chooses two random numbers: ***r1 = 79 and r2 = 94***. How would Alice encrypt numbers ***M1=<****last digit of your student number***>** and ***M2=<****second last digit of your student number***>**? What would Alice send to the cloud?

   iii. How would the cloud perform homomorphic multiplication? What encrypted result would the cloud send to Bob?

   iv. How would Bob decrypt the encrypted result?

Q4. Designing a Secure Authentication Protocol (Marks: 4)

The following mutual authentication protocol is proposed based on a symmetric-key cryptography algorithm. In this scenario, R_A is the nonce from Alice and R_B is the nonce from Bob. K_{AB} is the shared secret key (only known to Alice and Bob) that has been established by Alice and Bob using a secure method. **E(M, K_{AB})** is the symmetric encryption algorithm that encrypts a message ***M*** with K_{AB}. We assume that the symmetric encryption algorithm that is used here is secure.



Given that the following protocol does not provide mutual authentication. With proper diagram, briefly explain the Man-in-the-Middle (MiM) attack scenario performed by Trudy where Trudy can convince Bob that she is Alice.

5. Academic integrity and plagiarism (standard warning)

Academic integrity is about honest presentation of your academic work. It means acknowledging the work of others while developing your own insights, knowledge and ideas. You should take extreme care that you have:

- Acknowledged words, data, diagrams, models, frameworks and/or ideas of others you have quoted (i.e. directly copied), summarized, paraphrased, discussed or mentioned in your assessment through the appropriate referencing methods,
- Provided a reference list of the publication details so your reader can locate the source if necessary. This includes material taken from Internet sites.

If you do not acknowledge the sources of your material, you may be accused of plagiarism because you have passed off the work and ideas of another person without appropriate referencing, as if they were your own.

RMIT University treats plagiarism as a very serious offence constituting misconduct. Plagiarism covers a variety of inappropriate behaviors, including:

- Failure to properly document a source
- Copyright material from the internet or databases
- Collusion between students

For further information on our policies and procedures, please refer to the University website.

6. Assessment declaration

When you submit work electronically, you agree to the assessment declaration.