RMIT UNIVERSITY

School of Science

INTE2401/2402 Cloud Security

Assignment 2

	Assessment Type: Individual assignment; no group work. Submit online via Canvas→Assignments→Assignment 2. Marks awarded for meeting requirements as closely as possible. Clarifications/updates may be made via announcements/relevant discussion forums.
	Due date: **Week 9, Sunday the 27th September 2020 11:59pm** 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: **35 marks (Contributes 35% of the total Grade)**

1. Overview

The objective of Assignment 2 is evaluating your knowledge on the topics covered mainly in Lecture 2 to 8. Topics include AES, Hashing Techniques, Key Management and Distribution and Security Protocols for Cloud Computing. However, topics covered in Lecture 1 are required as prerequisite. Assignment 2 will focus on developing your abilities in application of knowledge, critical analysis and decision making. Assignment 2 contains several problems related to the topics mentioned above. You are required to prepare your answers and upload them as a single PDF or Word document in CANVAS.

In this assignment, there are 5 (five) questions related to AWS. Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. This means customers of all sizes and industries can use it to store and protect any amount of data for a range of use cases, such as websites, mobile applications, backup and restore, archive, enterprise applications, IoT devices, and big data analytics. You have two options for protecting data at rest in Amazon S3. **Server-Side Encryption** – Request Amazon S3 to encrypt your object before saving it on disks in its data centers and then decrypt it when you download the objects. **Client-Side Encryption** – Encrypt data client-side and upload the encrypted data to Amazon S3. In this case, you manage the encryption process, the encryption keys, and related tools. The first question of this assignment is to implement a client-side encryption tool built on Advanced Encryption Standard (AES).

Question 2 is on **Signing AWS Requests with Signature Version 4.** When you send HTTP requests to AWS, you need to sign the requests so that AWS can identify who sent them. You sign requests with your AWS access key, which consists of an access key ID and secret access key. The signing process helps secure requests in the following ways: verify the identity of the requester, protect data in transit, and protect against potential replay attacks. In this question, you are required to use AWS Signature Version 4 to generate a signature on a given string. Through this question, you are expected to understand the detail signature generation and verification process of AWS Signature Version 4.

Question 3 is about **AWS Key Management Service (AWS KMS)**, a managed service that makes it easy for you to create and control customer master keys (CMKs), the encryption keys used to encrypt your data. AWS KMS CMKs are protected by hardware security modules (HSMs) that are validated by the FIPS 140-2 Cryptographic Module Validation Program. AWS Key Management Service supports symmetric and asymmetric Customer Master Keys (CMKs). A symmetric CMK represents a 256-bit key that is used for encryption and decryption. CMKs are created in AWS KMS. Symmetric CMKs never leave AWS KMS unencrypted. In this question, you are required to create a data key to encrypt a data and then store it in AWS. Through the question, you are expected to understand how data is encrypted and store in AWS.

Question 4 is about **AWS Site-to-Site VPN** based on Diffie-Hellman key establishment. An AWS Site-to-Site VPN connection connects your Virtual Private Cloud (VPC) to your data centre. Amazon supports Internet Protocol Security (IPSec) VPN connections. Data transferred between your VPC and data centre routes over an encrypted VPN connection to help maintain the confidentiality and integrity of data in transit. Internet Key Exchange (IKEv2) is the protocol used to set up a security association (SA) in the IPSec protocol suite. IKEv2 uses X.509 certificates for authentication – either pre-shared or distributed and a Diffie–Hellman key exchange to set up a shared session secret from which cryptographic keys are derived. The question has three parts. In the first part, you are expected to implement the Diffie-Hellman key exchange protocol for AWS Site-to-Site VPN. In the second part, you are expected to perform a man-in-the-middle attack to the Diffie-Hellman key exchange protocol. In the last part, you are expected to propose an improved key exchange protocol which is able to overcome the man-in-the-middle attack.

The last question is on **Secure Socket Layer (SSL) Handshake Protocol.** Secure Sockets Layer (SSL) is a standard security technology for establishing an encrypted link between a server and a client - typically a web server (website) and a web browser. AWS Certificate Manager from Amazon Web Services (AWS) takes care of deploying certificates to help you enable SSL/TLS for your website. Assume that AWS Certificate Manager issues you a SSL certificate and you have installed the certificate in your website hosted on AWS. When a client browses your website, suppose the client will run a SSL handshake protocol with ephemeral public key with your website to establish an encrypted link between the client and your website. In this question, we are expected to demonstrate your understanding how SSL handshake protocol with ephemeral public key work and analyse client authentication, server authentication, and forward security of the SSL handshake protocol.

Develop this assignment in an iterative fashion (as opposed to completing it in one sitting). You should be able to start preparing your answers immediately after Lecture-5 (in Week-5). At the end of each week starting from Week-5 to Week-8, you should be able to solve at least one question.

If there are questions, you may ask via the relevant Canvas discussion forums in a general manner.

2. Learning Outcomes

This assessment is relevant to the following Learning Outcomes:

- understand how AWS applies hashing techniques, digital signature, key management, and security protocols to achieve cloud security.
- discuss various types of confidentiality, authentication and data integrity mechanisms in cloud computing.
- analyze the strength and limitations of security protocols for cloud computing.
- design and implement security mechanisms and protocols.

3. Submission

You must follow the following special instructions:

- You must use the values provided in the questions.
- Hand-written answers are not allowed and will not be assessed. Compose your answers using any word processing software (eg. MS Word).
- You are required to show all of the steps and intermediate results for each question.
- Upload your solutions as a single PDF or Word document together with programming codes in CANVAS.

This assessment will determine your ability to:

- Follow requirements provided in this document and in the lessons.
- Independently solve a problem by using security concepts taught over the first four weeks of the course.
- Meeting deadlines.

After the due date, you will have 5 business days to submit your assignment as a late submission. Late submissions will incur a penalty of 10% per day. After these five days, Canvas will be closed and you will lose ALL the assignment marks.

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 Q5) are provided in the **next page**.

RMIT UNIVERSITY

Q1. Cloud Client-Side Encryption Tool **(Marks: 2+2+2+2+2=10)**

Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. This means customers of all sizes and industries can use it to store and protect any amount of data for a range of use cases, such as websites, mobile applications, backup and restore, archive, enterprise applications, IoT devices, and big data analytics. You have two options for protecting data at rest in Amazon S3. Server-Side Encryption – Request Amazon S3 to encrypt your object before saving it on disks in its data centers and then decrypt it when you download the objects. Client-Side Encryption – Encrypt data client-side and upload the encrypted data to Amazon S3. In this case, you manage the encryption process, the encryption keys, and related tools.

In this question, you are required to implement a Client-Side Encryption Tool built on Advanced Encryption Standard (AES) as shown in Figure 1.

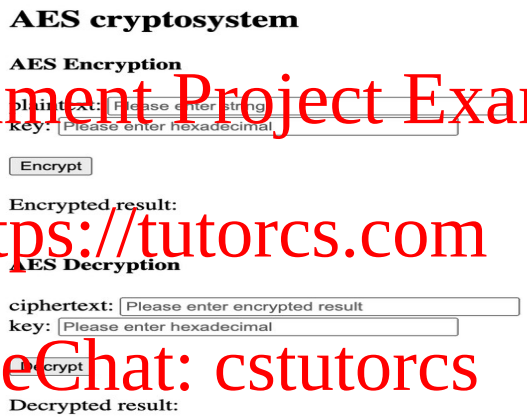

Figure 1. Cloud Client-Side Encryption Tool

Advanced Encryption Standard (AES) is a symmetric block cipher encryption that receives 128-bit size for each block and the size of key is 128, 192, and 256 bits. AES procedure involves some encryption rounds, which are determined by the cipher key size.

(1) Use JavaScript or Java to implement the Client-Side Encryption Tool Interface as shown in Figure 1.

(2) Use a Crypto Library to implement AES-256 encryption on a secret message with a list of your accounts, usernames, and passwords, where the encryption key is your email address.

(3) Output the encrypted message (in the hexadecimal form).

(4) Use a Crypto Library to implement AES-256 decryption on the encrypted message (in the hexadecimal form), where the decryption key is your email address.

(5) Output the decrypted message and check if it is the same as the original secret message.

Note: Please submit your codes and execution screenshots for (1)-(5).

Q2. Signing AWS Requests with Signature Version 4 **(Marks: 1+1+1+1+1=5)**

When you send HTTP requests to AWS, you need to sign the requests so that AWS can identify who sent them. You sign requests with your AWS access key, which consists of an access key ID and secret access key. The signing process helps secure requests in the following ways: verify the identity of the requester, protect data in transit, and protect against potential replay attacks. Creating a signed request includes 3 steps: (1) create a string to sign for Signature Version 4; (2) calculate the signature for AWS Signature Version 4; (3) add the signature to the HTTP request. **AWS Signature Version 4** is built on HMAC-SHA256 as shown in Figure 2.

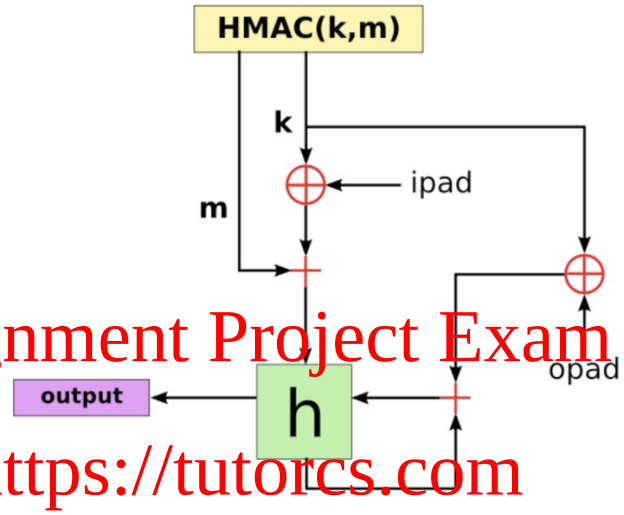

Figure 2. HMAC-SHA256 (k, m)

Suppose that a string to sign is as follows:

AWS4-HMAC-SHA256

20200920M123600Z

20200920/us-east-1/iam/aws4_request

f536975d06c0309214f805bb90ccff089219ecd68b2577efef23edd43b7e1a59

Assume that kSecret = your student ID/K7MDENG+bPxRfiCYEXAMPLEKEY.

(1) Compute kDate = HMAC("AWS4" + kSecret, Date), where Date = 20200920;

(2) Compute kRegion = HMAC(kDate, Region), where Region = us-east-1;

(3) Compute kService = HMAC(kRegion, Service), where Service = iam;

(4) Compute kSigning = HMAC(kService, "aws4_request");

(5) Compute the signature = HexEncode(HMAC(kSigning, string to sign))

Note: Please use SHA256 https://emn178.github.io/online-tools/sha256.html in HMAC-SHA256.

Please refer to https://docs.aws.amazon.com/general/latest/gr/sigv4-calculate-signature.html

Q3. AWS Key Management Service **(Marks: 1+1+1+1+1=5)**

AWS Key Management Service (AWS KMS) is a managed service that makes it easy for you to create and control customer master keys (CMKs), the encryption keys used to encrypt your data. AWS KMS CMKs are protected by hardware security modules (HSMs) that are validated by the FIPS 140-2 Cryptographic Module Validation Program.

AWS Key Management Service supports symmetric and asymmetric Customer Master Keys (CMKs). A symmetric CMK represents a 256-bit key that is used for encryption and decryption. CMKs are created in AWS KMS. Symmetric CMKs never leave AWS KMS unencrypted. In AWS KMS, a data key DK is created and used for encryption and decryption as shown in Figure 3.

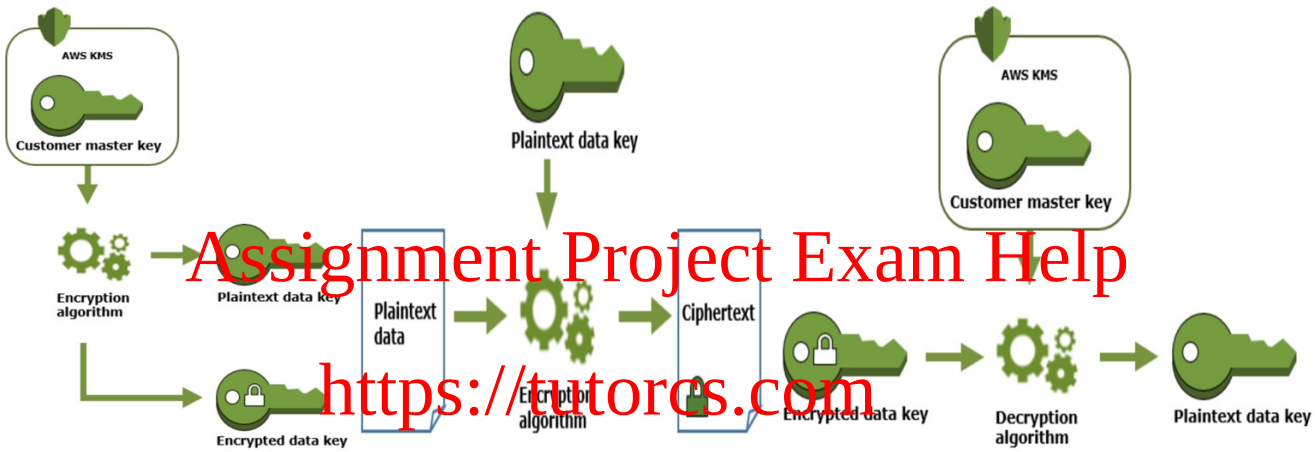

Figure 3 Create Data Key, Data Encryption and Decryption

Assume that the underlying encryption algorithm is AES-256 and the Customer Master Key CMK is SHA3-256(your student ID, your full name).

(1) If the data key DK generated by AWS KMS is SHA3-256(your email address), what are the outputs of AWS KMS when you create your data key DK? Please refer to Figure 3.

(2) If the data to encrypt is "your friend name, his postal address and mobile number", what is the encryption result?

(3) After the data is encrypted, what do you store in AWS?

(4) After the data is encrypted, what should you delete as soon as possible?

(5) If you want to find your friend's mobile number, how do you decrypt the encrypted data?

Note: Please use AES-256 implemented in Q1.

Please use SHA3-256 https://emn178.github.io/online-tools/sha3_256.html

RMIT UNIVERSITY

Q4. AWS Site-to-Site VPN based on Diffie-Hellman Key Establishment (Marks: 2+2+2+2+2=10)

An AWS Site-to-Site VPN connection connects your Virtual Private Cloud (VPC) to your data centre as shown in Figure 4. Amazon supports Internet Protocol Security (IPSec) VPN connections. Data transferred between your VPC and data centre routes over an encrypted VPN connection maintain the confidentiality and integrity of data in transit. Internet Key Exchange (IKEv2) is the protocol used to set up a security association (SA) in the IPSec protocol suite. IKEv2 uses X.509 certificates for authentication – either pre-shared or distributed and a Diffie–Hellman key exchange to set up a shared session secret from which cryptographic keys are derived.

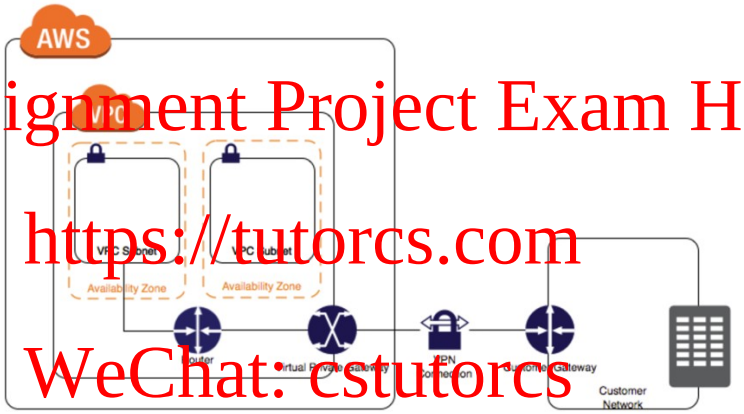

Figure 4. AWS Site-to-Site VPN

The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure channel. In this question, you are required to implement the Diffie–Hellman key exchange protocol (Group 2) between your VPC and your data centre.

For the Diffie-Hellman key exchange protocol, assume

--

p=178011905478542266528237562450159990145232156369120674273274450314442865788737020770612695252123463079567156784778466449970650770920727857050009668388144034129745221171818506047231150039301079959358067395348717066319802262019714966524135060945913707594956514672855690606794135837542707371727429551343320695239

g=174068207532402095185811980123523436538604490794561350978495831040599953488455823147851597408940950725307797094915759492368300574252438761037084473467180148876118103083043754985190983472601550494691329488083395492313850000361646482644608492304078721818959999

5649609776936801774927370896200668918795674421073O

--

(1) Implemenent 160-bit random number geneation;

(2) Use a Crypto Library to implement the modular exploentiation algorithm for larger integers.

(3) After a, b are randomly generated, output (a, g^a) and (b, g^b) and the secret key g^{ab} established between your VPC and your data centre by the Diffie-Hellman key exchange protocol.

(4) Can you perform a **Man-in-the-Middle Attack** to the Diffie-Hellman key exchange protocol? If so, show attacking steps.

(5) How does IKEv2 overcome the **Man-in-the-Middle Attack**? Show steps.

Note: Please submit your codes, computation results, security analysis and secure protocol.

Q5. SSL Handshake Protocol **(Marks: 1+1+1+1+1=5)**

AWS Certificate Manager from Amazon Web Services (AWS) takes care of deploying certificates to help you enable SSL/TLS for your website. Assume that AWS Certificate Manager issues you a SSL certificate and you have installed the certificate in your website hosted on AWS. When a client browses your website, suppose the client will run a SSL handshake protocol with ephemeral public key with your website to establish an encrypted link between the client and your website as shown in Figure 5.

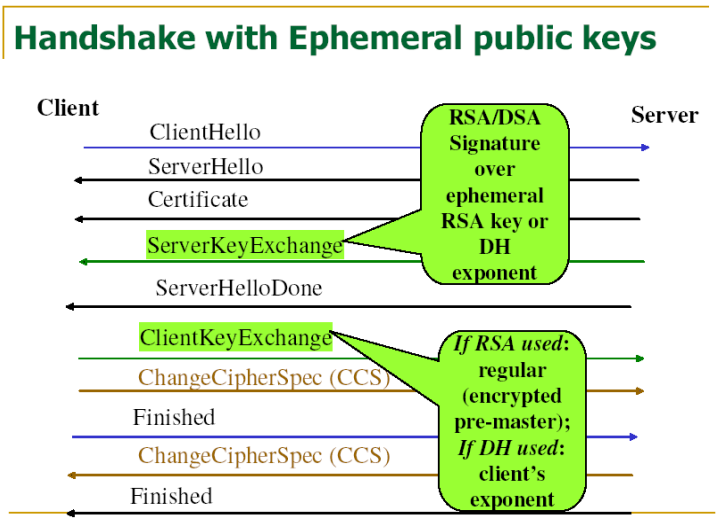

Figure 5. SSL Handshake Protocol

In the certificate of your website, if 2048-bit RSA public and private keys are

n=d71984b49b05be68473e112d79819f5b71d77d5468c2c9017896c245d2de745d26919cfa290edef287968b8

d1e63eb4026d730568a7bb0b65afddf85bc5256848938b4c3f9ab7938b1561a693e0188e5bc1710f3c7204af7b
4aa8f891f5d8b1d85bd8cc69bb5eb6ceaab9c6c2329196b66eb4b49460fe7a3db14fdc50232951156de171799f
7e29d88c72498e32d0414d34d43ef1ded13c15861d227ed686e7e0c33e1d1d2674b38a712dbf8c9ffca0c62838
d15ebbcb75c35cf952d54772d388236b99b7c76469320841de66347ce274ea98973be2374c9863a5827cf5238
931e408fc101dcc2edc5387a952dc621d3cfb7d440556829c37fa72471aca12717

e=$(10001)_{16}$

d=32e1ef7985be6b1761daf5d74b09f5b77d0b9bb32f00fce9a32c0e92d3da19aebb63f0bd609f0af05650af7c5
7770d7c6473bd148bb7cccaa665adcd8609f83b6bf6851462e84449bbf18157e9fa14f73b723d695d6e6f2d7f88
6561eb90864b1a8b0755281a75b19325bb5ffd4548a516788c9badbe2f6e9c71afc23dcdd7630e6bd5af7f363e
bca1a4f174dd91ad86a3ad058cf40a0190a865dfd19ddb8a36b5c72b0eca70a8c64feac4a91760e37c7b9c066c6
5000881adf9984b7f879211b331aacd1c7ff44922a1de42c3294220c49cc58529c4d5be218fd6adf2e98a907dc7
83d969ba61e178fb63a0a87f574a70433d22e4919b4a3b4e909ba24904c1

(1) Choose your ephemeral public key with 1024 bits and set e as the largest prime factor of your student number.

(2) What is the ServerKeyExchange message?

(3) If Pre_Master_Secret is SHA384(your full name and your student ID), where the hash function is SHA384 (https://emn178.github.io/online-tools/sha384.html), what is the ClientKeyExchange message?

(4) Analyse client authentication and server authentication of the handshake protocol.

(5) Analyse the forward security of the handshake protocol.

Hint: Compute modular exponentiations and inverse with online tool at
https://www.boxentriq.com/code-breaking/modular-exponentiation.
https://www.boxentriq.com/code-breaking/modular-multiplicative-inverse

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.

7. Rubric/assessment criteria for marking

All of the computations must be correct and only provided values must be used. Instructions must be followed.

Criteria The characteristic or outcome that is being judged.							**Total**
Question 1 Client-Side Encryption Tool	**Questions (1)-(5) are answered correctly.** **All of the implementations are done correctly.**	Any 4 of questions (1)-(5) are answered correctly. The implementations in the 4 questions are done correctly.	Any 3 of questions (1)-(5) are answered correctly. The implementations in the 3 questions are done correctly.	Any 2 of questions (1)-(5) are answered correctly. The implementations in the 2 questions are done correctly.	Any one of questions (1)-(5) is answered correctly. The implementation in the 1 question is done correctly.	Answer is not correct Or Not answered	10 Marks
	10 Marks	8 Marks	6 Marks	4 Mark	2 Mark	0 Marks	
Question 2 Signing AWS Requests with Signature Version	**Questions (1)-(5) are answered correctly.** **Step-by-step processes are shown with detail computations.** **All of the computations are shown correctly in detail.**	Any 4 of questions (1)-(5) are answered correctly. Step-by-step processes are shown with detail computations. The computations in the 4 questions are shown correctly in detail.	Any 3 of questions (1)-(5) are answered correctly. Step-by-step processes are shown with detail computations. The computations in the 3 questions are shown correctly in detail.	Any 2 of questions (1)-(5) are answered correctly. Step-by-step processes are shown with detail computations. The computations in the 2 questions are shown correctly in detail.	Any one of questions (1)-(5) is answered correctly. Step-by-step processes are shown with detail computations. The computations in the 1 question is shown correctly in detail.	Answer is not correct Or Not answered	5 Marks
	5 Marks	4 Marks	3 Marks	2 Mark	1 Mark	0 Marks	
Question 3	**Questions (1)-(5)**	Any 4 of questions (1)-	Any 3 of questions (1)-	Any 2 of questions (1)-	Any one of questions	Answer is not correct	5 Marks

AWS Key Management Service	**are answered correctly.** **Step-by-step processes are shown with detail computations.** **All of the computations are shown correctly in detail.**	(5) are answered correctly. Step-by-step processes are shown with detail computations. The computations in the 4 questions are shown correctly in detail.	(5) are answered correctly. Step-by-step processes are shown with detail computations. The computations in the 3 questions are shown correctly in detail.	(5) are answered correctly. Step-by-step processes are shown with detail computations. The computations in the 2 questions are shown correctly in detail.	(1)-(5) is answered correctly. Step-by-step processes are shown with detail computations. The computations in the 1 question is shown correctly in detail.	Or Not answered	
	5 Marks	4 Marks	3 Marks	2 Mark	1 Mark	0 Marks	
Question 4 AWS Site-to-Site VPN based on Diffie-Hellman Key Establishment	**Questions (1)-(5) are answered correctly.** **All of the implementations and security analysis are done correctly in detail.**	Any 4 of questions (1)-(5) are answered correctly. The implementations and security analysis in the 4 questions are done correctly in detail.	Any 3 of questions (1)-(5) are answered correctly. The implementations and security analysis in the 3 questions are done correctly in detail.	Any 2 of questions (1)-(5) are answered correctly. The implementations and security analysis in the 2 questions are done correctly in detail.	Any one of questions (1)-(5) is answered correctly. The implementations and security analysis in the 1 question is done correctly in detail.	Answer is not correct Or Not answered	5 Marks
	10 Marks	8 Marks	6 Marks	4 Mark	2 Mark	0 Marks	
Question 5 SSL Handshake Protocol	**Questions (1)-(5) are answered correctly.** **Step-by-step processes are shown with detail computations.** **All of the computations and**	Any 4 of questions (1)-(5) are answered correctly. Step-by-step processes are shown with detail computations. The computations and security analysis in the 4 questions are shown	Any 3 of questions (1)-(5) are answered correctly. Step-by-step processes are shown with detail computations. The computations and security analysis in the 3 questions are shown	Any 2 of questions (1)-(5) are answered correctly. Step-by-step processes are shown with detail computations. The computations and security analysis in the 2 questions are shown	Any one of questions (1)-(5) is answered correctly. Step-by-step processes are shown with detail computations. The computations and security analysis in the question are shown correctly in detail.	Answer is not correct Or Not answered	5 Marks

	security analysis are shown correctly in detail.	correctly in detail.	correctly in detail.	correctly in detail.			
	5 Marks	4 Marks	3 Marks	2 Mark	1 Mark	0 Marks	