UTM
UNIVERSITI TEKNOLOGI MALAYSIA

Department of Computer Science
Faculty of Computing

Lab 2

Programme	:	Bachelor of Computer Science (*Computer Network and Security*)
Subject Code	:	SECR3443
Subject Name	:	Computer Organization & Architecture
Session-Sem	:	2024/2025-1

Prepared by	:	1) Ahmad Hazim Bin Ahmad Najmi (A22EC0034) 2) Muhammad Izzuddin Bin Ahmad Fauzi (A22EC5023)
Section	:	03
Group / Member ID	:	8A

Lecturer	:	Dr. Muhalim Bin Mohamed Amin

Video Link	:	(*if any*) *http://utm.webex.com/meet/muhalim*
Date	:	2 January 2025

Turnitin (%)		**Marks / Remarks**
Similarity	**AI**	
20	0	

SECR3443 INTRODUCTION TO CRYPTOGRAPHY
(Lab 2)

Name	: AHMAD HAZIM BIN AHMAD NAJMI	Marks
Student ID	: A22EC0034	
Name	: MUHAMMAD IZZUDDIN BIN AHMAD FAUZI	
Student ID	: A22EC5023	
Section / Group	: 03/8A	

OBJECTIVES:

At the end of the laboratory work, student will be able:

i. To illustrate the steps of creating public and private key.
ii. To identify the content of a digital certificate.
iii. To demonstrate the encryption and decryption of RSA.

INSTRUCTIONS:

Answer all questions of Task 1 and Task 2. This lab work must be performed using *CrypTool*, which need to be downloaded and installed on your PC.

TASK 1 : Demonstration of RSA

(a) **Creating *p* and *q*.**

iv. Write down the selected values in Table 1.

Table 1

Selected Matric	A22EC5023	
Integer Value	225023	
	p	*q*
Initial Value	250	223
New Value	251	223

[5 *marks*]

(b) **Creating modulus, *n* and key pairs.**

iii. List the RSA derived parameters in Table 2.

Table 2

RSA Modulus n	55973
$\phi(n)$	55500
Public key, e	2*16+1
Private key, d	52973

[5 *marks*]

(c) **RSA Encryption & Decryption**.

iii. Fill Table 3 with the output values.

Table 3

M1	AhmadHaz
Data segmentation	A # h # m # a # d # H # a # z
Characters to Number Conversion, *P1*	065 # 104 # 109 # 097 # 100 # 072 # 097 # 122
Encrypted data, $C1 = P1^e \bmod n$	50519 # 15157 # 12465 # 21953 # 51731 # 02405 # 21953 # 10193

[5 *marks*]

(d) **Message Authentication.**

ii. Write down the selected values in Table 4.

Table 4

e	d
2^16+3	8359

iv. Note the output plaintext and write down your observation.

The decrypted message could not be decoded into a text message!

[5 *marks*]

TASK 2 : Generating Keys and User Certificates

(b)

Digital Certificate.

iii. Identify the terms in Table 5 by examining the certificate.

Table 5

Certificate Information	**Member 1**	**Member 2**
Serial Number	82:17:45:2C:88:13:24:1D	01:75:4D:CA:64:F0:27:CA
Validity: NotBefore	Wed Jan 01 15:47:25 2025 (250101074725Z)	Wed Jan 01 15:50:20 2025 (250101075020Z)
NotAfter	Thu Jan 01 15:47:25 2026 (260101074725Z)	Thu Jan 01 15:50:20 2026 (260101075020Z)

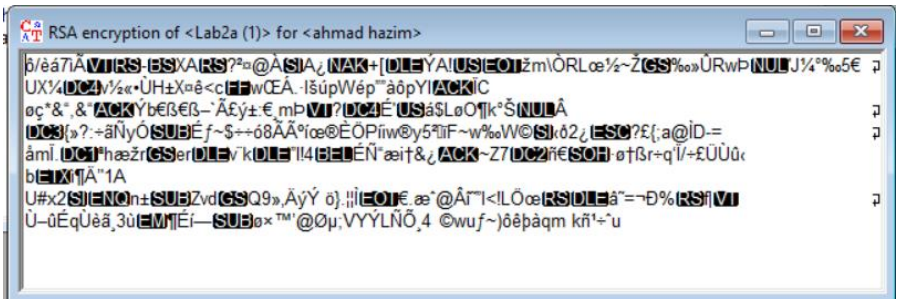
[5 *marks*]

[5 *marks*]

(c)

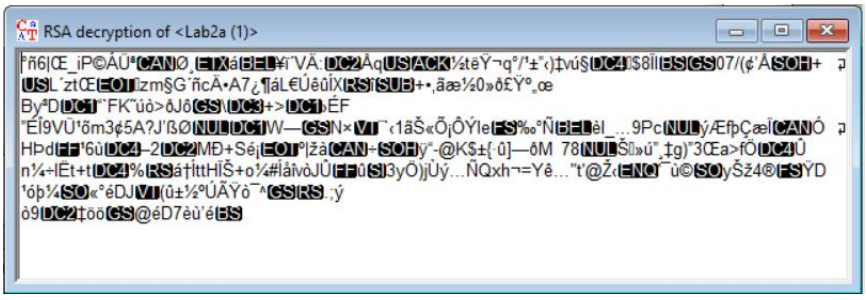
Encryption/Decryption

ii. Write the formula to calculate *C2* in terms of *M3* and the keys.



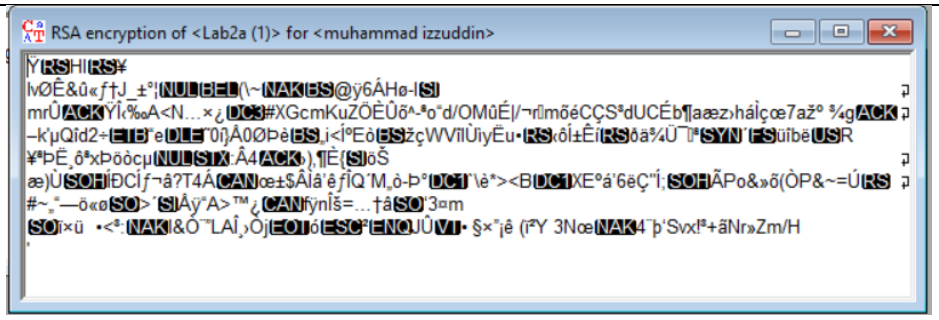
RSA Encyption for member 2

C2	C2 = M3^e mod N

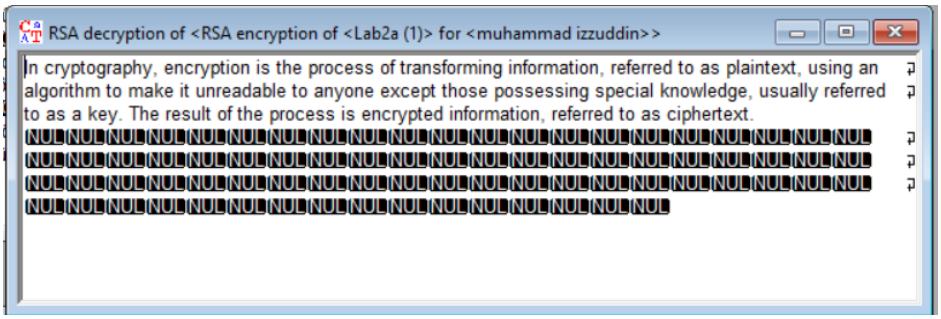


RSA Decyption for member 2

[5 *marks*]



RSA Encyption for member 1

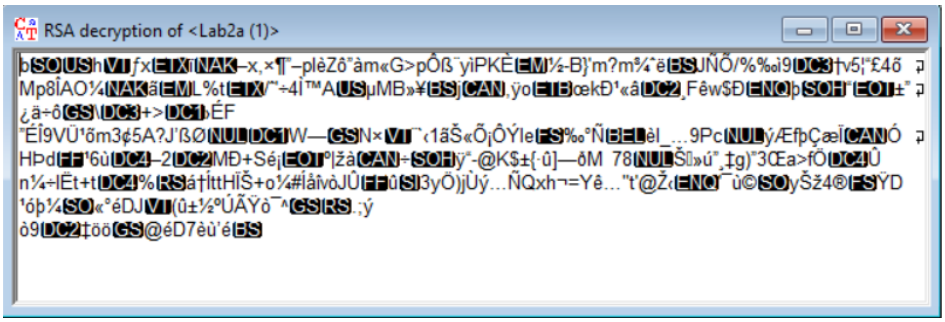


RSA Decyption for member 1

vi. Discuss your observation of the derived message.

The output does not match the original plaintext after decryption because RSA is an asymmetric encryption algorithm that uses different keys for encryption and decryption. Each individual has a unique key pair consisting of a public key and a private key. For example, if Member 3 encrypts a message using their public key, the decryption process must use Member 3's private key to retrieve the plaintext. Using Member 2's private key instead will result in an unreadable, gibberish value.

(d) **Message Integrity.** [5 *marks*]



iv. Write your observation.

Altering even the first number of the ciphertext will corrupt the

		message, rendering it unreadable. RSA encrypts messages block by block independently, so any modification to the first block directly affects its decryption.	

TASK 3 : Hybrid Cryptographic System: RSA and AES

(a) **Encryption.**

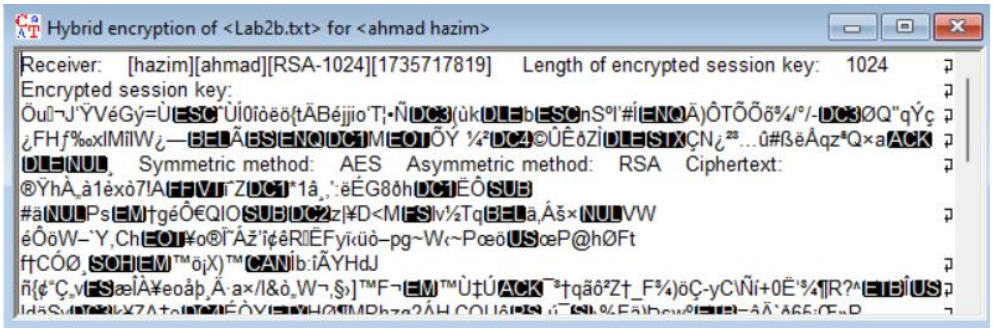
ii. Fill complete Table 7 with the values generate by *CrypTools*.

Table 7

Document	*Lab2b.txt*
Symmetric/ session key	4E 1C F5 12 93 DB 78 E9 BB 8B 81 56 54 0A 1A 60
Public key	179385398862498169068030 820834778917814219208771 344093215513297030603476 216852814267410155505983 9 572963444159241810136092 3 866547380364853453881681 7 827336901712457627645358 4 068155846706220079565353 1 700030900605173280793747 1 829069950247135234
Encrypted session key	D6757FAC4A919F56E947 FD3DD91B88D9CD30EEF 2EBF67B7490C442E96A6 A696F9154A695D11328F9 6B10621B6E53BA499223CD 05C429D454D5D5F5BE2F

[5 *marks*]

			B02FAD13D89D512271D DE7BF46488389786C4DEE 6C57BF9707C30805114D04D 5DDA0BCB214A9DBCAF 05ACC1002C74EBFB290 B385FB23DFEBC5717AAA5 1D761061000B8	



(b)

Decryption.

i. Fill up Table 8 with the generated output as you continue with the process.

Table 8

Recipient	Member 2
Public key	1502784160664622576001662 5961352925713343725253174 7024578655210749213767104 5954203232314534956595084 8286002513824725254723332 5457500979835692580675788 8563169512507977753223827 6304007745493125432077102 4714559473416777750918381 5537224780492822904185899 9605953064923918938312 47 3596895078431540134726 82

[5

			marks]

	06859276233
Symmetric /Session key	4E 1C F5 12 93 DB 78 E9 BB 8B 81 56 54 0A 1A 60

iv. Complete Table 9 with the decryption protocol.

Table 9

A → B	{E(K_s, D) || E(K_{PUB}, K_s)}
Recipient B	i. Use a private key to decrypt the encrypted session key
	ii. Retrieve the session key
	iii. Use the session key to decrypt the encrypted messag