

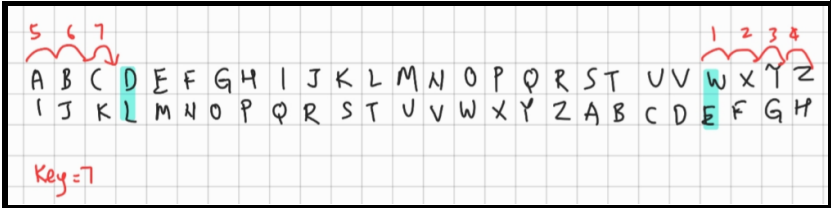
Question 1

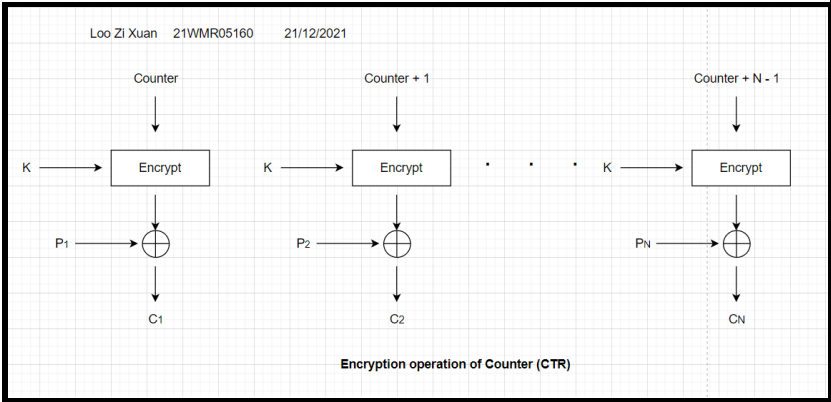
Qs	Your Answer	Marks Allocated	Marks Awarded
a)	<p>In this case, availability has been compromised.</p> <ul style="list-style-type: none">• Availability can be referred to as the ability of the system to work promptly and ensure the service is available when it is being requested by the authorized user regardless of the time and location.• For loss of availability, it can be defined as description of access to the information or system.• In this case, when Cindy tried to access the university website (system) to turn in her application, she couldn't make it as the admission website crashed.• Thus, she can't access the service provided by the university application which means the availability of the system has been compromised.	4	
b)	<p>Yes, I agree with the statement "Security experts recommend that we shouldn't change our passwords too frequently".</p> <ul style="list-style-type: none">• This is because if we currently have a strong and unique password (i.e password length with at least 8 characters with the combination of uppercase letter, lowercase letter, symbol, number, unicode character), we shouldn't change it unless we believe that our password has been compromised.• Moreover, changing a password too frequently does not improve the security as we gain nothing from the change, instead, if we constantly change a good password means that we are more likely to use a bad password instead.• Hence, we should change our password frequently, like twice a year but not too frequently (i.e changing passwords per month).	5	

c)	<ul style="list-style-type: none">• Drive-by-download is a malicious software that exploits software vulnerabilities or bugs in the user application in order to install malware. Thus, it can be spread whenever the user visits the malicious website that consists of code that will exploit the bugs, download and introduce malware without user knowledge and consent.• Keyloggers can be used to capture the keystroke on the infected device to monitor and gain sensitive information of the victim in which the attacker will receive a copy of all text on the infected machine from this malicious software. It typically will implement some filtering mechanism to return only the “keyword information” such as password and login.• Ransomware is a malware that will encrypt the user files and demand a ransom payment in bitcoin or other cryptocurrency form from the victim in order to let them regain access to their files.	6	
d)(i)	<ul style="list-style-type: none">• “My webcam can’t be hacked!” is a false statement, the webcam can actually be hacked by the hacker.• The hacker can secretly upload a Remote Access Trojan (RAT) or remote administration tool to hack into the webcam. After the webcam has been hacked, the attacker can take over our device’s camera and microphones which allow him/her to record the video and audio covertly and steal personal information from the victim.• There are few signs when your webcam has been hacked, one is the webcam on your device will be turned on at a strange time while another will be some unexpected webcam video files have been stored in our device. All of these indicate that our webcam has been hacked.	5	

d)(ii)	<ul style="list-style-type: none">• “Phishing emails are easy to recognize.” is a true statement, the phishing emails are actually easy to recognize. To illustrate, there are some signs to be recognized as phishing emails.• For example, a generic greetings will appear in the email such as “Dear Valued Customer”• Some emergency instructions namely “Failure to respond in 2 hours, we will terminate your account.”• The link in the email that looks suspicious• Misspelling and poor grammar has been used in the email• An email that will request your personal or privacy information such as name, credit card number, password, etc	5	
TOTAL Q1		25	

Question 2

Qs	Your Answer	Marks Allocated	Marks Awarded
a)	<p>Steps to illustrate how I identify the key :</p> <ol style="list-style-type: none"> 1. I choose the shortest cipher text form the encrypted message 2. In this case, DL and i will list out all the 26 alphabets in order sequence then put the L below the D 3. After that, I will continue put the alphabet that is after L which is M, N, O, etc 4. After write out all the alphabet, I will check which sentence is make sense 5. In this case, "WE" word is make sense 6. Next, I will count how many steps required from W to D and find out the step required is 7 which is the shift key in this case. <p>Diagram:</p>  <p>Key that has been used : 7</p> <p>Message decrypted : WE LOVE CRYPTOGRAPHY</p>	5	

b)	<p>I would choose stream cipher.</p> <ul style="list-style-type: none"> • This is because stream cipher (i.e RC4) processes the input continuously to produce one output at a time. • Moreover, stream cipher encrypts 1 byte (8 bits) at a time. • Stream cipher does not require large memory as it is used to process small chunks of data which means it is faster than block cipher as the block cipher will encrypt either 64 or 128 bits block size at one time (slower compared to stream cipher). • For the application that requires encryption and decryption of a stream of data over the data communication channel, stream cipher will be a better choice. 	6	
c)	<p>Diagram for encryption operation of Counter (CTR) :</p>  <ul style="list-style-type: none"> • The counter value for CTR mode has to be different for each plain text block that will be encrypted. • First, the counter will be initialized to some value (i.e 1) and then it will subsequently increment the counter by 1. • For encryption operation, the counter will be encrypted and then XOR with the plaintext block to create the ciphertext block. In CTR mode, there is no chaining in the Counter mode. 	6	

d)	<p>Encryption and decryption for $p = 11$, $q = 31$, $e = 7$, $M = 4$:</p> <p>Loo Zi Xuan 21wMRO5160 21/12/2021</p> $p = 11, q = 31, e = 7, M = 4$ $\text{Encryption} \Rightarrow C = M^e \pmod{n}$ $n = p * q$ $= 11 * 31$ $= 341$ $\therefore C = 4^7 \pmod{341}$ $= 16$ $\text{Decryption} \Rightarrow M = C^d \pmod{n}$ $\phi(n) = (p-1)(q-1)$ $= (10)(30)$ $= 300$ $d(7) \pmod{300} = 1$ $43(7) \pmod{300} = 1$ $d = 43$ $\therefore M = 16^{43} \pmod{341}$ $= 4$	8	
TOTAL Q2		25	

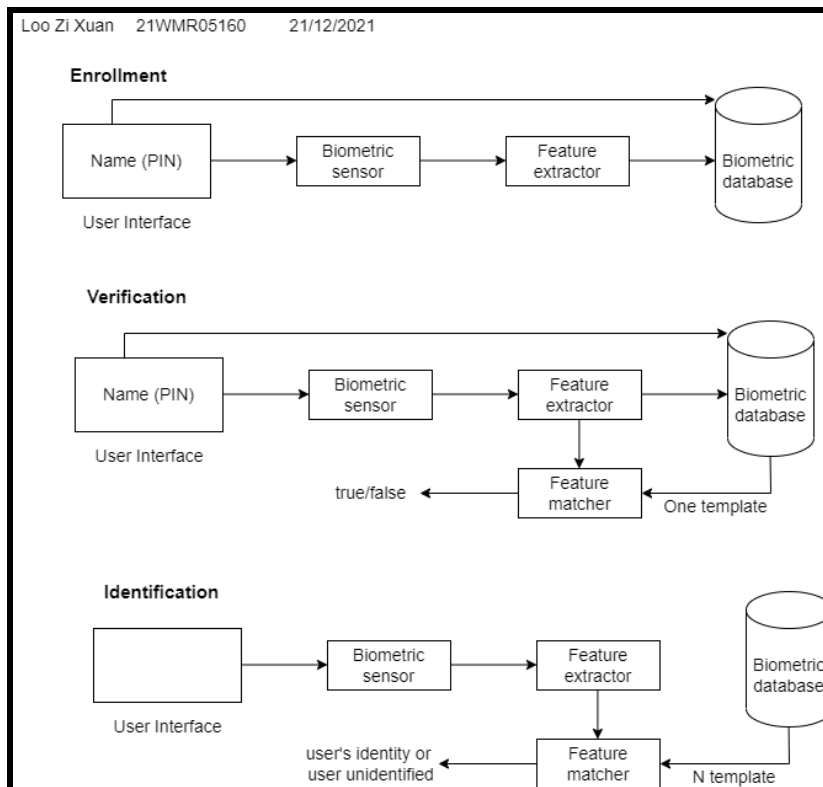
Question 3

Qs	Your Answer	Marks Allocated	Marks Awarded
a)	<p>Capability List :</p> <p>Handwritten notes at the top of the diagram: "Lee Zi Xuan", "2000RUST60", and "21/12/2021".</p> <p><u>Capability List</u></p> <p>Ali →</p> <ul style="list-style-type: none"> File 2: Own Read Write File 3: Read Write File 5: Own Read Write <p>Baba →</p> <ul style="list-style-type: none"> File 1: Own Read Write File 5: Read <p>Muthu →</p> <ul style="list-style-type: none"> File 1: Read File 2: Read Write File 4: Own Read Write File 5: Read <p>Ah Hack →</p> <ul style="list-style-type: none"> File 1: Read Write File 2: Read Write File 3: Own Read Write File 4: Read File 5: Read Write 	8	

b)

Enrollment, verification and identification of the biometric user authentication :

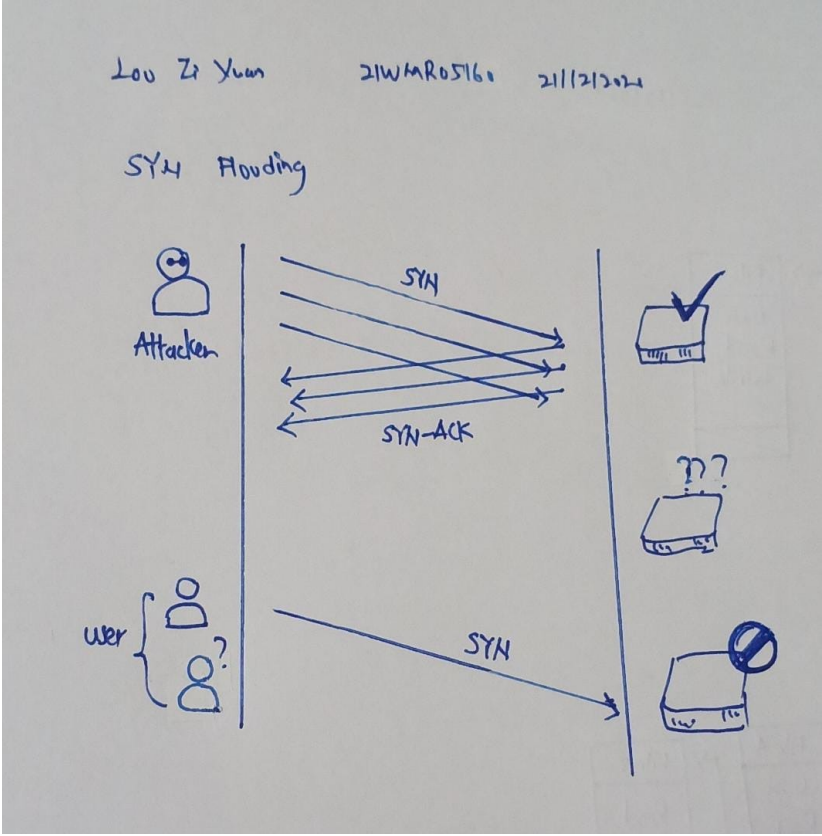
9



- Enrollment :** Each user who wants to be an authorized user must enroll in the system. It's like assigning a password to a user. For a biometric system, the user must present a name or password/pi number to the system, meanwhile the biometric sensor will sense some biometric characteristics such as fingerprint, then digitalize the input and store it as a number that can represent these unique biometric characteristics. This indicates that the user is now enrolled in the system.
- Verification :** In this operation, the user will enter the PIN number as well as use the biometric sensor. After that, the system will try to extract the corresponding characteristic and compare it to the template that has been stored for this user since enrollment. If it matches, the user will be authenticated.
- Identification :** In this operation, the user will only use the biometric sensor with no additional information. Then, the system will compare the stored template with templates presented by the user. If it matches, the user is identified, otherwise, the user is rejected.

c)	<p>4 measures for dealing with human-caused threats:</p> <ul style="list-style-type: none">• <i>Physical contact with resources is being restricted.</i> For example, the resource will be locked in a locked cabinet, safe or room to deny access to outsiders. However, it can't avoid the issue of unauthorized insiders or employees happening as they have the authority to access those resources.• <i>The machine can be accessed but it is being secured by permanently bolted</i> to make it difficult to move and stolen by others. This can prevent theft happening but not for misuse, vandalism and unauthorized access.• <i>The movable resource is equipped with a tracking device.</i> Hence, the sending portal inside the resource will trigger an automated barrier and alert the security personnel to protect and prevent the resource being moved out from the protected area.• <i>Install intruder sensors and alarms</i> to detect the movement of the equipment and unauthorized users. If someone has accessed the system without authentication or the equipment has been moved without permission, the sensor and alarms will detect it and respond to the incident to the respective personnel.	8	
TOTAL Q3		25	

Question 4

Qs	Your Answer	Marks Allocated	Marks Awarded
a)	<p>Diagram for SYN flooding attack:</p>  <p>The SYN flooding attack is an attack in which the attacker will flood the target computer's TCP buffer with a huge volume of crafted packet which will cause the target computer unable to build connections with other devices.</p> <p>The SYN flooding attack will be carried out by</p> <ol style="list-style-type: none"> 1. The attacker sends a huge amount of crafted packets to the target computer. 2. The victim's computer is required to send an ACK packet to the crafted source IP address contained in the SYN packet. 	8	

	<p>3. Since the crafted source IP address is unreachable, the victim's computer is unable to receive the ACK packet that it is waiting for. This makes the crafted SYN packet still remain in the TCP buffer.</p> <p>4. Now, the TCP buffer is fully occupied by the crafted SYN packets.</p>		
b)	<p>Strengths of firewall :</p> <ul style="list-style-type: none"> • Firewall can help a company to enforce its security policy and safeguard measurements. • Firewall can protect our device by allowing and blocking the network transmission according to the predetermined security rules such as implementing an access control to specify which group can pass through the authentication device and access to the services. • There are 2 types of firewall which are software firewall and hardware firewall. • For instance, a software firewall can be loaded on a user device such as a PC to perform the firewall function but this type of firewall will only protect that PC. • For a hardware firewall, it shall have a demilitarized zone (DMZ) to protect the internal network. To illustrate, DMZ allows the host to provide internal and external services to both the internal and external network whenever there is unauthorized user or intruders who want to compromise the device in that DMZ. <p>Weakness of firewall :</p> <ul style="list-style-type: none"> • A firewall cannot protect against the software and traffic that does not come through it such as unauthorized connections from wireless modem or the malware that is delivered through DVD, CD, pendrive, etc. • If the permission has been granted, the ability of the firewall to block the unwanted traffic will become limited. For instance, if a user grants the permission in which the spam 	8	

	<p>email is allowed to enter the mailbox, the email filtering firewall will not block the email even though the email has malicious link and attachments.</p> <ul style="list-style-type: none"> The filtering packet process by a software firewall will greatly degrade the device's performance. 		
c)	<p>Risk Acceptance :</p> <ul style="list-style-type: none"> This alternative is to accept the risk. There might be several reasons for doing this such as the cost and time to implement the control / treat the risk is greater than the loss. For this alternative, the management has to accept the responsibility for the consequence of using this risk treatment alternative. <p>Risk Avoidance :</p> <ul style="list-style-type: none"> This alternative will stop the activity or system that has a high potential to create the risk. However, this will always cause some inconvenience as some of the functionality of the system cannot be performed and carried out. Hence, the loss of capability is being traded off against the reduced risk. <p>Risk Transfer:</p> <ul style="list-style-type: none"> This alternative will share its responsibility for the risk with a third party such as an insurance company. Moreover, it can be achieved by signing a contract with another organization or the partnership using a joint venture. All of them shall share the responsibility and help to afford 30 to 50% of the loss and recover the system. 	9	
TOTAL Q4		25	