Question 1

a.

- Determine the value of an asset being protected. It depends on the asset's owner perspective and might be dependent or independent of monetary value.
- The vulnerabilities occurred within the system. Examples of the vulnerability include weak password within the system or firewall within a device that is not being well deployed.
- The potential threats (i.e loss of credential data , data damage) and the likelihood of attacks happening (i.e low, medium, high).

b. -

(i)

Confidentiality - Low because the information is actually public to the others
Integrity - Moderate because modifying the information might cause the inaccurate information being transmitted to the public
Availability - Moderate because it might cause unnecessary problems such as cannot get the necessary information and resources as the staff cannot access the system when requested.

(ii)

Confidentiality - High because the routine administrative information is highly confidential and should not be exposed to the public. If the information is leaked out, the company might suffer reputation loss issues and face lawsuits.
Integrity - High because if the routine administrative information has been modified by the unauthorized user, it causes the information and data to become inaccurate which will affect the operation.
Availability - Moderate because it might cause unnecessary problems such as cannot get the necessary information and resources as the staff cannot access the system when requested.

c. (i) Ransomware. A ransomware is a malware that will encrypt the files within the victim's PC and demand a ransom payment in Bitcoin from the victim in order to regain access to their files.

(ii) Countermeasure 1:

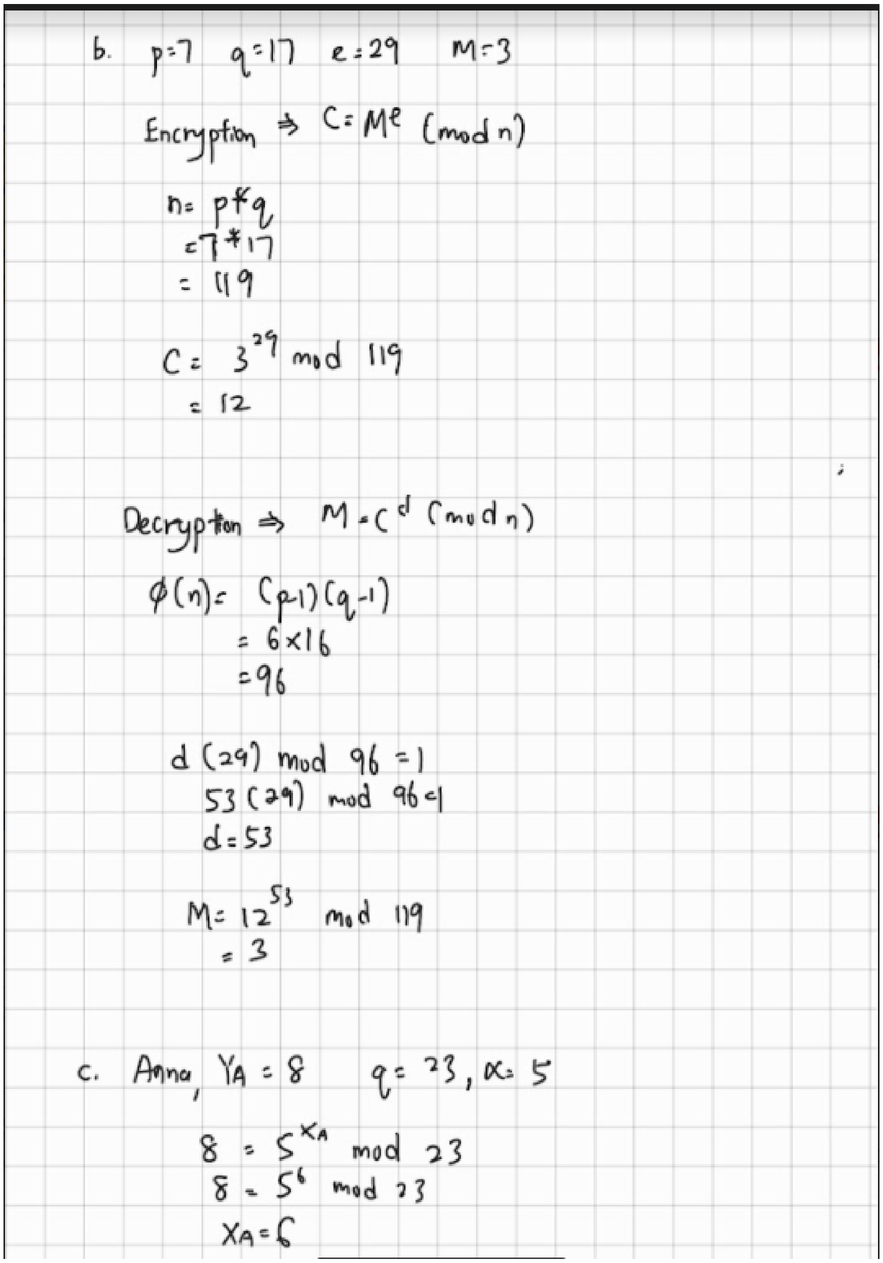
Organizations should ***keep all the operating systems (OS) and software up to date*** as one of the countermeasures against zero-day exploits. This is because the critical patch for the security flaw will often be developed and included in the new system release in order to remediate the discovered vulnerabilities. An up-to-date system ensures the organization from being attacked by exploiting the security vulnerability within its software system.

Countermeasure 2:
Organizations should ***deploy an effective firewall*** that can ensure maximum protection against zero-day attacks. To illustrate, the firewall will control the incoming and outgoing network traffic according to the predetermined security rules. This could greatly reduce unsolicited and unauthorized access which only allows necessary traffic to access over the organization network. By implementing a firewall, any suspicious traffic that travels in and out of the software system can be blocked immediately despite the nature of the attack being unrevealed.

Question 2

a. I did not agree with the above statement. Block cipher will process a fixed input into a fixed-size block. Hence, it normally produces a large chunk of output block for each of the input blocks. For stream cipher, it will process the input continuously into one output element at the time. It is always faster than the block cipher even with comparable key length. Stream cipher works best when dealing with small chunks of data as it can process rapidly such as a live streaming video whereas block ciphers are better in dealing with large chunks of data.

b. -
c. -



b. $p=7 \quad q=17 \quad e=29 \quad M=3$

Encryption ⇒ $C = M^e \pmod n$

$n = p * q$
$= 7 * 17$
$= 119$

$C = 3^{29} \bmod 119$
$= 12$

Decryption ⇒ $M = C^d \pmod n$

$\phi(n) = (p-1)(q-1)$
$= 6 \times 16$
$= 96$

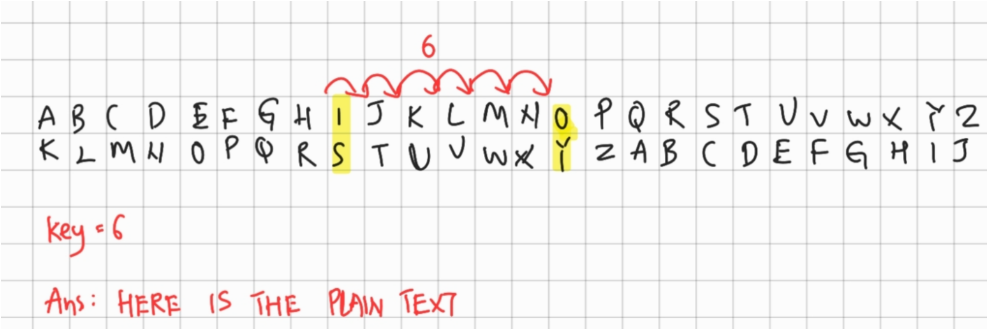
$d(29) \bmod 96 = 1$
$53(29) \bmod 96 = 1$
$d = 53$

$M = 12^{53} \bmod 119$
$= 3$

c. Anna, $Y_A = 8 \quad q = 23, \alpha = 5$

$8 = 5^{X_A} \bmod 23$
$8 = 5^6 \bmod 23$
$X_A = 6$

d. NKXK OY ZNK VRGOTZKDZ



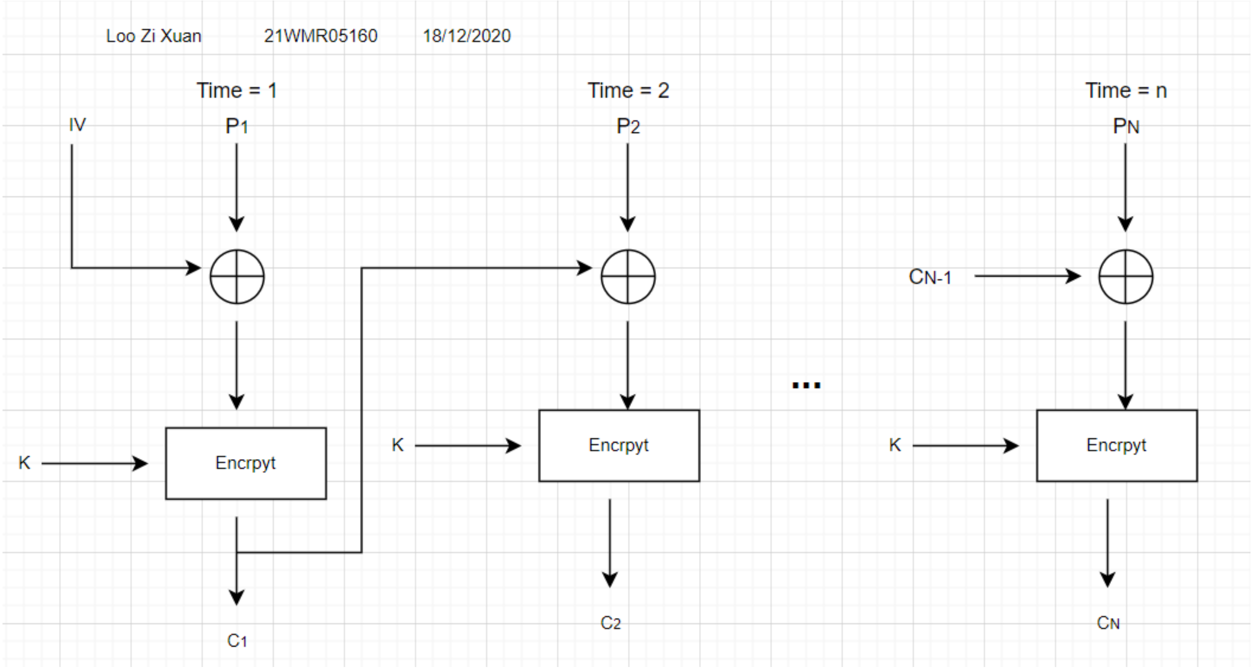
6

| | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J |

Key = 6

Ans: HERE IS THE PLAIN TEXT

e. CBC



For cipher block chaining encryption operation, it will XOR the current plain text block with the preceding cipher text block. Note that the same key, K will be used for each of the blocks. The CBC has chained together the processing of the sequence of plain text blocks.

Question 3

a. In my opinion, I think role-based access control (RBAC) is more suitable for the organization. This is because RBAC can simplify the security management as currently we have large groups of people who carry out the same task and require the same access level and type to access the file. In this case, we can define the role within the organization and assign the specified role to each of the users. The relationship of users with roles is many to many which means one user can be assigned to many roles, and each role can be assigned to many users. Each role will have its responding access right to the system resource within the organization.

b. -

- Salt can prevent password duplication from existing in the same password file. To illustrate, if two users had chosen the same password, the system would assign different salt values to be combined with the password selected by the user. Therefore, the hashed password that is stored in the password file will be different even if the same password has been inputted to the system.
- Salt can increase the difficulty of being attacked by the offline dictionary attack.

This is because a salt of length n bits will increase the amount of possible passwords by a factor of 2n and this will increase the difficulty for password guessing attacks.

- It makes the process to figure out whether a user has shared the same or similar password in different devices impossible as each of the passwords in different devices will be combined with different salt values to come out a different hashed value.

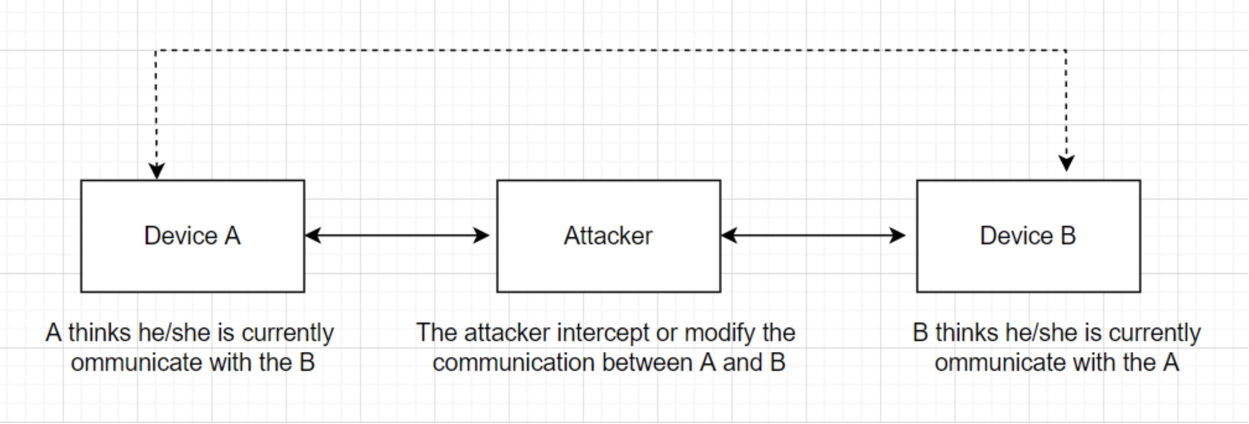
c. Access control list

d. -

- Design the air conditioning system as well as other ducts so that it would not spread fire. To illustrate, there will be standard guidelines and specifications to come out with such a design.
- Install the auto fire extinguisher. However, the fire extinguisher should be installed in which it is unlikely to cause damage to the equipment or human injury.
- Install fire detectors. For instance, the detector will sound an alarm in the IS room as well as some external authorities. Afterward, it will automatically trigger the fire extinguisher after a delay to allow human intervention.
- Equipment power-off switch. To illustrate, the location of the switch off button must be clearly marked and all employees must familiarize themselves with the procedures on how to switch off the power .

Question 4

a. -


Device A
Attacker
Device B
A thinks he/she is currently ommunicate with the B
The attacker intercept or modify the communication between A and B
B thinks he/she is currently ommunicate with the A

- Device A attempts to establish a communication session with device B.
- However, an attacker intercepts the transmission and disguises himself as device B.

- The attacker exchanges his own key to device A then establishes a communication session with device B which disguises himself as device A.
- Device B sends all messages either confidential or non-confidential to the attacker who might intercept, modify, replay or copy the message sent by device A, same goes to device A.
- Defense measures - Encrypting and authenticating IP packets

b. (i)

- IPsec can secure the branch office connectivity over the network. For example, an organization is able to build a secure virtual private network (VPN) over the network.
- IPsec can secure remote access. For instance, a user such as an employee can gain secure access to the other organization's network to access the resources over the Internet.
- IPsec can establish intranet and extranet connectivity. For instance, it can be used to establish secure connections/communication between the organization and other companies such as vendor companies.
- IPsec can encrypt and authenticate the traffic at Internet Protocol level which assure the security of data.

(ii)

- Use of an IPsec does not require us to change software/application on the end systems as it does not depend on the application used.
- IPSec is transparent to the application as it is located below the transport layer either TCP or UDP. Hence, the end user does not need to bother about the configuration of the IPsec.
- IPSec is transparent to the end user, hence it does not require user training for its security mechanisms.
- Provide strong security for individual users. To illustrate, the IPsec encrypts the data based on per-packet instead of per-flow base in which it greatly improves the IP security.

c.

- Motivation
- Capability
- Resources
- Probability of attack
- Deterrence