Question 1

Choose the correct answer to the following questions:

a) A friend calls you to ask for assistance. He is having trouble keeping an attacker out of his network. He tells you no matter what he tries, he can't seem to keep the attacker out of his network. He has no idea how the attacker keeps getting in. This is an example of what kind of attack. (1 mark)

A. Whack-a-mole attack
B. Advanced Persistent Threat
C. Privilege escalation
D. Passive injection

b) An attacker listens for all traffic being transferred over a network, in the hope of observing some unauthorized data. What kind of attack is this? (1 mark)

A. man-in-the-middle
B. sniffing
C. backdoor
D. phishing

c) What is the name of the term that is used to define vulnerabilities that are newly discovered and have yet addressed by a patch? (1 mark)

A. Single Point of Failure
B. Gray box attack
C. Buffer overflow
D. Zero-day

d) Which of the following could be an indicator of compromise? (1 mark)

A. Unusual out-band network traffic
B. Increased number of login
C. Large numbers of requests for the same file
D. All of the above

e) If both sender and receiver using the same secret key, the cryptographic system is called _______________. (1 mark)

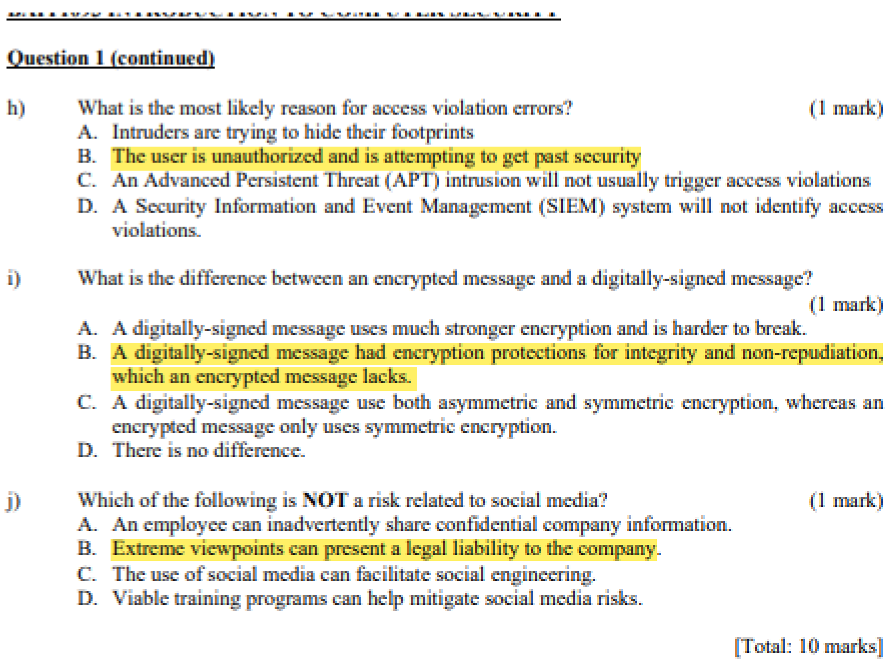
A. cryptanalysis
B. asymmetric encryption
C. symmetric encryption
D. brute-force attack

f) Biometrics authentication are based upon which of the following? (1 mark)

A. Advances in retinal scanning
B. The ability to rapidly scan biological markers
C. Parts of the human body that are unique
D. The original fingerprint studies of the 1880s

g) The hospital client you are working with would like to perform job restricting access to their patient records. They want doctors to have access only to records for their patients and only when the doctors are in the hospital. What type of access control method would you suggest they should use? (1 mark)

A. Attribute-based access control (ABAC) based on time access
B. Discretionary access control (DAC)
C. Role-based access control (RABC)
D. Mandatory access control (MAC)



Question 1 (continued)

h) What is the most likely reason for access violation errors? (1 mark)

A. Intruders are trying to hide their footprints
B. The user is unauthorized and is attempting to get past security
C. An Advanced Persistent Threat (APT) intrusion will not usually trigger access violations
D. A Security Information and Event Management (SIEM) system will not identify access violations.

i) What is the difference between an encrypted message and a digitally-signed message? (1 mark)

A. A digitally-signed message uses much stronger encryption and is harder to break.
B. A digitally-signed message had encryption protections for integrity and non-repudiation, which an encrypted message lacks.
C. A digitally-signed message use both asymmetric and symmetric encryption, whereas an encrypted message only uses symmetric encryption.
D. There is no difference.

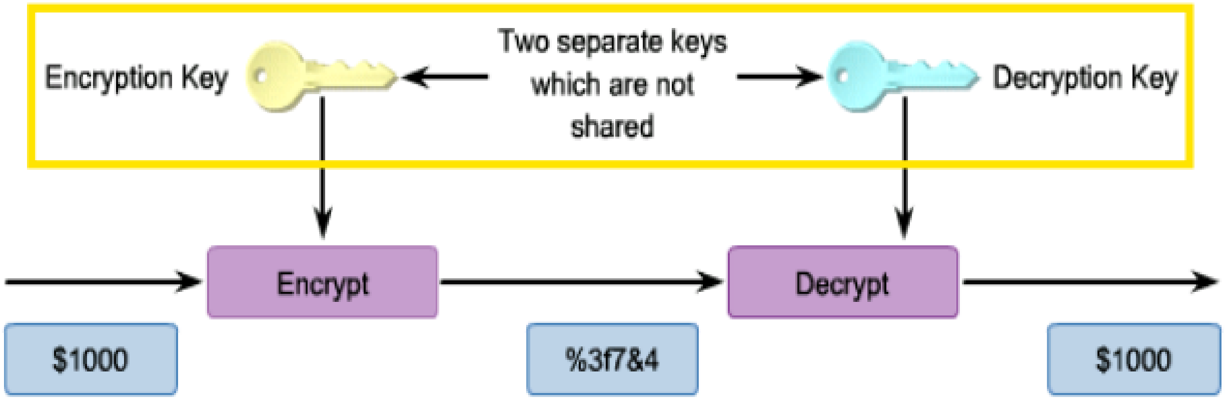
j) Which of the following is **NOT** a risk related to social media? (1 mark)

A. An employee can inadvertently share confidential company information.
B. Extreme viewpoints can present a legal liability to the company.
C. The use of social media can facilitate social engineering.
D. Viable training programs can help mitigate social media risks.

[Total: 10 marks]

Question 4

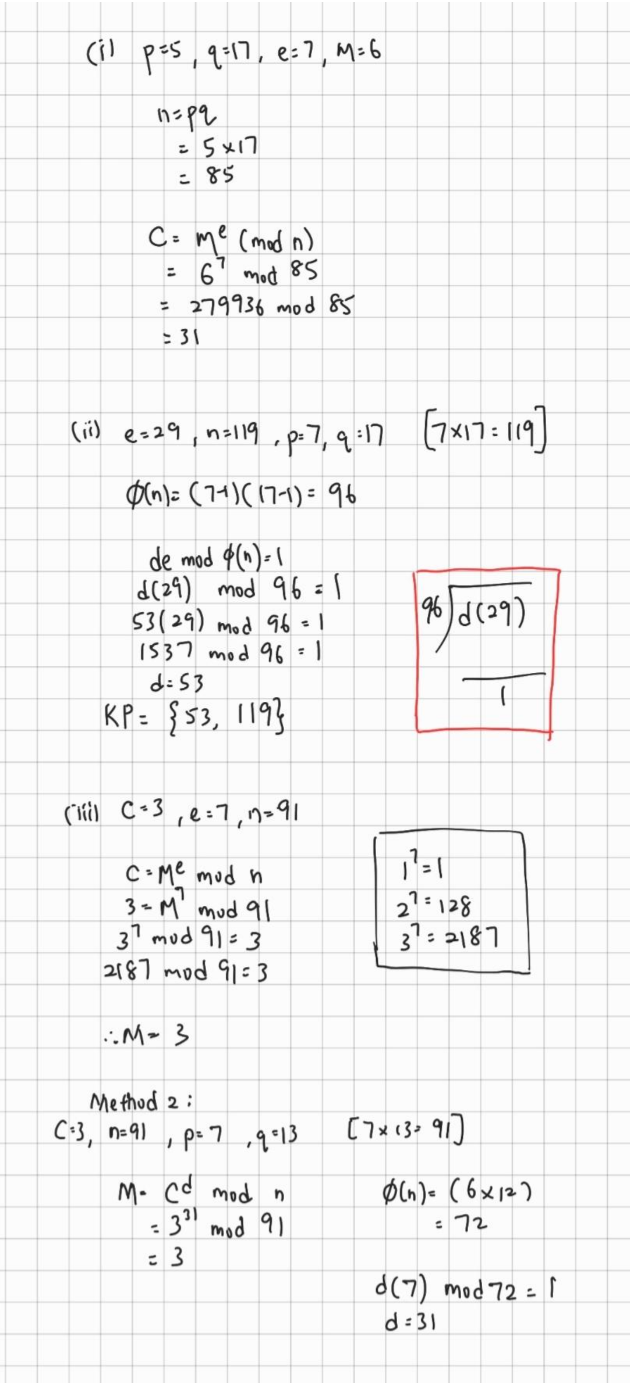
a. Diagram for asymmetric encryption : (draw own diagram in FOA)



- Asymmetric encryption also known a s public-key encryption because it uses 2 keys instead of 1 shared key compared to symmetric encryption for encryption and decryption. To illustrate, the private key will be kept safe and must only be known by its owner whereas the public key can be sent and known to anyone.
- For confidentiality purposes, the sender can use the receiver's public key to encrypt the data and the data will only be able to decrypt the message by using the receiver's private key. This can ensure the confidentiality of the message as only the receiver will know his/her private key.
- For authenticity purposes, the sender can use his/her private key to encrypt the data and anyone who knows the corresponding public key can decrypt the message.

- This encryption is called asymmetric because those who encrypt messages or verify signatures cannot decrypt the message or create signatures.

b.



(i) $p=5$, $q=17$, $e=7$, $M=6$

$n=pq$
$=5\times17$
$=85$

$C=M^e \pmod n$
$=6^7 \bmod 85$
$=279936 \bmod 85$
$=31$

(ii) $e=29$, $n=119$, $p=7$, $q=17$ $[7\times17=119]$

$\phi(n)=(7-1)(17-1)=96$

$de \bmod \phi(n)=1$
$d(29) \bmod 96=1$
$53(29) \bmod 96=1$
$1537 \bmod 96=1$
$d=53$
$KP=\{53, 119\}$

$96 \overline{)d(29)}$
$\overline{\quad 1}$

(iii) $C=3$, $e=7$, $n=91$

$C=M^e \bmod n$
$3=M^7 \bmod 91$
$3^7 \bmod 91=3$
$2187 \bmod 91=3$

$1^7=1$
$2^7=128$
$3^7=2187$

$\therefore M=3$

Method 2:
$C=3$, $n=91$, $p=7$, $q=13$ $[7\times13=91]$

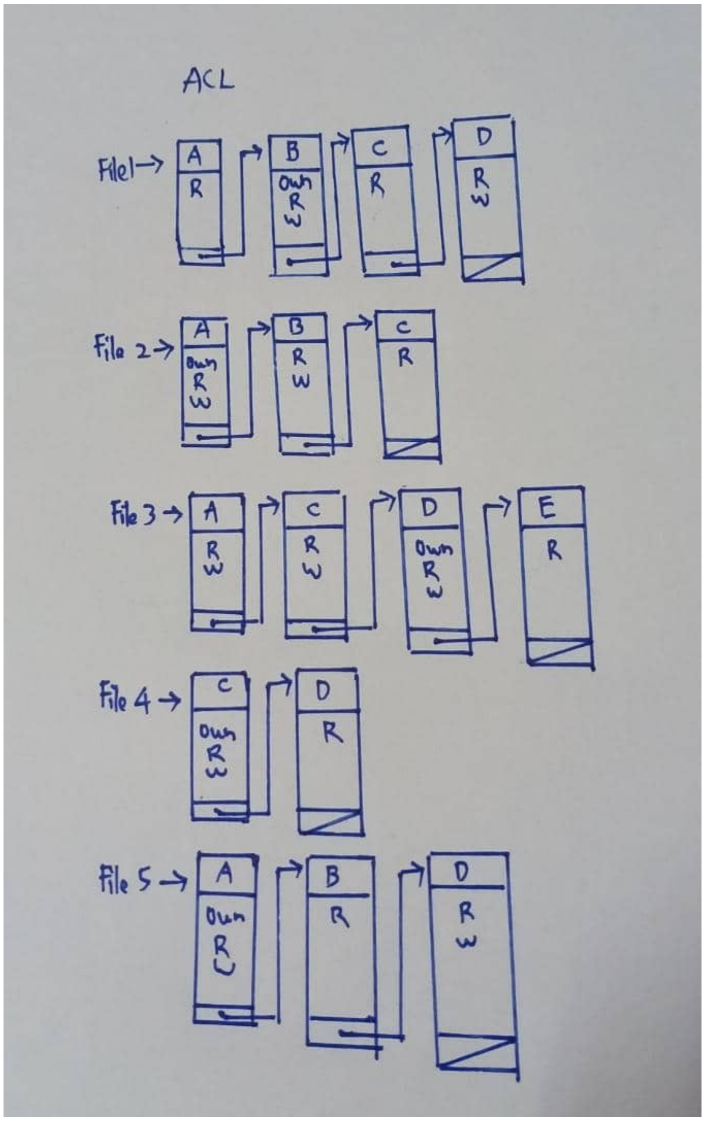
$M=C^d \bmod n$
$=3^{31} \bmod 91$
$=3$

$\phi(n)=(6\times12)$
$=72$

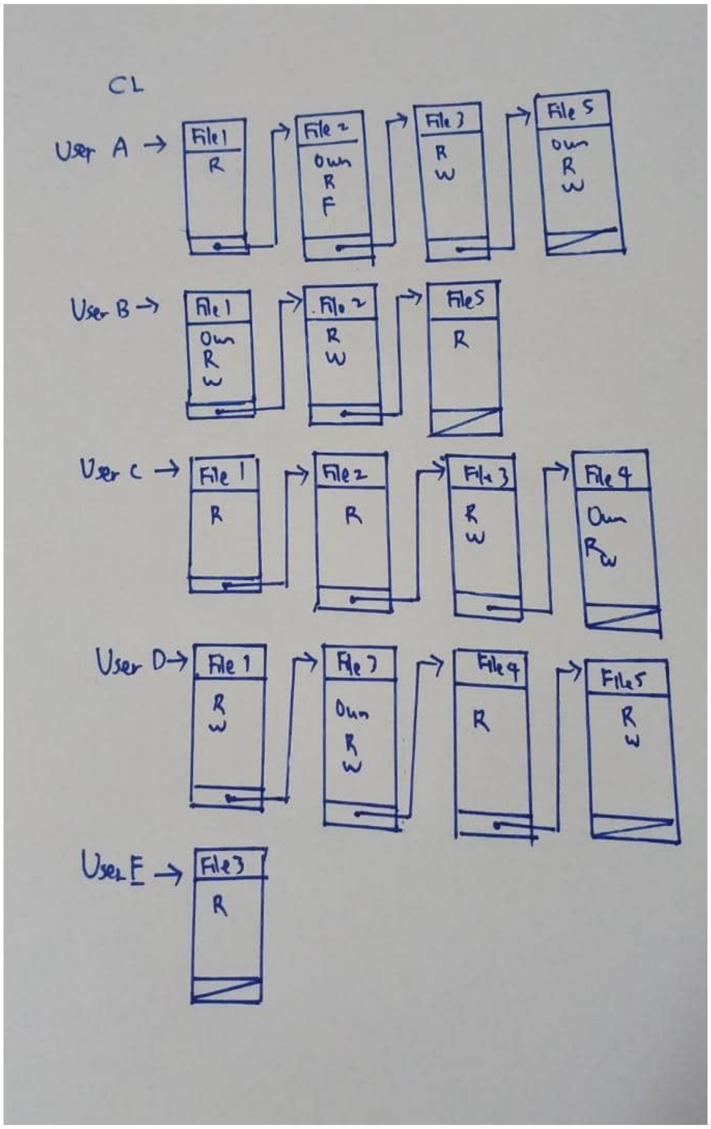
$d(7) \bmod 72=1$
$d=31$

Question 5

(i) Access control list



(ii) Capability list



Question 6

a. 3 mitigation measurement for human-caused threat:
   - **Physical contact with resources is being restricted**. 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.
   - **The machine can be accessed but it is secured** such as permanently bolted to make it difficult to move and stolen by others. This can prevent theft happening but not for misuse, vandalism and unauthorized access.
   - **The movable resource is equipped with a tracking device.** Hence, the sending portal inside the resource will alert the security personnel or trigger an automated barrier to prevent the resource being moved out from the protected area.

b. Baseline approach, Informal approach, Detailed risk analysis, Combined approach (most effective)