Name: **ID:**

Name: **ID:** ***(Total = 30 Marks)***

---

1) Confirming a User Identity can be performed by answering one or more of four questions. ***8 Marks***
List the four questions and use the following authentication words as examples to answer these questions:
Password, face, in Rector's office, ID card, PIN, Passport, voice, mother's name, smart card, fingerprints, in KFUPM

a)

b)

c)

d)

---

2) Which of the security strategies (**1-Exponential Back-off, 2-Disconnection, 3-Disabling, 4-Jailing**) are used in the authentication protection according to the following cases. Assume the possibility for more than one method to be used intending to give more protection: ***7 Marks***

a) Attacker is finding too much delay in the prompt asking for login and password to access the system. In fact, the delay is found to be increasing, then after ten hacking attempts the system is found to be reestablishing the network connection.

b) After any three normal attack attempts the system is found giving access. However, when a critical functionality is attempted the systems stops all actions and asks for administrator reset of the account. Even the normal user is not able to access the system after such malicious attack.

c) Any attack will case denial of access, such that the connection is there but the account is disabled and need to be reset.

d) Any wrong attempt makes the system allow browsing the account content without being able to do any action. The second wrong attempt will cut off the network. The third attempt will make the account inaccessible except with the account own user.

e) A mobile phone is being under hacking attempts, which will cause time delay for the password to be asked for. This time increases every time until fifth attempt. Then the mobile runs a special program that discharges the battery and makes the mobile not able to establish communication to the network. Also, after the fifth hacking attempt the account is stopped and cannot be accessed except by the administrator reset.

f) Wrong attempt to access this account more than two times makes it divert from its normal path to a honey-pot system.

g) The hacker was able to access an account within the bank system at attempt number 1,011,101. He has been able to transfer SR 1,011,101 to his account. The bank was able to trace back this malicious action and returned the money to its account with an official apology letter to the customer affected (the customer owning this account).

3) Specify the design principles matching the understanding below: ***7 Marks***

[1]	Least Privilege	[5]	Open Design
[2]	Fail-Safe Defaults	[6]	Separation of Privilege
[3]	Economy of Mechanism	[7]	Least Common Mechanism
[4]	Complete Mediation (Negotiation)	[8]	Psychological Acceptability

a) …. ……A subject should be given only those privileges necessary to complete its task. If a subject does not need an access right, the subject should not have that right

b) …. …….Function, not identity, controls rights assignment. Rights added as needed, discarded after use

c) …. …….Default action is to deny access

d) …. …….Access rights are explicitly granted. It should be denied access otherwise

e) …. …….If action fails, system as secure as when action began. Whenever a system security update is not complete, no changes are made to its security state. If the program fails, the system is safe

f) ….. …….Keep security mechanisms as simple as possible, less can go wrong. When errors occur, they are easier to understand and fix. Watch for Interfaces and interactions

g) ….. ……Check every access whether it is allowed

h) ….. ……Similar to Kerckhkoffs Principle in cryptography

i) ….. …….Security of a mechanism should not depend on *secrecy* of its design or implementation

j) ….. …….No "Security through obscurity"

k) …. ……..Require multiple conditions to grant privilege – single condition is not enough, such as separation of duty

l) …. ……..Mechanisms used to access resources should not be shared

m) …. ……..Security should not add much difficulty to accessing resources as if security mechanism is not present

n) …. ……..Security burden should be minimal and reasonable. Human factors critical here assuring ease of installation, configuration, and use.

---

4) Regarding the virus types, write the proper number below the type benefiting from the list below ***8 Marks***

a)	Boot sector infectors	[1] A virus that stays active in memory after application terminated
b)	Executable infectors	[2] A virus that conceals (covers) infection of files. Intercepts system calls. Example: Request for file length: return length of uninfected file
c)	Multipartite viruses	[3] A virus that can infect either boot sectors or executable. Contains a boot sector infector and executable infector
d)	Memory-resident (TSR) viruses	[4] A virus that changes its form each time it inserts itself into another program. Use different instructions with same effect. Harder than encrypted viruses
e)	Stealth viruses	[5] A virus that is enciphered except for a small deciphering routine. Uses random key; harder to detect!
f)	Encrypted viruses	[6] A virus that inserts itself into the boot sector of a disk. Executed when system boots
g)	Polymorphic viruses	[7] A virus that infects executable programs (eg .exe com)
h)	Macro viruses	[8] A virus composed of a sequence of instructions that are interpreted rather than executed directly