**Exercise 1: Indicate if the following statement is *true* or *false*.**

1. [ ] *Masquerading* attack can result in *deception* or *usurpation*.
2. [ ] *Confidentiality* goals also include hiding the existence of an entity or a piece of information.
3. [ ] In a system with discretionary access control, the owner of a file has no control over who may access the file.
4. [ ] In a mandatory access control model, a system mechanism controls access to an object and an individual user can occasionally alter that access.
5. [ ] A desirable goal of an IDS system is to reduce both *false positives* and *true positives*.
6. [ ] Confidentiality models can be used to prevent the spread of viruses.
7. [ ] *Speaker recognition* and *Speaker verification* techniques refer to *information verification* and *recognition of speaker’s* *voice characteristics verbal*, respectively.
8. [ ] If confidentiality of a system is violated, we can assume that integrity will be easily violated also; however, if integrity of that system is violated, we can still feel confident that confidentiality will be maintained.
9. [ ] The principle of least privilege states that privileges needed to carry out a critical task should not all be given out to a single person.
10. [ ] Public-private key systems work because given a public-private key pair, an attacker cannot easily compute private key even if he has access to its public key.
11. [ ] To achieve the goal of message integrity, a sender can simply send message *m* and its hash value *h*(*m*) to the received.
12. [ ] A digital certificate is used to prove that a person has a specific name.
13. [ ] A digital signature provides technical proof with regards to the origin or authenticity of a message.
14. [ ] Both the digital signature and a digital certificate can be supported by the symmetric cryptographic technique.
15. [ ] If the key size of any encryption system is 32 bits, it is practically.
16. [ ] Physically Unclonable Function technique uses unique physical characteristics of devices to identify the software.
17. [ ] A virtual private network represent securely interconnected systems and network components that use public Internet to transmit information.
18. [ ] In Bell LaPadula model a user is allowed to read-up and not allowed to write-down.
19. [ ] A user in Biba integrity model would be able to read an object that is at a higher integrity level than the user himself.
20. [ ] Assume that in a system, users’ programs run at a *high* security clearance level (in the sense of Bell LaPadula model) and the operating system programs are given *low* security classification level. If a user’s program is virus infected, then while this program runs it can easily infect the operating systems programs.

**Exercise 2. Multiple choice questions**

1. Integrity indicates to correctness and trustworthiness of something. In information security, integrity refers to
2. Data integrity
3. Origin integrity or authentication
4. Accountability
5. All of the above
6. Both (a) and (b)
7. Assume that in a given personalized EHR system, a patient can log in and change the permissions on files that contains his medical history such that his friend can now view these files. This EHR system enforces
8. Mandatory access control
9. Role based access control
10. Discretionary access control
11. Bell LaPadula model
12. CNSS 4011 is a security model that has three dimensions. The three dimensions, respectively, refer to:
13. Confidentiality, Information and Technology,
14. Confidentiality & Integrity, Policy, and Information
15. Information States, Security goals/components, Countermeasures
16. None of the above
17. Which of the following is not a secure design principle:
18. Separation of privilege
19. Economy of mechanism
20. Human acceptability
21. Security through obscurity
22. Given the message “HEAVY” and *k* = 5 what is the encrypted message using Caeser Cipher (refer to the alphabet table.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | B | C | D | E | F | G | H | I | J | K | L | M |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

1. LIEZC
2. MJFAD
3. NIEZD
4. NJFZC
5. Let PUBa and PRIa be the public and private key pair belonging to Alice. Let PUBa(M) indicate encryption of a message M with public key PUBa and PRIa(M) indicate the encryption of a message M. Which of the following is not true
6. PUBa(M) = PRIa(M)
7. PUBa(PRIa(M)) = PRIa(PUBa(M))
8. M = PRIa(PUBa(M))
9. M = PUBa(PRIa(M))
10. Alice’s public key pair is (PUBa, PRIa) and Bob’s public key pair is (PUBb, PRIb). Bob wants to send a confidential message M to Alice. Which one of the following is the correct message exchange between Alice and Bob?
11. Bob sends C= PUBb(M) and Alice computes M = PRIb(C)
12. Bob sends C= PUBa(M) and Alice computes M = PRIb(C)
13. Bob sends C= PUBa(M) and Alice computes M = PRIa(C)
14. Bob sends C= PRIa(M) and Alice computes M = PUBa(C)
15. Let’s consider Alice and Bob again as in (7). Assume that Bob wants to now send a confidential message and also ensure that its origin and message integrity is maintained. Which one of the following is the correct message exchange between Alice and Bob?
16. Bob sends C= PUBb(PUBa(M)) and Alice computes M = PRIa(PRIb(C))
17. Bob sends C= PUBa(PRIb(M)) and Alice computes M = PUBb(PRIa(C))
18. Bob sends C= PRIa(PUBb(M)) and Alice computes M = PRIb(PUBa(C))
19. Bob sends C= PUBa(PRIb(M)) and Alice computes M = PUBb(PRIa(C))
20. Which of the following represent the correct digital signature on message M sent by Alice? Assume that PUBa and PRIa are Alice’s public and private keys, and h is a hash function
21. Alice sends PUBa(M)
22. Alice sends h(M) and M
23. Alice sends PRIa(M) and M
24. None of the above
25. Given following integrity levels for subject and object, identify the statement that is false

|  |  |  |
| --- | --- | --- |
| *Integrity level* | *subject* | *object* |
| High Integrity | Samuel | File 1 |
| Medium Integrity | Tamara | File 2 |
| Low Integrity | Claire | File 3 |

1. Samuel can read File 1 and write to File 2
2. Tamara can read File 1 and File 2
3. Samuel and Tamara can write File 3
4. Claire can read and write File 2