Number of pages	**3**
Number of questions	**4**

UNIVERSITY OF SRI JAYEWARDENEPURA
Faculty of Technology

Bachelor of Information and Communications Technology Honours Degree

Third Year Second Semester End Examination

June 2023

ITC3093 Computer Security

Time allowed: Three (03) Hours **Answer ALL questions**

Read and follow the instructions given below:

- **"Index number" and course code "ITC3093"** should be written on top of each page of the answer script, and pages must be **numbered appropriately**.

Question 1 **[25 Marks]**

a) List three components of CIA triad in computer security.. [3 Marks]

b) Briefly explain the difference between stream cipher and block cipher? [5 Marks]

c) Secure Shell (SSH) can be used with a password or with a private key and public key combination. If you are requested to maintain a remote server, which model do you prefer? Justify your answer. [8 Marks]

d) While encryption ensure confidentiality, digital signature ensures authenticity protection, integrity protection and non-repudiation. Briefly explain how each of the following are achieved by using digital signature. [9 Marks]

i. Authenticity
ii. Integrity
iii. Non-repudiation

[25 Marks]

a) *List down four major characteristics of a Hash function which is securing information.* [4 Marks]

b) *Discuss the security challenges of using pirated operating systems in terms of computer security?* [5 Marks]

c) *Briefly explain the role of a Certificate Authority (CA) in securing information.* [8 Marks]

d) [8 Marks]

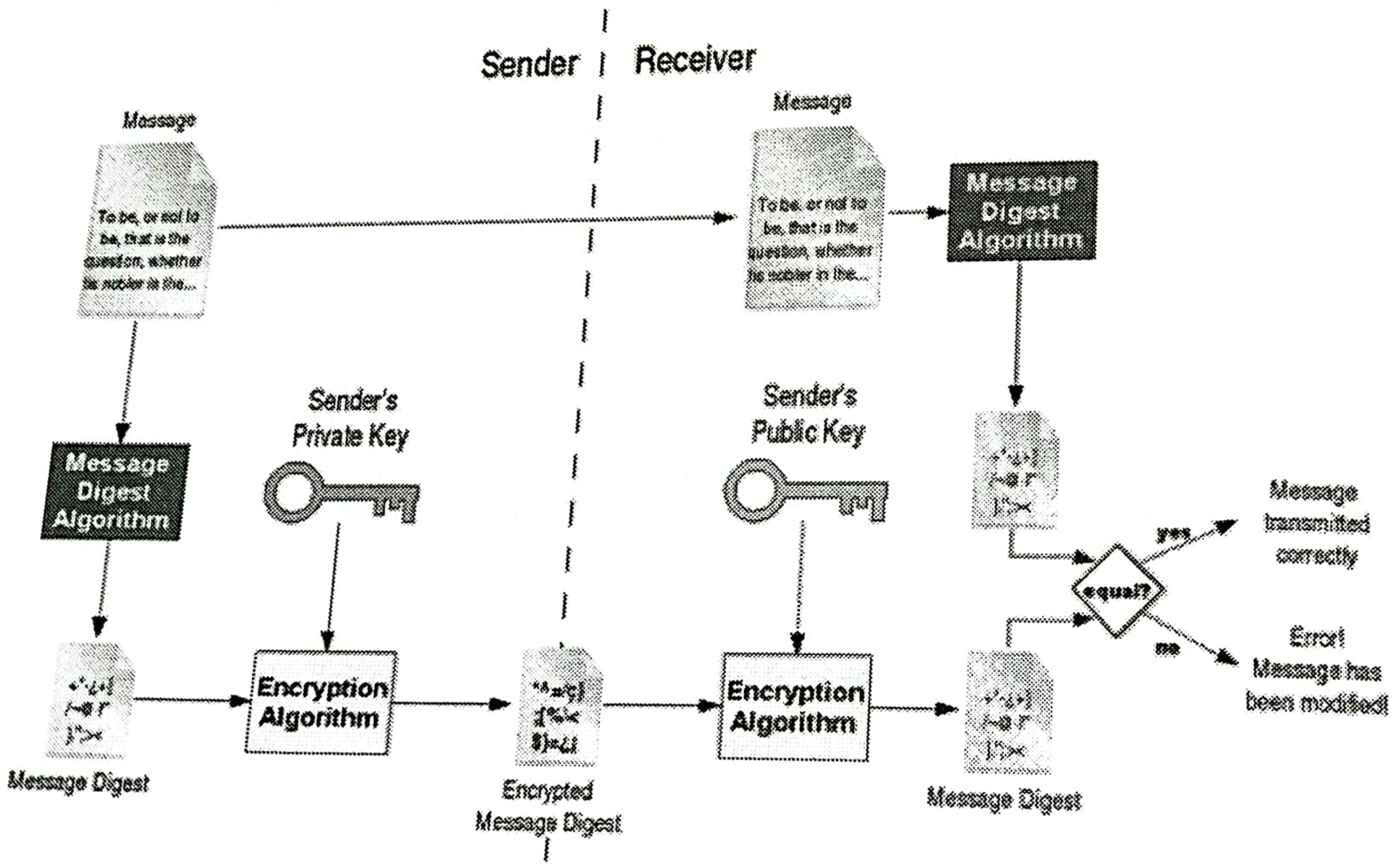


Diagram 01

The diagram (diagram 01) above explains the cryptographical process of digital signature. Answer the question below based on the above process

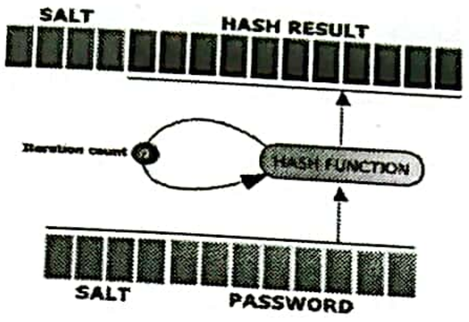
i. Can we use receiver's public key for the encryption process at sender's end and receiver's private key for the decryption at the receiver's end? Justify your answer.

ii. Propose a modification for the above process to ensure confidentiality of the message.

Question 3

[25 Marks]

a) Briefly explain the man in the middle (MIM) attack. [3 Marks]

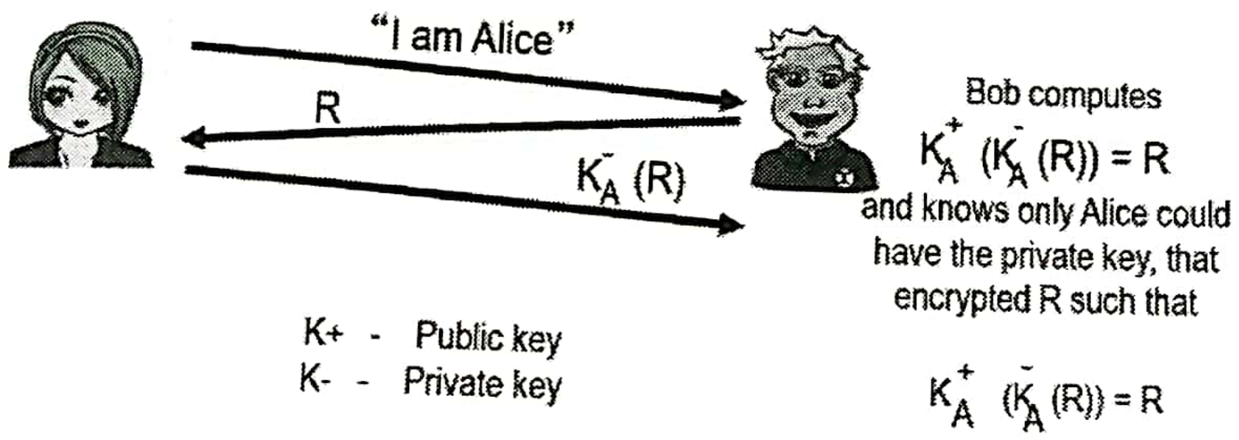
b) 

[6 Marks]

The image above depicts the process of adding SALT to the passwords. Compare and contrast the password saving process with SALT and without SALT.

c) i. Compare and contrast the private key encryption and public key encryption. [8 Marks]

ii. Propose a reason to use private key encryption over public key encryption.

d) 

[8 Marks]

Questions below are based on the challenge response authentication process depicted in above figure.

i. What is *R* in above process?

ii. Thought *R* can be read by anybody with the public key of Alice, this process is working well for authentication. Do you agree with this statement? Justify your answer.

Question 4 **[25 Marks]**

a) Compare and contrast Worms and Trojan malware types. [4 Marks]

b) Briefly explain the process of a dictionary attack. [5 Marks]

c) Some encryption algorithms are theoretically breakable but practically unbreakable. Do you agree with this statement? Justify your answer with an example. [8 Marks]

d) Using the Vigenere cipher, encrypt the text "*ALL IS WELL*" using the keyword "*USJP*". [8 Marks]

**** End of the Paper****