Name: _____ **İTÜ ID:** _____ **Signature:** _____.

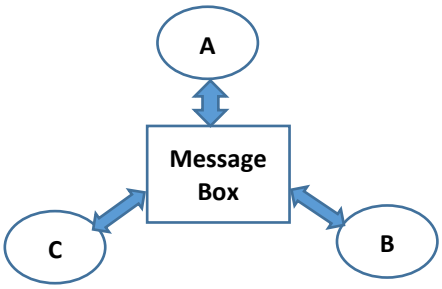
BLG 459E Computer Security, Final Exam
Fall 2020, Duration: 60 minutes

Instructions:

- *Do NOT communicate with other people, including your friends, classmates, and family members!*
- *This is an open-book exam.*
- *Give your answers in English.*
- *Write the question number, your Name and İTÜ ID on the top of each page and **sign all pages**. You will **not** receive any point from pages that do not contain all of this information!*
- *Scan or take photo of your answers and upload them on Ninova **before the deadline**! Answers sent via **email** will **not be accepted**!*
- *You will have 15 minutes to upload your answers on Ninova.*
- ***Accepted file formats** for your answers are *.pdf, *.jpeg, or *.png!*

Q-1	Q-2	Q-3	Total
/10	/10	/10	/30

Q-1. (10 pts) Message Box



Assume that there are three entities, A, B, and C in the environment that can communicate via Message Box as shown in the figure. When Message Box receives a message, it transmits the message to all entities excluding the sender. For example, assume that A sends a message to B. Message Box firstly receives the message and then sends it to B and C. The communication between two entities is confidential and cryptographic solutions are used to provide that confidentiality.

Assume that:

- *All cryptographic keys are distributed.*
- *There is no intruder in the system.*
- *Use the following notation to solve the problems:*
  - *PUx: Public Key of entity X,*
  - *PRx: Private Key of entity X,*
  - *Sxy: Secret key of between entities X and Y.*

a) (5 pts) Assume that A, B, and C use public-key cryptography. How many different keys does A contain to communicate with B and C? Explain briefly.

b) (5 pts) Assume that there are M entities who communicate with each other by using Message Box and symmetric key cryptography. How many different keys does the environment contain? Compute the number of keys for M=87.

Name: _____ **İTÜ ID:** _____ **Signature:** _____ .

Use the following text to solve Q-2 and Q-3

Assume that you have an **advanced malware (ADMAL)** that contains a **botnet**, a **worm**, and a **ransomware**. Botnet is a collection of bots that act in a coordinated manner. A bot is controlled via a botmaster by using Command-Control (CC) facilities. Assume that ADMAL implanted bots to computers of all instructors at İTÜ. The goal of ADMAL is to request 2021 Bitcoins as a ransom from the instructor of BLG459E to prevent him preparing a new final exam by occupying his time to collect the requested amount. The botnet of ADMAL implants either the worm or the ransomware on computers of İTÜ network according to the following conditions:

- **Implant the worm** if the owner of the computer is **other than the instructor of BLG459E**. The worm prints message "YOU ARE INFECTED" to the screen of the infected computer and removes itself from that computer.
- **Implant the ransomware** if the owner of the computer is the **instructor of BLG459E**. The ransomware encrypts all doc files (*.doc) with public key *PBransome* and it requests 2021 Bitcoins by printing message "SEND 2021 Bitcoins to HACKINSTUCTORS address until 30.02.2021". Then, the ransomware waits to receive private key *PRransome* until 30.02.2021. If the ransomware receives the private key, which means the instructor already sent 2021 Bitcoins to the address, then it decrypts the encrypted files, prints message "THANKS", and removes itself from the computer. Otherwise, the ransomware prints "FORGET YOUR FILES!" on the screen and removes itself from the computer.

Q-2) (10 pts) Write a pseudo code for the payload of *Worm* within a method (function/procedure).

Q-3) (10 pts) Write a pseudo code for *Ransomware*.