Notes from Exploring Network Security

Instructions

Make a copy of this document, rename it to “exploring-network-security-notes” and move it to your CSE 523 Google Docs collection. If at any point in this exercise you feel stuck, raise your hand and get some guidance. When you reach each GATE below, switch over to the Tracking Progress document and update your position. Try to be efficient with your time.

Overview

Today we will explore how to use encryption….

Referring to the slides from the Lecture: L08 Network Security - Revisited fill in the answers to the following questions concerning RSA:

---

1. How do we calculate ‘n’?
    a.
2. How do we choose ‘e’?
    a.
3. How do we choose ‘d’?
    a.
4. What are K_+ and K_- and what values are used for each of them?
    a.
5. How are K_+ and K_- used?
    a.

GATE 1

RSA Key pair #1

Consider this possible RSA key pair. Ignoring the fact that the values are too small, explain whether this is a valid RSA key pair or not.
(Hint: The prime numbers < 20 are: 2, 3, 5, 7, 11, 13, 17, 19).

K_+=(31,5) K_-=(31,11)

Record your reasons here:

GATE 2

RSA Key pair #2

Consider this possible RSA key pair. Ignoring the fact that the values are too small, explain whether this is a valid RSA key pair or not.
(Hint: The prime numbers < 20 are: 2, 3, 5, 7, 11, 13, 17, 19).

K_+=(91,11) K_-=(91,59)

Record your reasons here:

GATE 3

Using a valid key pair from above, what are the values of p, q, n, e and d?

GATE 4

Using the pair you selected, what would be your starting equation for encrypting a message m, where m=10?

GATE 5

From your last answer, solve for c using the properties of modulo arithmetic. Show your work!!

GATE 6

Using the pair you selected, what would be your starting equation for decrypting a message c, where c=23? Using a calculator like wolframalpha.com or bc on Linux or MacOS solve for m.

COMPLETE