CSS322 – Quiz 4

Name: _____ ID: _____ Marks: _____ (10)

Question 1 [5 marks]

(a) Generate your own RSA keys using two primes, $p = 19$ and $q = 13$. Use $e = 5$. Show your calculations and write your answers in the space provided. [3 marks]

$n =$ _____, $d =$ _____

(b) What are the values that are made public? [1 mark]

(c) What three values must be kept secret? [1 mark]

Question 2 [2 marks]

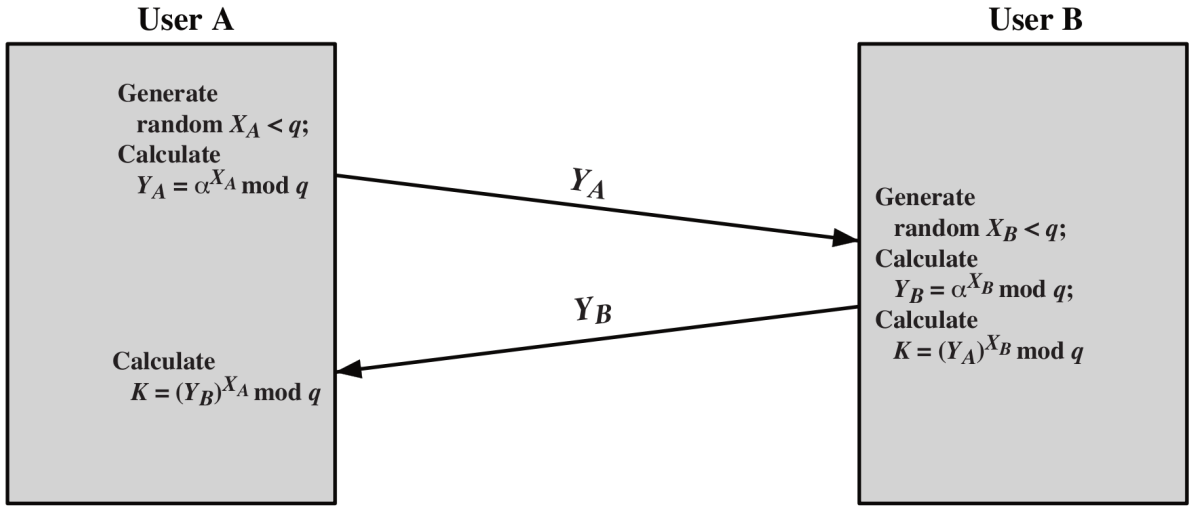
There are 3 users in a public-key cryptosystem: *Mirong*, *Chawanan* and *Nichanan*. Assume all relevant keys have been generated and distributed.

(a) Nichanan sent a message to Mirong. The message was encrypted so that the recipient is certain the message came from Nichanan. Can Chawanan read the message? If so, what key do they use to decrypt? If not, why not? [1 mark]

(b) An attacker, Nattapong, intercepts a confidential message sent by Nichanan to Mirong. What key does Nattapong need to discover in order to read the message? [1 mark]

Question 3 [3 marks]

The Diffie-Hellman Key Exchange algorithm is illustrated below. Recall that both α and q are public values.



(a) What values does an attacker know? [1 mark]

(b) What is the objective of the attacker? (i.e. what value(s) do they eventually want to find?) [1 mark]

(c) Explain why, when large values are used, it is computationally infeasible for the attacker to achieve their objective? [1 mark]