CSS322 – Quiz 8

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

Question 1 [2 marks]

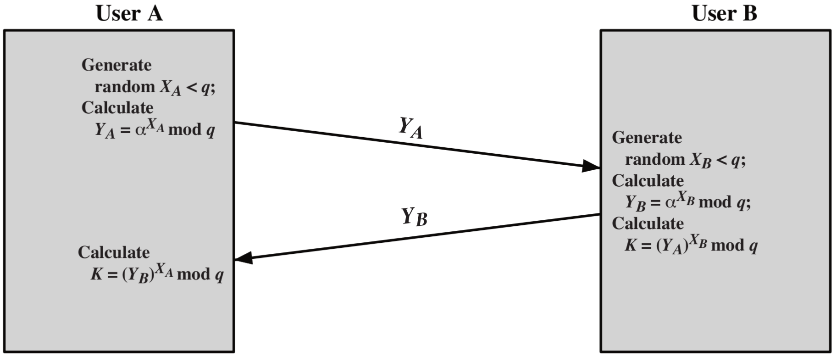
There are 3 users in a public-key cryptosystem: *Jakarin*, *Chakrit* and *Thanyathorn*. Assume all relevant keys have been generated and distributed.

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

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

Question 2 [3 marks]

The Diffie-Hellman Key Exchange algorithm is illustrated below.


User A
User B
Generate random $X_A < q$;
Calculate $Y_A = \alpha^{X_A} \bmod q$
Y_A
Generate random $X_B < q$;
Calculate $Y_B = \alpha^{X_B} \bmod q$;
Calculate $K = (Y_A)^{X_B} \bmod q$
Y_B
Calculate $K = (Y_B)^{X_A} \bmod q$

(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]

Question 3 [5 marks]

In this question you must show your calculations (or explain how you arrived at the answer). No calculations means no marks.

A message has been encrypted with one key from a RSA key pair. The key used is (3,55) and the resulting ciphertext is 13.

(a) What is the value of the other key in the RSA key pair? [3 marks]

(b) What is the value of the message? [2 marks] (Hint: There may be different approaches to solve this. One approach may take advantage of a property of modular arithmetic: if $z = x \times y$ then $a^z \bmod n = [(a^x \bmod n)(a^y \bmod n)] \bmod n$).