CSS322 – Quiz 4

Security and Cryptography, Semester 2, 2010

Prepared by Steven Gordon on 13 January 2011
CSS322Y10S2Q04, Steve/Courses/CSS322/Assessment/Quiz4.tex, r1624

Question 1 [5 marks]

(a) Generate your own RSA keys using two primes, $p =$ [13 | 11 | 13 | 19] and $q =$ [17 | 23 | 23 | 13]. Use $e =$ [5 | 3 | 5 | 5]. Show your calculations and write your answers in the space provided. [3 marks]

$n =$ _____, $d =$ _____

Answer. *First calculate n:*

$$n = p \times q$$

Then calculate $\phi(n)$:

$$\phi(n) = (p-1)(q-1)$$

since we know e, we calculate d, its multiplicative inverse in mod $\phi(n)$:

$$e \times d \equiv 1 \pmod{\phi(n)}$$

Now find an e that is relatively prime with $\phi(n)$. The answers are $(n, \phi(n), d)$: $(221, 192, 77), (253, 220, 147), (299, 264, 53), (247, 216, 173)$

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

Answer. *e and d*

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

Answer. *p, q and d. $\phi(n)$ should also be kept secret.*

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

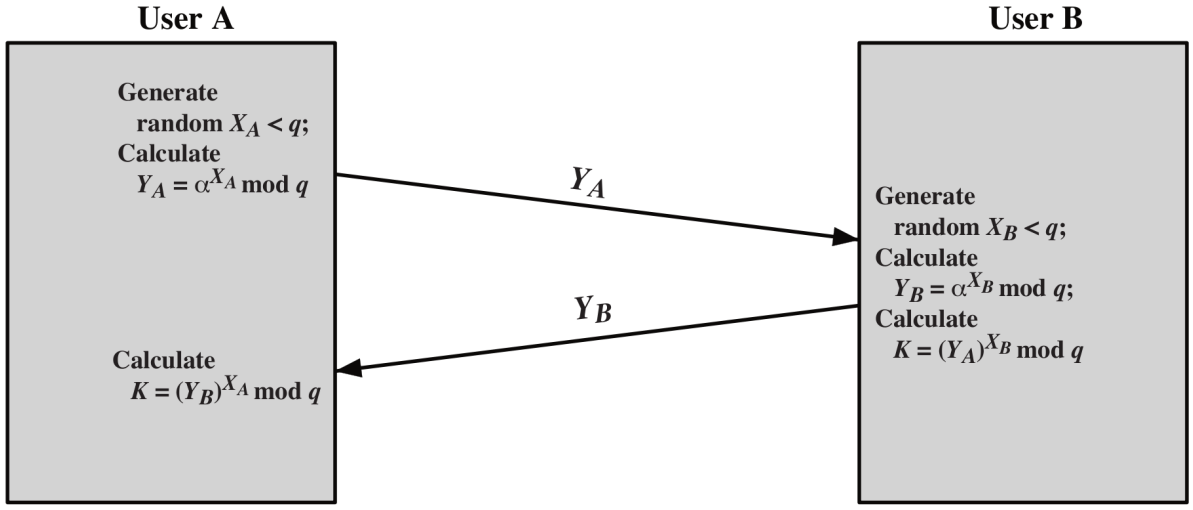
Answer. *Yes. The message is encrypted with the senders private key. Everyone has the corresponding public key (the public key of the sender) and can decrypt, seeing the message. This operation provides authentication, not confidentiality.*

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

Answer. *A confidential message is encrypted with the recipients public key and decrypted with the recipients private key. Therefore the attacker must discover the private key of the recipient.*

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]

Answer. *The public values are: α, q, Y_A and Y_B.*

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

Answer. *To find the secret K*

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

Answer. *To find the secret K, they must either perform a brute force attack to find X_A or X_B, or solve* $\mathrm{dlog}_{\alpha,q}(Y)$. *Discrete logs are computationally infeasible to solve.*