CSS322 – Quiz 8

Security and Cryptography, Semester 2, 2012

Prepared by Steven Gordon on 25 November 2012
CSS322Y12S2Q08, Steve/Courses/2012/s2/css322/assessment/quiz1.tex, r2575

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

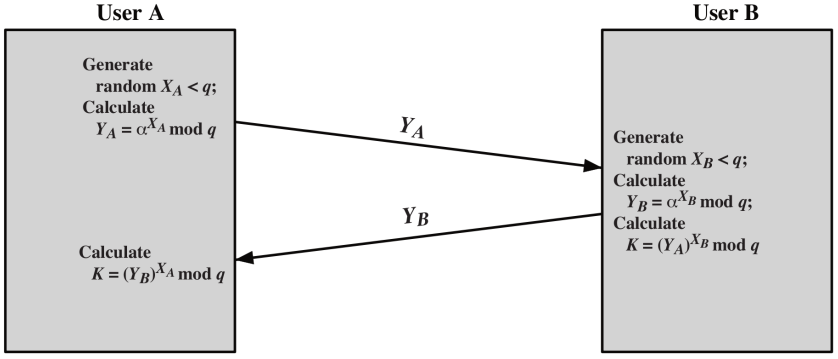
Answer. *Yes. The message is encrypted with the senders private key. Everyone has the corresponding public key (the public key of the sender) and can decrypt, seeing the message. This operation provides authentication, not confidentiality.*

(b) An attacker, Naphat, intercepts a confidential message sent by [Thanyathorn | Jakarin | Chakrit | Thanyathorn] to [Chakrit | Chakrit | Thanyathorn | Jakarin]. What key does Naphat 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 2 [3 marks]

The Diffie-Hellman Key Exchange algorithm is illustrated below.



(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* $\text{dlog}_{\alpha,q}(Y)$. *Discrete logs are computationally infeasible to solve.*

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) | (7,55) | (7,77) | (5,65)] and the resulting ciphertext is [13 | 5 | 5 | 9].

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

Answer. *Assuming the key given is (e,n), we need to find (d,n) where d is a multiplicative inverse of e in mod $\phi(n)$. Hence the first step is to find $\phi(n)$ by factoring n into its two prime factors, p and q:*

- $n = 55$, $p = 5$, $q = 11$
- $n = 77$, $p = 7$, $q = 11$
- $n = 65$, $p = 5$, $q = 13$

Now $\phi(n)$ can be calculated as $\phi(n) = (p-1) \times (q-1)$:

- $\phi(55) = 40$
- $\phi(77) = 60$
- $\phi(65) = 48$

Now we must try to find a d that satisfies the equation: $ed \bmod \phi(n) = 1$:

- $e = 3$, $n = 55$, $d = 27$
- $e = 7$, $n = 55$, $d = 23$
- $e = 7$, $n = 60$, $d = 43$
- $e = 5$, $n = 48$, $d = 29$

So the answer is the value of (d,n).

(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 $z = x + y$ then $a^z \bmod n = [(a^x \bmod n)(a^y \bmod n)] \bmod n$).

Answer. *The ciphertext is obtained by:* $C = M^e \bmod n$. *The message can be obtained by calculating* $M = C^d \bmod n$. *Since* C, d *and* n *are known, its just a matter of performing the calculation. But how to solve this without a computer (since a calculator may not have the precision to calculate* $C^d \bmod n$*)? Using the above mentioned property, and the first values as an example:*

$$\begin{aligned}
M &= C^d \bmod n \\
&= 13^{27} \bmod 55 \\
&= 13^{2\times 13+1} \bmod 55 \\
&= [(13^2 \bmod 55)^{13} \times (13^1 \bmod 55)] \bmod 55 \\
&= [(169 \bmod 55)^{13} \times 13] \bmod 55 \\
&= [4^{13} \times 13] \bmod 55 \\
&= [(4^3)^4 \times 4^1 \times 13] \bmod 55 \\
&= [(64 \bmod 55)^4 \times 52] \bmod 55 \\
&= [9^4 \times 52] \bmod 55 \\
&= [(81 \bmod 55) \times (81 \bmod 55) \times 52] \bmod 55 \\
&= [26 \times 26 \times 52] \bmod 55 \\
&= [(676 \bmod 55) \times 52] \bmod 55 \\
&= [16 \times 52] \bmod 55 \\
&= [832] \bmod 55 \\
&= 7
\end{aligned}$$

This example shows it is possible to simplify the calculation of $C^d \bmod n$, *and in this case even calculate on paper (although it is time consuming). For information,* $13^{27} = 1192533292512492016559195008117$.

The answers are:

- $e = 3$, $n = 55$, $d = 27$, $C = 13$, $M = 7$
- $e = 7$, $n = 55$, $d = 23$, $C = 5$, $M = 15$
- $e = 7$, $n = 60$, $d = 43$, $C = 5$, $M = 26$
- $e = 5$, $n = 48$, $d = 29$, $C = 9$, $M = 29$