Security

Assignment 10, Friday, November 25, 2016

Handing in your answers: For the full story, see

`http://www.sos.cs.ru.nl/applications/courses/security2016/exercises.html`

To summarize:

- Include your name and student number **in** the document (they will be printed!), as well as the name of your teaching assistant (Hans or Joost). When working together, include **both** your names and student numbers.
- Submit one single **pdf** file – when working together, only hand in **once**.
- Hand in via Blackboard, before the deadline.

Deadline: Monday, December 5, 09:00 sharp!

Goals: After completing these exercises successfully you should be able to

- efficiently compute modular exponentiations;
- use modular exponentiation to perform inversions;
- perform RSA computations

Marks: You can score a total of 100 points.

1. **(25 points)** Euler totient function ϕ.

   (a) What are the elements of $\mathbb{Z}_{21}^*$? And thus: what is $\phi(21)$

   (b) What is $\phi(127)$?

   (c) What is $\phi(125)$?

   (d) What is $\phi(1651)$?

   Where relevant, explain your answers / calculations.

2. **(25 points)** In this exercise, we will be computing big modular exponentiations by hand. You can use a calculator if you must, but make sure it's a simple one: you will not be allowed a 'graphical calculator' (or a smartphone/laptop/smartwatch) at the exam, either.

   (a) Compute $7^{1202} \mod 41$ using the square-and-multiply method.

   (b) Compute $9^{1202} \mod 23$, making use of Euler's theorem ($x^{\phi(n)} \equiv 1 \mod n$) to first reduce the problem to a much smaller exponent.

   (c) Use modular exponentiation to find the inverse of $2 \mod 13$.

3. **(50 points)** We take $n = p \cdot q$ with $p = 19$ and $q = 13$. Furthermore, we use $e = 7$. A calculator is allowed, but do show your computations. As opposed to the previous exercise, you can do exponentiations in one step.

   (a) What is $\phi(n)$?

   (b) Calculate d.

   (c) Alice wants to transfer €20 to Eve. Alice therefore sends this amount to the bank, encrypted with RSA, using the parameters above. Calculate the encryption for $m = 20$.

   (d) Show how the bank decrypts this message.

. . . . **The assignment continues on the next page!** . . . .

(e) Later, Alice wants to transfer €10 to Eve. The encrypted message Alice sends to the bank is 205. Eve intercepts the message and sends a different message instead. What message can she send, in order to be sure that she receives more money? Without using the private key, what is the amount she will receive? (*Hint:* Even though it may be appealing: do not simply try all options. Make use of the two messages and ciphertexts Alice sent).

(f) Using the parameters from the start of this exercise[1], what is the signature for $m = 2$?

[1] Note: in practice, one should never use the same keys to sign message and to encrypt/decrypt – for the sake of simplicity, we briefly ignore this for this exercise.