Security
Assignment 10, Monday, November 28, 2011

Handing in your answers: There are two options:

1. Put your solutions in Pim's post box (in the white cabinet, lower door, near the printer at the station-side-end of the corridor on the second floor of the Huygens building). Before handing in, make sure:
   - your names and student numbers are written on the document.
2. Send your solutions by e-mail to `pim@cs.ru.nl` with subject '*assignment 10*'. This e-mail should only contain a single PDF document as attachment. Before handing in, make sure:
   - your names and student numbers are included in the document (since it will be printed),
   - your names are part of the filename (example: PimVullers_FlavioGarcia-10.pdf), and
   - the file is a PDF document.

Deadline: Monday, December 5, 8:30 sharp!

Note: Do not forget to perform the modulo operations.

1. **(4 points)** Diffie-Hellman key exchange, see Wikipedia[1], is used to agree on a secret key between Alice and Bob. The following messages are exchanged:

   $$\begin{array}{lll} 1. & A \longrightarrow B & : \quad n = 719, g = 3, g^{s_A} = 191 \\ 2. & B \longrightarrow A & : \quad g^{s_B} = 543 \end{array}$$

   (a) Given Alice's secret $s_A = 16$, compute the shared secret key.

   (b) Derive Bob's secret from the exchanged messages. You have two options:

   i. Using a script/program. Give the source code, and explain what it does.

   ii. Do it by hand[2]. Explain how you did it.

   Remark: The numbers i producing $g^i \mod 719$ form a group of $359 = \frac{(719-1)}{2}$ elements; hence brute forcing requires at most 359 tries. Good luck!

   (c) Check that with this private key from (b) Bob has the same (shared) key as Alice (by doing the DH-computation for Bob's side)

2. **(6 points)** Consider the ElGamal cryptosystem, see Wikipedia[3]. Suppose $G = \mathbb{Z}_p^*$ for $p = 29$, with generator $g = 3$ and secret number $n = 17$.

   Reminder: All calculations are performed within the group G, that is modulo p.

   (a) Determine the corresponding h.

   (b) Give the public key in terms of G, g, n and h.

   (c) Give the private key in terms of G, g, n and h.

   (d) We are going to encrypt the message "banana" (in ECB mode) using ElGamal. We already applied the mapping used in assignment 8 and copied it into Table 1. For the following steps, fill out the according row in Table 1 and give intermediate steps:

   i. For each integer block calculate a separate session key $s = h^r$. Use for r the following values consequently: $3, 6, 9, 12, 15$ and 18.

[1] `http://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange`

[2] You can use a calculator on your PC (like `bc` for linux), or the Magma Calculator (`http://magma.maths.usyd.edu.au/calc/`, syntax: `x^y mod z`), to help you with the calculations.

[3] `http://en.wikipedia.org/wiki/ElGamal_encryption`

ii. For each integer block calculate the first component $c_1 = g^r$ of the ciphertext using that same sequence.

iii. Finally, for each integer block calculate the second component $c_2 = m \cdot s$ of the ciphertext.

(e) Lets now decrypt the ciphertext. Complete Table 1 and give the intermediate steps.

i. For each integer block calculate the inverse session key $s^{-1} = {c_1}^{-n}$, where ${c_1}^{-n}$ can be calculated by ${c_1}^{p-1-n}$.

ii. For each integer block use the inverse s^{-1} to cancel out s in c_2 and thus retrieve $m = c_2 \cdot s^{-1}$.

	b	**a**	**n**	**a**	**n**	**a**
Mapping	2	1	14	1	14	1
r	3	6	9	12	15	18
$s = h^r$	.	.	.	.	.	.
$c_1 = g^r$	.	.	.	.	.	.
$c_2 = m \cdot s$	.	.	.	.	.	.
$s^{-1} = {c_1}^{-n}$	.	.	.	.	.	.
$m = c_2 \cdot s^{-1}$	.	.	.	.	.	.

Table 1: Computation steps ElGamal