Security

Assignment 2, Monday, September 19, 2011

Important changes:

1. Working in *pairs* is now **mandatory** instead of optional.
2. The *deadline* is now **8:30**. So you must hand in your solutions before the lecture!

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 2*'. 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: PVullers_FGarcia_assignment-2.pdf), and
   - the file is a PDF document.

Deadline: Monday, September 26, 8:30 sharp!

Note: These tasks require that you study the material on substitution[1] and transposition[2] ciphers as well as the material on linear feedback shift registers[3].

1. **(1 point)** In mono-alphabetic substitution of the Latin alphabet (no digits, just 26 letters), how large is the key space?

   A. 26
   B. 26^2
   C. 2^{26}
   D. 26!
   E. 26^{26}

2. **(4 points)** Break the following transposition cipher. In a transposition cipher the characters are not changed but their position is permuted, e.g. the letter 'a' remains an 'a', only its position within the message changes.

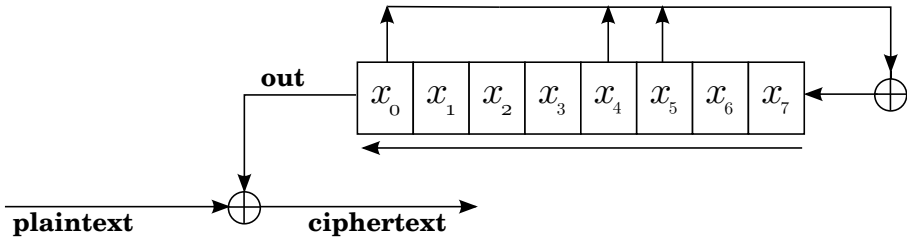
   > 'htsy nies ridd teun etei hpyt ryre lnon ewop elni onio wvrm roft tlts mgan iege rpcn teur auah pyex teer owvr fdrn aror ayno aroe eoyt ltvt'

   The plain text consists of letters only (no spaces), but is displayed here in groups of four for readability. [Note: the plain text is about **encryption**, so the word 'encryption' is likely to occur.]

   Explain briefly how you did it. [Note: 'I used a computer' is not accepted as an explanation.]

[1] `http://en.wikipedia.org/wiki/Substitution_cipher`
[2] `http://en.wikipedia.org/wiki/Transposition_cipher`
[3] `http://en.wikipedia.org/wiki/LFSR`

3. **(5 points)** Consider the following simple Linear Feedback Shift Register (LFSR). The plaintext is bitwise XOR-ed with the output bits of the LFSR which **first computes** $x_0 \oplus x_4 \oplus x_5$ and **then shifts** such that x_0 falls out.



Example:

The state	**0**	1	1	0	**1**	**1**	0	1
is followed by	**1**	1	0	1	**1**	**0**	1	0
and outputs	**0**							

(a) Describe the next five states of the state in the above example box. The first successor state is already given as illustration, so you have to give the four subsequent ones.

(b) Also do "rollback" and compute the *previous* 4 states, starting from the above example state.

(c) Assume you know the cipher is in this example state, and you intercept 1111 as resulting ciphertext. Reconstruct the 4 bits of plaintext that produces this ciphertext 1111.