Security
Assignment 4, Monday, October 3, 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 4*'. 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-4.pdf), and
   - the file is a PDF document.

Deadline: Monday, October 10, 8:30 sharp!

Note: These tasks require that you study the material on linear feedback shift registers[1] as well as the block cipher modes of operation[2].

1. **(2 points)** Which of the following authentication protocols are vulnerable to a replay attack? If so, write down the attack, using the $A \longrightarrow B : message$ notation. If not, explain why the replay attack fails. R_A and R_B are fresh random nonces, and K_{AB} is a shared secret key.

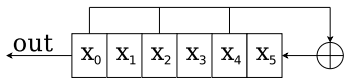
   (a)
   1. $A \longrightarrow B \;:\; hello$
   2. $B \longrightarrow A \;:\; B, K_{AB}\{B\}$
   3. $A \longrightarrow B \;:\; A, K_{AB}\{A\}$

   (b)
   1. $A \longrightarrow B \;:\; A, R_A$
   2. $B \longrightarrow A \;:\; B, R_B, K_{AB}\{R_A + 2\}$
   3. $A \longrightarrow B \;:\; A, B, R_A, R_B, K_{AB}\{R_B + 2\}$

   (c)
   1. $A \longrightarrow B \;:\; A, R_A$
   2. $B \longrightarrow A \;:\; B, R_B, K_{AB}\{B, R_A\}$
   3. $A \longrightarrow B \;:\; K_{AB}\{A, B, R_B\}$

   (d)
   1. $A \longrightarrow B \;:\; A, R_A, K_{AB}\{A, R_A\}$
   2. $B \longrightarrow A \;:\; B, R_B, K_{AB}\{B, R_B\}$
   3. $A \longrightarrow B \;:\; K_{AB}\{A, B, R_A\}$

2. **(2 points)** Consider the following Linear Feedback Shift Register (LFSR):

   First, this LFSR is initialized to some binary state like $\langle 1, 1, 1, 0, 1, 1 \rangle$. Then, every shift the state changes as follows: All the bits shift one position to the left. The leftmost bit (x_0) drops out and is the output bit of the LFSR. The rightmost bit (x_5) becomes the XOR-ed outcome of the bits located at the LFSR taps. So, $x_5 = x_0 \oplus x_2 \oplus x_4$.

[1] `http://en.wikipedia.org/wiki/LFSR`
[2] `http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation`

(a) Determine the number of different states that can be reached when we start with the following initial states (also list all the different states):

i. $\langle 1, 1, 1, 1, 1, 1 \rangle$

ii. $\langle 1, 0, 1, 0, 0, 1 \rangle$

iii. $\langle 1, 0, 1, 0, 1, 0 \rangle$

(b) If we start with $\langle 0, 0, 1, 0, 0, 1 \rangle$ as initial state, will the LFSR state ever become $\langle 0, 0, 1, 0, 0, 1 \rangle$ again? Explain what happens (for example by using a graph).

3. **(6 points)** Consider the following substitution cipher:

Plaintext	**Ciphertext**
000	110
001	100
010	011
011	111
100	010
101	000
110	101
111	001

So, for instance, encrypt(001) = 100 and decrypt(101) = 110. Compute the cipher text belonging to plain text 101 110 101 001 (using a block size of 3 bits) for the following different modes.

(a) In Electronic Code Book (ECB) mode.

(b) In Cipher Block Chaining (CBC) mode where the Initialization Vector (IV) is 110. Show intermediate steps.

(c) In Output Feedback (OFB) mode where the IV is 001. Show intermediate steps.

(d) In Cipher Feedback (CFB) mode where the IV is 100. Show intermediate steps.

(e) Explain briefly why the CBC mode is preferred over the ECB mode.

(f) Characterize the difference between Output Feedback (OFB) mode and Cipher Feedback (CFB) mode in one sentence.