Security

Assignment 11, Wednesday 10 December, 2008

Goals: After successfully completing this exercise you should have a working grasp of the block cipher modes and recapitulate your knowledge about traffic pricing.

Deadline: Friday December 19 or earlier. You have to send your answers to **Olha**, by e-mail or to the post-box. **Attention: Flavio is leaving on vacations on 11/12. He will not be reachable by e-mail or any other way.**

1. (8 points) Consider the substitution cipher below:

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

So, for instance, $E(001) = 100$ and $D(010) = 000$. Compute the cipher text belonging to plain text 011 101 110 000. (so block size is 3 bits)

   (a) in Electronic code book mode.

   (b) in Cipher block chaining, with initial vector 010. Show intermediate steps.

   (c) in Cipher feedback mode, with initial vector 101. Show intermediate steps .

   (d) Argue why in practice options (1b) and (1c) are preferred over option (1a).

   You may need 8.2.3 of Tanenbaum to prepare this task.

2. (2 points) Let the hash of the day to be sent to a traffic Pricing Authority (PA) have the form

$$\mathsf{hash}_{\mathsf{day}} = h\Big(h(\mathsf{TP}_{\mathsf{day},1})|| \ldots ||h(\mathsf{TP}_{\mathsf{day},1440})\Big)$$

   where h is a hash-function, $\mathsf{TP}_{\mathsf{day},i}$ is the Trajectory Part on the day number "day" on the minute i, and $||$ denotes concatenation of hashes. Recall that 1440 is the total amount of minutes in a day.

   Suppose that PA already knows that your car was at location ℓ between 9 : 42 and 9 : 43 on April the 1st, 2008 (i.e. min 583 of the day 92; remember, that in 2008 there are 29 days in February). You have already sent hash_{92}. What else does the PA need to receive from you in order to verify that the observation at location ℓ matches hash_{92}?

   You may need Bart's paper "Privacy-friendly Electronic Traffic Pricing via Commits" to prepare this task.