Student Seminar: Security Protocols and Applications
Final Exam Part 1/2

Philippe Oechslin and Serge Vaudenay

28.6.2011

- duration: 3h00
- no document allowed
- a pocket calculator is allowed
- communication devices are not allowed
- answers to every exercise must be provided on separate sheets
- readability and style of writing will be part of the grade
- it is unlikely we will answer any technical question during the exam
- do not forget to put your full name on your copy!

Family Name: . . . .

Given Name: . . . .

Section: . . . .

I XTS Encryption Mode

We denote by Enc and Dec the encryption and decryption algorithms of a block cipher. Throughout this exercise, a plaintext block which is supposed to be written at index j of a sector i in a memory unit is denoted by $x_{i,j}$. Its ciphertext (the value which is actually stored at this place) is denoted by $y_{i,j}$. To encrypt a data block $x_{i,j}$ with key (K_1, K_2), we compute

$$y_{i,j} = \mathsf{Enc}_{K_1}(x_{i,j} \oplus t_{i,j}) \oplus t_{i,j} \quad \text{where} \quad t_{i,j} = \alpha^j \times \mathsf{Enc}_{K_2}(i)$$

where α is a constant and $\alpha^j \times u$ denotes standard GF operations. Since there may be some incomplete block, we use ciphertext stealing to encrypt the last two blocks: if $x_{i,j-1}$ and $x_{i,j}$ are two consecutive blocks, $x_{i,j-1}$ being of complete length and $x_{i,j}$ having a reduced length, we store $y_{i,j-1}$ and $y_{i,j}$ respectively, obtained by

$$y_{i,j} \| u = \mathsf{Enc}_{K_1}(x_{i,j-1} \oplus t_{i,j-1}) \oplus t_{i,j-1} \quad \text{and} \quad y_{i,j-1} = \mathsf{Enc}_{K_1}((x_{i,j} \| u) \oplus t_{i,j}) \oplus t_{i,j}$$

where $y_{i,j} \| u$ is splitted so that $y_{i,j}$ has the same length as $x_{i,j}$.

Q.1 Explain how to decrypt the last two ciphertext blocks $y_{i,j-1}$ and $y_{i,j}$ of a sector when $y_{i,j}$ is incomplete.

Q.2 Assume that within the same sector i, there are two different indices j and j' such that $x_{i,j} \oplus t_{i,j} = x_{i,j'} \oplus t_{i,j'}$. Show that $x_{i,j} \oplus y_{i,j} = x_{i,j'} \oplus y_{i,j'}$.

Q.3 Again, assume that within the same sector i, there are two different indices j and j' such that $x_{i,j} \oplus t_{i,j} = x_{i,j'} \oplus t_{i,j'}$. Given i, j, j', j'', $y_{i,j}$, $y_{i,j'}$, show that we can compute $t_{i,j''}$ for any j''.

Q.4 Given a sector i and a block index j where a ciphertext block $y_{i,j}$ corresponding to a plaintext block $x_{i,j}$ is stored, assume that $t_{i,j}$ is known (e.g. due to the previous attack). Show that an adversary can corrupt one block j'' of sector i so that it would decrypt to something satisfying

$$x_{i,j''} = x_{i,j} \oplus \Delta$$

for a large set of Δ's. More precisely, show that from $t_{i,j}$, $y_{i,j}$, and Δ, an adversary can (for many Δ's but not all of them) find j'' and $y_{i,j''}$ so that storing $y_{i,j''}$ at position (i, j'') will decrypt to a block satisfying the above relation.

Q.5 What would you propose to thwart the previous attack without changing the encryption mode?

Q.6 We are encrypting random blocks. We assume that each sector is encrypted with a single key (which is not necessarily the same from one sector to the other). Given the memory capacity M (in bits) of a hard disk, the number ℓ of blocks per sector, and the bitlength n of a block, what is the probability p that there is a sector i with two different indices j and j' such that $x_{i,j} \oplus t_{i,j} = x_{i,j'} \oplus t_{i,j'}$?

Application: $M = 2^{43}$bits, $n = 128$ and $\ell = 256$.

Hint: let E be the average number of pairs $(i, \{j, j'\})$ (composed with a sector index i and an unordered pair $\{j, j'\}$ of block indices within the sector) for which the equation $x_{i,j} \oplus t_{i,j} = x_{i,j'} \oplus t_{i,j'}$ is satisfied. Then assume $p \approx E$.

Q.7 Conversely, assume that within the same sector i, there are two different indices j and j' such that $x_{i,j} \oplus y_{i,j} = x_{i,j'} \oplus y_{i,j'}$. What is the probability that $x_{i,j} \oplus t_{i,j} = x_{i,j'} \oplus t_{i,j'}$?
Hint: write $x_{i,j} \oplus y_{i,j} = f(x_{i,j} \oplus t_{i,j})$ and think of the Bayes rule.