Security Protocols and Applications (Part 1)

Final Exam
June 25\textsuperscript{th}, 2010
Duration: 3:00

This document consists of 6 pages.

Instructions

Electronic devices and documents are \textit{not} allowed.

This exam contains 2 \textit{independent} parts.

Answers for each part must be written on its separate sheet.

Answers can be either in French or English.

Questions of any kind will certainly \textit{not} be answered. Potential errors in these sheets are part of the exam.

You have to put your full name on the first page and have all pages \textit{stapled}. 
1 On Plaintext-Dependent Decryption in Secure Channels


We use some parameters \( w, B, a, b, c, d, d'. \) Considering a set of words \( Z = \{0, 1\}^w \) of \( 2^w \) elements, a finite sequence \( x \in Z^n \) has a length (in words) denoted by \( |x| \). (Namely, the bitlength is \( w|x| \).) We assume a binary encoding function \( V_n \) mapping an integer \( m \in \{0, 1, \ldots, B_n\} \) to an element \( V_n(m) \) of \( Z^n \) so that it can be decoded unambiguously by a function \( V_n^{-1} \). For instance, we may consider binary encoding with \( B_n = 2^{wn} - 1 \). We use a block cipher \( \text{Enc} \) with blocks of \( 2^d \) words in CBC mode (with secret initial vector \( K_3 \)) and a message authentication code \( \text{MAC} \) of \( 2^{d'} \) words. We assume a secure communication channel which is considered as a continuous stream from \( A \) to \( B \) based on some secret keys \( K_1, K_2, \) and \( K_3 \). To send a new message \( x \) such that \( |x| \leq 2^B \) from Alice to Bob, Alice waits until messages in the queue have been sent. Then, \( x \) is first transformed into a payload

\[
y = V_a(b + |x| + |\text{pad}_x|) \| V_d(|\text{pad}_x|) \| |x| \| \text{pad}_x
\]

where \( \text{pad}_x \) denotes the padding for message \( x \) such that \( |\text{pad}_x| \geq c \) and \( |y| \) is multiple of \( 2^d \).

The exact way that \( \text{pad}_x \) is constructed is unimportant. Then, it is transformed into

\[
z = \text{Enc}_{K_1}(y) \| \text{MAC}_{K_2}(\text{header} \| y)
\]

where \( \text{header} \) contains some extra protocol information which is not important here. Practically, the stream is split into packets which are sent sequentially in an asynchronous channel. For applications, we will assume \( aw - B = 14 \).

1. In the case of AES and openSSH, what are the values of \( w, a, b, c, d, \) an \( B' \)?

2. Recall how the CBC mode works.
3. Assuming that Bob receives $z'$, explain the algorithm to extract $x'$ from $z'$ such that $x' = x$ when $z' = z$. In this exercise, we assume that errors in extraction are immediately notified but that there are no differences between the types of error.

4. If an adversary sends a random block as a leading packet of $z'$, what is the probability $p$ that no error is returned?
5. Show how an adversary can decrypt $aw - B$ bits of information of a payload block $y_i$ from $z$ with probability $p^{-1}$.

6. To thwart the previous attack, could we have $|x|$ put at the end instead? Why?

7. Could we have $|x|$ sent in clear instead? Why?
8. Could we have \( z = \text{Enc}_{K_1}(y\|\text{MAC}_{K_2}(\text{header}\|y)) \) instead? Why?

9. Could we have \( \text{MAC}_{K_2}(\text{header}\|y) \) checked before the length instead? Why?

10. Could we have \( V_a(b + |x| + |\text{pad}_x|) \) authenticated in a separate way instead? Why?

11. What would you propose as a countermeasure?
Any attempt to look at the content of these pages before the signal will be severely punished.

Please be patient.