Security

Assignment 5, Friday, October 7, 2016

Handing in your answers: For the full story, see

`http://www.sos.cs.ru.nl/applications/courses/security2016/exercises.html`

To summarize:

- Include your name and student number **in** the document (they will be printed!), as well as the name of your teaching assistant (Hans or Joost). When working together, include **both** your names and student numbers.
- Submit one single **pdf** file – when working together, only hand in **once**.
- Hand in via Blackboard, before the deadline.

Deadline: Monday, October 17, 09:00 sharp!

Goals: After completing these exercises successfully you should be able to

- understand what the reasons and consequences for using diversified keys are;
- work with different modes of operation for block ciphers;
- recognize and avoid pitfalls of these modes.

Marks: You can score a total of 100 points.

1. **(20 points)** In the last lecture, diversified keys were discussed. A similar scheme is used in many of the smart card systems that are around today, such as the Dutch OV-chipkaart and in PIN transactions.

   (a) Why is it necessary to use diversified keys in scenarios such as these, from a practical point of view?

   (b) Consider the following protocol. Assume that each card stores an identification number Id_c and a key $K_c = K_m\{Id_c\}$ that is generated when the card is issued (here, K_m is the master key). Furthermore, assume that the terminals all have this master key K_m. What form of authentication is achieved here (*i.e.* what party has been authenticated)? Explain why.

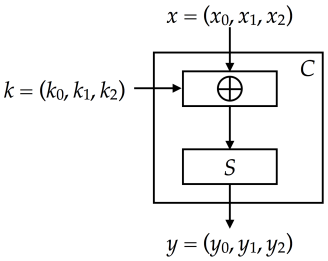
$$
\begin{array}{lcll}
C & \longrightarrow & T & : \; Id_c \\
 & & \multicolumn{2}{l}{\text{Terminal computes } K_c = K_m\{Id_c\}} \\
T & \longrightarrow & C & : \; K_c\{N\} \\
C & \longrightarrow & T & : \; N
\end{array}
$$

   (c) We now change the protocol to the one described below. What form of authentication is achieved here? Explain why.

$$
\begin{array}{lcll}
C & \longrightarrow & T & : \; Id_c, N_c \\
 & & \multicolumn{2}{l}{\text{Terminal computes } K_c = K_m\{Id_c\}} \\
T & \longrightarrow & C & : \; K_c\{N_t, N_c\} \\
C & \longrightarrow & T & : \; N_t
\end{array}
$$

The assignment continues on the next page!

2. **(60 points)** Assume a block cipher C that encrypts a plaintext block with a key in two steps.



In particular, C maps a 3-bit input block $x = (x_0, x_1, x_2)$ to a 3-bit output block $y = (y_0, y_1, y_2)$ using a 3-bit key $k = (k_0, k_1, k_2)$ and a function S as follows:

$$y = C(x, k) = S(x_0 \oplus k_0, x_1 \oplus k_1, x_2 \oplus k_2),$$

where S is the following substitution:

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

So, for instance encrypting `001` with key `101` becomes $C(001, 101) = S(100) = 010$ and decrypting `100` with key `110` becomes $C^{-1}(100, 110) = S^{-1}(100) \oplus 110 = 110 \oplus 110 = 000$.

(a) Compute the ciphertext belonging to plaintext `011 111 101 001` (so, using blocks of three bits) with key $k =$ `101` using Electronic Code Book (ECB) mode. Show intermediate steps.

(b) Do the same for Cipher Block Chaining (CBC) mode, where the Initialisation Vector (IV) is `111`. Show intermediate steps.

(c) Give at least one reason why CBC mode is preferred over the ECB mode.

(d) CBC can also be used to produce a code, for message integrity. This is called a 'CBC-MAC' (message authentication code), which is effectively the last block of a CBC encryption (see the lecture slides for more details). CBC-MAC only provides integrity for fixed-length messages. Which block (so which three bits) can you add *in front* of the plaintext message, to come to the same CBC-MAC (again with IV `111`). Why does this work?

(e) The previous question was a concrete example of a generic problem. Say an attacker has a message m, and the CBC-MAC of this message, which we will call T (for tag). He also knows a second message m' with its corresponding CBC-MAC T'. The IV is considered public information, so the attacker knows this as well. How can an attacker use all of this to create a third message (which we will call m'') so that the CBC-MAC for m'' will still be the same T'?

(f) Suppose Alice sends a message to Bob using this cipher in CBC mode. The ciphertext is `111 100 101`, the key is `100` and the IV is `010`. Unfortunately, the channel is noisy and the third bit of the ciphertext flips, so Bob receives `110 100 101`. Answer the following questions. Show intermediate steps.

i. How much difference will there be between the plaintext messages that were sent and received in terms of bits (so-called *Hamming distance*)?

ii. How many blocks are different?

iii. Is this the same for any block cipher in CBC mode, in general?

3. **(20 points)** In this exercise, we will take a look at the CTR mode. We use the same block cipher C that was introduced in the previous exercise.

   (a) Assume that the key $k = \texttt{101}$, and $IV = \texttt{100}$. Compute the first 9 bits of key stream. Show intermediate computations! *Hint:* interpret the IV as a 3-bit binary number.

   (b) Assume that the plaintext is `001 110 111`. Compute the matching ciphertext.

   (c) While CTR is generally a great choice, there is one pitfall: an IV should never be repeated. Assume you have a plaintext $p_1 = \texttt{010 110 110}$ and a corresponding ciphertext $c_1 = \texttt{110 001 101}$, for a certain unknown key and IV, as well as a different ciphertext $c_2 = \texttt{101 011 111}$ that was obtained by encrypting p_2 with the same key and IV. Compute the matching plaintext p_2. Show your computations!