University of Haifa — Spring Semester – 22/3/11

Introduction to Cryptography – Exercise no. 2

Submit in Pairs/Single to **mailbox** 19 by 10/4/11, 1:00 p.m.

1. In this problem, we encrypt a message of length 768 bits under AES using one of the following modes of encryption, with the IV set to 0 (i.e., $IV = 00\dots0$): ECB, CBC, OFB, CFB, and Counter Mode. Assume that A and B share an AES key. A uses it to encrypt a 768-bit message x for B. Let y be the corresponding ciphertext. On the way between A and B the 243th bit i of y is flipped, i.e., B receives y' which differs from y only in the 243th bit. Upon reception B decrypts y' and obtains x'. For each of the above modes, which bits of x' are certain to remain identical to the corresponding bit of x?

2. A student in the course "Cryptology for Primates", from the planet of the apes, suggested the following mode of operation, called Xor Mode:

   - The mode accepts an IV.
   - To encrypt a message $M = M_1M_2\dots M_n$, compute

   $$C_i = E_k(IV \oplus M_1 \oplus M_2 \oplus \cdots \oplus M_i).$$

   (a) How decryption is performed (i.e., given a ciphertext $C = C_1C_2\dots C_n$, how is M_i is deduced)?

   (b) Does $C_i = C_j$ imply that $M_i = M_j$?

   (c) If we would like to change the value of M_i, how many blocks do we need to re-encrypt to update the ciphertext?

   (d) At the end of the exam in the course, King Kong, the lecturer, has sent the grades of three students, Able, Bubbles, and Marcel, to the secretariat using AES in Xor Mode (with the IV set to 0), where the format of the plaintext is $M_1||M_2||M_3$, and M_1, M_2, M_3 are 128-bit strings encoding the grades of Able, Bubbles, and Marcel, respectively. Able, found out that he is going to get 30, while Bubbles is going to get 75, and Marcel is going to get 100. Can Able change the encrypted message sent by King Kong, such that his grade is the highest?

   (e) Following Able's attempts, King Kong decided that he is going to send the new grades using the Xor Mode, this time, with an IV that he selects randomly and which is attached to the message. As he did not know which of the apes was to blame, King Kong passed the grade 0 to all three apes. Can Able change his grade to 100, while leaving the grades of the others as 0?

3. This question deals with a variant of AES.
Recall that in AES (Rijndael), a round of encryption consists of the following four operations:

- SubBytes
- ShiftRows
- MixColumns
- AddRoundKey

For each of the following changes to AES, determine whether they are weaker than AES, or as secure as AES. In the case of weaker variants, describe an attack that breaks the new cipher. For similar security, explain why it is as secure as the original AES.

(a) If all the MixColumns operations are omitted from the cipher.

(b) If all ShiftRows operations are omitted from the cipher.

(c) If all operations of the same time are put together, i.e., the encryption is changed to:
   - 10 SubBytes, followed by
   - 10 ShiftRows, followed by
   - 9 MixColumns, followed by
   - 11 AddRoundKey

(d) the ShiftRows operation is changed such that the rotation is to the right (instead of to the left).

When describing an attack, give the expected time, memory, and data complexities.

4. It was suggested to reduce the size of a Diffie-Lamport signatures in the following way: Let $f : \{0,1\}^{128} \rightarrow \{0,1\}^{128}$ be a one way function. Let $g : \{0,1\}^{128} \rightarrow \{$ The subsets of $\{0,1\}^{132}$ with hamming weight 66 $\}$ (i.e., 132-bit strings with 66 0 and 66 1). The signer U chooses in advance 132 random values (instead of 256) denoted by $x_0, x_1, \ldots, x_{131}$ and calculates the vector $y_0, y_1, \ldots, y_{131}$, by $y_i = f(x_i)$, for $i = 0, 1, \ldots, 131$. The vector $y_0, y_1, \ldots, y_{131}$ is stored in a public file. Given a document $M = m_0 m_1 \ldots m_{127}$, U chooses an unused vector from the public file, marks it as used, and calculates the signature $S = s_0, s_1, \ldots, s_{65}$, which are the 66 values x_i for which the ith bit in $g(M)$ equals 1.

(a) How does the received check that the signature is valid?

(b) What is the size of the signature in bits? What would have been the Diffie-Lamport signature size in this case?

(c) Prove that this system is secure as the Diffie-Lamport signature system (it is enough to show that one needs to invert f in order to forge a signature).