University of Haifa Spring Semester – 29/11/12

Introduction to Cryptography – Exercise no. 2

Submit in Pairs/Single to **mailbox** 19 by 13/12/12, 1:00 p.m.

1. (a) Prove the complementation property of DES: If $C = E_K(P)$ then $\bar{C} = E_{\bar{K}}(\bar{P})$.

   (b) Consider the following suggestion for a change of E:

16	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	1
32	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	17

   i. When using this E there exists another complementation property. Describe it and prove its correctness.
   Hint: notice that 28 key bits are used for creating the inputs of S_1, S_2, S_3, S_4, and that the other 28 key bits are used for creating the inputs of S_5, S_6, S_7, S_8.

   ii. Use this property to reduce the complexity of exhaustive search to 2^{54} (2^{53} in the average case). Describe your attack and explain.

2. 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., $IV = 00\ldots0$): 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?

3. To deal with the main problem of ECB, that the encryption of the same block twice results in two equal ciphertext blocks (i.e., encrypting $M = M_1||M_2$ where $M_1 = M_2$ results in $C = C_1||C_2$ with $C_1 = C_2$), a new mode was suggested. The mode, ECBC — Electronic Code Book with Counter takes the i'th message block and encrypts it as:

$$C_i = E_k(M_i \oplus i).$$

   (a) Prove that when encrypting $M = M_1||M_2$ with $M_1 = M_2$, the resulting ciphertext $C = C_1||C_2$ satisfy that $C_1 \neq C_2$.

   (b) When two ciphertext blocks C_i and C_j are equal, does this reveal any information concerning the corresponding message blocks M_i and M_j?

(c) Prove that any chosen plaintext attack on a cipher in ECBC mode can be transformed into a chosen plaintext attack on the same cipher in ECB mode. (Hint: use reductions).

(d) Show that for ECBC, obtaining the ciphertext $C = C_1||C_2||\ldots||C_8$ of $M = M_1||M_2||\ldots||M_8$, allows to generate a ciphertext C' which is the encryption of $M' = M_1||M_2||\ldots||M_6$. Explain how to do so.

4. 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.

5. It was suggested to reduce the size of a Diffie-Lamport signatures in the following way: Let $f : \{0,1\}^{128} \to \{0,1\}^{128}$ be a one way function. Let $g : \{0,1\}^{128} \to \{$ The subsets of $\{0,1\}^{138}$ with hamming weight 69 $\}$ (i.e., 138-bit strings with 69 0 and 69 1). The signer U chooses in advance 138 random values (instead of 256) denoted by $x_0, x_1, \ldots, x_{137}$ and calculates the vector $y_0, y_1, \ldots, y_{137}$, by $y_i = f(x_i)$, for $i = 0, 1, \ldots, 131$. The vector $y_0, y_1, \ldots, y_{137}$ 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 $S = s_0, s_1, \ldots, s_{68}$, which are the 69 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).