Modern Cryptology (236506) – Exercise no. 3

Submission in singles until 13/05/2019

The exercise must be typed and printed.

1. (a) Given an input and an output to DES’ F-function, how many different (48-bit) subkeys can lead from the given input to the given output?

(b) Is it possible to find a subkey $K$ and two inputs $I_1 \neq I_2$ for which $F(I_1, K) = F(I_2, K)$? If your answer is yes, find such inputs for the subkey $K = 0F0F0F0F0F0F_{\times}$ (Hexadecimal representation).

2. Devise a simple attack on three-round DES. This attack should use only two plaintext/ciphertext pairs, and its complexity should be bounded by $2^{30}$ steps. A possible attack may use the properties of the key scheduling algorithm (i.e., division of the key into two halves, C,D, that correspond to different S boxes).

3. Double-DES encrypts a 64-bit message $M$ in the following manner:

$$ C = DES_{K_2}(DES_{K_1}(M)) $$

Here, $K_1$ and $K_2$ are bitstrings of 56 bits each.

(a) What is the average complexity of a “naive” exhaustive key search?

(b) Show that it is possible to find $K_1$ and $K_2$ with complexity not exceeding $2^{60}$ DES encryptions (or decryptions) by using a meet-in-the-middle attack. Describe your attack algorithm by a detailed pseudo code (use as least memory as you can). What are the time and memory complexities of the attack you described?

Two-Key Triple-DES encrypts a 64-bit message $M$ in the following manner:

$$ C = DES_{K_1}(DES_{K_2}^{-1}(DES_{K_1}(M))) $$

Here, $K_1$ and $K_2$ are bitstrings of 56 bits each.

(c) What is the average complexity of a “naive” exhaustive key search?

(d) What are the time and memory complexities of a “naive” meet-in-the-middle attack (as in (b))? Describe your attack algorithm by a pseudo code (use as least memory as you can).
4. Assume that Bob sends encrypted messages using DES in the OFB mode of operation with secret (but fixed) IV value. Assume also that the key is fixed.

(a) Show how to perform a known plaintext attack in order to decrypt transmitted messages.
(b) Does your attack work if Bob uses the CFB mode? Can it recover partial information? Explain.
(c) Does your attack work if Bob uses the CBC mode? Can it recover partial information? Explain.

5. A cipher is called closed under composition if for every two keys $K_1$, $K_2$ (not necessarily distinct) there exists a key $K_3$, such that $E_{K_1}(E_{K_2}(P)) = E_{K_3}(P)$ for all $P$.

(a) Explain why the substitution cipher is closed under composition.

For the purpose of this question we assume that $E$ is DES, and that it is closed under composition (In practice, DES is not closed under composition).
Moreover, assume that there are no colliding keys in DES, i.e., if $K_1 \neq K_2$ then there exists $P$ such that $E_{K_1}(P) \neq E_{K_2}(P)$.

(b) Show that there exists a key $I$ for which for all $P$ it holds that: $E_I(P) = P$.
(c) Show that for every key $K$ there exists an inverse key $K'$, such that for all $P$ it holds that: $E_{K'}(E_K(P)) = P$.
(d) Show that for every key $K_3$, and every key $K_2$, there exists a key $K_1$, such that $E_{K_1}(E_{K_2}(P)) = E_{K_3}(P)$ for all $P$.
(e) Show that it is possible to break $E$ (with high probability) with complexity not exceeding $2^{33}$ encryptions/decryptions, given a plaintext $P$ and its ciphertext $C$ under the key $K$. Provide a detailed pseudo code of the attack. What is the complexity of the attack you describe?

Instruction: Observe the key in use as a composition of two other keys, and given $P$ and $C$, show how is it possible to encrypt and decrypt every message (in case of need the attacker can require several plaintexts and their encryption).