Cryptography

Problem set 3 - 26-27 III 2015

Problem 1 (from the problem set no 1) Let $\Pi_1 = \langle Gen_1, Enc_1, Dec_1\rangle$ and $\Pi_2 = \langle Gen_2, Enc_2, Dec_2\rangle$ be two encryption schemes for which it is known that at least one is CPA-secure. The problem is that you don't know which one is CPA-secure and which may not be.

Show how to construct an encryption scheme Π that is guaranteed to be CPA-secure as long as at least one of Π_1 or Π_2 is CPA-secure.

Hint: Generate two plaintext messages from the original plaintext so that knowledge of either one of the parts reveals nothing about the plain-text but knowledge of both does yield the original plaintext.

Provide a full proof of your answer.

Problem 2 Show that for a block cipher F' defined using a block cipher F by making the key longer:

$$F'_{k_1,k_2,k_3}(x) := k_1 \oplus F_{k_2}(x \oplus k_3),$$

where k_1, k_2, k_3 are independent, is not secure.

Problem 3 Consider a variant of CBC where in each encryption IV is increased by 1 (instead of choosing it at random). Show that the variant is not CPA-secure.

Problem 4 Write a program and try to find which of the DES' S-boxes are the most linear.(The definition of the DES can be found here `http://www.itl.nist.gov/fipspubs/fip46-2.htm`).

You need to compute the probability that the following equation holds:

$$S_i(z) \oplus S_i(z \oplus x) = y,$$

for all $i = 1, \ldots, 8$, $x \in \{0,1\}^6$ i $y \in \{0,1\}^4$ and random $z \in \{0,1\}^6$.

Problem 5 Show that selecting S-boxes at random for an SP-network is not a good idea. Show that for randomly selected S-box linear attacks will be possible.

Problem 6 (for Security-track, 2pts) As the problem 5 but with regard to differential attacks.