Cryptography

Problem set 4 - 10-11 IV 2013

Problem 1 Let G be a pseudorandom generator where $|G(s)| > 2|s|$.

1. Define $G'(s) = G(s0^{|s|})$. Is G' necessarily a pseudorandom generator?
2. Define $G'(s) = G(s_1 \cdots s_{n/2})$, where $s = s_1 \cdots s_n$. Is G' necessarily a pseudorandom generator?

Problem 2 Let G be a pseudorandom generator and define $G'(s)$ to be the output of G truncated to n bits (where $|s| = n$). Prove that the function $F_k(x) = G'(k) \oplus x$ is not pseudorandom.

Problem 3 Consider a variant of CBC-mode encryption where the sender simply increments the IV by 1 each time a message is encrypted (rather than choosing IV at random each time). Show that the resulting scheme is not CPA-secure.

Problem 4 Show that CBC, OFB, CFB and counter modes of encryption do not yield CCA-secure encryption schemes (regardless of F).

Problem 5 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 6 Show that for a block cipher F' defined using a block cipher F by making the key longer:

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

where k_1, k_2 are independent, is not secure (in particular, there exists a faster than brute-force attack). What is the time and memory complexity of your attack.

Problem 7 Problems 3 and 4 from: `http://zagorski.im.pwr.wroc.pl/courses/kibi_2012/lista3.pdf`.

Problem 8 Find a complexity of an attack on a three round SP-network for the parameters as in the Problem 7.