Cryptography

Problem set 2 - 19-20 III 2015

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 $G'(s) = G(s_1 \dots s_{n/2})$, where $s = s_1 \dots s_n$. 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 the following LFSR over $\mathcal{Z}_2$: $z_{i+4} = z_i + z_{i+1} + z_{i+2} + z_{i+3} \bmod 2$, for $i \geq 0$. (a) Draw the corresponding LFSR. (b) For all possible vectors (z_0, z_1, z_2, z_3) find a period of the LFSR (period of an i-bit LFSR is the smallest $n > 0$, for which $(z_0, \dots, z_{i-1}) = (z_n, ldots, z_{n+i-1})$). (c) Repeat the exercise for $z_{i+4} = z_i + z_{i+3} \bmod 2$.

Problem 4 Output of an LFSR can be written in a matrix form:

$$(z_{m+1}, z_{m+2}, \dots, z_{2m}) = (c_1, c_2, \dots, c_m) \begin{pmatrix} z_1 & z_2 & z_3 & \dots & z_m \\ z_2 & z_3 & z_4 & \dots & z_{m+1} \\ \vdots & \vdots & & & \vdots \\ z_m & z_{m+1} & z_{m+2} & \dots & z_{2m-1} \end{pmatrix},$$

where $z = \langle z_1, \dots, z_m \rangle$ corresponds to the initial content of the LFSR and $c = \langle c_1, \dots, c_m \rangle$ defines which registers are used to compute the next bit.

For an LFRS defined by: $c = \langle 0, 1, 0, 0, 1 \rangle$, a key $z = \langle 0, 1, 0, 1, 1 \rangle$ (initial state) one obtains:

$$(0, 0, 1, 0, 0) = (0, 1, 0, 0, 1) \begin{pmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Knowing that $c = \langle 1, 0, 0, 1, 0 \rangle$ and $\langle z_6, z_7, z8, z_9, z_{10} \rangle = \langle 0, 0, 1, 1, 0 \rangle$ find the key $z = \langle z_1, z_2, z_3, z_4, z_5 \rangle$.

Problem 5 (2 pts) What is the compleity of an attack on A5/1 if in each round all LFSRs are moving (instead of applying a majority rule).

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 (2 pts) Show how to get possible round keys from a three-round SP-network. You can assume that you know m pairs of the corresponding plaintext-ciphertext pairs. You can assume that each S-box has 4-bit input and 4-bit output and that the whole SP-network encrypts 64-bit messages (so there are 16 S-boxes).

What is the complexity of the attack if 64-bit block is replaced with 128-bit block and each S-box has 8-bit input and output?

Problem 8 What is the result of an r-round Feistel network on input (L_0, R_0) if each of the round functions $F_k(x)$ is: (a) an identity function $F_k(x) = x$ (b) equal to $F_k(x) = 0^n$?