Institut for Matematik og Datalogi
Syddansk Universitet

September 21, 2016
JFB

Cryptology – E16 – Lecture 4

Lecture, September 12

We covered chapter 9 and motivated the study of pseudorandom functions for stream ciphers.

Lecture, September 14

We will cover section 11.2, including the proof of Lemma 2.3 and the birthday bound at the top of page 24. Then, we will cover sections 12.1 and 12.2.

Lecture, September 20

We will finish chapter 12 and begin on chapter 13.

Problem session September 21

1. Consider the following family of pseudorandom function generators: $F_{(\ell,w)}(n) = n \cdot w \pmod{\ell}$. Design an adversary (Eve) which efficiently (using q calls to the oracle, where $q \geq 2$ is not large) obtains the result $\mathrm{Adv}^{\mathrm{PRF}}_{\{F_k\}_K}(A; q) \geq 1 - (1/|C|)^{q-2}$. Hint: Try to find w first, assuming that $b = 1$.

   For which k is this function a permutation of the set $\mathbb{Z}_\ell$?

2. Explain (intuitively) why the birthday paradox is relevant in the proof of Lemma 11.2.

3. Suppose we construct a keystream in a synchronous stream cipher using the following method: Let $K \in \mathcal{K}$ be the key, let $\mathcal{L}$ be the keystream alphabet, and let Σ be a finite set of *states*. First, an *initial state* $\sigma_0 \in \Sigma$

is determined from K by some method. For all $i \geq 1$, the state σ_i is computed from the previous state σ_{i-1} according to the following rule:

$$\sigma_i = f(\sigma_{i-1}, K),$$

where $f : \Sigma \times \mathcal{K} \to \Sigma$. Also, for all $i \geq 1$, the keystream element $\_i$ is computed using the following rule:

$$z_i = g(\sigma_i, K),$$

where $g : \Sigma \times \mathcal{K} \to \mathcal{L}$. Prove that any keystream produced by this method has period at most $|\Sigma|$. Note that to be periodic, you don't have to start from the beginning, just be ultimately periodic. (Problem 2.10 in CTP.)

4. Suppose that a linear feedback shift register sequence is produced using a register of length L and has period $2^L - 1$. In general, exactly how many zeros are there among the first $2^L - 1$ bits produced. Prove your answer.

5. Suppose that you are able to obtain the ciphertext "01100111101001", and you learn that the first eight bits of the plaintext are "10110110". You know that the encryption was done with the aid of a linear feedback shift register over the field GF(2), with length four. Determine the linear feedback shift register and the remainder of the message.

6. I may lecture at the end.