Institut for Matematik og Datalogi
Syddansk Universitet

September 14, 2006
JFB

Cryptology – E06 – Week 3

Lecture, September 14

We covered linear feedback shift registers from chapter 1 in the textbook and covered most of chapter 2 (We skipped Huffman coding, which is covered in DM19). We also covered section 3.1 of chapter 3.

Lecture, September 21

We will cover chapter 3 in the textbook, skipping most of the first four sections. The original Rijndael specification (which can be found through the course's homepage) will be used as the basis for the description of AES.

Lecture, September 28

We will finish chapter 3 and begin on chapter 5 in the textbook. Note that section 5.2.1 was covered earlier.

Problem session September 25

1. Problem 2.4 in the textbook.
2. Problem 2.10 in the textbook.
3. Problem 2.11 in the textbook.
4. Problem 2.17 in the textbook.
5. Suppose a cryptosystem has $P = \{a, b, c\}$, $C = \{1, 2, 3, 4\}$ and $K = \{K_1, K_2, K_3\}$. The encryption rules are as follows:

	a	b	c
K_1	1	2	3
K_2	4	3	2
K_3	3	4	1

Suppose $p_K(K_i) = 1/3$ for $1 \leq i \leq 3$, $p_P(a) = 1/2$, $p_P(b) = 1/3$, and $p_P(c) = 1/6$.

a. Compute the probabilities $p_C(y)$ for all $y \in \{1, 2, 3, 4\}$.

b. Does this cryptosystem achieve perfect secrecy? Explain your answer.

6. Suppose a plaintext alphabet, P, and a ciphertext alphabet, C, are both equal to $\mathbb{Z}_p^*$, where p is an odd prime. Consider the following symmetric key cryptosystem. A message $m = m_1 m_2 \ldots m_s$, consisting of s symbols from P is encrypted using a shared secret key, $K = k_1 k_2 \ldots k_s$, consisting of s values chosen randomly, uniformly and independently from $\mathbb{Z}_p^*$. Symbol m_i from the message is encrypted using k_i, giving the result $c_i = m_i \cdot k_i \pmod{p}$. A key is never us ed more than once.

   a. How is decryption performed?

   b. Show that this cryptosystem has perfect secrecy.

   c. What advantage or disadvantage does this system have over the one-time pad defined in the textbook?

7. Do problem 3.3 in the textbook.

8. Do problem 3.7 in the textbook.