Institut for Matematik og Datalogi
Syddansk Universitet

September 22, 2016
JFB

Cryptology – E16 – Lecture 6

Lecture, September 20

We covered chapter 12, concentrating on sections 12.1 and 12.2, and gave an introduction to block ciphers.

Lecture, September 26

We will cover DES and AES from chapter 13.

No class on September 28

The first assignment is due at 12:15 on October 3. (Note that class will also be cancelled on November 1.)

Lecture, October 3

We will cover the rest of chapter 13, except for subsection 13.5, which we will cover later.

Problem session October 4

1. How is decryption performed in CFB mode?

2. Suppose a sequence of plaintext blocks, $x_1, ..., x_n$, yields the ciphertext sequence, $y_1, ..., y_n$. Suppose that one ciphertext block, say y_i is transmitted incorrectly (i.e., some 1's are changed to 0's and/or vice versa). Show that the number of plaintext blocks that will be decrypted incorrectly is equal to one if ECB, OFB or CTR modes are used for encryption; and equal to two if CBC or CFB modes are used. (Problem 3.7 in CTP.)

3. For the attack described in the textbook against CFB mode with a Nonce IV, is it known plaintext, chosen plaintext, or chosen ciphertext? Explain the attack.

4. To make sure you still know how to use some number theoretic algorithms, try the following:

   (a) Use the Extended Euclidean Algorithm to find $18^{-1} \bmod 97$ (page 15 in the text, but they return the wrong x and y – what is correct?).

   (b) Use fast modular exponentiation to compute $2^{11} \bmod 15$. There is more than one algorithm in section 6.2. Let's use Algorithm 6.2.

   (c) Use the algorithm for the Chinese Remainder Theorem to compute an x satisfying: $x \equiv 1 \bmod 3$, $x \equiv 3 \bmod 5$, $x \equiv 4 \bmod 7$. See page 16 in the textbook.

   (d) Solve the following system of congruences: $15x \equiv 5 \bmod 35$ and $x \equiv 1 \bmod 8$. (The notes on number theory, on the course homepage, contain some explanation for when linear congruences are solvable.)

5. I may lecture at the end.