Institut for Matematik og Datalogi
Syddansk Universitet

November 10, 2006
JFB

Cryptology – E06 – Week 9

Lecture, November 2

We covered the McEliece Cryptosystem (copied from an earlier edition of the textbook), introduced digital signatures from chapter 7, and covered up through section 4.3 of chapter 4, except the subsection on the Merkle–Damgård construction.

Lecture, November 9

We will first cover SHA–256 and then cover the last two secitons of chapter 4. Then we will return to chapter 7, covering up through section 7.4.2.

Lecture, November 16

We will cover chapter 8.

Announcement

STUDIEORIENTERENDE SAMTALER P IMADA

ALLE studerende på studieretningerne matematik, mat.øk. og datalogi, som læser på andet studieår og opefter, indkaldes herved til obligatoriske studieorienterende samtaler med lærerrepræsentanter. Samtalerne finder sted i kalenderugerne 45 og 46. Tilmeldingslisterne er fremlagt på IMADAs sekretariat.

Set fra jeres synspunkt giver samtalerne en mulighed for at stille spørgsmål om f.eks. hvilke valgfri kurser, I kan og bør tage, og hvilke muligheder for specialer, der findes på institutterne. Vort formål med samtalerne er at få overblik over, hvor mange studerende vi rent faktisk har på de forskellige

"udviklingstrin". Desuden benytter vi lejligheden til at opdatere vort fotogalleri.

Der gøres opmærksom på, at alle ikke-aktive studenterkonti på UNIX-systemet vil blive nedlagt i løbet af november. De studieorienterende samtaler er måden, hvorpå man registreres som værende aktiv.

Studieudvalget på IMADA

Problem session November 13

1. Do problem 4.1 in the textbook. For part (d), use the fact that the left-hand side in (c) is at least zero.

2. Do problem 4.6.

3. Do problem 4.12. For part (b), you can find a (1,1)-forger.

4. Let p be an odd prime and g_0 and g_1 be generators of $\mathbb{Z}_p^*$. Consider the following two functions: $f_0(x) = g_0^x \pmod p$ and $f_1(x) = g_1^x \pmod p$. Use these two functions to create a hash function which will hash an arbitrary length message down to a value in $\mathbb{Z}_p^*$. Can you make it secure under the assumption that the discrete log problem is infeasible?

5. Do problem 6.21 in the textbook.

6. Do problem 7.1 in the textbook. (You might want to look at the notes on the course home page on number theory to recall how to solve linear congruences.)

7. In the discussion of the Schnorr signature scheme on page 286, it says that to find a qth root of 1 modulo p, one should begin with a primitive element α_0 of $\mathbb{Z}_p^*$ and compute $\alpha_0^{(p-1)/q}$. (Recall that p and q are both primes.)

    a. Why is this correct? What subgroup does the result generate?

    b. How long does it take to do this computation?

    c. Is it necessary that α_0 be a primitive element?