Institut for Matematik og Datalogi
Syddansk Universitet

April 12, 2013
JFB

Cryptology – F13 – Week 8

Lecture, April 8

We finished through section 7.4.2 of chapter 7. We then discussed subliminal channels and began on chapter 8, covering the Goldwasser-Micale public-key cryptosystem in section 8.4.

Lecture, April 12

We covered the first three sections of chapter 8, and possibly return to section 7.6, which we will do from some notes.

Lecture, April 17

We will finish section 8.4 and cover undeniable signatures from section 7.6 using notes.

Lecture, April 22

We will begin on zero-knowledge (from the notes on commitment schemes and zero-knowledge by Ivan Damgård and Jesper Buus Nielsen, available through the course's homepage).

Problem sessions April 15 and 19

We will continue first with those we didn't finish on April 11, listed below.

1. Do problem 4.6.
2. Do problem 4.12. For part (b), you can find a (1,2)-forger. Skip the difficult case mentioned.

3. Let p be an odd prime and g_0 and g_1 be generators of 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 Z_p^*. Can you make it secure under the assumption that the discrete log problem is infeasible?

4. Do problem 6.21 in the textbook.

5. 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.)

6. In the discussion of the Schnorr signature scheme on page 293, it says tha t to find a qth root of 1 modulo p, one should begin with a primitive element α_0 of 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?

7. Consider the following proposal for a hash function, where $E(K, M)$ is encryption of the 128 bits of M using a 128-bit key K in Rijndael (AES). Let IV be a 128-bit random string. Pad the document to be hashed with that the number of bits is divisible by 128. Let the resulting document be $M = m_1||m_2||...||m_r$, where each block m_i contains exactly 128 bits and the operation $||$ is concatenation.

$$\begin{array}{rcl} H_0 & \leftarrow & IV \\ H_1 & \leftarrow & E(m_1, H_0) \\ H_2 & \leftarrow & E(m_2, H_1) \\ & . & \\ & . & \\ & . & \\ H_r & \leftarrow & E(m_r, H_{r-1}) \\ H & \leftarrow & E(m_1 \oplus m_2 \oplus ... \oplus m_r, H_r) \end{array}$$

The operation $\oplus$ is bit-wise exclusive-or, and the output of the hash function is (H_0, H). (Note that there a message which has zeros at the end will hash to the same value as that message with the zeros truncated (removed). Thus, finding collisions is trivial, but we will ignore that type of collision in the following.)

a. Using the Birthday Paradox, define and analyze (how many calls to Rijndael) an algorithm for finding a collision.

b. The above hash function would be much less secure if the steps with the ByteSub transformations were simply removed from Rijndael. Which is the hardest of the three problems Preimage, Second Preimage, and Collision, which could now be solved efficiently? How would you solve that problem?

8. Do problems 7.3a and 7.4a in the textbook.

9. Do problem 8.1 in the textbook. In part b, it should say "$s_o = \frac{-b}{a-1} \pmod{M}$".

10. Recall the quadratic residuosity implementation of probabilistic encryption, from the original paper by Goldwasser and Micali. Design a subliminal channel for use with this cryptosystem.

    Here we are assuming that the two prisoners are allowed to send encrypted messages to each other, but the warden always forces the receiver to decode the message for him (and the sender suspects that this is happening). With the subliminal channel, the receiver will decrypt an innocuous (or even deceptive) message for the warden, but the warden will never know about the true message which the receiver gets at the same time.

    If the warden actually carries the message, he can defeat this plan and eliminate the subliminal channel. To do this, the warden takes the encoded message from the sender and changes it. Afterwards the new cryptogram will still be an encryption of the same message, but the subliminal channel will be gone.

    Explain how this can all be done even though the prisoners are not allowed to use a redundant representation of the original message.

11. Do problem 8.5. Argue that if the Discrete Logarithm Problem is hard, then this generator is secure, i.e. there is no probabilistic polytime ϵ-Distinguisher.

12. In the verification protocol for undeniable signatures (in the textbook), the verifier chooses randomly two values e_1 and e_2. Why are there two values? Why not just let $e_2 = 0$ always?

13. Give a protocol for digital signatures in which the verification (which can be shown to the judge) does not reveal to the judge the contents of the document which was signed.

14. Some applications are sensitive to *replay attacks*, where an adversary takes a copy of an original signed message and sends it again later. (For example, it should not be possible to repeat a request to transfer money from one bank account to another.) Design a protocol (using signatures) to prevent replay attacks.