Institut for Matematik og Datalogi
Syddansk Universitet

November 14, 2006
JFB

Cryptology – E06 – Week 10

Lecture, November 9

We covered SHA–256 and the last two secitons of chapter 4. Then we also covered covering up through section 7.4.2.

Lecture, November 16

We will cover chapter 8.

Lecture, November 23

We will begin on chapter 9.

Announcement

There will be a "pizza-meeting" for all students of Imada on Wednesday, Nov 22 at 16.10-18.30 in room U49. At the meeting Imada will give general information on the Bachelor and Candidate studies, and specific information on the elective courses in Mathematics and Computer Science planned for the next semester. The meeting will end with a free pizza, beer, and soft drink session.

Problem session November 20

1. In class, we looked at a bit commitment scheme which had its security based on the Quadratic Residuosity Assumption. User A has a public key pair (N, y), where N is the product of two large primes and y is a quadratic nonresidue with Jacobi symbol $+1$. To commit to a bit b, user A chooses a random $r \in \mathbb{Z}_N^*$ and produces the blob $y^b r^2$

(mod N). Suppose that user A has committed to two bits b_1 and b_2, producing blobs B_1 and B_2. Show how A can use the blobs B_1 and B_2 to reveal c such that $c = b_1$ XOR b_2, and to prove to another user B that $c = b_1$ XOR b_2, without revealing b_1 or b_2. (The fact that this can be done means that this system for producing blobs has what is called the *equality property*, because it can be used to show that two blobs are commitments to equal bits, showing that the XOR is zero.)

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

3. 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.

4. 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 c-Next Bit Predictor for any constant c.

5. Do problem 8.7. Use the following definition of period: $z_{i+t} = z_i$ for all $i \geq c$ for some c (i.e. it should be ultimately periodic). (The result holds with the original definition, though.) For part b, use p=7 and q=11. :-)