Institut for Matematik og Datalogi
Syddansk Universitet

November 1, 2019
JFB

Cryptology – 2019 – Lecture 10

Announcements

1. All lectures on Thursdays will start at 16:10, instead of 16:15.
2. Lectures on Thursday, October 24, and Thursday, November 21, are cancelled.
3. There will be a Cyber Security Challenge which you can sign up for until October 16: https://challenges.dk/da/challenge/cyber-security-challenge-2019. This is not part of the course.
4. There is an IMADA Talks at 15:15 on Friday, October 11, in the DIAS conference room.

Lecture, October 7

We finished chapter 14, including section 11.7.3 for security of MACs, and covered section 11.4. We also began on chapter 15, introducing RSA and giving the proof that encryption followed by decryption with RSA gives the correct result. The two slides used for this can be found among those RSA slides on the course homepage.

Lecture, October 10

We will cover Rabin's encryption scheme (subsection 15.1.1) and cover subsections 2.2. We may also cover sections 1.3.5, 1.3.6 and 1.3.9 from chapter 1.

Lecture, October 22

We will cover subsections 1.3.7 and 1.3.8 and continue with chapters 2 and 15.

Problem session October 28

1. Show all steps in an execution of Shank's algorithm to find a square root of 65 modulo 97. What is the other square root.

2. Show all steps in the calculations of the Jacobi symbol $\left(\frac{29}{35}\right)$, using the standard algorithm (using the four properties of the Legendre symbol given in the textbook).

3. The Solovay-Strassen algorithm for primality testing is as follows:

   procedure Solovay-Strassen(n, k):
   for $j = 0$ to $k - 1$ **do**
   Choose a random a such that $1 \leq a \leq n - 1$
   $x \leftarrow \left(\frac{a}{n}\right)$
   if $x = 0$ **then return** "Composite a"
   $y \leftarrow a^{(n-1)/2} \pmod{n}$
   if $x \neq y$ **then return** "Composite a"
   return "Probable prime"

   The algorithm answers "Probable prime" for primes.

   Note that the loop is executed k times for a security parameter k. We will show that the error probability (probability of declaring a composite prime) is at most $(1/2)^k$. Define

   $$G(n) = \{a \in \mathbb{Z}_n^* \mid \left(\frac{a}{n}\right) = a^{(n-1)/2} \pmod{n}\}$$

   (a) Prove that $G(n)$ is a subgroup of $\mathbb{Z}_n^*$.

   (b) Suppose $n = p^\ell q$, where p and q are odd, p is prime, $\ell \geq 2$, and $\gcd(p, q) = 1$. Let $a = 1 + p^{\ell-1}q$. Prove that

   $$\left(\frac{a}{n}\right) \neq a^{(n-1)/2} \pmod{n}$$

   Hint: Use the binomial theorem to compute $a^{(n-1)/2} \pmod{n}$.

   (c) Suppose $n = p_1 \cdots p_s$, where the p_i's are distinct odd primes. Suppose $a \equiv u \pmod{p_1}$ and $a \equiv 1 \pmod{p_2 p_3 \cdots p_s}$, where u is

a quadratic non-residue modulo p_1 (note that such an a exists by the Chinese Remainder Theorem). Prove that

$$\left(\frac{a}{n}\right) = -1 \pmod{n},$$

but

$$a^{(n-1)/2} \pmod{n} \equiv 1 \pmod{p_2 p_3 \cdots p_s},$$

so

$$a^{(n-1)/2} \pmod{n} \neq -1 \pmod{n}.$$

(d) If n is odd and composite, prove that $|G(n)| \leq (n-1)/2$, and conclude that the error probability is at most $(1/2)^k$.

(Problem 5.22 in CTP.)

4. Show all steps in one execution of the **for** loop in the Solovay-Strassen Primality Test, checking if 35 is prime. Assume that the random integer a chosen is 19.