

Cryptology – 2019 – Lecture 11

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.

Lecture, October 10

We covered Rabin's encryption scheme (subsection 15.1.1) and covered subsection 2.2. We also covered sections 1.3.5, 1.3.7 and 1.3.8 from chapter 1. More slides can be found on course homepage, saying related to RSA.

Lecture, October 22

We will cover subsections 1.3.6 and 1.3.9 and cover section 2.1

Lecture, October 29

We will continue with chapters 2 and 15.

Problem session October 31

We will finish the problems not finished on October 28. If there is time, we will start on the following:

1. A *Carmichael number* is a composite integer n such that for all $x \in \mathbb{Z}_n^*$, $x^{n-1} \equiv 1 \pmod{n}$.

- (a) Explain why the existence of Carmichael numbers (there are in fact infinitely many of them) make primality testing more difficult.
 - (b) Explain why Carmichael numbers are easy to factor using intermediate calculations from the Miller–Rabin primality test.
 - (c) Show that 561 is a Carmichael number. Try to do it without explicitly checking all elements of \mathbb{Z}_{561}^* .
2. Find a primitive element (generator) in the multiplicative group modulo 103 (\mathbb{Z}_{103}^*) and show that it is a primitive element.
3. Suppose that two parties, Alice and Bob, possess integers p_A, q_A and p_B, q_B , respectively, and they have used a protocol to compute an $N = (p_A + p_B)(q_A + q_B)$, without revealing their own integers to the other party. Now they use the following protocol (repeated many times) to check that N is the product of two primes $p \equiv 3 \pmod{4}$ and $q \equiv 3 \pmod{4}$. Suppose that $N \equiv 1 \pmod{4}$; otherwise they should reject the values.
- (a) Bob and Alice let $g = N - 1$. Alice computes $v_A = g^{(N-p_A-q_A+1)/4} \pmod{N}$, and Bob $v_B = g^{-(p_B+q_B)/4} \pmod{N}$. They exchange these values and check that $v_A v_B = -1 \pmod{N}$. If this fails, they reject N . Also if they cannot do the divisions by 4, they reject N .
 - (b) Bob and Alice agree on a random $g \in \mathbb{Z}_N^*$, choosing values until the Jacobi symbol $\left(\frac{g}{N}\right) = 1$. (It could just be one player choosing g , but the other should check, too.)
 - (c) Alice computes $v_A = g^{(N-p_A-q_A+1)/4} \pmod{N}$, and Bob $v_B = g^{-(p_B+q_B)/4} \pmod{N}$. They exchange these values and check that $v_A v_B = \pm 1 \pmod{N}$. If this fails, then both parties output that N is not the product of two primes of the correct form. Otherwise, they output that N probably is the product of two primes of the correct form.
 - i. Consider which values of p_A, p_B, q_A , and q_B work modulo 4.
 - ii. Suppose that $N = pq$, where p and q are both prime, $p \equiv 1 \pmod{4}$, $q \equiv 1 \pmod{4}$, $p = p_A + p_B$, and $q = q_A + q_B$. Will N pass this test? What does this say about the probability of

Alice and Bob incorrectly outputting that N is the product of two primes of the correct form?

- iii. Suppose that q is a product of at least two distinct primes, but p is prime. What are some cases where N would be rejected? Consider the Solovay-Strassen primality test.