Homework 10 in Cryptography I

Prof. Dr. Rudolf Mathar, Michael Reyer, Henning Maier

07.07.2011

Exercise 32. We consider Wilsons' primality-criterion:

$$\text{An integer } n > 1 \text{ is prime} \Leftrightarrow (n-1)! \equiv -1 (\operatorname{mod} n).$$

(a) Prove Wilsons' primality-criterion (both "$\Rightarrow$" and "$\Leftarrow$").

(b) Check if 29 is a prime number by using the criterion above.

(c) Is it useful in practical applications?

Exercise 33. We examine the properties of the discrete logarithm.

(a) Compute the discrete logarithm of 18 and 1 in the group $\mathbb{Z}_{79}^*$ with generator 3 (by trial and error if necessary).

(b) How many trials would be necessary to determine the discrete logarithm in the worst case?

Exercise 34. Prove Proposition 7.5 from the lecture, which gives a possibility to generate a primitve element modulo n:

Let $p > 3$ be prime, $p - 1 = \prod_{i=1}^{k} p_i^{t_i}$ the prime factorization of $p - 1$. Then $a \in \mathbb{Z}_p^*$ is a primitive element modulo $p \Leftrightarrow a^{\frac{p-1}{p_i}} \not\equiv 1 \pmod{p}$ for all $i \in \{1, \ldots, k\}$.

Exercise 35. Alice and Bob perform a Diffie-Hellman key exchange with prime $p = 107$ and primitive element $a = 2$. Alice chooses the random number $x_A = 66$ and Bob the random number $x_B = 33$.

(a) Calculate the shared key for both users.

(b) Show that also $b = 103$ is a primitive element mod p.