Homework 11 in Cryptography I

Prof. Dr. Rudolf Mathar, Wolfgang Meyer zu Bergsten, Steven Corroy

19.01.2010

Exercise 31.

Prove Wilson's primality-criterion:

n is a prime number if ond only if

$$(n-1)! \equiv -1 (\mathrm{mod}\, n).$$

Use this to show that 29 is a prime number. Why might the criterion be useless in practical applications?

Exercise 32.

Solve the following system of linear congruences using the Chinese Remainder Theorem and compute the smallest positive solution:

$$\begin{aligned} x &\equiv 17 \pmod{29} \\ x &\equiv 13 \pmod{15} \\ x &\equiv 5 \pmod{16} \\ x &\equiv 8 \pmod{23}. \end{aligned}$$

Exercise 33.

You know that n is a product of two primes.

a) Factor $n = 4386607$ knowing that $\varphi(n) = 4382136$.

b) Factor $n = 9990991$ knowing that $9040420^2 \equiv 1 \pmod{n}$.