Homework 10 in Advanced Methods of Cryptography

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

24.01.2014

Exercise 28. A uniformly distributed message $m \in \{1, \dots, n-1\}$ with $n = p\,q$ with two primes $p \neq q$ is encrypted using the RSA-algorithm with public key (n, e).

(a) Show that it is possible to compute the secret key d if m and n are not coprime, i.e., if $p \mid m$ or $q \mid m$.

(b) Calculate the probability for m and n having common divisors.

(c) How large is the probability of (b) roughly, if n has 1024 bits and the primes p and q are approximately of same size ($p, q \approx \sqrt{n}$).

Exercise 29. Alice is using the ElGamal encryption system for encrypting the messages m_1 and m_2. The generated cryptograms are

$$\mathbf{C}_1 = (1537, 2192) \text{ and } \mathbf{C}_2 = (1537, 1393).$$

The public key of Alice is $(p, a, y) = (3571, 2, 2905)$.

(a) Verify that the public key is valid.

(b) What did Alice do wrong?

(c) The first message is given as $m_1 = 567$. Determine the message m_2.

Exercise 30. Prove Euler's criterion: Let $p > 2$ be prime, then

$$c \in \mathbb{Z}_p^* \text{ is a quadratic residue modulo } p \Leftrightarrow c^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$