Exercise 11 in Cryptography

Prof. Dr. Rudolf Mathar, Henning Maier, Jose Angel Leon Calvo

2015-07-16

Problem 36. *(baby-step giant-step algorithm)* Consider the following algorithm to compute the discrete logarithm:

Algorithm 1 Baby-step Giant-step Algorithm

Require: p prime, α is a primitive element mod p, $\beta = \alpha^x \mod p$ for an unknown $x \in \{0, \ldots, p-1\}$

Ensure: $x = \log_\alpha \beta$,

(1) $m \leftarrow \lceil \sqrt{p} \rceil$

(2) Compute a table of *baby-steps* $b_j = \alpha^j \mod p$ for all indices $j \in \mathbb{Z}$ with $0 \leq j < m$.

(3) Compute a table of *giant-steps* $g_i = \beta\alpha^{-im} \mod p$ for indices $i \in \mathbb{Z}$ with $0 \leq i < m$, until you find a pair (i, j) such that $b_j = g_i$ holds.

return $x \equiv mi + j \mod p - 1$.

a) Prove that the given algorithm calculates the discrete logarithm.

b) Why is α a primitive element modulo p?

c) Compute the discrete log for $\alpha^x \equiv \beta \mod p$ with $\alpha = 3$, $\beta = 13$ and $p = 29$ using the given algorithm.

Remark: The *ceiling-function* is defined as $\lceil x \rceil = \min\{k \in \mathbb{Z} \mid k \geq x\}$.

Problem 37. *(Weak public-key cryptosystem)* Consider the following insecure cryptosystem: Alice secretly chooses four integers $a, b, a', b' \in \mathbb{N}$, with $a > 1, b > 1$, and computes:

$$M = ab - 1, \qquad e = a'M + a, \qquad d = b'M + b, \qquad n = \frac{ed - 1}{M}.$$

Her public key is (n, e), her private key is d. To encrypt a plaintext m, Bob uses the map $c = em \bmod n$. Alice decrypts the ciphertext received from Bob by $m = cd \bmod n$.

a) Verify that the decryption operation recovers the plaintext.

b) How can the Euclidean algorithm be applied to break the cryptosystem.

Problem 38. (*How not to use the ElGamal cryptoystem*) Alice and Bob are using the ElGamal cryptosystem. The public key of Alice is $(p, a, y) = (3571, 2, 2905)$. Bob encrypts the messages m_1 and m_2 as

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

a) Show that the public key is valid.

b) What did Bob do wrong?

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