Cryptography

Prof. Dr. Joachim von zur Gathen, Konstantin Ziegler

9 Assignment: The ElGamal Signature Scheme and the Schnorr Signature Scheme

(Due: Thursday, 21 January 2010, 23^{59})

On this assignment you will get some hands-on experience with the ElGamal Signature Scheme.

Let $p = 2^{28} + 3$ and $g = 3$ a generator of $G = \mathbb{Z}_p^\times = \{1, \ldots, p-1\}$. The injective encoding function $G \to \mathbb{Z}_{p-1} = \{0, \ldots, p-2\}, x \mapsto x^\star$ is given by

$$x^\star = \begin{cases} 0 & \text{for } x = p-1 \\ x & \text{else.} \end{cases}$$

Our message m will be the first four letters of your given name. Add an exclamation mark, if your given name has less than four letters and mind the capitalization.

Exercise 9.1. (1 point) Look up the 7-bit ASCII encodings for each letter and concatenate them for the 28-bit number m.

Let us take the role of Alice and let $a = 100$ be our secret key.

Exercise 9.2.
1. (4 points) Choose a random session key k (of at least three digits) and generate a signature for your message m.
2. (2 points) What is your public key? Use it to verify the signature you just produced.

In the lecture you encountered a clever method to produce many triples (m, x, b), such that (x, b) is a valid signature for m.

Exercise 9.3.
1. (3 points) Given the public key $y = 45\,193\,911$, produce three different messages with valid signatures.

2. (2 points) Translate your messages back into four-letter ASCII words.

This attack allows EVE to produce many signed messages. But she still cannot sign a given one. Things are different if additional information is provided.

Exercise 9.4. 1. (2 points) ALICE sends the signed message

$$(m, x, b) = (500, 10\,296\,631, 248\,708\,422).$$

By accident the secret session key $k = 787$ is revealed. Compute ALICE's secret key a.

2. (3 points) After this experience, ALICE changes her secret key and the public version is now $y = 138\,309\,740$. Unfortunately a bug/feature in the random number generator revealed that the same value for k was generated twice in a row. This is known for the signed messages

$$(501, 32\,067\,479, 51\,030\,675)$$

and

$$(502, 32\,067\,479, 60\,076\,072)$$

Compute ALICE's secret key.

Exercise 9.5 (Schnorr signatures (DSA))**.** Take a 10-bit prime d and find a 29-bit prime p, s.t. $d \mid p - 1$.

1. (3 points) Give an element $g \in G = \mathbb{Z}_p^\times = \{1, \ldots, p-1\}$ of order d. Describe how you found it.

2. (3 points) Produce Schnorr signatures for the three messages $m = 500, 501, 502$ given above and compare their length to the length of the respective ElGamal signatures.

3. (3 points) Which information is public in this signature scheme and how does BOB check the validity of the signatures. Do it for the signatures produced in 2.