Cryptography

Prof. Dr. Joachim von zur Gathen, Konstantin Ziegler

10. Assignment: The ElGamal Signature Scheme
(Due: Wednesday, 21 January 2009, 13:40, b-it bitmax)

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 \( G = \mathbb{Z}_p^\times \). The injective encoding function \( G \to \mathbb{Z}_{p-1}, x \mapsto x^* \) is given by:

\[
x^* = \begin{cases} 
0 & \text{for } x = p - 1 \\
x & \text{else}.
\end{cases}
\]

Our message \( m \) will be the first four letters of your given name. Mind the capitalization.

Exercise 10.1. (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 10.2. (i) (4 points) Choose a random session key \( k \) (of at least three digits) and generate a signature for your message \( m \).

(ii) (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 10.3. (i) (3 points) Given the public key \( y = 45\,193\,911 \), produce three different messages with valid signatures.

(ii) (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 10.4.  (i) (2 points) Alice sends the signed message

\[(m, x, b) = (500, 10296631, 248708422).\]

By accident the secret session key \(k = 787\) is revealed. Compute Alice’s secret key \(a\).

(ii) (3 points) After this experience, Alice changes her secret key and the public version is now \(y = 138309740\). 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

\[(501, 32067479, 51030675)\]

and

\[(502, 32067479, 60076072)\]

Compute Alice’s secret key.