Homework sheet 6, due 11 January 2024 at 13:30

Make sure to justify your answers in detail and to give clear arguments. Document all steps, in particular of algorithms; it is not sufficient to state the correct result without the explanation. If the problem statement asks for usage of a particular algorithm other solutions will not be accepted even if they give the correct result.
Submit your homework (pdf and code, if any) by encrypted and signed email to all TAs (and not to Tanja). Do not forget to attach your public key and the public key of anybody you put in cc. Make sure to have different members of your group handle the submission. This is the last homework sheet, hence your last chance to fulfil the requirement that you must at least once send an encrypted and signed homework to the TAs.

1. Alice is a web merchant offering encrypted connections using semi-static DH in $\mathbb{F}_{103}^*$ in the subgroup of order $\ell = 51$ generated by 2.

   For this exercise you should not use your computer for more functions than a pocket calculator offers you; in particular make sure to give full details when computing inverses and exponentiations and document all steps.

   (a) Verify that 2 has order 51, justify your computation and try to use not too many multiplications and squarings. 2 points

   (b) Alice's public key is $h_A = 30$. Use the baby-step giant-step algorithm to compute an integer a between 0 and 50 so that $g^a = h_A$, i.e. compute the discrete logarithm of Alice's key. Solutions using brute-force search for a will not be accepted. Make sure to verify your result by computing g^a.
   Remember that BSGS expects you to make a table of all baby steps so those should be written out as well as any giant step you check against the table. The table is small enough, you need not sort it. 7 points

2. NSA cryptographer Rick Proto noticed independently of Diffie and Hellman that exponentiation in finite fields is easy while computing discrete logarithms can be hard. The scheme he came up with requires several interactions between the sender and receiver.

   The system parameter is a large prime p.

   To send message $m < p$ to user Bob, Alice chooses a random integer $A < p$ with $\gcd(A, p-1) = 1$ and computes $a \equiv A^{-1} \bmod (p-1)$. She then computes $c_1 \equiv m^A \bmod p$ and sends c_1 to Bob.

   Bob chooses a random integer $B < p$ with $\gcd(B, p-1) = 1$ and computes $b \equiv B^{-1} \bmod (p-1)$. Bob then computes $c_2 \equiv c_1^B \bmod p$ and sends c_2 to Alice.

   Alice then computes $c_3 \equiv c_2^a \bmod p$ and sends c_3 to Bob.

   Bob decrypts the message by computing $m' \equiv c_3^b \bmod p$.

(a) Let $p = 23$. Execute one run of the protocol in which Alice wants to send $m = 2$ and picks $A = 5$ and computes $a = 5^{-1} \equiv 9 \bmod 22$, and Bob picks $B = 3$ and computes $b = 3^{-1} \equiv 15 \bmod 22$. Compute c_1, c_2, c_3, and m'. 5 points

(b) Explain why the system works, i.e., explain why $m' = m$.

3 points

(c) Attacker Eve observes the conversations between Alice and Bob and obtains c_1, c_2, and c_3; she also knows the system parameter p. Assume that Eve can compute discrete logarithms in $\mathbb{F}_p^*$. Show how she can obtain m from the observed ciphertexts.
Note that you need to show where to find a DLP in this system and how to use the solution. 3 points