Homework sheet 4, due 09 January 2020 at 13:30
Note, there are no lectues or exercise sessions on that day

Submit your homework (text and code) by encrypted and signed email to all three TAs. Make sure to test early whether your encryption program can handle Jonathan's key and if not, contact him for an alternative. 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. Do not forget to attach your public key if we don't have it yet.

1. Users A, B, C, D, and E are friends of S. They have public keys $(e_A, n_A) = (5, 62857), (e_B, n_B) = (5, 64541), (e_C, n_C) = (5, 69799), (e_D, n_D) = (5, 89179)$, and $(e_E, n_E) = (5, 82583)$. You know that S sends the same message to all of them and you observe the ciphertexts $c_A = 11529, c_B = 60248, c_C = 27504, c_D = 43997$, and $c_E = 44926$. Compute the message.
   For this exercise use your computer as a calculator with arbitrary precision – but do not use built in functions for computing CRT or inverses. [8 points]

2. Alice has RSA public key $(e, n) = (3, 262063)$. You capture two messages $c_1 = 156417$ and $c_2 = 6125$ to her and know that the corresponding plaintexts are related as $m_2 = 7m_1 + 19$. Compute the messages m_1 and m_2. [3 points]

3. 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.

   (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. [7 points]