Homework sheet 5, due 21 December 2023 at 13:30

There is no exercise session on the 21st but homework is still due on that day so that you can get the feedback in time.
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. Do not forget to attach your public key and the public keys of anybody you put in cc. Make sure to have different members of your group handle the submission.
As always, make sure to document all steps and submit all code you used.

1. For this exercise do not use more functions from your computer than addition, subtraction, multiplication, and division. This means writing out steps of XGCD in full. Perform RSA key generation for primes $p = 127$ and $q = 149$ and exponent $e = 17$. 4 points

2. 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 solutions via factoring n are not accepted. You need to document all steps for two full modular inversions, i.e., show all the steps of the XGCD computation. The others can be done using a computer algebra system such as sage and you only need to document the functions you used in the computation. You do need to show in full how you use these modular inverses to compute the solution (in code and with results). For the integer root computation you can again use your computer but need to show what function you used. 10 points

3. 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

4. For this exercise you can use a computer-algebra system but solutions via factoring n are not accepted.
   The ciphertext $c = 12609836836808423540662900683841941376$ is the RSA PKCS#1 v1.5 encryption to a user with public key $(n, e) = (166881708320858625209862155717361008839, 65537)$ and private key (n, d) with $d = 133783939964746499007904287583965323393$.

   Decrypt c to get pad(m) and show how you obtain m.
   Note that the last part requires hexadecimal representation and the answer expects

m in hexadecimal.

Hint: If you are using Sage you can get the hexadecimal representation using `m.str(16)` for some integer variable `m`. $\boxed{\text{3 points}}$