Homework sheet 5, due 23 December 2021 at 13:30

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 key 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 you need to document 2 full inversions showing all steps of XGCD and you need to show the detailed steps for how you solve the CRT computation. 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.
   The ciphertext $c = 25050963005650062524319676466232736 2$ is the RSA PKCS#1 v1.5 encryption to a user with public key $(n, e) = (66461399789245810650782545965010557 1, 65537)$ and private key $(n, d) = (66461399789245810650782545965010557 1, 43853956886737962193934720629997440 1)$.

   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. 3 points