Homework sheet 1, due 8 December 2016 at 13:45

If you use sage for your computations note that you can compute modulo a polynomial using %. In Pari the function `Mod` also works for polynomials.

For the RSA exercises, i.e. exercises 2 and 3, 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 exponentitations.

Submit your homework by encrypted and signed email. Do not forget to attach your public key and the public key of anybody you put in cc.

1. For both of the following sequences

$$s_{k+8} = s_{k+5} + s_{k+2} + s_{k+1} + s_k \qquad s_{k+6} = s_{k+3} + s_k$$

   do the following subexercises:

   (a) Draw the LFSR corresponding this sequence.

   (b) State the associated matrix corresponding to the LFSR state update and compute its order.

   (c) State the characteristic polynomial f and compute its factorization.

   (d) For each of the factors of f compute the order.

   (e) What is the longest period generated by this LFSR? Make sure to justify your answer.

   (f) State the lengths of all subsequences so that each state of n bits appears exactly once.

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 arbitray precision – but do not use built in functions for computing CRT.

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.