Homework sheet 1, due 28 November 2019 at 13:30

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.

Submit your homework 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.

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. The points are for both LFSRs.

(a) Draw the LFSR corresponding this sequence. [2 points]

(b) State the associated matrix corresponding to the LFSR state update and compute its order. [5 points]

(c) State the characteristic polynomial f and compute its factorization. [3 points]

(d) For each of the factors of f compute the order. [4 points]

(e) What is the longest period generated by this LFSR? Make sure to justify your answer. [3 points]

(f) State the lengths of all subsequences so that each state of n bits appears exactly once. [3 points]