Homework sheet 2, due 26 November 2026 at 13:30

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.
Include the code you write and state what the answers are. Submit Sage or Python code as `.py` or `.sage` files or as Jupyter notebook. Include comments to explain what you are doing.
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 4 TAs. Do not include Tanja.
Put your teammates in cc and do not forget to attach your public key and those of your teammates, else the TAs cannot reply to you.

1. For both of the following sequences

$$s_{j+8} = s_{j+5} + s_{j+2} + s_{j+1} + s_j \qquad s_{j+6} = s_{j+3} + s_j$$

do the following subexercises. The points are for both LFSRs.

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

   (b) State the state-update matrix and compute its order. [5 points]

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

   (d) For each of the factors of P 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]