T: Please let me know on the zulio chat before class what topics you would like to see covered so that I can prepare some slides on the topics and not just have the same slides as in class.

Also, please engage in the discussion about the exam format (on Zulip).

Extra reading(non compulsory but recommended):
A tale of two sieves: https://www.ams.org/notices/199612/pomerance.pdf

Question 1: Where can I find the solutions to the old exams on the crypto page?
A1: They won't be posted, solve them yourself and if you want to check your answers, send an email to Tanja and she will give you feedback.
T: please check computational exercises yourself with Sage or Pari.

Question 2: What is the difference between 'schoolbook RSA' and 'normal RSA'?
A2: schoolbook RSA is what we have seen so far and normal RSA is with padding, e.g OAEP. See also the notes from Jonathan's session on 8 Sep.

Question 3: In the Coppersmith method we saw for something like 'thepasswordisswordfish' how to get the 'swordfish' part. But this only works if the password is mentioned at the end of the message, doesnt it? If m = 'swordfishistodayspassword' than it wouldnt work?
A3 : You can also transpose the method, i the end is known then you're missing x with (x*2^(1024-86)+a)^3-c =0 mod n (if top 86 bits are missing)

Question 4 : Do we have to be able to use LLL since we didnt go into how it works?
A4 : Yes. You can use it as a black box, knowing that it will find integer linear combinations of the rows which are small (more precisely, have snall Euclidean norm).

Question 5 : I don't fully understand what the differences and befefits of the quadratic sieve are with respect to Dixon's in general, can you explain this?
A5 : Dixon's method of random squares uses random a_i to find relations, the Q-sieve has the benefit that you can sieve -- which helps for finding small factors (it's faster that trial division). The quadratic sieve and the number-field sieve additionally have the benefit of generating smaller numbers that need to be factored, thus increasing the smoothness probability.

Question 6 : I understand how to use the rational (Q) sieve, but why is it better?
A6 : Same as Q5

Question 7 : How much should we understand about the lattice RSA attacks? Because I don't really understand why it works.

A7 : See Q4 for the LLL part. You should understand the basic setup -- that each row has the solution as the root and that thus any solution has the root as a solution. In the lecture for next week I have a theorem which hopefully sheds more light on this; I had hoped to present that today but then the first part of the lecture (+exam discussions) took too long.