Homework 9

due on Friday, March 9

Read sections 8.2, 8.3 in the book. Solve problems 7, 8, 12 to section 8.2 and 14a) to section 8.3.

Remark. In problem 8, both the encryption and decryption is done using blocks of length 2 (i.e each block codes 2 letters). This is incorrect in general when $m = 2419$ but works fine if letters Y and Z do not appear in the text. If we had a block YT for example, we would assign to it 2419 then encipher it into some number by raising it to power 13 and taking the result modulo 2419. This would yield 0000 and then the deciphered number would be 0000 too which would mean AA. In the encryption part of problem 8 we have YS, which corresponds to 2418, which is still fine. To get the RSA work all the numbers which we encipher need to be smaller than the modulus m. Only then we can recover them in the decryption process.