Homework 2 for 01410, 2019 (8 points)

Exercise 2.1 (4 points) Let $n = pq$, where p and q are distinct, odd primes. In RSA the encryption and decryption exponents are chosen such that their product is congruent to 1 modulo $\phi(n)$, where $\phi(n) = (p-1)(q-1)$ (Euler). Let $\psi(n) = \text{lcm}(p-1, q-1)$, so

$$\psi(n) = \frac{(p-1)(q-1)}{\gcd(p-1, q-1)}.$$

Let e be an integer such that $\gcd(e, \psi(n)) = 1$, compute $\tilde{d}$ such that $e\tilde{d} \equiv 1 \bmod \psi(n)$.

1. Show that $m^{e\tilde{d}} \equiv m \bmod n$ for all $m \in \mathbb{Z}_n$.
2. Let $p = 881, q = 461$, and let $n = pq$. Show that $e = 3$ is an allowed encryption exponent for an RSA encryption system with modulus n. → e must have multiplicative inv mod n ⇒ $e \in \mathbb{Z}_{\phi(n)}^*$ $\gcd(\phi(n), e) = 1$
3. Find d_1 such that $ed_1 \equiv 1 \bmod \phi(n)$.
4. Find d_2 such that $ed_2 \equiv 1 \bmod \psi(n)$.
5. Discuss the advantages of using d_2 instead of d_1.

Exercise 2.2 (4 points).
This exercise is used to demonstrate how good the Miller-Rabin test is to find primes. In the first exercise we determine the exact number of prime numbers in a certain interval. Then we use Miller-Rabin with k iterations for different values of k to determine the number of primes in the interval.

a. Let s be the number of prime numbers between 25 and 25000. Find s using trial division.

b. Implement the Miller-Rabin algorithm with k iterations.

c. Use your Miller-Rabin implementation to determine the number of (probable) prime numbers between 25 and 25000 for $k = 1, 2, 3, ...$ What is the smallest number of iterations needed such that one gets the correct answer, s ?

What you should do

- Write the solutions to the exercises in one document. Explain how you arrived at the solution!
- Upload your document via the "Assignments" link (DK: "Opgaver") in DTU Inside.
- Deadline: March 26, 2019, at noon 12.00 (Denmark time).
- You are encouraged to work in groups of at most two students. In this case, make a group handin.
- The format of your document should be PDF.