IDATT2503 - 2024 - Assignment 4

Problem 1

a) Alice wants to set up her RSA encryption with private key (n, d) with $n = pq$, using two primes p and q, and private key $d = 3$. She chooses $p = 1283$, but wonders which of the following choices for q she should use (NB! They are all prime numbers):

$$1307,\ 1879,\ 2003,\ 2027$$

Explain why she should use $q = 2027$ for the system to work and to be most secure. For the weak choices of q, name an effektive attack to factorize n (of course, these numbers are far too small to be secure, so consider the security in relative terms.)

b) Find the corresponding public key e using the extended Euclidean algorithm. Write a program to do the calculation. In the lectures I have written the algorithm in a way that is easier to understand, but it may be easier to implement it using another setup like explained in `https://en.wikipedia.org/wiki/Extended_Euclidean_algorithm`. Here one performs the backward part in parallell with the forward part.

c) Encrypt the message 111 using repeated squaring. Implement the algorithm yourself. There are different variants of the method, choose one you prefer.

Problem 2

a) Show that encryption in RSA has the following property:

$$e_K(x_1)e_K(x_2) \mod n = e_K(x_1x_2) \mod n$$

b) Show how RSA is vulnerable to **chosen cipher text attack**: For ciphertext y, then Eva can choose some $r \not\equiv 1 \bmod n$, and construct $y' = y \cdot r^e$. If she then knows the decryption $x' = d_K(y')$, show how she can calculate $x = d_K(y)$. (Hint: She can also calculate $r^{-1} \bmod n$)

Problem 3

Factorize $n = 275621053$. You can assume that $n = pq$, where $p - q$ is relatively small. Show your calculation steps.

Problem 4

Alice and Bob want to have an common key using Diffie-Hellmann key exchange. They agree on using the prime 101, and base $n = 3$. Alice choosed her secret $a = 33$, and Bob chooses $b = 65$.

a) Write a program that prints out all the powers 3^i for $i = 1, ..., 100$. Do the same for 5^i. What is a major difference between these two sequences?

b) Find their common key.

Problem 5

a) Shanks algorithm is used to find discrete logarithms. Implement the algorithm.

b) Use your algorithm to find the exponent x so that

$$5^x \equiv 144363234 \mod 1000000007$$