Assignment: RSA factoring

artur.garcia@bsc.es

January 2024

In this assignment you have to perform an execution of the full RSA [1] method. To do this, you have to prepare and submit a set of code functions in a notebook format, and send them before the exam.

RSA is formed by the *encrypt* and *decrypt* functions. To start, you need to create a pair of private-public keys, and use them in these functions. Additionally, this assignment asks you to explore the limitations of current factoring algorithms visualizing the complexity as the number grow. Finally, you have to use a Quantum register to perform the factoring operation.

Your analysis, in the form of a notebook, should include the following sections:

1. A code generation routine. This is similar to the one you have found in Xanadu´s codebook.
2. A detailed implementation of the *encrypt* and *decrypt* functions for arbitrary numbers., with some examples.
3. A graph showing the running time of factoring numbers of growing size. Identify hard and easy instances.
4. Using the Quantum Fourier routine over a simple Quantum state (you do not need to create Modular exponentiation routines, use the shortcut method as we discussed in class), show how to crack a simple key of 6 bits.

References

[1] https://ntietz.com/blog/rsa-deceptively-simple/