

I'm a student in the Bachelor's Programme in Science (BSc) degree. I'll be using the Python programming language to write my code. I'm also knowledgeable about R coding and SQL, having used both for my courses. I'll be using the RSA algorithm, also known as the Rivest-Shamir-Adleman public-key cryptography algorithm. One of the main data structures used in the RSA is the Array since most encrypted and decrypted messages are represented as byte arrays.

The aim of the project is to ensure secure data transmission from the sender to the receiver as seen in many aspects of our life due to the highly digitised society we live in. The input into the code would be a text that let's say person A wants to send person B. The algorithm aims to convert the text into decimal numbers which are then converted to binary codes and encrypted with a private key. The message is then sent by person A through the server/secure/insecure channel and then decrypted using person B's private key to use Euler's totient formula and get the decimal numbers and put together the message back to its original state.

From one of the videos which I've seen on YouTube explaining the RSA algorithm in detail, what I understood the time complexity to be (due to use of modular arithmetic) is $O(\log e \cdot n^2)$ where n is the number of bits when given two numbers, for example p and q where p is n bits and q is m bits and $n \geq m$. However, another website and some other sites on Google as well as on Reddit, many said that the time complexity would be $O(n^2)$ due to the multiplication and inversion arithmetic operations.

I intend on using Google (website links that come up as well as the AI overview); Copilot and or ChatGPT to brush up and debug my code if I can't do it myself; videos on YouTube.