1 RSA Encryption Scheme

In our project, we chose to implement the RSA public encryption scheme. This scheme has been around since the 1970s when it was invented by Ron Rivest, Adi Shamir, and Leonard Adleman. The general idea of the scheme is to use the factorization of a large composite integer as a trapdoor function in order to be able to reverse encryption that was done via modular exponentiation.

1.1 Background Math

This encryption scheme relies heavily on modular arithmetic, notably exponentiation.