Perhaps the most famous public-key cryptosystems algorithm is the RSA (Rivest-Shamir-Adleman) algorithm. The RSA algorithm is a public key cryptosystem that's used to encrypt communication between two nodes of a network. It takes advantage of the difficulty of finding the prime factorization of large numbers. It was developed and published by MIT Faculty Ronald Rivest, Adi Shamir, and Leonard Adleman in '77.

We begin the encryption process by selecting two large primes, p and q, and calculating their product, n = pq. Next, we pick a random integer e relatively prime to \totient{n}. The public key (the published numbers everyone has access to) consists of (n, e), whereas p and q are kept a secret.

To encrypt a message, we execute the following steps:

1. Convert message to numerical digits, e.g., a = 01, b = 02, …, z = 26, blank = 27, etc.
2. Break the converted message into blocks less than n.
3. For each block B, encrypted block C is formed such that:

$$C \equiv B^e \pmod{n}$$

To decrypt an already encrypted message, apply the following steps:

1. Calculate an integer d such that $de \equiv 1 \pmod{\totient(n)}$ using the euclidean algorithm.
2. Convert back using $B \equiv C^d \pmod{n}$.

The decryption process described above makes use of Euler's theorem. Some decryption algorithms make use of other mathematical theorems of relation, including the Chinese Remainder Theorem.

The RSA Algorithm, while nearly unbreakable, isn't as untouchable as originally thought, as the example number n = pq that Rivest, Shamir, and Adleman published as a challenge in '77 was broken in '94. This proves that as we progress farther into the future until a new, more effective encryption algorithm is developed, the best we can do to keep communications secure is to increase the primes p and q (and thus n) in order to make prime factorization as difficult as possible.

The RSA algorithm's application is one of the most valuable encryption methods of communication. It's used regularly in web browsers, chat applications, email, VPNs, etc. This section of our project will include creating a computer simulation of a scaled-down version of the RSA algorithm, as well as explore different applications.