A User-friendly Computer Program Implementation of the RSA Public-key Encryption Algorithm in Python 3.3

Seo, Yun Ha

For many centuries, ways of delivering secret messages that only the sender and receiver could understand have been created and used, but many were ineffective. First, there were eavesdroppers and interceptors, who stole messages between the sender and receiver, thus putting the confidentiality of the message in jeopardy. In an attempt to lower that risk, an encoding method of an open, one-way system was created: the RSA encryption algorithm. The algorithm makes use of the characteristics of prime numbers to create a trap-door problem – it is easy to multiply prime numbers but difficult to factor the result of prime numbers. Computer programming language is rapidly becoming a global language. In the Northern Mariana Islands, the place I come from, computer programming is considered a very foreign activity, with majority of the population unfamiliar with such things. Thus, my project highlights a total of four programs that were created through Python and implement the RSA algorithm. The encrypting programs ask you for the values of the variables you desire and the message you want to encrypt. It then shoots out a list of numbers, which becomes the encrypted message. The decrypting programs, asks for the values of the variables you previously chose and the list of encrypted message you want to decrypt. The program will shoot out the message you originally put in to encrypt. A pair of the program created focuses on making the easiest-to-understand code, while the other pair focuses on creating the shortest code.