Group 7

Assembly RSA Encryption

Professor Bell

Requirement Specifications

This problem is clear and concise, we must create a program that takes in a string and uses RSA public key cryptography using the RSA Algorithms. There needs to be a private key and public key, These two keys form a pair. This type of specification aids the multi-prime RSA, meaning the modulus contains more than two prime factors. This helps the functionality for lower computational affects. In the encryption process it produces a ciphertext with control from the public key, the decryption process is under control of the private key. No high level languages were used, all code is developed using assembler. First create a main menu function, this function will have a menu to ask the user to decrypt a message using a hex string or encrypt a message. The encryption process will happen in the main using a square root process, and RSA methods.