REPORT
ENCRYPTION – Decryption on Cryptography for [RSA]

L&T Technology Services

SUMBITTED BY,
SHALINI VISWANATH S
2^{ND} APRIL - 2022

Document History:

INTRODUCTION:

RSA Algorithm is used to encrypt and decrypt data in modern computer systems and other electronic devices. RSA algorithm is an asymmetric cryptographic algorithm as it creates 2 different keys for the purpose of encryption and decryption. It is public key cryptography as one of the keys involved is made public. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman who first publicly described it in 1978.

RSA makes use of prime numbers (arbitrary large numbers) to function. The public key is made available publicly (means to everyone) and only the person having the private key with them can decrypt the original message.

OBJECTIVE:

a) To build a system that can receive input freom the user and generate automatically output in easy way and short time.

b) To build an algorithm which detects the security of the message all times round.

c) Combination of Ciphering Algorithm and Rivest Shamir Adleman Algorithm for Securing Document Files and Text Messages

d) To build Confidentiality, Authenticity, Integrity of information

e) To protect the data against corruption

BENEFITS:

Cryptography is an essential information security tool. It provides the four most basic services of information security −

`Confidentiality` − Encryption technique can guard the information and communication from unauthorized revelation and access of information.

`Authentication` − The cryptographic techniques such as MAC and digital signatures can protect information against spoofing and forgeries.

`Data Integrity` − The cryptographic hash functions are playing vital role in assuring the users about the data integrity.

`Non-repudiation` − The digital signature provides the non-repudiation service to guard against the dispute that may arise due to denial of passing message by the sender.

All these fundamental services offered by cryptography has enabled the conduct of business over the networks using the computer systems in extremely efficient and effective manner.

OPPORTUNITIES:

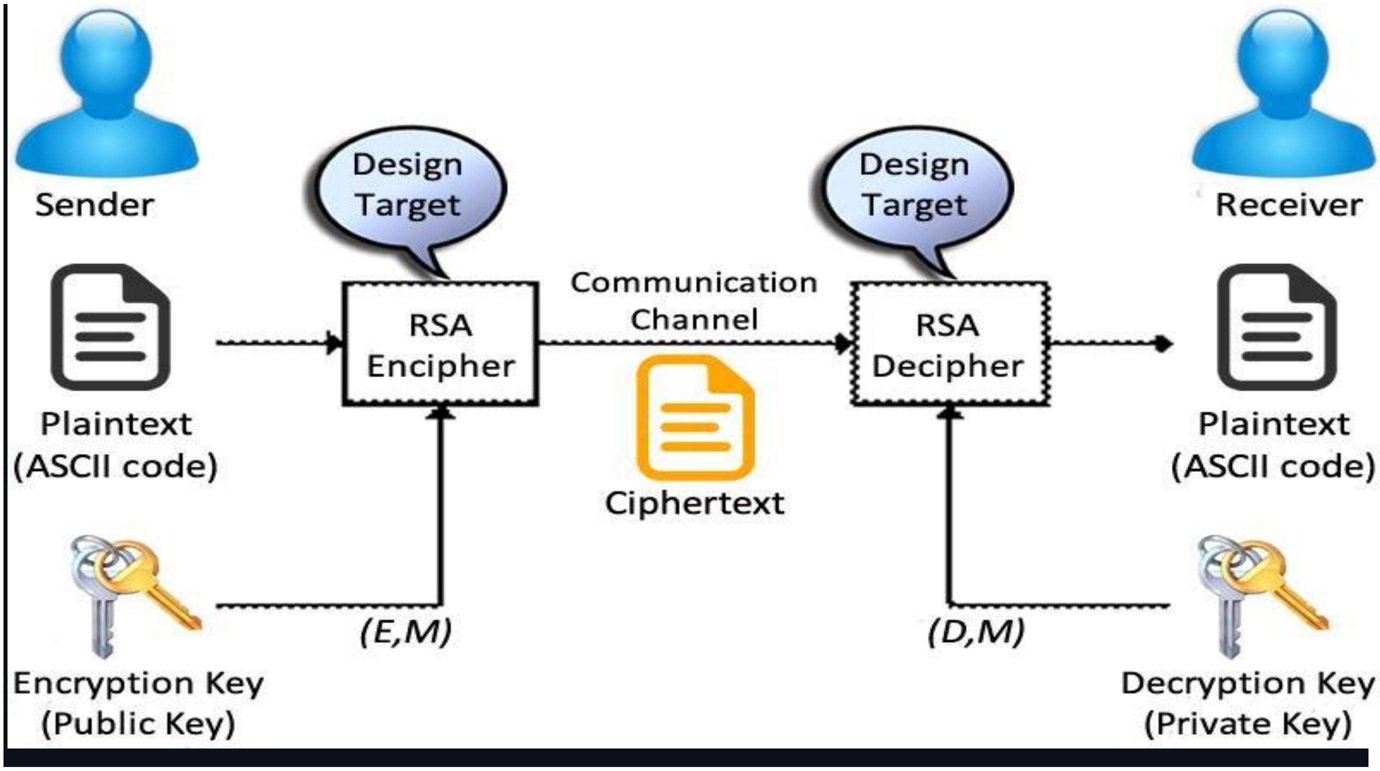
Efforts to lower such costs have been met with success in recent years, and new innovations on the horizon will soon offer organizations better ways to protect themselves from both current and emerging cybersecurity threats. IBM conveyed that message during its recent “Future of Cryptography” online event, citing advances in three critical emerging areas of data privacy and encryption:

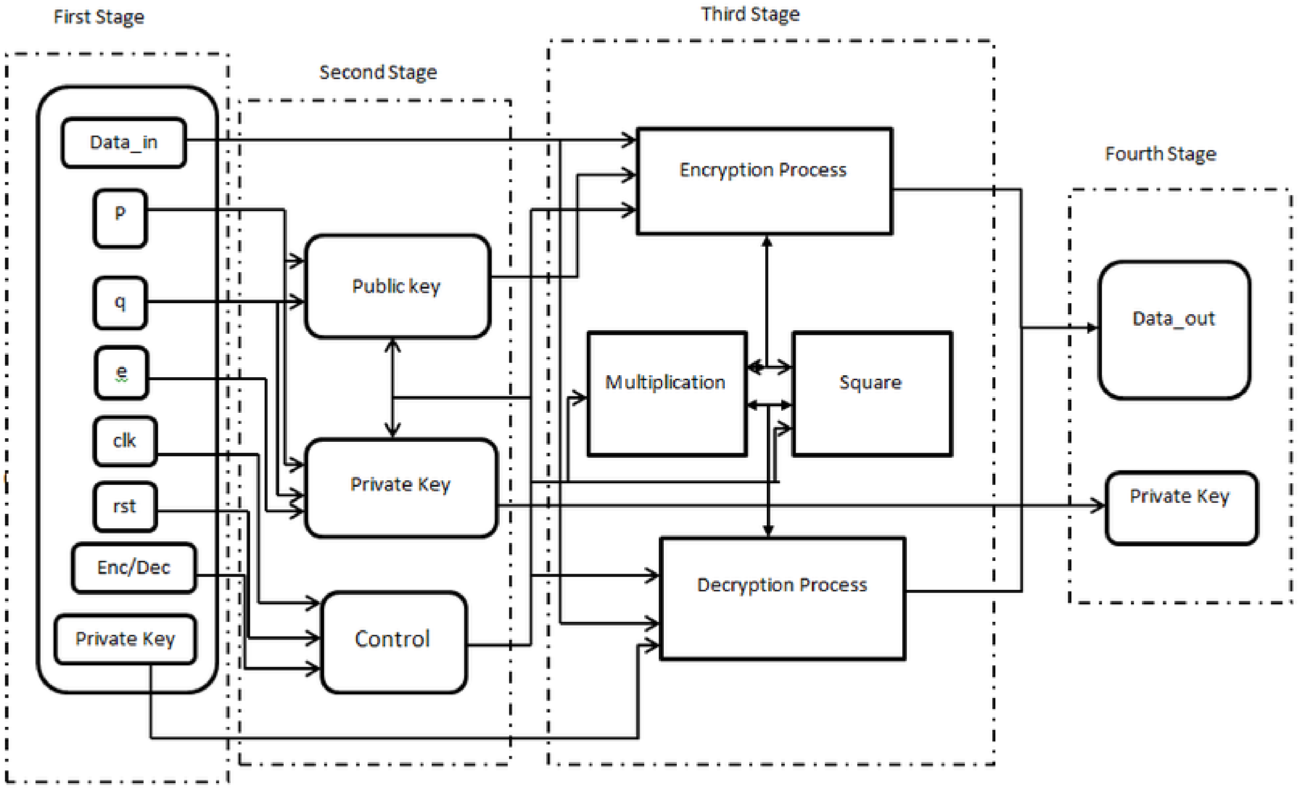
~ Confidential computing,

~ Quantum-safe cryptography

~ Fully homomorphic encryption.

ARCHIETECTURE:




First Stage
Second Stage
Third Stage
Fourth Stage
Data_in
p
q
e
clk
rst
Enc/Dec
Private Key
Public key
Private Key
Control
Encryption Process
Multiplication
Square
Decryption Process
Data_out
Private Key

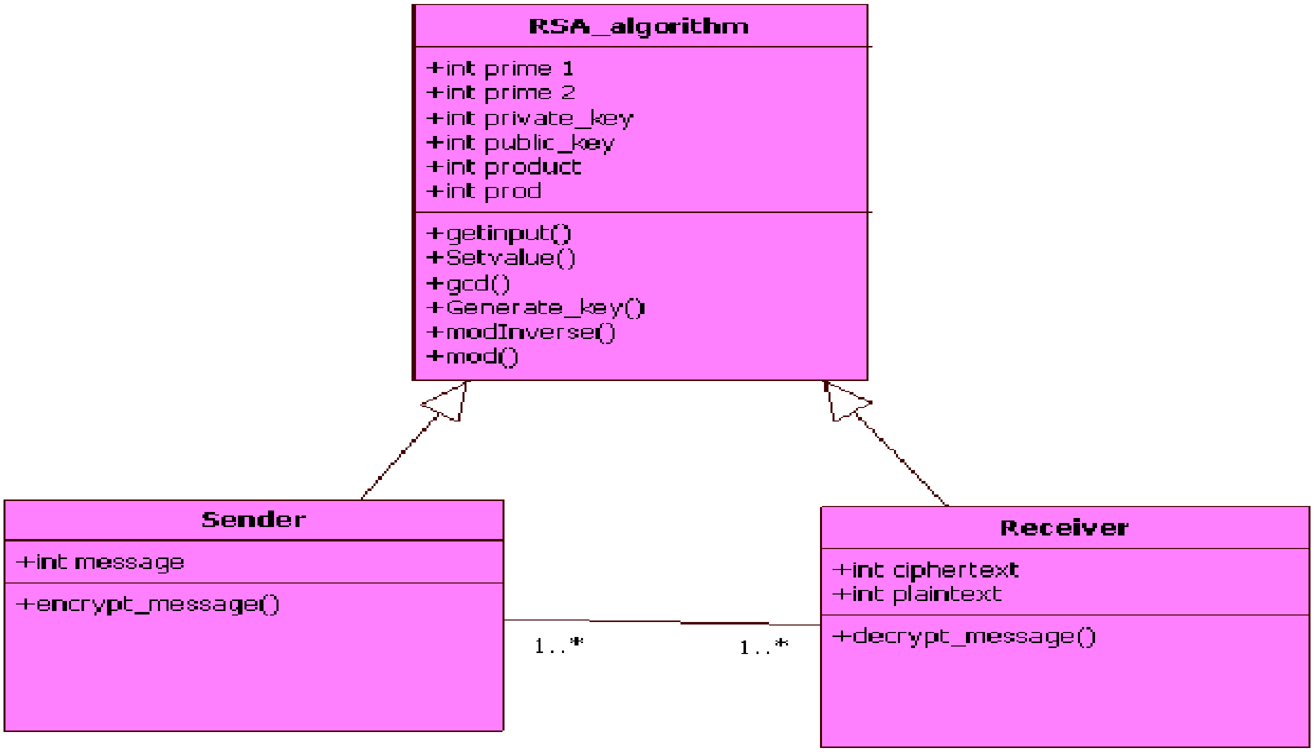
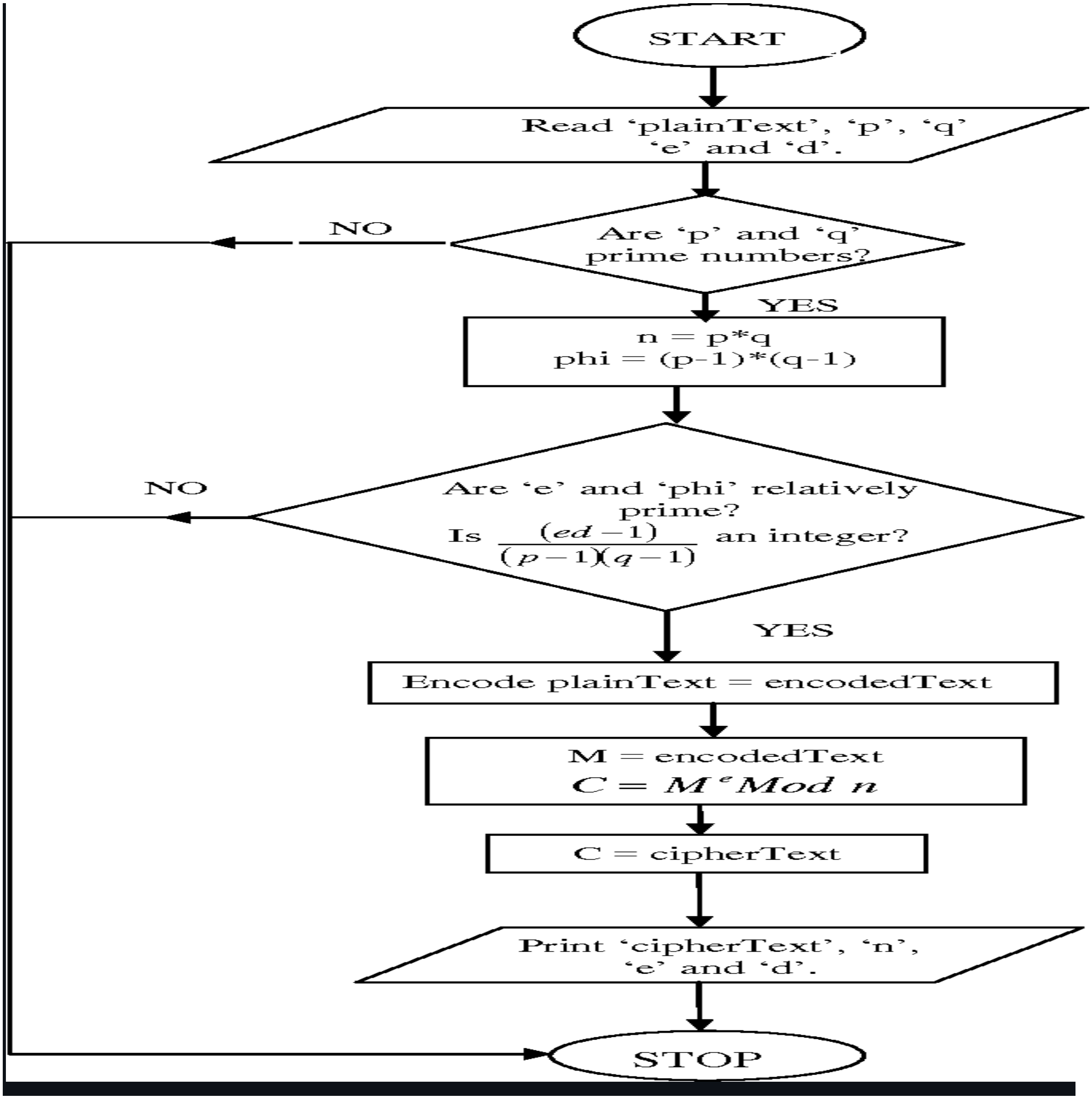


Figure 3 Class diagram of the RSA algorithm


START
Read ‘plainText’, ‘p’, ‘q’ ‘e’ and ‘d’.
Are ‘p’ and ‘q’ prime numbers?
NO
YES
n = p*q
phi = (p-1)*(q-1)
Are ‘e’ and ‘phi’ relatively prime?
Is $\frac{(ed-1)}{(p-1)(q-1)}$ an integer?
NO
YES
Encode plainText = encodedText
M = encodedText
$C = M^{e} Mod\ n$
C = cipherText
Print ‘cipherText’, ‘n’, ‘e’ and ‘d’.
STOP

Conclusion:

The encryption and decryption for a RSA based cryptography algorithm using C is excecuted in .c and .h file and the multifile concept has been established. The make is developed for different file through Visual studio code and final result is being implemented.