।। सिद्धिः भूषयते विद्याम् ।।

avantika UNIVERSITY

Course Name	:	Discrete Mathematics
Course Type	:	DCC
Course Credit	:	3

By

Shivam Singh (AU17B1021)

Date of Submission	:	9th January 2019

B.Tech (Computer Science and Engineering)

2nd year, Semester 4th

2018-19

1. Problem Statement:

Secure Data Transmission system using Cryptography (RSA Algorithm).

2. Introduction:

The System has two ends Transmission and Receiver with Arduino Uno Board along with RF 433 (Tx, Rx pair) module as data (signal) transmission medium and MATLAB programming for integration and interface of the system. The system uses Discrete Mathematics based RSA Algorithm (including ASCII character conversion) in MATLAB for encryption and decryption on transmission and receiver end respectively.

3. Cryptography and RSA Algorithm:

Cryptography is a process in which we convert a plain text or clear text message to cipher text message which is based on an algorithm that both sender and receiver know, and in this way the cipher text message can be obtained to its original form. In this way, a message cannot be read by anyone but the authorized receiver. The process of converting a plain message to its cipher text form is called enciphering. Reversing this process is known as deciphering. Enciphering and deciphering are other names of encryption and decryption. There are numerous methods used to perform encryption and decryption. The most usable method uses a key. A key is a parameter of algorithm by which encryption and decryption takes place. Key-based cryptographic techniques are divided into two methods: symmetric and asymmetric. In symmetric cryptography, same key is used for encryption and decryption. In asymmetric cryptography, one key is used for encryption and another for decryption. In this project, asymmetric method is used for cryptography that is RSA Algorithm.

RSA (Rivest–Shamir–Adleman) is one of the first public-key cryptosystems and is widely used for secure data transmission which uses prime factorization as the trapdoor one-way function. In such a cryptosystem, the encryption key is public, and it is different from the decryption key which is kept secret, that is anyone can encrypt the message (with public key) but only the person with private key can decrypt the message.

The Original Algorithm is as follows:

a) Generate two large random primes, p and q, of approximately equal size such that their product $n = p*q$ is of the required bit length, e.g. 1024 bits.
b) Compute $n=p*q$ and $\phi(n)=(p-1) * (q-1)$
c) Choose an integer e, $1<e<\phi$, such that $\gcd(e,\phi)=1$

d) Compute the secret exponent d, 1<d<ϕ, such that e*d≡1*(mod ϕ(n))

e) The public key is (n,e) and the private key (d,p,q). Keep all the values d, p, q and ϕ secret. [Sometimes the private key is written as (n,d) because the value of n is needed when using d. Other times the key pair might be written as ((N,e),d).

Note:

i) n is known as the modulus.

ii) e is known as the public exponent or encryption exponent.

iii) d is known as the secret exponent or decryption exponent.

Hence, the above original RSA algorithm was adopted for encryption and decryption that is in development of this project.

4. Technologies Used:

a) Programming Language and Tools:

i) MATLAB – MathWorks MATLAB R2018b

ii) Arduino – Arduino IDE

b) Hardware:

i) Arduino Uno R3 board (x2)

ii) RF 433 Transceiver Module (1 pair)

Calculation of antenna height:

$$\text{RF Module Antenna height} = \frac{\lambda}{2} = \frac{\left(\frac{c}{f}\right)}{2}$$

$$\left(\frac{(3 * 10^8)}{(433 * 10^6)}\right) * \frac{1}{2} = 0.3464\ meters = 35\ cm$$

C = speed of light = $3 * 10^8$ m/s

f = frequency of RF module hardware = 433 MHz = $433 * 10^6$ Hz

λ = wavelength of the Radio Frequency emitted by the RF module.

iii) Connecting Wires and Antenna

5. Work flow of the System:

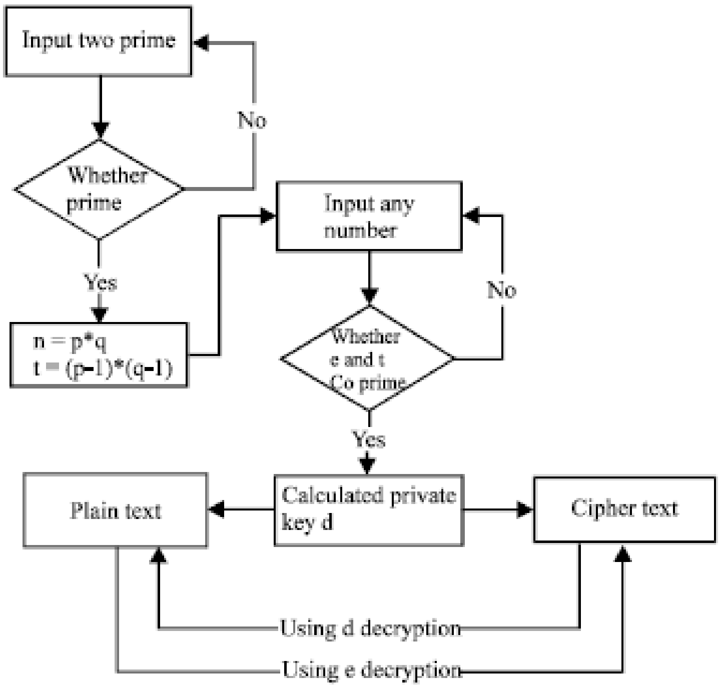


Figure: Flow chart of RSA algorithm program.

a) Encoder, Transmitter, Sender side:

i) User inputs values of **p** and **q** (both must be prime numbers, and the higher the value of **p** and **q** the more secure the encryption will be.)

ii) The program calculates the values of **n=p*q**, **ϕ(n)=(p−1) * (q−1)**, **e (integer e, 1<e<ϕ, such that gcd(e,ϕ)=1)** and **d (e*d≡1*(mod ϕ(n)))** according to the algorithm.

iii) User inputs the message (**m**) that is to be encrypted such that the letters in m = **1<m<n,** and then the program converts the message letters into its ASCII characters (American Standard Code for Information Interchange) for performing encryption.

iv) At last the program computes the ciphertext $c = m^e \bmod n.$

v) This Cipher text is then sent to the receiver via Radio Frequency (***Tx***) module directly from MATLAB program on user's choice.

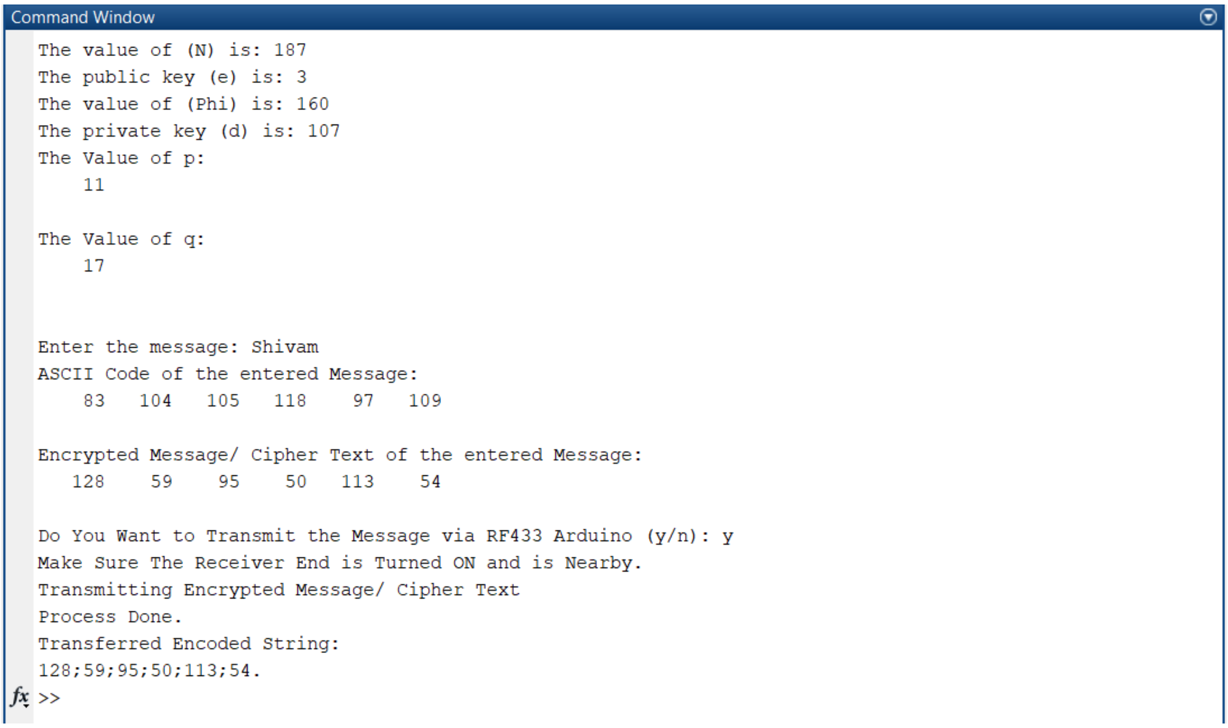
b) Decoder, Receiver side:

i) The Radio Frequency (***Rx***) module searches for the string that is cipher text which is transferred from the ***Tx*** side, until the string that is cipher text is stored on the ***Rx*** module and is passed to the MATLAB program.

ii) The MATLAB program then confirms the end user to confirm the string to continue, then the user inputs the values **n** and **d** which acts as private key of the algorithm for successful decryption of the message.

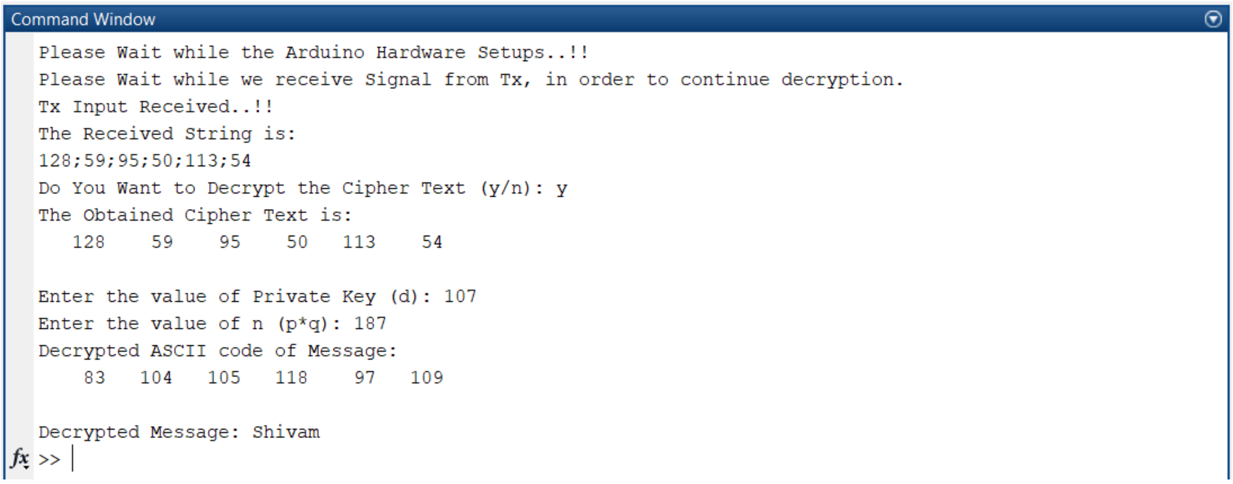
iii) The program then computes $m = c^{d} \bmod n$, m being the ASCII character representation of the original message.

iv) The program then converts the ASCII characters back to string for displaying the original form of message to the user.



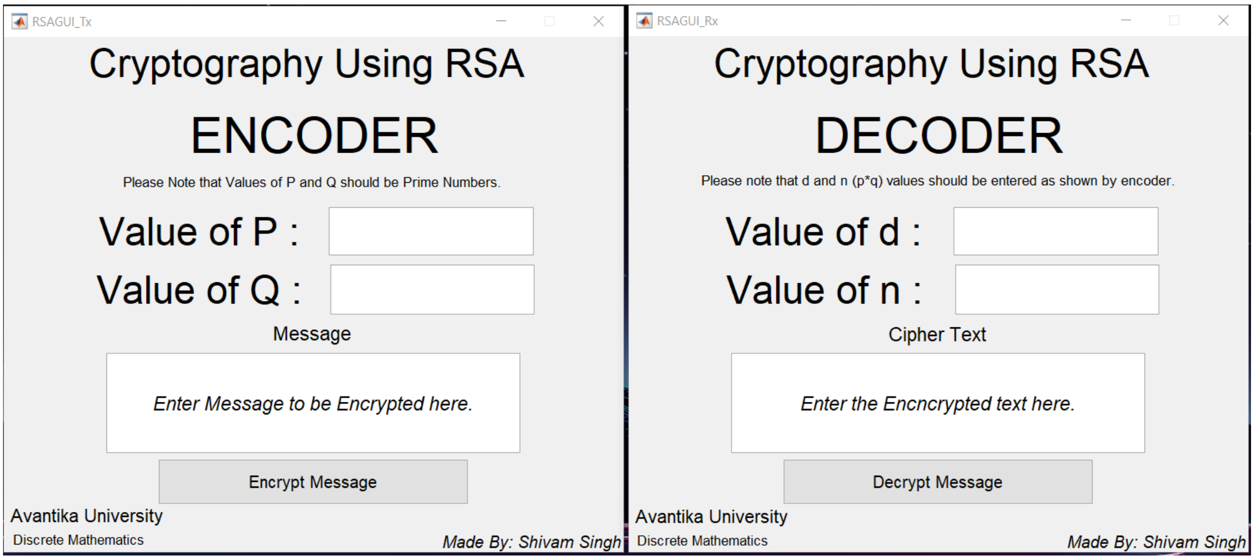
```
The value of (N) is: 187
The public key (e) is: 3
The value of (Phi) is: 160
The private key (d) is: 107
The Value of p:
    11

The Value of q:
    17


Enter the message: Shivam
ASCII Code of the entered Message:
    83   104   105   118    97   109

Encrypted Message/ Cipher Text of the entered Message:
   128    59    95    50   113    54

Do You Want to Transmit the Message via RF433 Arduino (y/n): y
Make Sure The Receiver End is Turned ON and is Nearby.
Transmitting Encrypted Message/ Cipher Text
Process Done.
Transferred Encoded String:
128;59;95;50;113;54.
>>
```

Figure: Tx – Encoder Side of the MATLAB program output window



```
Please Wait while the Arduino Hardware Setups..!!
Please Wait while we receive Signal from Tx, in order to continue decryption.
Tx Input Received..!!
The Received String is:
128;59;95;50;113;54
Do You Want to Decrypt the Cipher Text (y/n): y
The Obtained Cipher Text is:
   128    59    95    50   113    54

Enter the value of Private Key (d): 107
Enter the value of n (p*q): 187
Decrypted ASCII code of Message:
    83   104   105   118    97   109

Decrypted Message: Shivam
>>
```

Figure: Rx – Decoder Side of the MATLAB program output window



RSAGUI_Tx

Cryptography Using RSA

ENCODER

Please Note that Values of P and Q should be Prime Numbers.

Value of P :

Value of Q :

Message

Enter Message to be Encrypted here.

Encrypt Message

Avantika University

Discrete Mathematics

Made By: Shivam Singh

RSAGUI_Rx

Cryptography Using RSA

DECODER

Please note that d and n (p*q) values should be entered as shown by encoder.

Value of d :

Value of n :

Cipher Text

Enter the Encncrypted text here.

Decrypt Message

Avantika University

Discrete Mathematics

Made By: Shivam Singh

Figure: MATLAB GUI programs to compute and display cryptography using RSA algorithm.

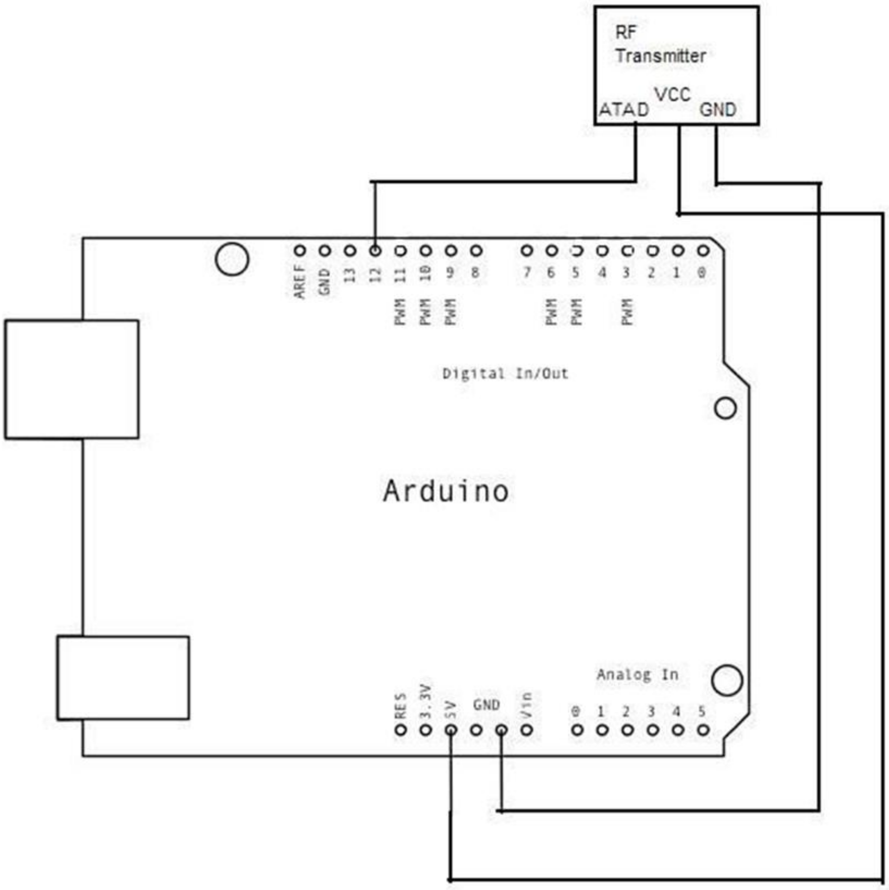


Figure: Arduino circuit (both Rx and Tx) used for project.

6. Visualization of the working of system:

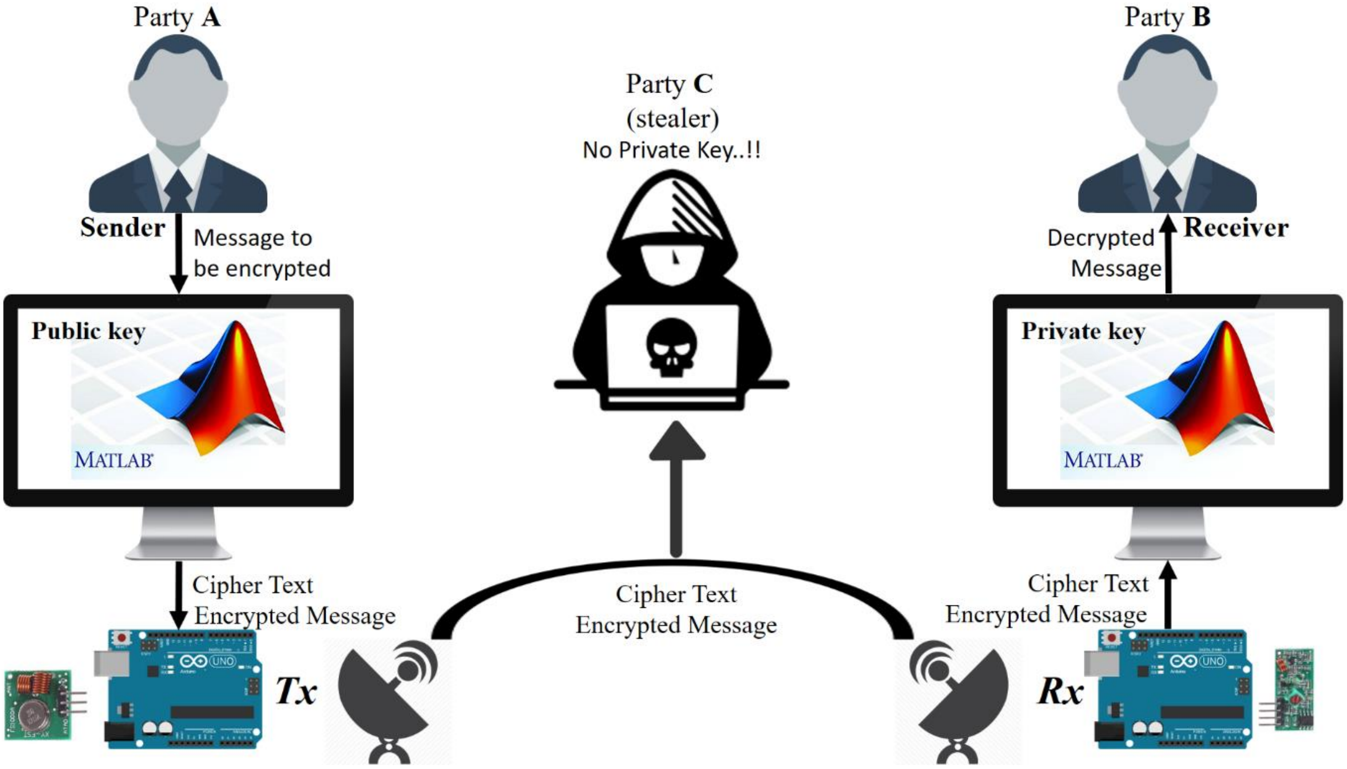


Figure: Visualization of working of system.

7. **Applications and future scope:**

a) The system can be used at many places where there is need for secure data transmission system for sensitive data – by various Institutes, government departments etc.

b) The system is currently designed to be used for simple plain text encryption and transmission but on further modification can be used to encrypt and transmit large files such as images, documents etc.

c) The Radio frequency used is rated as prototyping model and can be replaced by commercial Radio Frequency modules/ systems for long distance transmission of data with better capabilities.

References:

1. RSA Algorithm – Wolfram: http://mathworld.wolfram.com/RSAEncryption.html
2. Cryptography using RSA Algorithm demonstration – Wolfram: http://demonstrations.wolfram.com/RSAEncryptionAndDecryption/
3. RSA Algorithm brief explanation – Wikipedia: https://simple.wikipedia.org/wiki/RSA_algorithm
4. Introduction to RSA – MTHOLYOKE.edu : http://www.mtholyoke.edu/~jjlee/Teaching/Math%20232%20Introduction%20to%20RSA.pdf
5. MATLAB help and support documentation – MATLAB (MathWorks): https://in.mathworks.com/help/matlab/
6. Arduino board usage with RF 433 module – Instructables (Autodesk): https://www.instructables.com/id/Wireless-communication-Arduino-RF/