INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN: 2278 – 0211 (Online)

Data Security Using RSA Algorithm In Matlab

Shikha Kuchhal
B.E, M Tech (ECE), Research Scholar
Ishank Kuchhal
B Tech, M Tech Scholar

Abstract:
Organizations in both public and private sectors have increasingly dependent on electronic data processing. Protecting these data is of utmost concern to the organizations and cryptography is one of the primary ways to do the job. Cryptography is a German word which means secret writing. Cryptography is necessary while communicating over any untrusted medium, which includes just about any network, particularly the Internet. Encryption and decryption algorithm's security depends on the algorithm as well as on the key's confidentiality, once the key is leaked, it means any one can encrypt or decrypt the data, it means the whole procedure become useless. Therefore, how to distribute the private key and how to save both transmission keys are very important. This document briefly introduces the concept of RSA algorithm, and, thereby design and analyze the performance of our improved implementation. We have developed a program for encrypting and decrypting text files. In addition, the encryption procedure and code implementation is provided.

Key words: *RSA, encryption, decryption, MATLAB*

1.Introduction

Information security is an important issue in our information society. When we transmit valuable information, it is frequently protected physically through the use of shielded cable, and the like. Such measures do not securely protect information, and they expensive and uneconomical. More efficient technique must be employed.

Encryption is one of the best tools to guarantee the security of sensitive information. It not only provides the information's security but also functions with digital signature, authentication, secret sub-keeping system security etc. therefore, the purpose of adopting encryption techniques is to ensure the information's integrity and confidentiality, that is prevent information from tampering, forgery and counterfeiting.

RSA cryptosystem, named after its inventors R.Rivest, A.Shamir, and L.Adleman, is most widely used public Key cryptosystem. A desirable property of any encryption scheme is a proof that breaking it is as difficult as solving a computational problem that is widely believed to be difficult, such as integer factorization or the discrete length problem.

In this paper we have improved implementation of RSA algorithm and analyze our implementation, we have developed a program for encrypting and decrypting text.

Standard encryption methods usually have two basic flaws: 1) A secure channel must be established at some point so that sender may exchange the decoding key with the receiver, and 2) There is no guarantee who sent a given message.

RSA solves one of the most difficult problems of all prior cryptography: the necessity of establishing a secure channel for the exchange of the key.

1.1.This Paper Has Been Divided Into Different Sections

Section 1: Introduction to MATLAB
Section 2: The RSA algorithm defines the RSA encryption algorithm.
Section 3: Security of the RSA algorithm defines the faults and security in RSA algorithm.
Section 4: Implementation of RSA algorithm defines modules for generating public and private exponents.
Section 5: Performance analysis it shows the different outputs of different modules.
Section 6: conclusion it conclude the overall paper.
Section 7: References.

2.Introduction To Software Used

3.MATLAB - The Language Technical Of Computing

MATLAB is a high-level technical computing language and interactive environment for algorithm development, data visualization, data analysis, and numeric computation. Using the MATLAB product, you can solve technical computing problems faster than with traditional programming languages, such as C, C++, and FORTRAN.

One can use MATLAB in a wide range of applications, including signal and image processing, communications, control design, test and measurement, financial modeling and analysis, and computational biology. Add-on toolboxes (collections of special-purpose MATLAB functions, available separately) extend the MATLAB environment to solve particular classes of problems in these application areas.

MATLAB provides a number of features for documenting and sharing your work. You can integrate your MATLAB code with other languages and applications, and distribute your MATLAB algorithms and applications.

4.The RSA Algorithm

4.1.Brief Introduction Of Public Key Cryptography

Public key introduces concept involving key pairs, one for encrypting, and the other for decrypting the data. This concept is very clever and attractive, and provides a great deal of advantages over symmetric key:-

- Simplified key distribution
- Digital signature
- Long term encryption.

Data encrypted with the public key can only be decrypted with its private key.

Digital signature is a mechanism by which a message is authenticated that is proving that a message is effectively coming from a given number, much like a signature on a paper document.

A successful decryption constitutes digital signature verification, meaning that there is no doubt that is transmitter's public key that encrypts the message.

RSA algorithm's depends on the decomposition of large prime numbers. In the algorithm, two large prime numbers. In the algorithm, two large prime numbers are used to construct public key and private key.

In order to achieve maximum efficiency, the symmetric key algorithm and public key algorithm are always combined together. That is, using a symmetric key algorithm to encrypt the confidential information needed to be sent, while using the RSA algorithm to encrypt the key. This takes advantages of both the kinds of cryptography, namely high speed DES and key management using RSA algorithm which is of convenience and security.

4.2.The Rsa Algorithm

Key generation:

- Select random prime numbers p and q, and check p! =q.
- Compute modulus n=p*q.
- Compute phi, Ø=(p-1)(q-1).
- Select public exponent e, 1<e<Ø such that gcd (e, Ø)=1.
- Compute private exponent, (d*e) mod Ø=1.
- Public key is {n, e},private key{d}.

Encryption:

c = (m^e) mod n.

Decryption:

m = (c^d) mod n.

Digital signature:

s = (H(m)^d)mod n

Verification:

m'=(s^e) mod n.

If m'=H(m) signature is correct.

H is publicly known hash function

5.Security Of The Algorithm

The premise behind RSA's Security is the assumption that factoring a big number is hard. And thus it is difficult to determine 'g' ,it would be hard to derive 'd' based on the knowledge of 'e'.

P and q must be of same length in bits, must not be equal and they should not be close to each other, that is, p-q should not be a small number. If primes are chosen random, and even when they are in same length, it is extremely likely that these conditions are met.

Smaller keys are now a day considered insecure. If you need long time security compute 2048 bit keys or longer. Also, compute always new n for each key pair. Do not share n with any other pair.

If m is shorter than n-1 it must be padded, otherwise it may be possible to retrieve the m from c. also, if m is sent to more than one recipient each m must be made unique by adding pseudo-random bits to the m.

Attacks exist against RSA if these conditions are not met.

6.Implementation Of RSA Algorithm

6.1.Exponent Generating Process

```
Public exponent generating process
while(1)
   t1=input('enter value for e :','s')
   t=str2num(t1)
   f1=factor(t);
   f2=factor(g);
   for index = 1:length(f1),
      for j = 1:length(f2)
         f3=isequal(f1(index),f2(j));
         if f3==1
            break;
         end
      end

   end

end

 private exponent generating process

for k=1:g

   if mod((g*k+1),t)==0
      disp('value of d : ')
      d=(g*k+1)/t
      break;
   end

   k=k+1

end
```

7.Performance Analysis

7.1.Performance Of The Project Is Shown Below

Figure 1 for the original text.
Figure 2 for the encrypted text.
Figure 3 for the decrypted text.

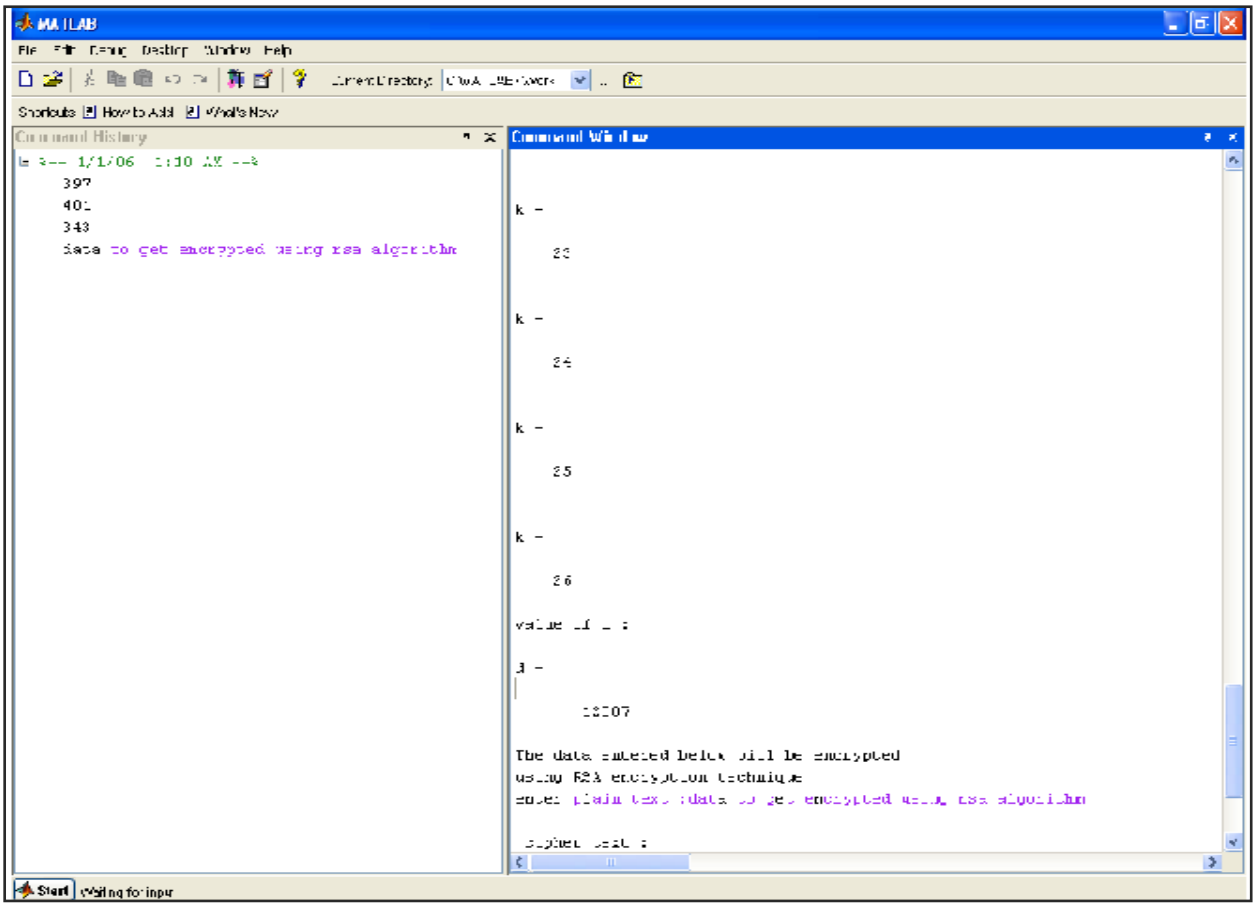

Figure: 1

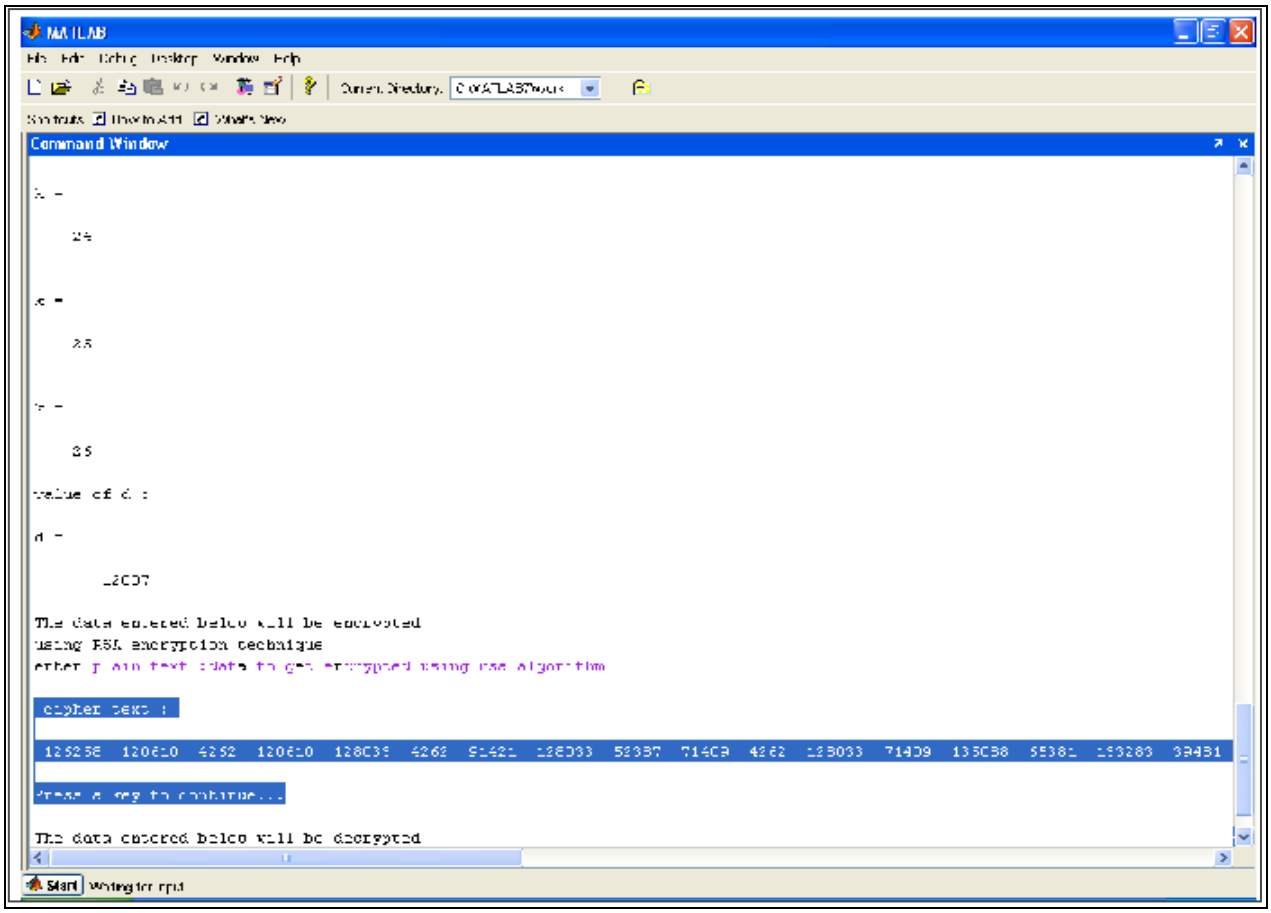

Figure: 2

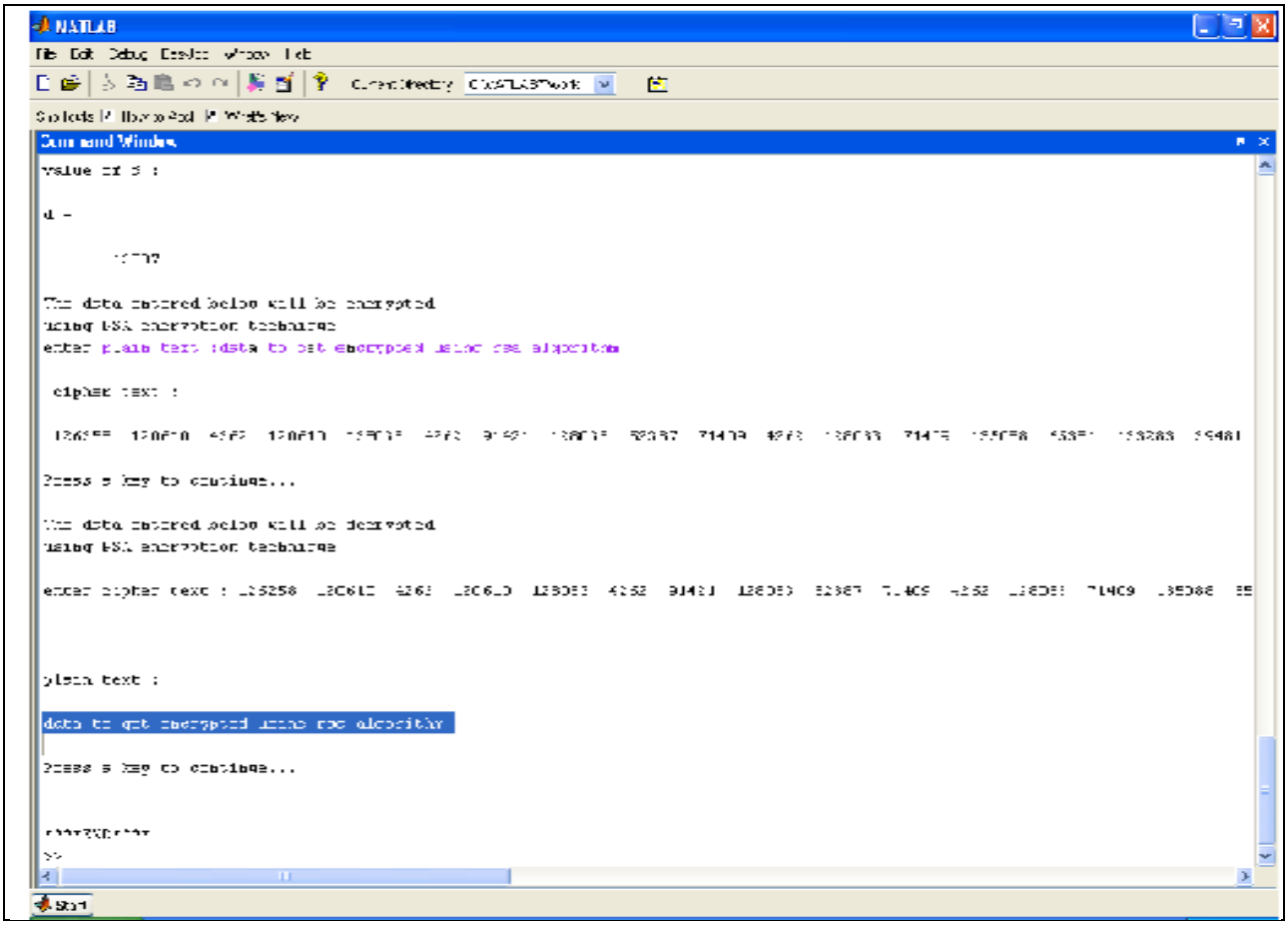

Figure 3

With this implementation, we have successfully developed a program for encrypting and decrypting text

8.Conclusion

The volume of information exchanged by electronic means such as internet, wireless phones, fax, etc. is increasing very rapidly.it is very serious that information through internet is vulnerable to hackers and that privacy of wireless phones without security can be invaded [8]. Hence improved and efficient implementations of cryptographic algorithms are required.

The security of data is not only dependent on the secrecy of encryption algorithm, and more dependent on the security of the key.the whole RSA encryption algorithm is analysed in this paper.

In this paper an efficient implementation of RSA is shown by using various tools from MATLAB toolbox. Encryption and decryption algorithm's security depends on the algorithm as well as on the key's confidentiality, once the key is leaked, it means any one can encrypt or decrypt the data, it means the whole procedure become useless[1]. Therefore, how to distribute the private key and how to save both transmission keys are very important. In this paper we have improved implementation of RSA algorithm and analyze our implementation, we have developed a program for encrypting and decrypting text.

9.References

1. W.Diffie and M.E.Hellman, "New directions in cryptography", IEEE Trans. Inform. Theory, Nov.1976,22: 644-654.
2. R.L.Rivest,A. Shamir, and L.Adleman, "A method for obtaining digital signature and public key cryptosystem", comm..ACM feb1978, 21(2):120-126
3. J.-H Hong, RSA public key crypto-processor core design and hierarchical system test using IEEE 1149 family, PhD dissertation dept. Elec. Eng, National Tsing Hua Univ., Hsinchu, Taiwan R.O.C.,2000: 322-334.
4. Steve Burnett and Stephen Paine, "The RSA securities official guide to cryptography", CA USA: Osborne/Mc-Graw-Hill, 2001.
5. Xin Zhou and Xiaofei Tang, "Research and implementation of RSA algorithm for Encryption and Decryption, IEEE International Forum on Strategic Technology, 2011, 1118-1121.
6. Jiezhao Peng and Qi Wu," research and implementation of RSA algorithm in Java", IEEE, International Conference on management of e-Commerce and e-Government, 2008, 359-363.
7. Rajorshi Biswas,Shibdas Bandyopadhyay,Anirban Banerjee,"A Fast Implementation of the RSA Algorithm using the GNU MP Library",
8. Seung-Jo Han,Heang-Soo Oh,Jongan Park,'the improved Data Encryption Stamndard(DES) Algorithm.",IEEE,1996,1310-1314.