ISSN No: 2350-1278
Peer Reviewed & Refereed Journal
National Research Refereed Journal

SECURED DATA USING RSA

Vinshy

Research Scholar, Department of Computer Science, University of Kerala, Kerala, India

ABSTRACT:

There are various methods used to keep the data secure from cyberpunk. These are passwords, cryptography and biometrics. Data security is an important parameter in data communication. It is required for all the organizations, so that, information remains secured from the cyberpunk. Passwords are not so good from security point of view due to their low randomness. Biometrics is too costly and sometimeharmful effects to the human beings have been observed. Cryptography is the best solution for data security. Various encryption algorithms have been criticallyanalyzed. The simulation results for RSA have also been achieved using MATLAB 7.9.0 and it has been observed which is used in RSA algorithm, can easily encrypt and decrypt the data.

Keywords- Ron Rivest, Adi Shamir and Leonard algorithm (RSA), Chosen Plain-text Attacks (CPA), Chosen Cipher-text Attacks (CCA), Identity-Based Secure Distributed Data Storage Schemes(IBSDDSS), Attribute Based Encryption (ABE).

INTRODUCTION

Cryptography is the practice and study of techniques for secure communication in the presence of third parties. It is analyzing code that overcome the influence of enemy and which are related to various aspects in information security such as data confidentiality, data integrity, certificate and non-renunciation [10]. Modern cryptography intersects the disciplines of mathematics. Cryptography in the modern age was effectively similar with encryption, the conversion of information from a plain-text to cipher-text [10]. The originator of an encrypted message shared the decoding technique needed to recover the original information only with intended recipients. Modern cryptography is heavily based on mathematical theory. Algorithmsare project around complex assumptions, making such algorithms difficult to break in practice by any method. It is on paper possible to break such a system but it is infeasible to do so by any known practical means. These schemes are computationally secure theoretical advances and faster computing technology require these solutions to be continually adapted. In cryptography there are some important terms, which are, Plaintext is the original text before it is encrypted.Cipher text (encrypted text) the text obtains after encoding the data with the help of a key is known as cipher text.Key is a word or value that is used to encrypt the plain text or decrypt the cipher text.It is the method of converting the data into coded form with the help of key is called encryption. It is a method to lock information so, that hackers cannot access it without a key. It is the method of converting the encoded data to the original form is called decryption [10]. There are basically two types of Cryptography**.** Private Cryptograph refers to encryption methods in which both the sender and receiver share the same key. It consists of two parts: a) The algorithm and b) The Key. The private key method is an encryption process where one key is used for both encryption and decryption. Symmetric-Key encryption is used for large data transmissions and it is very fast and efficient. Public-KeyCryptographyrefers to encryption methods in which both sender and receiver share different keywhere asinSymmetric-key cryptosystems we use the same key for encryption and decryption of a message. Required number of keys increases as the square of the number of network members.

LITERATURE SURVEY

This section involves the work done by the various researchers in the field of cryptographic algorithm for data security. The literature survey has been carried out by using different schemes of data security. Jinguang Han [2] et al. worked on Identity-Based Secure Distributed Data Storage Schemes. They proposed two new IBSDDS schemes in standard model, a) The first scheme is only secure against the chosen plaintext attacks (CPA),b) The second scheme is secure against the chosen cipher-text attacks (CCA). The file owner in an IBSDSS scheme has less control on his secret key than that in other public key encryption schemes. Chun-I Fan [3] et al. worked on Arbitrary-State Attribute-Based Encryption with Dynamic Membership. These advantages will make an ABE service more efficient and flexible for practical applications. Jin Li [6] et al. proposed a Securely Outsourcing Attribute-Based Encryption with Check-ability. Secure Outsourced ABE system supports both secure outsourced key-issuing and decryption. It has been found that it takes more time than the original ABE system. Xiaofeng Chen [4] et al. worked on New Algorithms for Secure Outsourcing of Modular Exponentiations. They propose two outsource-secure and efficient algorithms for modular exponentiations and simultaneous modular exponentiations. Xiaojiang Du [8] et al. worked on Cryptography Based Key Management Scheme for Heterogeneous Sensor Networks. They presented an efficient key management scheme for heterogeneous sensor networks. They propose further idea to use public key algorithm-Elliptic Curve Cryptography (ECC) for improve the key management scheme.Jing Liu [5] et al. worked on Collusion-Resistant Multicast Key Distribution Based on HOFT. They instantiate the general notion of one-way function tree to obtain a new cryptographic construction named HOFT. They propose further idea to focus on the provable security of OFT-based code. Koji Nuida [9] et al. worked on the Security of Pseudo randomized Information-Theoretically Secure Schemes. They proposed novel ideas and techniques for evaluation of in-distinguish-ability between random and pseudorandom cases in PRG-based randomness reduction of cryptographic schemes. They alsopropose a further idea for improving the effect of the PRG-based randomness reduction.Joseph K. Liu [7] et al. worked on Linkable Ring Signature with Unconditional Anonymity. They have shown that it is possible to have a linkable ring signature scheme with unconditional anonymity.They proposed further idea is to shorten the size of the signature.R.H. Torres [1] et al. worked on identification of keys and cryptographic algorithms using genetic algorithm and graph theory. According to them genetic algorithms that use the Calisnki-Harabasz index as its evaluation function and graphs techniques that are both used to identify patterns in cryptograms generated by cryptographic algorithms.From the above section it is observed thatin order to keep the primitives in limit optimized hard-wares are required and the objective drawn from the observationis thatto make efficient encryption algorithms which takes less time to compute and has better performance.

PROPOSED WORK

The RSA public key cryptosystem was invented by R. Rivest, A. Shamir and L. Adleman. It is based on ease of finding large primes numbers and the difficulty of factoring the product of two large prime numbers. The key used for encryption is different from the key used for decryption. Numbers e, d and N are chosen suchthat if A is less than N, then (Ae mod N)d mod N=A.This means that you can encrypt A with e and decrypt using d. The pair of numbers (e,N) is known as the public key and can be published. The pair of numbers (d,N) is known as the private key and must be kept secret.The number e is known as the encryption exponent, the number d is known as the secret exponent, and N is known as the modulus. Key length in connection with RSA, this is the modulus length.An algorithm that uses different keys for encryption and decryption is said to be asymmetric.Anybody knowing the public key can use it to create encrypted messages, but only the owner of the secret key can decrypt them. The owner of the secret key can encrypt messages that can be decrypted by anybody with the public key. This fact is the basis of the digital signature technique.

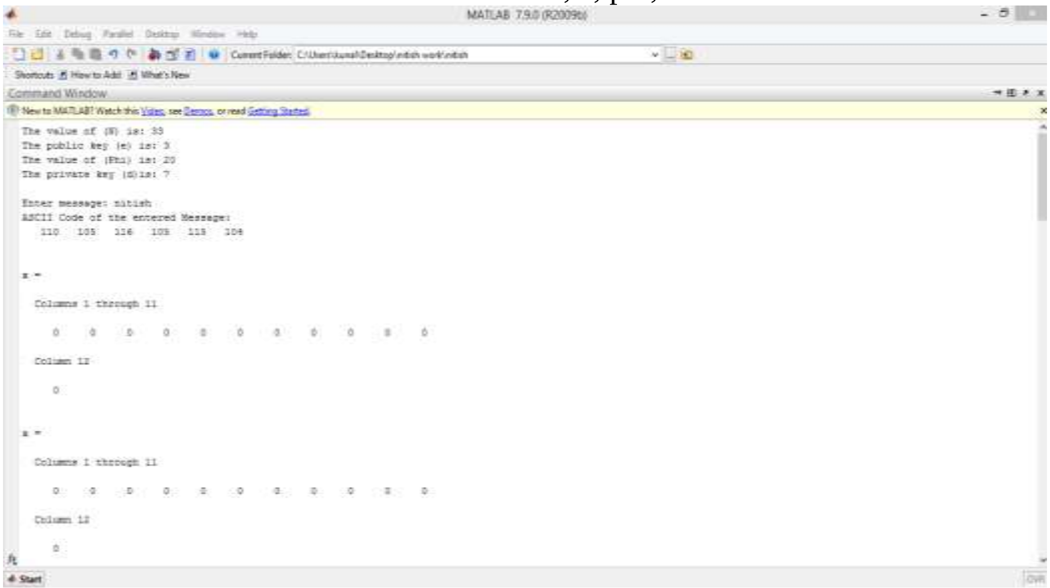
Key Generation Algorithm: Generate two large random primes, p and q, of approximately equal size such that their product $n = pq$ is of the required bit length, e.g. 1024 bits.Compute $n = pq$ and (phi)φ $= (\mathrm{p} - 1)(\mathrm{q} - 1)$.Choose an integer e, $1 < e < phi$, such that gcd(e, phi) = 1. Compute the secret exponent d, $1 < d < phi$, such that ed≡ 1 (mod phi).The public key is (n, e) and the private key (d, p, q). Keep all thevalues d, p, q and phi secret. [We prefer sometimes to write the private key as (n, d) because you need the value of n when using d.n is known as the modulus.e is known as the public exponent or encryption exponent or just the exponent.d is the secretor decryption exponent

RSA ALGORITHM: Choose two distinct prime numbers, p and q.Let$n = pq$. Let $\varphi(pq) = (p - 1)(q - 1)$. (φis totient function).Pick an integer e such that $1 < e < \varphi(pq)$, and e and φ(pq) share no divisors other than 1 (e and φ(pq) are co-prime). Find d which satisfies d is a secret private key exponent.The public key consists of e (often called public exponent) and n(often called modulus). The private key consists of e and d (private exponent).

RESULTS AND DISCUSSION

RSA algorithm implemented in MATLAB 7.9.0 and the results are shown below :

The values of N, e, phi, d:

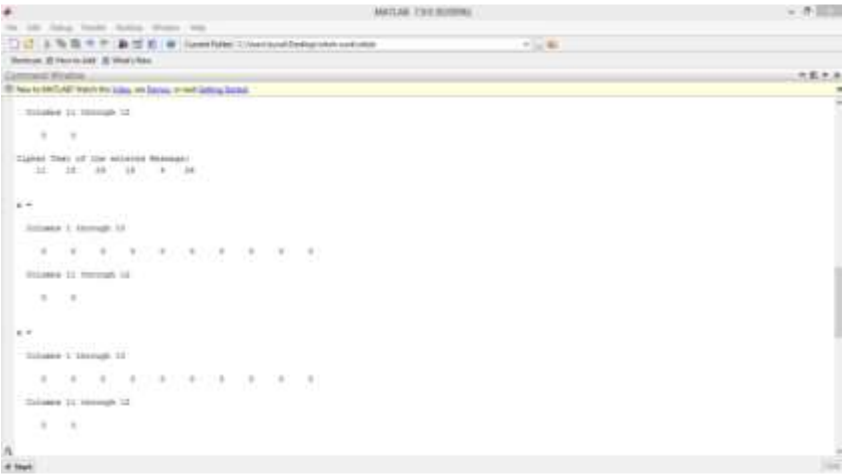

MATLAB 7.9.0 (R2009b)
File Edit Debug Parallel Desktop Window Help
Current Folder: C:\Users\kunal\Desktop\nitish work\nitish
Shortcuts How to Add What's New
Command Window
New to MATLAB? Watch this Video, see Demos, or read Getting Started.
Start

```
The value of (N) is: 33
The public key (e) is: 3
The value of (Phi) is: 20
The private key (d)is: 7

Enter message: nitish
ASCII Code of the entered Message:
   110   105   116   105   115   104


x =

  Columns 1 through 11

     0     0     0     0     0     0     0     0     0     0     0

  Column 12

     0


x =

  Columns 1 through 11

     0     0     0     0     0     0     0     0     0     0     0

  Column 12

     0
```

Figure4.1: ASCII Codes of entered message

Generation of cipher-text:

The original data has been encrypted using public key which is dynamic. The outcome of the same has been achieved using MATLAB 7.9.0 and shown below:

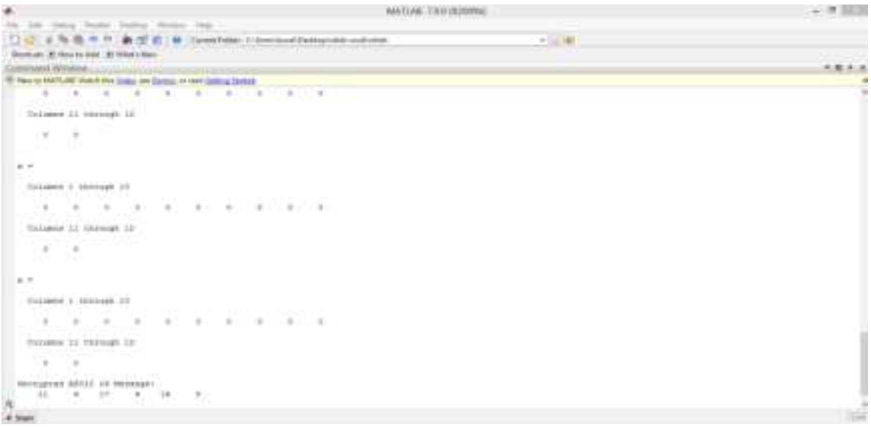


```
  Columns 11 through 12

    [illegible]

Cipher Text of the entered Message:
   [illegible]

[illegible] =

  Columns 1 through 10

    [illegible]

  Columns 11 through 12

    [illegible]

[illegible] =

  Columns 1 through 10

    [illegible]

  Columns 11 through 12

    [illegible]
```

Figure 4.2: Cipher Text

Generation of decrypted code:

The encrypted data has been decrypted using public key. The output of the same has been achieved using MATLAB 7.9.0 and shown below



```
    [illegible]

  Columns 11 through 12

    [illegible]

[illegible] =

  Columns 1 through 10

    [illegible]

  Columns 11 through 12

    [illegible]

[illegible] =

  Columns 1 through 10

    [illegible]

  Columns 11 through 12

    [illegible]

Decrypted ASCII of Message:
   [illegible]
```

Figure 4.3: Decrypt Message

The fig 4.1 shows that ASCII Codes of Entered Message is generated by using MATLAB codes. Similarly, in fig 4.2 and fig 4.3 shows generated cipher-text and generated decrypted text respectively.

Conclusion and Future Work

The key generation in RSA has been successfully done. Using the same key encryption and Decryption of data sequence has also been done. The key generation mechanism will be extended for multiple keys to encrypt the data.

REFERENCES

1. R. H. Torres, G. A. Oliveira, W. A. R. Souza and R. Linden, “Identification of Keys and Cryptographic Algorithms using Genetic Algorithm and Graph Theory”, IEEE Latin America Transactions, Vol. 9, No.2, .pp. 178-183, 2011.
2. Jinguang Han,:” Identity-Based Secure Distributed Data Storage Schemes”, IEEE Transactions on computers, Vol. 63, No.4, .pp. 941-953, April 2014.

3. Chun-I Fan, "Arbitrary-State Attribute-Based Encryption with Dynamic Membership", IEEE Transactions on computers, Vol. 63, No.8, .pp. 1951-1961, August 2014.
4. Xiaofeng Chen, Jianfeng Ma, Qiang Tang, and Wenjing Lou, "New Algorithms for Secure Outsourcing of Modular Exponentiations", IEEE Transaction on parallel and distributed systems, vol. 25, no. 9, .pp. 2386-2396, September 2014.
5. Jing Liu and Bo Yang, "Collusion-Resistant Multicast Key Distribution Based on Homomorphic One-Way Function Trees", IEEE Transactions on information forensics and security, vol. 6, no. 3, .pp. 980-991, September 2011.
6. Jin Li, Xinyi Huang, Jingwei Li, Xiaofeng Chen, and Yang Xiang, "Securely Outsourcing Attribute-Based Encryption with Check ability", IEEE Transaction on parallel and distributed systems, vol. 25, no. 8, .pp. 2201-2210, August 2014.
7. Joseph K. Liu and Man Ho Au ," Linkable Ring Signature with Unconditional Anonymity", IEEE transactions on knowledge and data engineering, vol. 26, no. 1 .pp. 157-165 , January 2014.
8. Xiaojiang Du ," A Routing-Driven Elliptic Curve Cryptography Based Key Management Scheme for Heterogeneous Sensor Networks", IEEE Transactions on wireless communications, vol. 8, no. 3 .pp. 1223-1229 , March 2009.
9. Koji Nuida and Goichiro Hanaoka ," On the Security of Pseudorandomized Information-Theoretically Secure Schemes", IEEE Transactions on information theory, vol. 59, no. 1, .pp. 635-653 January 2013.
10. Bruce Schneier," Applied Cryptography", John Wiley & Sons, Second Edition , January 1996.