IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 3, Issue 6, Dec -Jan, 2016
ISSN: 2320 – 8791 (Impact Factor: 2.317)
www.ijreat.org

An Efficiency Analysis For Data Hiding With Use of Random Key Cryptography over Rivest-Shamir-Adleman Algorithm

Sunita Rani[1], Savita[2]
School of Engineering&Sciences, Bhagat Phool Singh Mahila Vishwavidyalaya, Khanpur Kalan, Sonipat,India

Abstract— **The main function of cryptographic mechanism is basically to secure the data when use full data is distribution in an open environment. There are various kind of secure cryptographic approaches available depending upon the type of data, application or the user. In this paper, the different type of cryptographic approaches is discussed in a detailed manner. The efficiency of these approaches depends on the size of message and the size of key. This paper compares the two main cryptographic approaches which are discussed along with comparative analysis. Those approaches are Random Key Cryptography and RSA algorithm. The comparison of these approaches is performed on real time data. The obtained results from the system show that Random key cryptography is effectively efficient.**

Keywords- RSA, Random Key Cryptography, efficency of key size, efficency of message size.

I. INTRODUCTION

To perform the secure and reliable communication over the network, there are number of available approaches such as cryptography, steganography, watermarking etc. One of such most reliable and data oriented scheme is cryptography. Cryptography is about to encode different kind of data so that undesirable person will not recognize the information. The cryptographic approach is based on information type such as images, text, audio, video etc. Cryptography basically saves the information from any kind of active attack that is performed by attacker to reveal the information. Cryptography prevents the unauthorized access on data. Cryptographic process is itself divided in two stages called encryption and decryption.

Encryption is about to convert the information in encoded unreadable and unrecognizable form whereas the decryption process is reverse to that. It actually converts the encoded information to its actual form. To provide the authorization of communication involving parties, some authentication key is incorporated the cryptographic information. Number of keys depends on the level of security involved. In case of simplest form of cryptographic structure, single symmetric key is used to encode and decode the data. Such cryptographic approach is called private key cryptography. To restrict the operation performed on sender and receiver side, some complex cryptography approach is required. One such approach is public key cryptography in which encoding and decoding process is performed by separate keys. If more than one person is involved in cryptographic operation with equal data contribution, then to maintain the trust level, the concept of shared key is used. In this concept, multiple keys which are taken from different users work as single key to the cryptographic operation. The shared key can be public or private. Here in figure 1 some of the important cryptographic approaches are shown

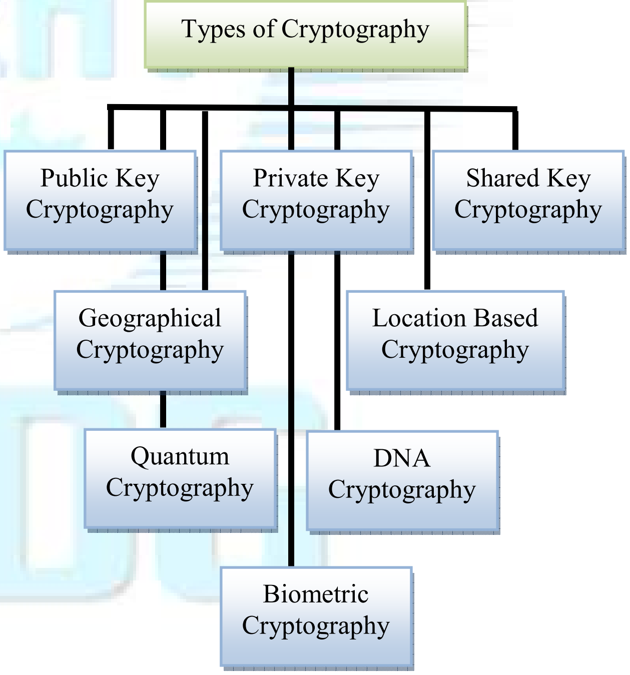


Figure 1 : Types of Cryptography

The above define cryptographic approaches are the standard cryptographic forms that covers the maximum usage of information encoding. Other than these some more cryptographic approaches are used to cover the challenges associated with cryptographic approaches. Once such cryptographic approach is location based cryptography. This cryptographic approach is used to secure the data from social hacking. As the name suggest, this cryptographic approach uses the location key for sender and receiver identification. It means, to open the cryptographic location, the racier must be available at the particular location specified as the cryptographic key. The location key can be the IP Address, Longitude or latitude position that represents the geographical location of the receivers [8] [9] [10].

Another aspect of cryptographic approach is presented by geographical cryptography. In this approach, data is encoded to some geographical shape initially. Once the data is encoded to this form, the next work is to perform the geographical transformation on this shape data to perform the information encoding. Geographical cryptographic use the graphical aspects for encoding and key specifications. Another complex form of cryptography is the quantum key cryptography. Quantum is used to provide the high level security for high speed servers where layered cryptography is performed under the quantum law of encoding. This kind of encoding approach uses the mathematical integrated aspects to encode and decode the information. Another cryptographic approach used in last few years is to encode the data based on the biometric features of the sender or the receiver. It means the key is extracted from any of the human feature such as fingerprint, sign, face etc. Now while extracting the information back, same key is required. The personal authenticated keys are used to gain the person specific security. One more cryptographic approach adapted in many secure communication approaches is the DNA cryptography. DNA is the most advanced form of information representation. In this form, the DNA patterns or the sequence is considered as the generation of the key [11] [12] [13] [14].

In this paper, a comparative analysis on some of the effective cryptographic approaches is defined. In section I, the introduction to the cryptographic concepts and the description of some of some of the available cryptographic approaches and their categorization is given. In section II, the work defined by the earlier authors is defined. In section III, the comparative analysis on different cryptographic approaches is defined. In section IV, the results obtained from the work are discussed. In section V, the conclusion obtained from the work is presented.

II. RELATED WORK

In this section, the work defined by the earlier authors is discussed. With the beginning of digital data communication, the side effects of this kind of communication are identified in terms of information leakage. To prevent this kind of information loss, there are number of cryptographic approaches suggested by different researchers. The main theory of cryptography represented as the security principal, was presented by Kerchhoff [5]. Author designed cryptosystem to secure the information. As the earlier approach, author observed the requirement of the cryptography and to involve the number of person in the cryptographic Approach. According to this approach, the receivers know about the algorithmic approach used for the cryptography. But it gives the information leak and the information insecurity. Because of this, there was the requirement to secure the information without revealing the cryptographic algorithm. Because of this, the cipher text cannot get cracked in the absence of algorithmic approach [2].

Another main aspect of cryptographic process is the cryptography key. Key is the actual mutual information used by the sender and receiver to secure the information. There are number of adaptive approaches to reduce the key size and space. One of such approach was defined by [3]. Author concluded that the large key size increases the security level. The key generation is also based on the key space or the data range on the basis of unique keys can be generated. Author observed that as the key length increases, the information decoding becomes more complex. Author discussed different aspects of cryptographic key such as key length, key sharing, key generation etc.

Based on these parameters, there are number of cryptographic approaches defined by different researchers. Author [4] discussed the concept of symmetric and asymmetric key cryptography. Author discussed the key based algorithms so that the effective security and reliability to system will be achieved. One of such cryptographic approach was discussed by the author [5] called Triple DES approach. In this cryptographic form 168 bit key is used to encode the information. This cryptographic approach is based on the cryptographic algorithm and the comparative algorithm with some other cryptographic algorithms is also defined [5] [6]. Another important concept with cryptographic data communication is the cryptanalysis. It is basically used by the attackers or crackers to reveal the information from encoded data. As the data access is performed by unauthorized person, so that the data extraction is performed without the knowledge of cryptographic key. This information extraction is considered as the integrity attack over data [7] [8].

III CRYPTOGRAPHIC APPROACHES

As discussed in earlier sections there are number of cryptographic approaches available to secure the information. The type of information that is required to transfer can be the parameter to decide the adapted cryptography approach. The purpose of information security or the organization or the person who is involving in the secure communication can decide the cryptographic level required to attain the secure communication. Some of the most used cryptographic approaches are explored here with algorithmic and result specification.

A) Random Key Cryptography

As the name suggest, in such kind of cryptographic system, a random secret key is generated of fixed size. To estimate the randomize character to generate the crypto data, base value analysis is performed. Here table 1 is showing the relation between the key length and the base values.

Table 1: Key Length to Base Value Conversion Table

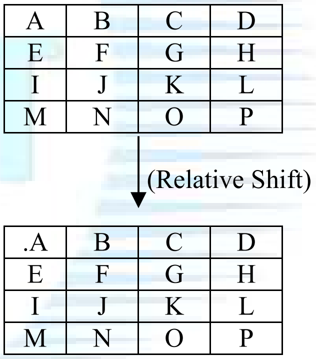
Key Length	1	2	3	4	5	6	7	8
Base Value	17	16	15	14	13	12	11	10
Key Length	9	10	11	12	13	14	15	16
Base Value	9	8	7	6	5	4	3	2

Now from this table, the conversion of key-length txt data conversion can be performed. The steps involved in cryptographic process are given here under

Table 2: Cryptographic Algorithm

```
Algorithm(Text)
/*Text is the plain information that is required to
    encode*/
{
 1.  Calculate S=  $\sum_{i=1}^{N} Ascii(Text(i)) *$
         [Obtain the sum of ASCII character values by
     multiplying each ASCII code with bit range value]
 2.  Identify the Random Number called N1
 3.  Estimate the Encryption Number(N2)
 4.  Perform a series of Transformation Operations for
     cryptography
         a.  Perform Cycling
         b.  Shift Data UP
         c.  Shift Data Down
         d.  Shift Left
         e.  Shift Right
         f.  Cycle Diagonal Elements
 5.  Collect data back after transformation operations
     and present it as the cryptographic information.
}
```

The relative transformation operations are shown in figure 2.



A	B	C	D
E	F	G	H
I	J	K	L
M	N	O	P

.A	B	C	D
E	F	G	H
I	J	K	L
M	N	O	P

Figure 2: Example Transformation Operation

B) RSA Cryptography

RSA is the public key cryptography scheme adapted because of mathematical concept and the number theory involvement. The concept of RSA algorithm is based on the prime numbers. This central part is defined as the critical role definition and the key generation so that relative and effective security will be obtained for the system. This kind of cryptosystem generate large key to gain the effective security. The algorithmic concept is based on the value Zn generated from the product of two uniquely defined prime numbers called p and q. Now an intermediate value is generated between 0 and N-1 for the cryptographic key generation. The procedure of RSA is shown in table 3.

Table 3: RSA Algorithm

Select Two Unique Prime Number (p & q)
Calculate n= p*q
Generate d=(p-1)*(q-1)
Identify an integer e so that d lies between 1 and d
Identify Private Key (d,n)
Identify Public Key (e.n)

The encryption process for Message M
Crypto Text=M^{e} Mod n

The decryption process for Message M
Plain Text = Crypto Text^{d} mod N

The encoding process of RSA algorithm is given here under

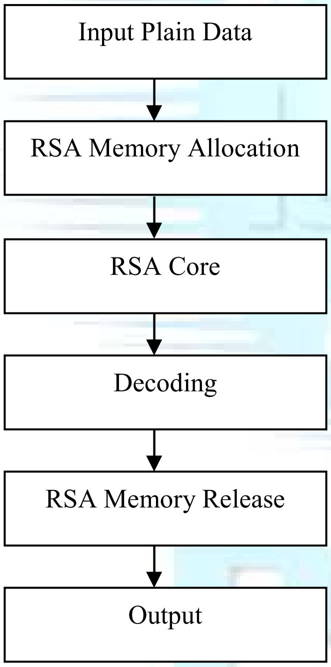


Figure 3: RSA Process Model

Here figure 3 is showing the RSA process model. Here at the earlier stage, plain data is passed as input to the system. The first step is to allocate the memory for message in the buffer. This allocation can be done block wise or the whole data allocation for one time. Once the space is allocated, the execution of main RSA module is performed. During at first data is converted to binary form and then encoding is done using algorithmic approach. The encoding process of two symbols "XY" is shown in the table 4.

Table 4: RSA Encoding

Character	Integer Value	Binary Value	Converted Value
A	65	01000001	10000010
B	66	01000010	01000010

The encoding process along with RSA core procedure is shown in figure 4. Just after the conversion to binary form, the algorithmic RSA approach is implemented as shown in the flowchart. After the encoding process, the cipher text is obtained. Now, this cipher text is obtained transferred to the receiver side. Here the decoding process is performed to convert this cipher text back to the plain text. After converting data back to plain text, the allocated memory is released.

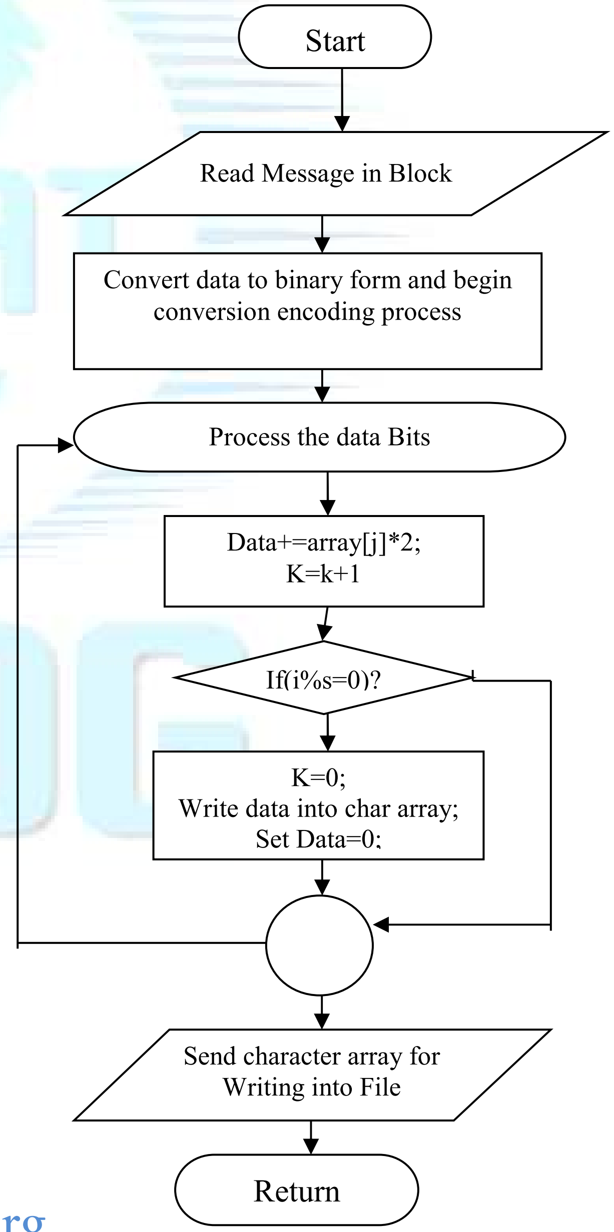

Start
Read Message in Block
Convert data to binary form and begin conversion encoding process
Process the data Bits
Data+=array[j]*2;
K=k+1
If(i%s=0)?
K=0;
Write data into char array;
Set Data=0;
Send character array for Writing into File
Return

Figure 4: RSA Core Procedure

RSA core module is here defined to perform the actual encryption-decryption process. This process includes a series of block operations such as addition, subtraction etc. The table 5 is showing the whole encryption-decryption process. The operations in RSA are performed on fixed block size.

IV. RESULTS

In this section, the results obtained from the implementation of the algorithmic approach are shown. In this work, two main algorithms are implemented called Random Key Cryptography and RSA algorithm. The basic assumptions considered for result analysis are:

1. The input taken for the cryptographic process is in Text Format.
2. Data is process in blocks of fixed size.
3. The numeric and random key is generated.
4. Input is taken in the form of text file and output is saved in the form of text file.

The input and the relative outcome to perform the cryptography are shown in Table 5

Table 5: Output

Input Text
India is a great country
Random Key based Cipher Text Conversion
w Ä Ñ ╝ ╙ Ω ♣ ∟ 3 J a x Å ª ╜ ╘ δ ♠ ↔ 4 K b y É º ╛ ╒ ∞ ▲ 5 L c z æ ¿ ┐ ╓ φ ▼ 6 M d { Æ ⌐ └ ╫ ε 7 N
Random Key based Decoding Output
India is a great Country
RSA Input Text
India is a great country
Cipher Text
$; R i Ç ù « ┼ ▄ ≤ ♫ % < S j ü ÿ » ╞ ▌ ⌠ ☼ & = T k é Ö ░ ╟ ▐ ⌡ ► ' > U l â Ü ▒ ╚ ▀ ÷ ◄ (? V m ä ¢ ▓ ╔ α ≈ ↕) @ W n à £ │ ╨ ß ° ‼ * A X o å ¥ ┤ ╥ Γ · ¶ + B Y p ç ₧ ╡ ╠ π · § , C Z q ê ƒ ╢ ═ Σ √ ▬ - D [r ë á ╖ ╬ σ
Decoding
India is a great Country

The results comparison in the form of complexity analysis between these two algorithms depends on key size and number of data blocks. The complexity of the Random key cryptography also depends on the matrix generation and the number of shift operations. Let the matrix is of NxN size and M number of shift operations are performed over it. Then the complexity of Random key cryptography is given by O (m x N^2) or O (N^2). Whereas in case of RSA algorithm the complexity is higher and represented by O (N^3). The results obtained in terms of time taken are shown in figure 5. Here the time based comparison is given between two cryptographic approaches under different size input blocks. Here X axis represents the size of data blocks and y axis represents the time taken by the algorithm.

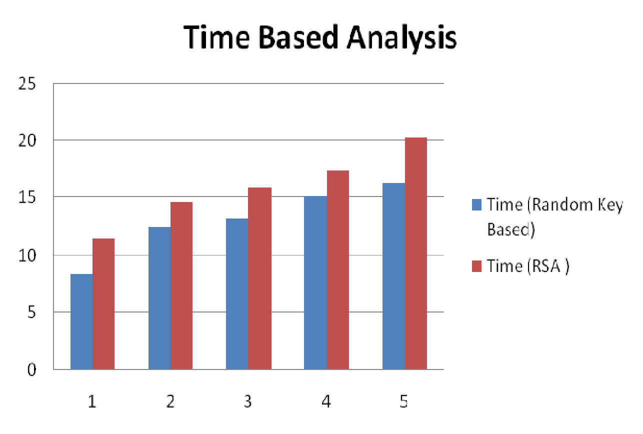


Figure 5 : Time Comparision (Random Key Vs. RSA)

The result shown here represents that the random key cryptography is effectively better than RSA in terms of time efficiency.

VI. CONCLUSION

One of the major aspect of information security is represented by cryptographic approaches. In this paper, the exploration to the available cryptographic approaches is defined. The paper has explored two main cryptographic approaches called random key cryptography and RSA Cryptography with the definition of algorithm and the time based analysis. The results obtained from the system shows that the presented work is effective enough to provide the effective throughput for encoding process.

REFERENCES

1. Louis J. Freeh, Keynote talk at International Cryptography Institute, Sept. 1995. Available through http://www.fbi.gov/crypto.htm .
2. Liao H, Lee P, Chao Y, Chen C (2007). "A location-dependent data encryption approach for mobile information system", in the 9th International Conference on ADVANCED Communicate Technology 1: 625-628. Mundt TM (2005).
3. "Location dependent digital rights management system", in preceding the 10th IEEE sympositon on computers and communication pp. 617-622.
4. Pandian PS (2008) "Wireless Sensor Network for Wearable Physiological Monitoring", J. Networks.
5. Richard W (2006). "Cryptography and trust", information security technical report. 11(6): 8 – 71.
6. GPP, 3G TS 35.201 "Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*.
7. Document 1: General" L.I. Millett, S.H. Holden, "Authentication and its privacy effects", IEEE Internet Computing, Nov. 2003.
8. Heikki Kaaranen, Ari Ahtiainen, Lauri Laitinen, Siamak Naghian, and Valtteri Niemi, UMTS Networks: Architecture, Mobility and Services, 2nd Edition, John Wiley & Sons, Ltd., 2005.
9. F. Zhang, W. Susilo, and Y. Mu, Identity-based partial message recovery signatures (or How to shorten ID- based signatures), In Proceedings of Financial Cryptography- FC'05, LNCS 3570, pp.45-56, 2005.
10. M. Abe and T. Okamoto, A Signature Scheme with Message Recovery as Secure as Discrete Logarithm, In Proceedings of the International Conference on the Theory and Applications of Cryptology and Information Security, LNCS 1716, pp. 378-389, 1999.
11. C. Y. Chow, M. Mokbel, and X. Liu, "A peer-to-peer spatial cloaking algorithm for anonymous location-based services," in *Proc. of the ACGIS*, 2006, pp. 247–256.
12. G. Ghinita, P. Kalnis, and S. Skiadopoulos, "PRIVE: Anonymous location-based queries in distributed mobile systems," in *Proc. of the 1st Int. Conference on World Wide Web (WWW)*, 2007, pp. 371–380.
13. B. Gedik and L. Liu, "Privacy in mobile systems: A personalized anonymization model," in *Proc. of ICDCS*, 2005, pp. 620–629.
14. M. Mokbel, C. Chow, and W. Aref, "The new casper: Query processing for location services without compromising privacy," in *Proc. of VLDB*, 2006, pp. 219–229.