# Dual Encryption by Random Segmentation and Random Re-Arrangement (RSRA) using Two Dimensional Array

**Ganesh M Dahane**

***Abstract*—Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit. However, in today's computer-centric world, cryptography is most often associated with scrambling plaintext (ordinary text, sometimes referred to as cleartext) into ciphertext (a process called encryption), then back again (known as decryption). Individuals who practice this field are known as cryptographers. To make a secure and successful transaction of message, the security of cipher text is must before transmission over communication channel. This paper propose a new encryption technique with the help of random segmentation and random re-arrangement of cipher text using two dimension array before transmission over communication channel so that the transmitted cipher text is more complex to decrypt by any attacker.**

## I. INTRODUCTION

Until modern times, cryptography referred almost exclusively to *encryption*, which is the process of converting ordinary information (called plaintext) into unintelligible text (called ciphertext). Decryption is the reverse, in other words, moving from the unintelligible ciphertext back to plaintext. A *cipher* (or *cypher*) is a pair of algorithms that create the encryption and the reversing decryption. The detailed operation of a cipher is controlled both by the algorithm and in each instance by a "key". The key is a secret (ideally known only to the communicants), usually a short string of characters, which is needed to decrypt the ciphertext. Formally, a "cryptosystem" is the ordered list of elements of finite possible plaintexts, finite possible cyphertexts, finite possible keys, and the encryption and decryption algorithms which correspond to each key. Keys are important both formally and in actual practice, as ciphers without variable keys can be trivially broken with only the knowledge of the cipher used and are therefore useless (or even counter-productive) for most purposes. Historically, ciphers were often used directly for encryption or decryption without additional procedures such as authentication or integrity checks.

## II. LITERATURE REVIEW

Modern encryption methods can be divided by two criteria: by type of key used, and by type of input data

1. By type of key used ciphers are divided into:

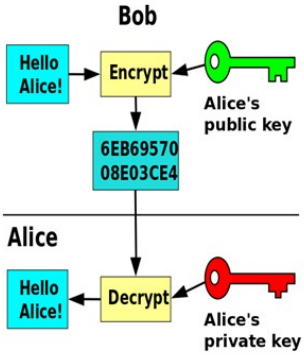
1.1 Symmetric key algorithms
(Private-key cryptography)

In symmetric systems the same key (the secret key) is used to encrypt and decrypt a message. Data manipulation in Symmetric systems is faster than asymmetric systems as they generally use shorter key lengths. Symmetric models include the commonly used AES (Advanced Encryption Standard) which replaced the older DES (Data Encryption Standard).

**(Figure 1.1 : Symmetric-key cryptography, where a single key is used for encryption and decryption)**

1.2 Asymmetric key algorithms (Public-key cryptography)

Asymmetric systems use a public key to encrypt a message and a private key to decrypt it. Use of asymmetric systems enhances the security of communication. Examples of asymmetric systems include RSA (Rivest-Shamir-Adleman), and ECC (Elliptic Curve Cryptography).




**(Figure 1.2 : Public-key cryptography, where different keys are used for encryption and decryption)**

2. Ciphers can be distinguished into two types by the type of input data:

2.1 Block ciphers
which encrypt block of data of fixed size, and
2.2 Stream ciphers
which encrypt continuous streams of data
Although there are various algorithm to encrypt any plain text to cipher text but there are also various legal and illegal activities around the world in which any one try to steal our encrypted message over the communication channel and try to decode it to get the access of plain text.

**Cryptanalysis** is the study of analyzing information systems in order to study the hidden aspects of the systems. Cryptanalysis is used to breach cryptographic security systems and gain access to the contents of encrypted messages, even if the cryptographic key is unknown. The goal of the *cryptanalyst* is to gain as much information as possible about the original, unencrypted data.

Attacks can be classified based on what type of information the attacker has available:

- *Ciphertext-only*: the cryptanalyst has access only to a collection of ciphertexts or codetexts.
- *Known-plaintext*: the attacker has a set of ciphertexts to which he knows the corresponding plaintext.
- *Chosen-plaintext* (*chosen-ciphertext*): the attacker can obtain the ciphertexts (plaintexts) corresponding to an arbitrary set of plaintexts (ciphertexts) of his own choosing.
- *Adaptive chosen-plaintext*: like a chosen-plaintext attack, except the attacker can choose subsequent plaintexts based on information learned from previous encryptions. Similarly *Adaptive chosen ciphertext attack*.
- *Related-key attack*: Like a chosen-plaintext attack, except the attacker can obtain ciphertexts encrypted under two different keys. The keys are unknown, but the relationship between them is known; for example, two keys that differ in the one bit.

## III. PROPOSED SYSTEM

So now we can see that there can be any type of attack on our cipher text over the communication channel by which any attacker can get the access to our original message by trying any of attacking method. So it is very necessary that we apply a method, which will make our cipher text more secure and unbreakable over the communication channel. In this proposed method 1st we convert plain text to middle level cipher text by using any of encryption technique (Symmetric or Asymmetric) and 2nd we randomly rearrange this middle level cipher text by splitting the cipher text in random number of parts and then positioning each part in random sequence and by storing all these information in a 2 dimensional array.

Following are the steps in the proposed method :

Step 1 : Convert the Plain text to Cipher Text by using any of encryption technique (*Symmetric key algorithm in this example)*

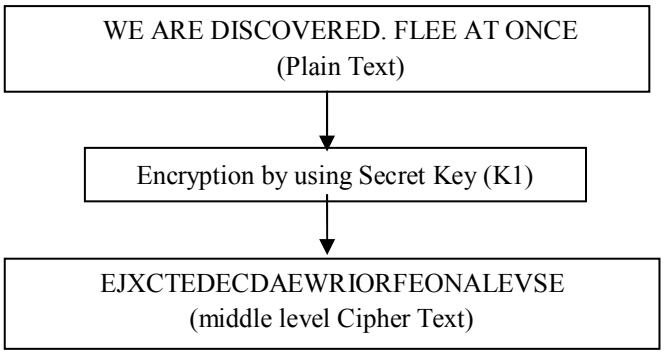



**Figure 2.1**

Step 2 : Split the cipher text in random number of blocks with random length by using following algorithm

```
n = number of alphabets in cipher text.
c= cipher text.
sc=0. (starting index)
ec=0. (end index)
i=0;
Array a[][];

while (ec<=n)

start

if sc=0
start
ec=random(0,n-2);
a[0][0]=sc;
a[0][1]=ec;
sc=ec+1;
i++;
end

else
start
a[i][0]=sc;
ec=random(sc,n-1);
a[i][1]=ec;
sc=ec+1;
i++;
end
end while loop
```

For example, if we apply this process on above cipher text

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18
E J X C T E D E C D A E W R I O R F E

1 2 3 4 5

19 20 21 22 23 24 25 26
O N A L E V S E

6 7 8 9

n = 27
c= EJXCTEDECDAEWRIORFEONALEVSE
sc=0. (starting index)
ec=0. (end index)
i=0;

*in 1st while loop:*
sc=0;
ec=5 (let's consider)=random(1,25);
a[0][0]=0;
a[0][1]=5;

*in 2nd while loop:*
sc=5+1=6;
ec=8 (let's consider)=random(6,26);
a[1][0]=6;
a[1][1]=8;

and so on...

By following above algorithm, after end of while loop the array 'a' will look as follow:

| sc | ec | Seq. |
|---|---|---|
| 0 | 5 | |
| 6 | 8 | |
| 9 | 12 | |
| 13 | 14 | |
| 15 | 18 | |
| 19 | 21 | |
| 22 | 23 | |
| 24 | 24 | |
| 25 | 26 | |

**Table 1.1**

Step 3 : Now assign random sequence no to each row of array a

For Example :

| sc | ec | Seq. |
|---|---|---|
| 0 | 5 | 6 |
| 6 | 8 | 2 |
| 9 | 12 | 5 |
| 13 | 14 | 9 |
| 15 | 18 | 1 |
| 19 | 21 | 4 |
| 22 | 23 | 8 |
| 24 | 24 | 3 |
| 25 | 26 | 7 |

**Table 1.2**

Step 4: Now arrange each segment of cipher text according to its randomly assigned sequence number.

O R F E D E C V O N A D A E W E J X C T
E S E L E R I

(Final Cipher Text)

Now this final cipher text can be transmitted over communication channel. The Array 'a' is converted into a linear arrangement of each row of array 'a' according to randomly assigned sequence number and will be provided to receiver by any secret method as a key to decrypt the final cipher text to middle level text. Again this middle level cipher text will be converted to plain text by using Secret Key K1.

In above example the information of Array 'a' will be arranged as follow :

K2 | 15 18 1 6 8 2 24 24 3 19 21 4 9 12 5 0 5 6 25 26 7 22 23 8 13 14 9

The reverse process will be applied for decryption of above cipher text to the plain text.

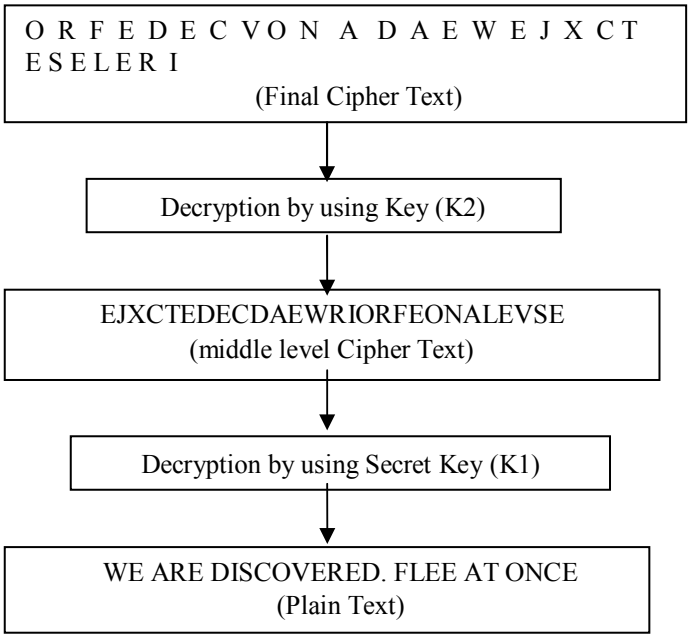



**Figure 2.2**

This proposed method can be applied on both Symmetric and Asymmetric encryption algorithm as follow :

**A. For Symmetric encryption algorithms:**

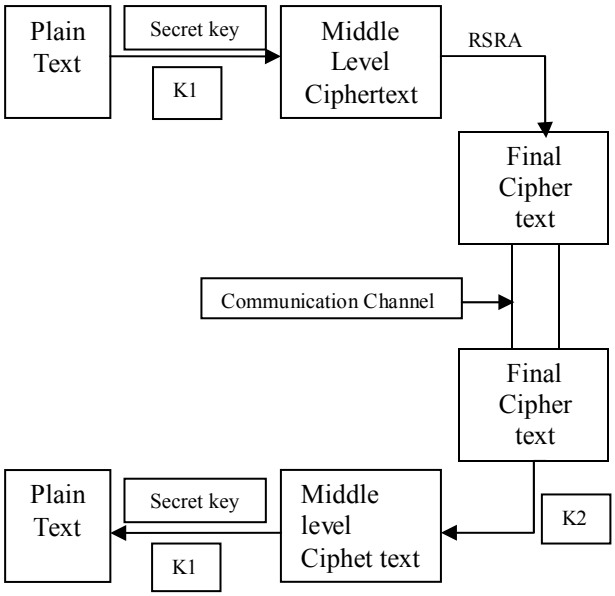



**Figure 2.3**

**B. For Asymmetric encryption algorithms:**

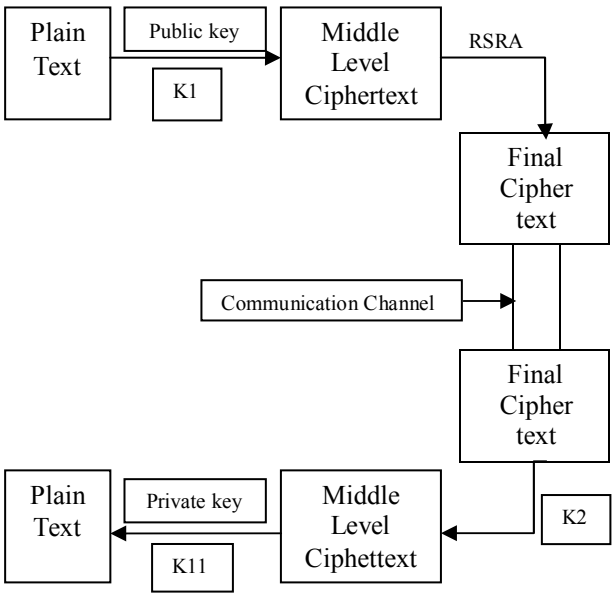



**Figure 2.4**

## IV. CONCLUSION

Hence as described in above proposed method, the cipher text can be made more complex with the help of random segmentation and random re-arrangement of cipher text using two dimensional array before transmission over communication channel so that the transmitted cipher text can not be decrypted by any attacker.

## V. ACKNOWLEDGMENT

I am extremely indebted to my guide Professor Dr. Jayant Shekhar, Department of Computer Science, Subharti Institute of Technology & Engineering, Meerut. I am very grateful to him for continual encouragement, motivation for literature, and continuous hours of sitting together and discussing the problems, which helped me to understand the subject and methodology.

I would like to express my deep and sincere gratitude to Head of Department, Dr. Amit Asthana, Computer Science & Engineering, Subharti Institute of Technology & Engineering, Meerut , for his consultation, encouragement and personal guidance.

## REFERENCES

[1] T. H. Barr. *Invitation to Cryptology*. Prentice Hall, Upper Saddle River, 2002.
[2] A. Beutelspacher, J. Schwenk, and K. D. Wolfenstetter. *Moderne Verfahren in der Kryptographie*.Vieweg,Wiesbaden, 1995.
[3] E. Biham and A. Shamir. *Differential Cryptanalysis of the Full 16-Round DES, LectureNotes in Computer Science 740*. Springer, 1993.
[4] J. Buchmann. *Einführung in die Kryptographie*. Springer, Berlin, 2nd edition, 2001.
[5] J. Buchmann. *Introduction to Cryptography*. Springer, New York, 2nd edition, 2004.
[6] H. Delfs and H. Knebl. *Introduction to Cryptography, Principles and Applications*.Springer, Berlin, 2002.
[7] D. E. Denning. *Cryptography and Data Security*. Addison-Wesley, 1983.
[8] W. Fumy and H. P. Rieß. *Kryptographie*. Oldenburg, München, 2nd edition, 1994.
[9] D. Hankerson, A. Menezes, and S. A. Vanstone. *Guide to Elliptic Curve Cryptography*.Springer, New York, 2004.
[10] D. R. Hankerson, D. G. Hoffman, D. A. Leonard, C. C. Lindner, K. T. Phelps, C. A. Rodger,and J. R. Well. *Coding Theory and Cryptography, the Essentials*. Marcel Dekker, NewYork, 2000.
[11] N. Koblitz. *A Course in Number Theory and Cryptography*. Springer, Berlin, 2nd edition,1994.
[12] N. Koblitz. *Algebraic Aspects of Cryptography*. Springer, Berlin, 1998.
[13] A. G. Kohnheim. *Cryptography, A Primer*. Wiley, New York, 1981.
[14] E. Kranakis. *Primality and Cryptography*. Wiley-Teubner, Stuttgart, 1986.
[15] M. Luby. *Pseudorandomness and Cryptographic Applications*. Princeton University Press,Princeton, 1996.
[16] R. Mathar. *Informationstheorie*. Teubner, Stuttgart, 1996.
[17] A. J.Menezes, P. C. van Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography*.CRC Press, Boca Raton, 1996 (http://www.cacr.math.uwaterloo.ca/hac).
[18] C. H. Meyer and S. Matyas. *Cryptography*. Wiley, New York, 1982.
[19] M. Miller. *Symmetrische Verschlüsselungsverfahren*. Teubner, Stuttgart, 2003.
[20] A. Salomaa. *Public-Key Cryptography*. Springer, Berlin, 1990.
[21] B. Schneier. *Applied Cryptography*. Wiley, New York, 2nd edition, 1996.
[22] B. Schneier. *Secrets and Lies*. Wiley, Indianapolis, 2000.
[23] B. Schneier. *Angewandte Kryptographie*. Wiley, München, 2006.
[24] J. Seberry and J. Pieprzyk. *Cryptography: An Introduction to Computer Security*. Prentice-Hall, New York, 1989.
[25] A. Sinkov. *Elementary Cryptanalysis*. MAA Publications, 1996.
[26] D. R. Stinson. *Cryptography, Theory and Practice*. CRC Press, Boca Raton, 1995.
[27] D. R. Stinson. *Cryptography, Theory and Practice*. Chapman and Hall/CRC, Boca Raton,2nd edition, 2002.
[28] D. R. Stinson. *Cryptography, Theory and Practice, Third Edition*. Chapman and Hall/CRC,Boca Raton, 3rd edition, 2006.

Web References :
1. http://www.slideshare.net/mohammedarif89/cipher-techniques
2. https://en.wikipedia.org/wiki/Cipher
3. https://en.wikipedia.org/wiki/Encryption
4. http://searchsoftwarequality.techtarget.com/definition/cryptography
5. https://en.wikipedia.org/wiki/Algorithm.
6. http://practicalcryptography.com/cryptanalysis
7. http://whatis.techtarget.com/glossary/Network-Security

**AUTHOR'S PROFILE**

**Er. Ganesh Dahane** received his Bachelor of Engineering(B.E) degree in Information Technology in 2006 from Dr. vithalrao vikhe patil college of engineering Ahmednagar, India. He has around three and half year industrial working experience. leader. He received Master of Technology (M.Tech) degree in CSE from LNCT Indore. His area of research is Data structure.