ISSN: 2456-043X

International Journal of Engineering Science and Generic Research (IJESAR)
Available Online at www.ijesar.in
Volume 2; Issue 6; November-December; 2016; Page No. 01-06

CRYPTOGRAPHIC TECHNIQUE BY SQUARE MATRIX AND SINGLE POINT CROSSOVER ON BINARY FIELD

MR.G.RAVI KISHORE [1], MS.SABA NAUSHEEN[2]

[1] Associate Professor, Department of ECE, Vidya Jyothi Institute of Technology, Hyderabad, India

[2] PG Scholar, Department of ECE, Vidya Jyothi Institute of Technology, Hyderabad, India

sabanausheen29@gmail.com

Abstract

We have two types of encryption algorithms symmetric and asymmetric. Symmetric algorithm is encryption and decryption with same key. Asymmetric is encryption and decryption with different keys, like private key and public key. In our proposed algorithm, encryption is performed using Substitution Matrix and single Point Crossover. We require two different keys for encryption and decryption. First substitution generates intermediate cipher from plaintext. Then single point crossover is going to perform on intermediate cipher to get final cipher text. The decryption process is same as the encryption but in Reverse order. This algorithm is implemented in Xilinx 13.2 version and verified using Spartan 3e kit.

Index Terms: Substitution Matrix, Single Point Crossover

Introduction

Encryption is a mechanism that protects your valuable information, such as your documents, pictures, or online transactions, from unwanted people accessing or changing it. Encryption works by using a mathematical formula called a cipher and a key to convert readable data (plain text) into a form that others cannot understand (cipher text). The cipher is the general recipe for encryption, and your key makes your encrypted data unique. Only people with your unique key and the same cipher can unscramble it. Keys are usually a long sequence of numbers protected by common authentication mechanisms, such as passwords, tokens, or biometrics (like your fingerprint) Sensitive information, including medical, financial, or business records, may reside on your mobile devices, such as your laptop, USB stick, Smartphone, or tablet. These devices are easily lost or stolen, and if not encrypted, their contents can be read by anyone who has access to them. One of the best ways to protect data on a mobile device is to encrypt it. In general, there are three ways to encrypt data stored on your mobile devices. You can encrypt specific files, encrypt entire folders, or encrypt the entire hard drive. Most operating systems support one, if not all three, options. Encrypting your entire disk, commonly called full disk encryption (FDE), is often considered the most secure. FDE encrypts all data on your hard drive, including any temporary files. It also simplifies the process, as you do not have to decide what to encrypt and not to encrypt. If you cannot encrypt your entire hard drive, encrypt any files or folders that contain sensitive information. Information is also vulnerable when it's in transit. If the data is not encrypted, it can be monitored and captured online. This is why you want to ensure that any sensitive online communications, such as online banking, sending e-mails, or perhaps even accessing your Face book account, are encrypted. The most common type of online encryption is HTTPS, or connecting to secure websites. This means the traffic between your browser and the website is encrypted. Look for https:// in the URL or the lock icon in your browser. Many sites support this by default (such as Google Apps) and websites like Face book and Twitter give you the option in your account settings to force HTTPS. In addition, when you connect to a public Wi-Fi network, use an encrypted network whenever possible. WPA2 is currently one of the strongest encryption mechanisms and the type you should choose. Finally, whenever sending or receiving e-mail, make sure your email client is set up to use-encrypted channels. One of the most commonly used is SSL (Secure Socket Layer); many e-mail clients use SSL by default. Cryptography is the art of achieving security by encoding messages to make them nonreadable. Cryptography is the practice and study of hiding information. In modern times Cryptography is considered a branch of both mathematics and Computer science and is affiliated closely with information theory, Computer security and engineering. Cryptography is used in applications present in technologically advanced societies; examples include the security of ATM cards, computer passwords and electronic commerce, which all depend on cryptography. There are two basic types of cryptography: Symmetric Key and Asymmetric Key. Symmetric key algorithms are the quickest and most commonly used type of encryption. Here, a single key is used for both encryption and decryption. There are few well-known Symmetric key algorithms i.e. DES, RC2, RC4, IDEA etc. This paper describes cryptography, various symmetric key algorithms in detail and then proposes a new symmetric key algorithm. Algorithms for both encryption and decryption are provided here. In secret key cryptography, a single key is used for both encryptions and decryption. As shown in Figure 2, the sender uses the key (or some set of rules) to encrypt the plaintext and sends the cipher text to the receiver. The receiver applies the same key to decrypt the message and recover the plaintext. Because a single key is used for both functions, secret key cryptography is also called symmetric encryption. With this form of cryptography, it is obvious that both the sender and the receiver must know the key; that, in fact, is the secret. The biggest difficulty with this approach, of course, is the distribution of the key.

Public or asymmetric key cryptography involves the use of key pairs: one private key and one public key. Both are required to encrypt and decrypt a message or transmission. The private key, not to be confused with the key utilized in private key cryptography, is just that, private. It is not to be shared with anyone. The owner of the key is responsible for Securing it in such a manner that it will not be lost or compromised. On the other hand, the public key is just that, public. Public key cryptography intends for public keys to be accessible to all users. In fact, this is what makes the system strong. If a person can access anyone public key easily, usually via some form of directory service, then the two parties can communicate securely and with little effort, i.e. Without a prior key distribution arrangement.

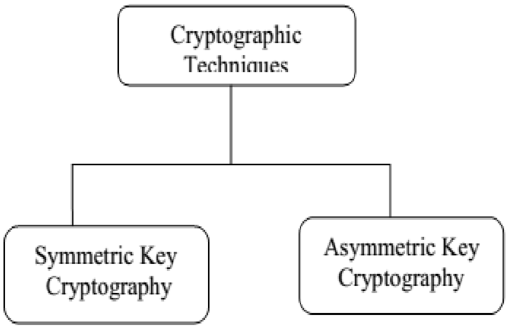


Figure 1 Cryptography techniques

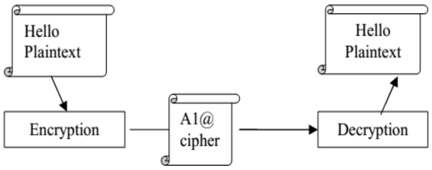
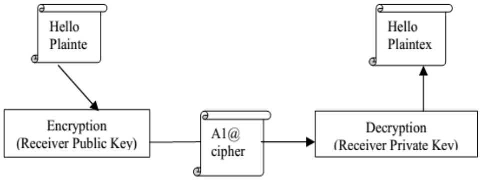
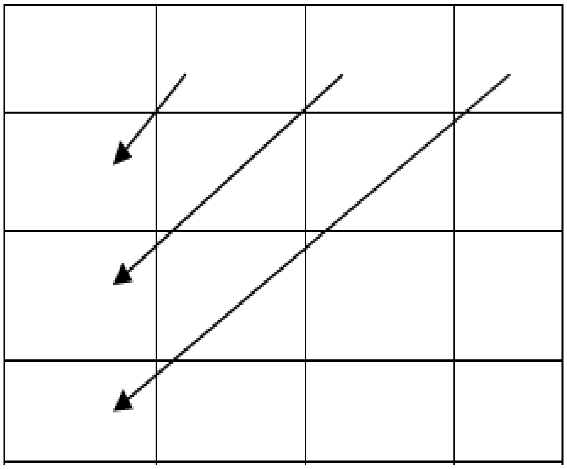


Figure 2 Secret Key Cryptography


Hello Plainte
Encryption (Receiver Public Key)
A1@ cipher
Decryption (Receiver Private Kev)
Hello Plaintex

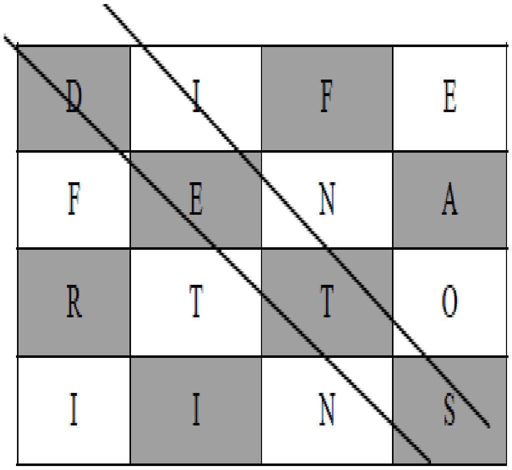
A. PROPOSED ALGORITHM



In the proposed technique placed each letter of input stream into a Substitution matrix. Each letter is placed diagonally in the matrix. Substitution matrix is selected according to the size of input stream. Square number before placing the text into the box. All the letters of intermediate cipher text are converted into its binary code and generate a fixed 5 digit random number. The first digit of random number is the section number by which all the bits are divided into small sections. If there is any remainder part, then will be discarded for future use. Each section is divided into blocks according to the last 4 digits of random number. This 5 digit random number is Key – 2. Genetic function double point crossover is followed on blocks of bits of each section. The total block number of a section/partition is even, each block crossed over with the next block and produce Level 1 child blocks otherwise first block, N block (where N is odd) and second block, fourth block is crossed over and so on to produce Level 1 child blocks.

a. SUBSTITUTION MATRIX

Let the Plain text is DIFFERENTIATIONS Size of the plain text is 16. Squire Matrix has been taken 4*4 and all letters of plaintext is placed into the box of the matrix according to the proposed technique which is shown in the



D	I	F	E
F	E	N	A
R	T	T	O
I	I	N	S

Key 1= Position Value of 'D' + Position Value of 'E' +Position Value of 'T' + Position Value of 'S' = 4 + 5 + 20 +19 = 48 [Where, A=1……………z=26]Now the Key 1 will be added with each letter's position value of matrix to generate the intermediate cipher text.

D = 4 + 48 = 52 = **Z**,

I = 9 + 48 = 57 = **E**,

F = 6 + 48 = 54 = **B**,

E = 5 + 48 = 53 = **A**,

F = 6 + 48 = 54 = **B**,

E = 5 + 48 = 53 =**A**,

N = 14 + 48 = 62 = **J**,

A = 1 + 48 = 49 = **W**,

R = 18 + 48 =66 = **N**,

T = 20 + 48 = 68 = **P**,

T = 20 + 48 = 68 = **P**,

O = 15 +48 = 63 = **K**,

I = 9 + 48 = 57 = **E**,

I = 9 + 48 = 57 = **E**,

N = 14+ 48 = 62 = **J**,

S = 19 + 48 = 67 = **O** Intermediate cipher text:

ZEBA BAJW NPPK EEJO

B. SINGLE POINT CROSSOVER

5 digit fixed random number has been generated as Key – 2. The Randomly generated number is: 54623 (Key – 2)Depending on the Key – 2, 1024 bits will be partitioned into 5 Sections, because the first digit of Key – 2 is 5 and each Section will be divided into 4, 6, 2, 3 blocks respectively as Because 4, 6, 2, 3 are the next digits of Key 2.

Section 1 is divided into 4 blocks.

Section 2 is divided into 6 blocks.

Section 3 is divided into 2 blocks.

Section 4 is divided into 3 blocks

Section 5 divided into 4 blocks.

Each section contains (1024 / 5) bits = 204 bits.

Discard the remainder (1024 % 5) bits = 4 bits for future use.

Partition 1 (Each Block contain (204 / 4) bits or 51 bits)

Partition 2 (Each Block contain (204 / 6) bits or 34 bits)

Partition 3 (Each Block contain (204 / 2) bits or 102 bits)

Partition 4 (Each Block contain (204 / 3) bits or 68 bits)

Partition 5 (Each Block contain (204 / 4) bits or 51 bits)

Total block number of each partition will be treated as Pivot Point or Crossover Point. "X" symbol is represented crossover in the following.

Single point crossover

a

0	1	2	3

b

0	1	2	3

a(0)	b(1 to 2)	a(3)

b(0)	a(1 to 2)	b(3)

Partition 1: Number of Blocks 4 (Even)
Block1 X Block2
Block3 X Block4

Partition 2: Number of blocks 6 (Even)
Block1 X Block2
Block3 X Block4
Block5 X Block6

Partition 3: Number of Blocks 2 (Even)
Block1 X Block2

Partition 4: Number of Blocks 3 (Odd)
Block1 X Block3
Block 2 will remain same

Partition 5: Number of Blocks 4 (Even)
Block1 X Block2
Block3 X Block4

Concatenate all child blocks section/partition wise and discarded bits ‘0101’ to produce cipher text in binary form. Length of the binary field will be 1024 bits. 1024 bits will be divided into 16 blocks of each 64 bits.

The **DECRYPTION** process is similar to the above encryption process but follows the reverse order.
Total number of bits: 1024

Key 1 = 48 and Key 2 = 54623
1024/5=204
1024 % 5=4;
Discard the last four bits ‘0101’ and store it for future use.
According to Key 2, 1024 bits will be divided into 5 Sections/partitions.

Partition 1 (Each Block contain (204 / 4) bits or 51 bits)

Partition 2 (Each Block contain (204 / 6) bits or 34 bits)

Partition 3 (Each Block contain (204 / 2) bits or 102 bits)

Partition 4 (Each Block contain (204 / 3) bits or 68 bits)

Partition 5 (Each Block contain (204 / 4) bits or 51 bits)

Partition 1: Number of Blocks 4 (Even)
Block1 X Block2
Block3 X Block4

Partition 2: Number of blocks 6 (Even)
Block1 X Block2
Block3 X Block4
Block5 X Block6

Partition 3: Number of Blocks 2 (Even)
Block1 X Block2

Partition 4: Number of Blocks 3 (Odd)
Block1 X Block3
Block 2 will remain same

Partition 5: Number of Blocks 4 (Even)
Block1 X Block2
Block3 X Block4

Now partitions are made in the similar order as in encryption process and then Decryption algorithm is applied of genetic function to generate the intermediate cipher text. Block number of each partition is pivot point or crossover point. “X” represents crossover.

Concatenate all child blocks section/partition wise and discarded bits ‘1111’ to produce intermediate cipher text in binary form. Length of the binary field will be 1024 bits. 1024 bits will be divided into 16 blocks of each 64 bits.

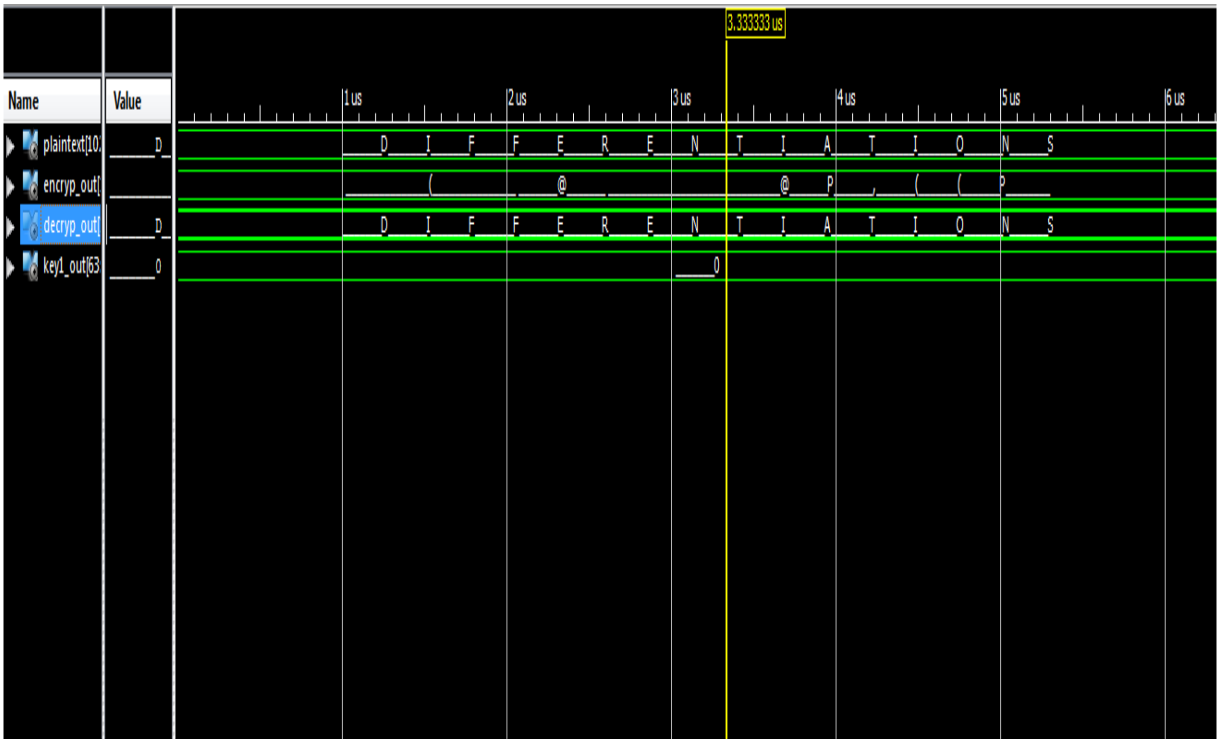
The intermediate cipher text will be as given below in ASCII value

Intermediate cipher text = ZEBA BAJW NPPK EEJO.
Now c1<= ((position of Z)+52)-(key1)=26+52-key1=4=D, calculating similarly we get
The final plaintext text output as DIFFERENTIATIONS.
Similarly the whole data will undergo the same process producing the original message...” DIFFERENTIATIONS”

C. CONCLUSION

In the proposed technique two keys is used which will increase the security of the proposed algorithm. Genetic function double point crossover is used to make the technique susceptible from the attacker. Different block division process in binary field of intermediate Cipher confirms the more security of the algorithm.

VI.SIMULATION WAVEFORMS



D. REFERENCES

1. S. Som, M. Banerjee, “Cryptographic Technique Using Substitution through Circular Path Followed By Genetic Function”, CCSN-2012, 1stInternational conference on Computing, Communication and Sensor Network, November 22ndand 23rd, 2012, Roukela, India. Accepted
2. Poonam Garg, “Genetic algorithms and simulated annealing: a comparison between three approaches for the crypto analysis of transposition cipher” IMT, INDIA-2004.
3. A.J.Bagnall, “The Applications of Genetic Algorithms in Cryptanalysis”, School of Information Systems, University Of East Anglia, 1996.
4. N.Koblitz, “A Course in Number Theory and Cryptography‟, Springer-Verlag, New York, Inc., 1994.
5. Menzes A. J., Paul, C., Van Dorschot, V., Vanstone, S. A., “Handbook of Applied Cryptography”, CRS Press 5th Printing; 2001.
6. National Bureau Standards, “Data Encryption Standard (DES),” FIPS Publication 46; 1977.
7. Tragha A., Omary F., Mouloudi A.,”ICIGA: Improved
8. Cryptography Inspired by Genetic Algorithms”, Proceedings of the International Conference on Hybrid Information Technology (ICHIT'06), pp. 335-341, 2006. [8] Melanie Mitchell, “An introduction to Genetic Algorithms”. A Bradford book.

9. H. Bhasin and S. Bhatia, “Application of Genetic Algorithms in Machine learning”, IJCSIT, Vol. 2 (5), 2011.

10. Pisinger D (1999). "Linear Time Algorithms for Knapsack Problems with Bounded Weights". Journal of Algorithms, Volume 33, Number 1, October 1999, pp. 1–14.

11. Harsh Bhasin, “Use of Genetic Algorithms for Finding Roots of. Algebraic Equations”, IJCSIT, Vol. 2, Issue 4.

12. Yu Tak Ma, David K. Y. Yau, Nung Kwan Yip and Nageswara S. V. Rao“Extended Abstract: Cipher Techniques to Protect Anonymized Traces from Privacy Attacks”, 10th International Conference, ACNS 2012, Singapore, June 26-29, 2012.

13. Wensheng Zhang and Chuang Wang, “AdHocSign: an Ad Hoc Group Signature Scheme for Accountable and Anonymous Access to Outsourced Data”, 10th International Conference, ACNS 2012, Singapore, June 26-29, 2012.

14. Dr. G. Raghavendra, Nalini N, “a new encryption and decryption algorithm combining the features of genetic algorithm (GA) and cryptography” NIE, Mysore.

15. J. Bagnall, “the application of genetic algorithms in cryptanalysis” School of information system, University of East Anglia, 1996

16. N. Koblitz, “a coursein number theory and ryptography’, Springer- verlag, New York, 1994

17. R. Toeneh, S. Arumugam, “Breaking Transposition ipher with genetic algorithm”, Chennai, India

18. Bethany Delman, “Genetic algorithm in cryptography”, Rochester, New York, July – 2004

19. Atul Kahate, “Cryptography and Network Security” 2ndedition, TATA McGRAW HILL

20. Ankita Agarwal, “Secret Key Encryption Algorithm Using Genetic Algorithm”, IJARCSSE, Volume 2, Issue 4, April 2012