SCAN PATTERNS FOR KEY GENERATION

[1]Dr. R. Pradeep Kumar Reddy,[2]Dr. S. Kiran,[3]Dr. A. Ashok Kumar
[1]Assistant Professor, [2]Assistant Professor ,[3]Assistant Professor ,
[1,2]Department of Computer Science and Engineering, [3]Department of Physics,
[1]Y.S.R Engineering College of Yogi Vemana University, Proddatur, India.

Abstract : Day to day with the heavy usage of networks, it became very difficult to provide security to the data. Many Steganography and Cryptography algorithms are existing in networks to solve security issues. At one end researchers are proposing so many different techniques to provide security to the data and at the other end the development of unauthorized access mechanisms are also increasing rapidly to break these security methods. Hence there is more urge to develop new methodologies which increases the complexity to prevent unauthorized access to the data and fixes the vulnerabilities of security. In this paper some innovative methods such as Scan patterns, Crossover operation and Elegant Pairing functions are implemented step by step to encrypt the text in which selection of partition pattern plays a vital role. The proposed methods were simple enough and robust in the process of providing security using scan pattern.

Index Terms **- Steganography, Cryptography, Scan Patterns, Crossover Operation, Elegant Pairing.**

I. INTRODUCTION

In this digital era, the data security is very important and high priority topic. With rapid growth in communication and computer technologies, there is a huge data transaction in teleconferencing and military applications. These applications are the fast-growing technology trend but security and privacy are still largely ignored. Since they are hard to achieve, because of their limited computation and energy resources available at all levels.

However, providing security to the data is a requirement for all these applications. Various encryption algorithms have been proposed recent years as possible solutions for the protection of the data. But the basic problem with these encryption algorithms is that they have high encryption time, making them unsuitable for real time applications. In this project different techniques are applied to provide better security to the data.

1.1 Objective

The main objective of this project is to provide security to the data. Convert the bits into ASCII values and then convert them into binary. Select middle values from the binary by excluding MSB. Various partition patterns are to be applied to generate the key. Then different techniques like XOR operation, Two's complement, Crossover operation and Elegant pairing functions are used step by step to obtain ciphertext. Decryption is the exactly reverse process converting cipher text to plaintext by using these techniques.

1.2 Scope

The scope of this paper is to provide security by different techniques which reduces computational power and overheads in communication. Following are the modules of proposed system.

1.3 Key Generation

- Convert plaintext into ASCII values.
- Convert ASCII to binary values.
- Middle values are selected from these binary values and partition patterns are applied.
- Key is generated.

1.4 Encryption

- XOR operation is done between plaintext and key.
- Two's complement is performed to the result.
- Crossover operation is applied.
- Elegant pairing function is applied to the result.
- Ciphertext is obtained after encryption.

1.5 Decryption

- Elegant unpairing function is applied to the ciphertext.
- Crossover operation is to be performed.
- Two's complement is done to the result.
- XOR operation is performed to the result and the key.
- Plaintext is obtained after decryption.

1.6 Why Do We Need Cryptography

One might need cryptography in any situation which warrants privacy or secrecy to protect data, trade secrets, or embarrassing situations. Examples include business transactions, E-commerce, extramarital affairs, political campaigns, and Government actions. The art of protecting information by transforming it into an unreadable format, called Cryptography. It is a science that applies complex mathematics and logic to design strong encryption methods. The plaintext converted into ciphertext by using key is called encryption. Only those who possess a secret key can decipher the message into plaintext. Encrypted messages can sometimes be

broken by cryptanalysis, also called code breaking, although modern cryptography techniques are virtually unbreakable. As the Internet and other forms of electronic communication become more prevalent, the need for security is growing. Cryptography is used to protect messages, credit card information, and corporate data.

Cryptography systems can be broadly classified into two categories.

1.Symmetric Cryptograph

2.Asymmetric Cryptograph

Symmetric Cryptography:

The symmetric cryptography uses a single key. Single key is used for both encryption and decryption. The sender and recipient share the same key.

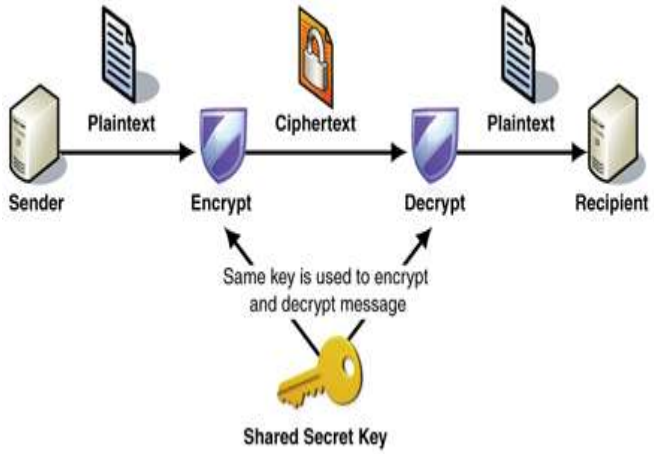

Fig.1.1: *Symmetric key cryptography*

Asymmetric Cryptograph:

The asymmetric cryptography uses two keys.

1. Public key 2. Private key

Public key is to be known by everyone. Private key is known to a single person. In this cryptography system one key is used for encryption where another key is used for decryption.

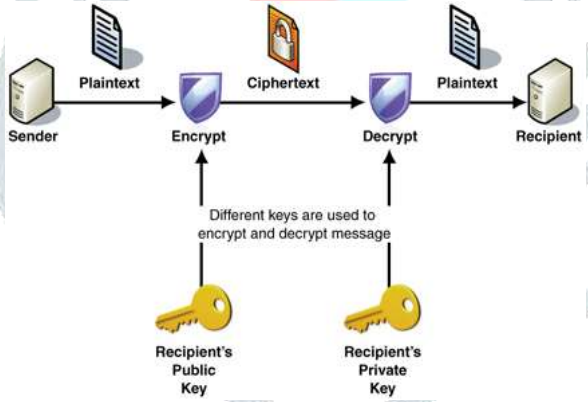

Fig.1.2: Asymmetric key cryptography

Cryptography is the practice and study of techniques for secure communication in the presence of third parties. More generally, it is about constructing and analyzing protocol that overcome the influence of adversaries and which are related to various aspects in information security.

Modern cryptography intersects the disciplines of Mathematics, Computer Science, and Electrical Engineering. Applications of cryptography include ATM card, computer passwords, and electronic commerce.

Cryptography prior to the modern age was effectively synonymous with encryption, the conversion of information from a readable state to apparent nonsense. The originator of an encrypted message shared the decoding technique needed to recover the original information only with intended recipients, thereby precluding unwanted persons to do the same. Since World War I and the advent of the computer, the methods used to carry out cryptology have become increasingly complex and its application more widespread.

Modern cryptography is heavily based on mathematical theory and computer science practice, cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary. It is theoretically possible to break such a system but it is infeasible to do so by any known practical means.

Classical Encryption Technique

Plaintext- original message

Cipher text – coded message

Enciphering(or)encryption – process of converting plaintext to cipher text

Deciphering(or)decryption – restoring the plaintext from the cipher text.

II. PROPOSED METHOD

2.1 Proposed System

In the proposed method, it is hard to evaluate the key for the third party since it generates multiple keys. In this method no separate key generation algorithm is used as key is entrenched in the text itself. So, that it provides more security. Here it uses some logical operations for the encryption as well as for decryption. Encryption and decryption are performed in three rounds. Pairing functions are used to arrange the intermediate cipher text into final cipher text.

2.2 Methods Used in Proposed System

Crossover

In genetic algorithms, crossover is a genetic operator used to vary the programming of a chromosome from one generation to the next. Cross over is a process of taking more than one parent solutions and producing a child solution from them. There are methods for selection of the chromosomes. Those are also given below.

Crossover Techniques

Many crossover techniques exist for organisms which use different data structures to store themselves.

Single-point Crossover

A single crossover point on both parents' organism strings is selected. All data beyond that point in either organism string is swapped between the two parent organisms. The resulting organisms are the children.

Two-point Crossover

Two-point crossover calls for two points to be selected on the parent organism strings. Everything between the two points is swapped between the parent organisms, rendering two child organisms:

Uniform Crossover and Half Uniform Crossover

The uniform crossover uses a fixed mixing ratio between two parents. Unlike single- and two-point crossover, the uniform crossover enables the parent chromosomes to contribute the gene level rather than the segment level. If the mixing ratio is 0.5, the offspring has approximately half of the genes from first parent and the other half from second parent, although cross over points can be randomly chosen. The uniform crossover evaluates each bit in the parent strings for exchange with a probability of 0.5. Empirical evidence suggests that it is a more exploratory approach to crossover than the traditional exploitative approach that maintains longer schemata. This results in a more complete search of the design space with maintaining the exchange of good information. Unfortunately, no satisfactory theory exists to explain the discrepancies between the uniform crossover and the traditional approaches.

Three Parent Crossover

In this technique, the child is derived from three randomly chosen parents. Each bit of the first parent is compared with the same bit of the second parent. When these bits are the same it is used in the offspring, otherwise the bit from the third parent is used in the offspring. For example, the following three parents:

p_1 110100010
p_2 011001001
p_3 110110101

Will produce the following offspring:

o_{p1p2p3} 110100001

Crossover for ordered chromosomes

Depending on how the chromosome represents the solution, a direct swap may not be possible. One such case is when the chromosome is an ordered list, such as an ordered list of the cities to be travelled for the travelling salesman problem. There are many crossover methods for ordered chromosomes. The already mentioned N-point crossover can be applied for ordered chromosomes also, but this always needs a corresponding repair process, actually, some ordered crossover methods are derived from the idea. However, sometimes a crossover of chromosomes produces recombination's which violate the constraint of ordering and thus need to be repaired.

Elegant Pairing

In mathematics a pairing function is a process to uniquely encode two natural numbers into a single natural number. When x and y are non-negative integers, elegant Pair (x, y) function outputs single non-negative integer that is uniquely associated with that pair. The inverse function elegant Unpair(z) outputs the pair associated with each non-negative integer

Logical XOR

The logical XOR gate is also called Exclusive disjunction. It gains the name "exclusive or" because the meaning of "or" is ambiguous when both operands are true; the exclusive or operator excludes that case. Its output is "TRUE" if the inputs are the different, and "FALSE" if the inputs are same.

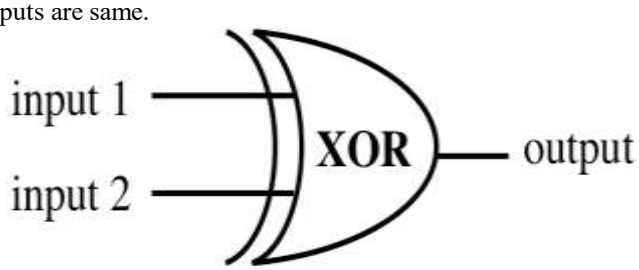

Fig 2.1: *Two's Complement*

Representation of XOR

Two's complement as shown in fig 2.1 is a mathematical operation on binary numbers, as well as binary signed number representation based on this operation. Its wide use in computing makes it the most important example of a radix complement.

2.3 Encryption and Decryption

General working procedure of encryption and decryption is as shown in Fig 2.2

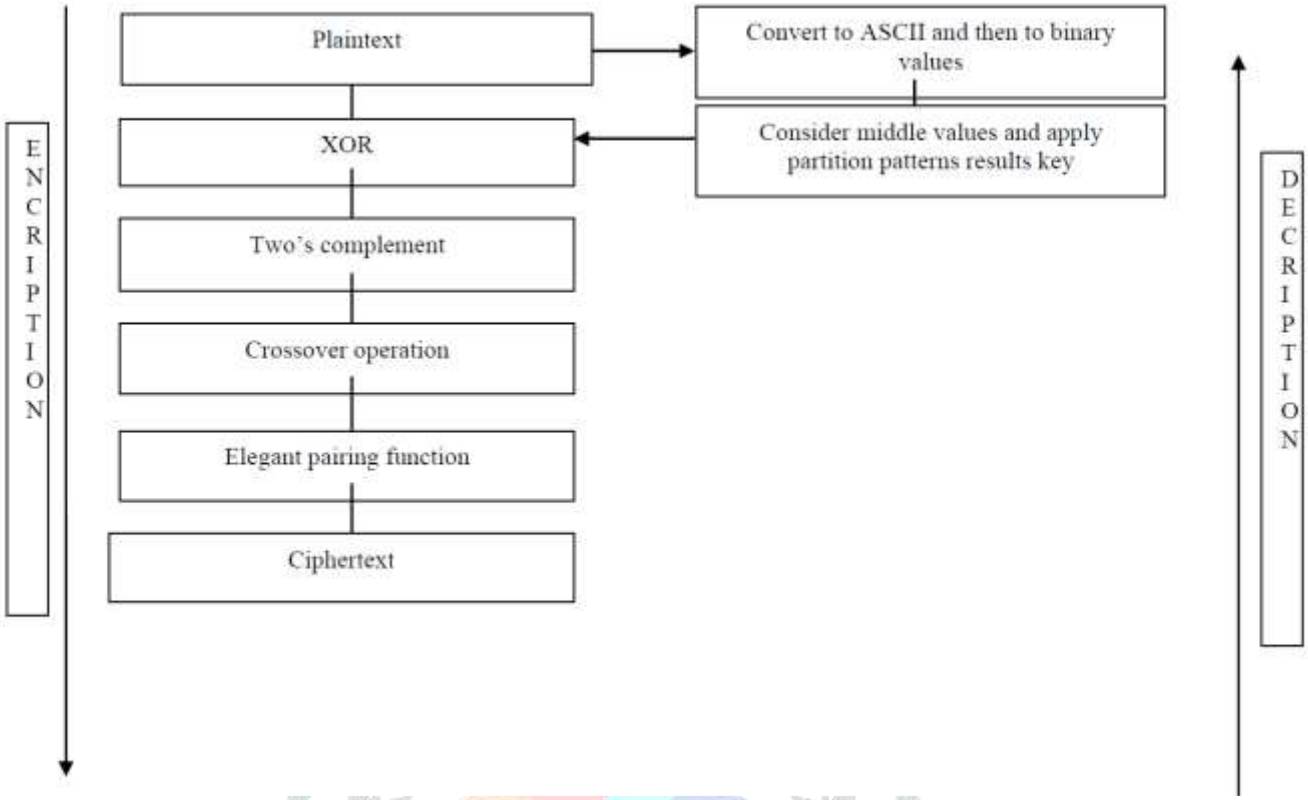

***Fig 22**: General working procedure for proposed system*

2.4 Encryption in Proposed System

Proposed method processed in four rounds of encryption as follows. Initially it reads the file as input and converts it into equivalent ASCII values. Then, equivalent binary values are calculated for the corresponding ASCII values. From the calculated binary values middle bits are taken by excluding MSB. Partition patterns are applied to this middle bit's which generates key. XOR is performed to the key and plaintext in round1. Two's complement is taken for the result after XOR in round-2. In round-3 crossover operations is performed and elegant pairing function is applied to the result in round-4.

Round 1:

In the first round of encryption, we are taking ASCII values to plaintext and converting them into binary. Middle bits are collected from those binary and partition patterns are applied which generates key taking. Logical XOR operation is performed to the Key and the ASCII values of plain text.

Round 2:

In the second round of encryption, two's complement is performed to the result of Round 1. The two's complement is performed by converting the binary value into one's complement and adding one to it. One's complement is obtained by inverting the binary values.

Round 3:

In third round of encryption, crossover operation is performed to the result of round 2. The crossover can be performed by considering two or more parent values and generating a child value. The value after the crossover operation is different to the previous value.

Round 4:

In fourth round of encryption, elegant pairing function is applied to the result of round 3. In this elegant pairing function, the size of the text is reduced to half. This function takes two values as inputs and gives only one value as output.

2.5 Decryption in Proposed System

The two's complement of an N-bit number is defined as the complement with respect to 2^N. This is also equivalent to taking the one's complement and then adding one, since the sum of a number and its ones' complement is all 1 bits. The two's complement of a number behaves like the negative of the original number in most arithmetic, and positive and negative numbers can coexist in a natural way.

In two's-complement representation, positive numbers are simply represented as themselves, and negative numbers are represented by the two's complement of their absolute value; In general, negation (reversing the sign) is performed by taking the two's complement. This system is the most common method of representing signed integers on computers. An N-bit two's-

complement numeral system can represent every integer in the range $-(2^{N-1})$ to $+(2^{N-1}-1)$ while one's complement can only represent integers in the range $-(2^{N-1}-1)$ to $+(2^{N-1}-1)$. The sum of a number and its two's complement will always equal 0 (since the last digit is truncated), and the sum of a number and its one's complement will always equal -0.The two's-complement system has the advantage that the fundamental arithmetic operations of addition, subtraction, and multiplication are identical to those for unsigned binary numbers.

Round 1:

In the first round of decryption it takes the input as the cipher text. Here the cipher text will be subjected to the elegant unpairing function. The size of the ciphertext is doubled after unpairing. Pairing function that means here the intermediate cipher text is obtained as like the result generated after third round of encryption.

Round 2:

Crossover operation is performed on the intermediate cipher text in this second round of decryption. After this crossover operation in the decryption the result is equal to the encrypted result at second round.

Round 3:

In the third round of decryption it takes the input as result of the second round. Two's complement is performed. After this decryption process the result is the one obtained in encryption after completion of the first round.

Round 4:

In this fourth round of decryption the result obtained after twos complement is XOR. XOR operation is performed between the result and the key. Thus, the resultant plaintext is obtained in this decryption.

III ALGORITHMS FOR ENCRIPTION AND DECRIPTION WITH EXAMPLES

3.1 Algorithm for Encryption:

Step 1: Start.
Step 2: Read the plain text.
Step 3: Convert plaintext into equivalent ASCII values and convert them into binary.
Step 4: Take middle values from each ASCII value and apply partition patterns which results key.
Step 5: XOR operation is done between plaintext and key. The result is two's complemented.
Step 6: Crossover operation is performed to the result and elegant pairing function is applied.
Step 7: Here we can get cipher text where size is reduced to half of the original size.

3.2 Algorithm for decryption:

Step 1: Start.
Step 2: Read the resultant cipher text as the input file.
Step 3: Elegant unpairing function is applied to the cipher text.
Step 4: Crossover operation is to be performed to the result.
Step 5: The result is to be two's complemented.
Step 6: XOR operation is done to the result after two's complement and the key.
Step 7: Thus the obtained result is the plaintext.
Step 8: Stop.

3.3 Example for Encryption

Let us consider plaintext "ysreccse". The encryption and decryption are done as shown below.
Encryption:
Step 1: Start
Step 2: plaintext: ysreccse
Step 3: ASCII values for plain text are

y – 121
s – 115
r – 114
e – 101
c – 99
c – 99
s – 115
e – 101

The binary values for those ASCII values are

121 – 01111001
115 – 01110011
114 – 01110010
101 – 01100101
99 – 01100011
99 – 01100011
115 – 01110011

101 – 01100101

Step 4:

Middle values obtained by eliminating MSB are 10000000

Partition patterns are to be applied to the result.

We select any one of the pattern B0 pattern is selected and applied. The patterns b0 and its complement are applied and the key is generated.

Key : 01000000

Step 5:

XOR operation is performed to plaintext and key.

y – 01111001
01000000
00111001

s – 01110011
01000000
00110011

r – 01110010
01000000
00110010

e – 01100101
01000000
00100101

c – 01100011
01000000
00100011

c – 01100011
01000000
00100011

s – 01110011
01000000
00110011

e – 01100101
01000000
00100101

Two's complement is performed to the results obtained after XOR.

	Result after XOR		Result after two's complement
y	- 00111001	-	11000111
s	- 00110011	-	11001101
r	- 00110010	-	11001110
e	- 00100101	-	11011011
c	- 00100011	-	11011101
c	- 00100011	-	11011101
s	- 00110011	-	11001101
e	- 00100101	-	11011011

Step 6:

Crossover operation is performed to the result.

1100 0111	11001101 - 205
1100 1101 ↓	11000111 - 199
1100 1110	11001011 - 203
1101 1011 ↓	11011110 - 222
1101 1101	11011101 - 221
1101 1101 ↓	11011101 - 221
1100 1101	11001011 - 203
1101 1011 ↓	11011101 – 221

Elegant pairing function is applied to the resulted decimal values

205,199 - 42429
203,222 - 49487
221,221 - 49283
203,221 - 49044

Step 7: The obtained ciphertext is 42429 49487 49283 49044

3.4 Example for Decryption process

Step 1: Start ⊕

Step 2: Ciphertext obtained after encryption is given as input.

Input – 42429 49487 49283 49044

Step 3: Elegant unpairing function is applied to the cipher text and those decimal values are converted into binary.

42429 – 205,199
49487 – 203,222

49283 – 221,221
49044 – 203,221

Step 4: Crossover operation is performed to the obtained result.

1100 1101	11000111
↓	
1100 0111	11001101
↓	
1100 1011	110011100
1101 1110	11011011
1101 1101	11011101
↓	
1101 1101	11011101
1100 1011	11001101
↓	
1101 1101	11011011

Step 5:

Two's complement is to be performed. The results obtained after two's complementing the results in step 4 are

00111001
00110011
00110010
00100101
00100011
00100011
00110011
00100101

Step 6: XOR operation is performed between the result and the key.

```
  00111001
  01000000
  --------
  01111001
  00110011
  01000000
  --------
  01110011
  00110010
  01000000
  --------
  01110010
  00100101
  01000000
  --------
  01100101
  00100011
  01000000
  --------
  01100011
  00100011
  01000000
  --------
  01100011
  00110011
  01000000
  --------
  01110011
  00100101
  01000000
  --------
  01100101
```

Step 7: The obtained result is

01111001 – y
01110011 – s
01110010 – r
01100101 – e
01100011 – c
01100011 – c
01110011 – s
01100101 – e

Thus plaintext "ysreccse" is obtained after decryption.

Step 8: Stop.

IV CONCLUSION

Security plays an important role in the communication channel via an untrusted media such as Internet. In order to protect the data from hackers or intruders and unauthorized persons, one need better security standards.

The proposed method is providing better security when compared to existing method. In this paper we have used four different techniques to provide better security. They are XOR, Two's complement, Crossover operation, and Elegant pairing. Hence the

encrypted text is difficult to break. Partition patterns and Pairing function used in this project are distinct techniques that cannot be seen in general algorithms which are the strengths of this proposed method.

V FUTURE ENHANCEMENT

The design, development, deployment and testing of security problem has been successfully demonstrated by the use of different partition patterns, XOR operation, two's complement, crossover operation, elegant pairing function. In future the effort can be put on to extend the work to cloud computing, to read the text, and encrypted, decrypted by applying all these techniques. Another point which is left to the future development is the applied techniques can be interchangeably used in order to encrypt the text. Extensions of this work could be the investigation of new partition patterns applied efficiently for data transformation. Hence there is a lot of future scope of the research work to be carried out in this area for great significance to mankind.

References

[1]. William Stallings, "Cryptography and Network Security: Principles and Practices", 4th edition, Prentice Hall, 2006.

[2]. A Novel Symmetric Key Cryptographic Technique at Bit-Level based on Spiral Matrix Concept, International Conference on Information Technology, Electronics and Communications (ICITEC - 2013), Bangalore, India, March 30-31, 2013.

[3]. Jeff Connelly: A Practical Implementation of a One Time Pad Cryptosystem-CPE 456, June 11, 2008.

[4]. Ms. Drashti H. Bhatt1, Mr. Kirit R. Rathod, Mr. Shardul J. Agravat, "A Study of Local Binary Pattern Method for Facial Expression Detection", International Journal of Computer Trends and Technology (IJCTT) – volume 7 number 3– Jan2014, pagenumbers152-153.

[5]. Tata Mc Graw-Hill Edition 2005, Java, The Complete Reference, J2SE fifth edition by Herbert Schildt.

[6]. NidhiSinghal, J.P.S.Raina "Comparative Analysis of AES and RC4 Algorithms for Better utilization" International Journal of Computer Trends and Technology-July to Aug Issue 2011.

[7]. D. KHAN, "The Codebreakers", Macmillan Publishing Company, New York, 1967.

[8]. P. P Charles & P. L. Shari, "Security in Computing: 4th edition", Prentice-Hall, Inc.,2008.

[9]. A. S. Tanenbaum, "Modern Operating Systems", Prentice Hall, 2003.

[10]. JananAteya Mahdi, Design and Implementation of proposed B-R Encryption Algorithm, IJCCCE, VOL.9, NO.1, 2009