2nd International Conference on Current Research Trends in Engineering and Technology
ET | Volume 4 | Issue 5 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Pattern Based Data Security Algorithm

Mansi Patel, Meet Patel, Nancy Patel, Ajaysinh Rathod
B.E. Computer, Vadodara Institute of Engineering, Vadodara, Gujarat, India

ABSTRACT

During the last decades, information security has become an area of concern. Encrypting and decrypting data has been widely developed because there is a demand for a highly secured data in today's world. Encryption, is the process of changing intelligible data into unintelligible data which is unreadable by anyone except those possessing special knowledge (usually referred to as a "key") that allows them to change the information back to the original form. Encryption is important because it secures the data that you don't want anyone else to have access to. People try to protect their physical assets such as networked computers, databases, servers, etc. Encryption protects the data that lives on and between those devices. It is one of the most powerful way to keep your data safe, and while it isn't impenetrable, it's a major deterrent to hackers. Even if data does end up getting stolen, it will be unreadable and nearly useless if it's encrypted. "Pattern Security" provides new encryption methodology without the use of key. The method follows the rules of pattern which is already designed by the organization. The pattern security provides three level database security. The ultimate goal of Pattern Security is Easy Encryption and Difficult Decryption.

Keywords: - Encryption, Decryption, Plain Text, Cipher Text, Patterns, Binary Value, Decimal Value

I. INTRODUCTION

In daily life we use information for various purposes and use network for communication and exchange information between different parties. In many cases this information is sensitive so we need to take care that only authorized party can get that information. For maintaining such privacy, we require some mechanism or physical device which ensures that it is safe. Such mechanism or physical device are known as security system. Computer security protection afforded to an automated system in order to attain the applicable objectives of preserving the **integrity, availability,** and **confidentiality** of information system resources. To provide security to the data cryptography plays an important role.

Cryptography is the area of study containing the principles and methods of transforming an intelligible message into one that is unintelligible, and then retransforming that message back to its original form. Applications of cryptography include electronic commerce, chip-based payment cards, digital currencies, computer passwords and military communications. Cryptography prior to the Modern age was effectively synonymous with **encryption**.

Encryption is the process or algorithm of transforming an intelligible message into an unintelligible message. In technical terms we can say that **Encryption** is the process of transforming **plain text** into **cipher text**(meaningless) by applying key.

ET | Volume 4 | Issue 5 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

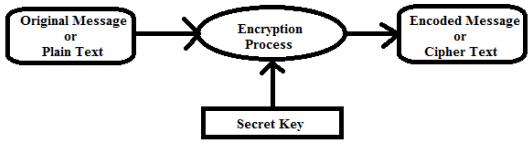


Fig.1 Encryption Process

Decryption is the reverse process of encryption. Here, the plain text is obtained back from the available cipher text by applying key in vice-versa.

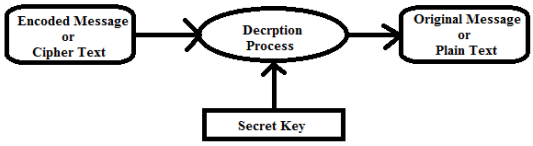


Fig.2 Decryption Process

Cryptographic systems are characterized along three independent dimensions:

1. **The types of operations used for transforming plain text to cipher text.**
   All encryption algorithms are based on two general principles **substitutions** and **transpositions**.

2. **The number of keys used.**
   If both sender and receiver use the **same key**, the system is referred to as **symmetric, single-key, secret-key, or conventional encryption**.
   If the sender and receiver use **different keys** the system is referred to as **asymmetric, two-key or public-key encryption**.

3. **The way in which the plain text is processed.**
   A **block cipher** process a block at a time and produce an output block for each input block.
   A **stream cipher** process the input element continuously, producing output one element at a time, as it goes along.

II. LITERATURE REVIEW

As we know to provide security we need some mechanism. This mechanism is an encryption algorithm. There are so many algorithms available for encryption. Among them Caesar cipher is the easiest and simplest algorithm. Due to less combination of key value pair it is very easy to break the same for any hacker. Frequency of the letter pattern provides a big clue in deciphering the entire message. Hence Caesar cipher is not widely used for providing high security of the data.

The most secure algorithm till date is AES. It follows 18 rounds of substitution and transformation techniques. But still AES is not practically applicable for banking, militaries, money transfer services, etc. to encrypt the data with instance of time. Now-a-days, all the web developers have to mention code to detect and prevent the security related issues[10].

The organizations are using some encryption algorithms to protect the data. But still their security mechanism is not efficient to prevent hacking. So we require that kind of algorithms whose ultimate goal is to provide easy encryption and difficult decryption.

III. INTRODUCTION TO PATTERN SECURITY

"Pattern security" is an algorithm for encryption using patterns that represent a character. As we know that for any encryption algorithm there is a need for a key, but in this algorithm there is **no key value**. Here we have a **pattern to represent a character**. Fig.3 makes it clear to understand.

ET | Volume 4 | Issue 5 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

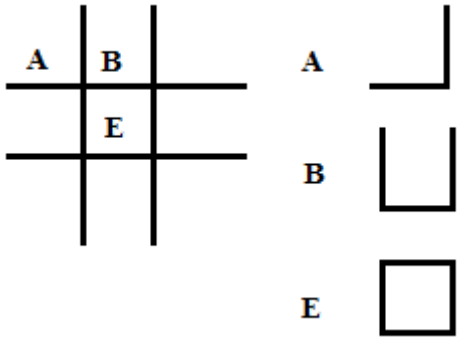
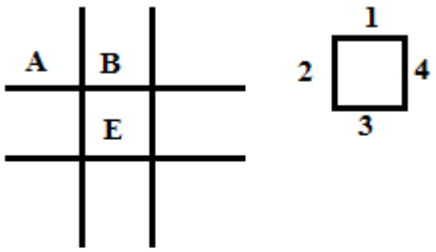


Fig.3
Representation of character as pattern

But computationally it is not possible to store such pattern as a data. So there arise a need to convert pattern into some data. Mathematical operations are used in this algorithm to convert the pattern into data. Fig.4 depicts the conversion of pattern to binary string. Mainly **binary-decimal conversion and ASCII conversion** is used. Hence it is a type of **stream cipher** using **substitution** technique.



	1	2	3	4
A	0	0	1	1
B	0	1	1	1
E	1	1	1	1

Fig.4 conversion of pattern to data

FLOWCHART FOR ENCRYPTION

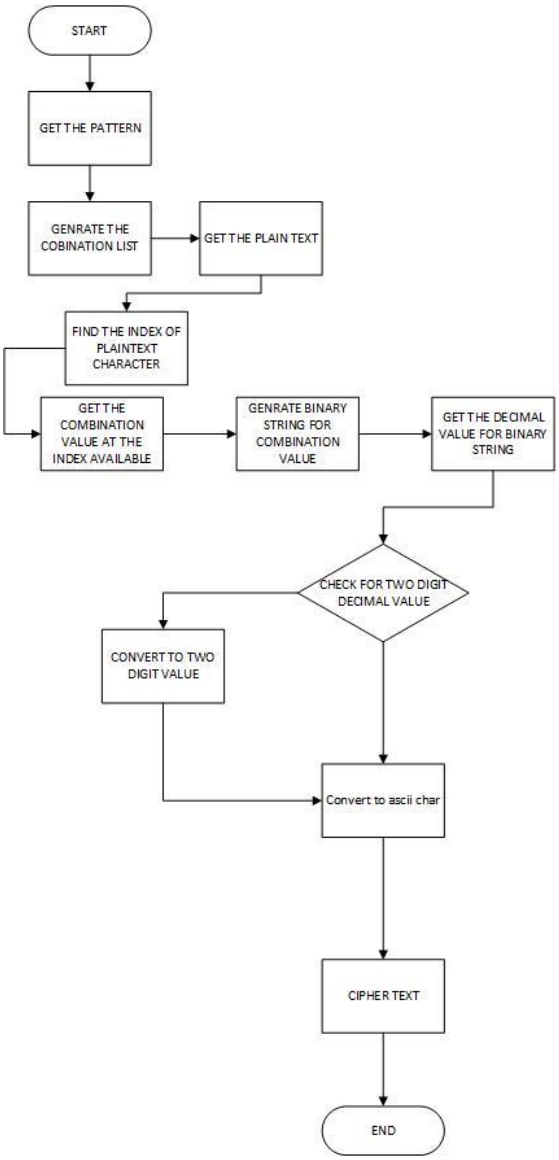


Fig.5 Flow diagram for pattern security algorithm

IV. ALGORITHM FOR PATTERN SECURITY

Input: plain text string

Output: encrypted text

Algorithm:PattenEncrypt(Input_string)

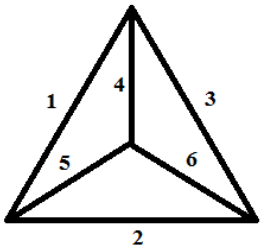
ET | Volume 4 | Issue 5 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

```
1:  start
2:  array_char:=character array(A-Z,a-z,0-
    9);
3:  array_combi:=list of combinations;
4:  Enc:=final encrypted text;
5:  Enc:= empty;
6:  for j from 0 to Input_string.length
7:  do
8:  select_char:=Input_string.charAt(j);
9:  for i from 0 to 63
10: do
11: if select_char equals array_char[i]
12: do
13: index:=i;
14: end if
15: end for
16: combi_value:=array_combi[index];
17: binary_string:=GenrateBinary(combi_v
    alue);
18: decimal_string:=Integer.ParseInt(binar
    y_string,2);
19: temp_string:=empty + decimal_string;
20: if (decimal_string/10 <1)
21: do
22: temp_string = 0 + decimal_string;
23: end if
24: asc_char:=char(temp_string);
25: Enc=Enc+asc_char;
26: end for
27: return Enc;
28: End;
```

V. APPLICATION OF ALGORITHM TO PERFORM ENCRYPTION

Step 1: Select a pattern

Here we select a pyramid pattern.



Step 2: Generate a combination list

1	235
2	236
3	245
4	246
5	256
6	345
12	346
13	356
14	456
15	1234
16	1235
23	1236
24	1245
25	1246
26	1256
34	1345
35	1346
36	1356
45	1456
46	2345
56	2346
123	2356
124	2456
125	3456
126	12345
134	12346
135	12356
136	12456
145	13456
146	23456
156	123456
234	

Step 3: Get the plain text

Let us take plain text as “GOLD”

Step 4: Get the index value of characters from predefined character array

Input:	G	O	L	D
Index:	6	14	11	3

Step 5: Obtain the combination value from combination list and index available

Input:	G	O	L	D
Index:	6	14	11	3
Value:	12	26	23	4

Step 6: Generate the binary string

Input:	G	O	L	D
Index:	6	14	11	3
Value:	12	26	23	4

Binary: 110000 010001 011000 000100

Step 7: Covert to binary to decimal

Input:	G	O	L	D
Index:	6	14	11	3
Value:	12	26	23	4

Binary: 110000 010001 011000 000100

Decimal:	48	17	24	4

Step 8: Convert to two-digit decimal no

Input:	G	O	L	D
Index:	6	14	11	3
Value:	12	26	23	4

Binary: 110000 010001 011000 000100

Decimal:	48	17	24	04

Step 9: Convert the decimal no into ascii character

Input:	G	O	L	D
Index:	6	14	11	3
Value:	12	26	23	4

Binary: 110000 010001 011000 000100

Decimal:	48	17	24	04
Ascii:	O	R	Y	D

Step 10: obtained string this the cipher text

Hence the cipher text for “GOLD” is “ORYD”.

VI. LIMITATIONS

Our algorithm mainly protects the data which is in the form of numerical, alphanumerical or special symbols. It does not support to encrypt the audio, video and images types of data sources.

VII. FUTURE SCOPE

As our algorithm encrypts the numeric and alphanumeric, so it is not possible to encrypt the audio, images or video. So we are working on this. In future we will make our algorithm that can encrypt any kind of data source.

VIII. CONCLUSION

Many type of application where user wants to communicate securely with each other.so there is a need to develop some security mechanisms to protect users confidential data. In this paper, we come to the point that our research is mainly based in terms of security and after its implementation it will provide data protection that will lead to extreme security for the human kind. “Pattern Security Algorithm” will provide a new step towards Digital India.

IX. REFERENCES

[1]. Swarnalata Bollavarapu and Ruchita Sharma – "Data Security using Compression and Cryptography Techniques"

[2]. Sarita Kumari – "A research Paper on Cryptography Encryption and Compression Techniques"

[3]. Nirmaljeet Kaur, Sukhman Sodhi – "Data Encryption Standard Algorithm (DES) for Secure Data Transmission"

[4]. www.ijarcs.info/index.php/Ijarcs/article/download/1588/1576

[5]. https://pdfs.semanticscholar.org/187d/26258dc57d794ce4badb094e64cf8d3f7d88.pdf

[6]. www.ijsrp.org/research-paper-1301/ijsrp-p1315.pdf

[7]. www.ijarcs.info/index.php/Ijarcs/article/download/2990/2973

[8]. www.ijarcs.info/index.php/Ijarcs/article/download/3777/3258

[9]. www.ijcscn.com/Documents/Volumes/vol1issue3/ijcscn2011010310.pdf

[10]. Disha Patel, Hitarthi Hora, Prof. Ajaysinh Rathod,: Analysis of Security Threats On Data In Distributed Application, International Journal of AdvanceEngineering and Research Development, Special Issue SIEICON-2017 e-ISSN : 2348-4470, April -2017.