Comparative analysis of cryptographic streams

Anand Patil[1] ,OmkarShendre [2], Shashank Singh [3] , Shivam Singh [4],Shubham Gupta [5] and Deepti Dave[6].

[12345]*U.G. Student, SOE, ADYPU, Lohegaon, Pune, Maharashtra, India*

[6] *Senior Faculty-IT, iNurture, Bangalore, India*

Abstract- This paper introduces cryptography techniques. The cryptographic process is explained through various algorithms like rail fence cipher, play fair cipher. Cryptography nowadays is used widely in keeping military data, diplomatic in protecting national security. However, the domain was limited in the past but now it is used in every aspect for secured communications, passwords, and payments methods like e-commerce.

Keywords- Rail Fencechiper, Play fair chiper, columnar chiper,Ceaser cipher, Cryptography, Security, Encryption, Decryption

I. INTRODUCTION

Cryptography or Cryptologyis the practice and study of hiding information. ... When a message is sent using Cryptography, it is changed (or encrypted) before it is sent. The method of changing text is called a "code" or, more precisely, a "cipher". The changed text is called "cipher text".

Cryptography is used in many applications like banking transactions cards, computer passwords, and e- commerce transactions.Cryptography is associated with the process of converting ordinary plain text into unintelligible text and vice-versa.It 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.

a. HISTORY

The earliest known use of cryptography is found in non-standard hieroglyphs carved into the wall of a tomb from the Old Kingdom of Egypt circa 1900 BC.

Cryptography, the use of codes and ciphers to protect secrets, began thousands of years ago. Until recent decades, it has been the story of what might be called Cryptography, the use of codes and ciphers to protect secrets, began thousands of years ago. Until recent decades, it has been the story of what might be called classic cryptography that is, of methods of encryption that use pen and paper, or perhaps simple mechanical aids. In the early 20th century, the invention of complex mechanical and electromechanical machines, such as the Enigma rotor machine, provided more sophisticated and efficient means of encryption

b. WORLD WAR II CRYPTOGRAPHY

By World War II, mechanical and electromechanical cipher machines were in wide use, although where such machines were impractical manual systems continued in use. Great advances were made in both cipher design and cryptanalysis, all in secrecy. Information about this period has begun to be declassified as the official British 50-year secrecy period has come to an end, as US archives have slowly opened, and as assorted memoirs and articles have appeared.

The Germans made heavy use, in several variants, of an electromechanical rotor machine known as Enigma. Mathematician Marian Rejewski, at Poland's Cipher Bureau, in December 1932 deduced the detailed structure of the German Army Enigma, using mathematics and limited documentation supplied by Captain Gustavo Bertrand of French military intelligence. This was the greatest breakthrough in cryptanalysis in a thousand years and more, according to historian David Kahn. Rejewski and his mathematical Cipher Bureau colleagues, Jerzy Różycki and Henrik Zygalski, continued reading Enigma and keeping pace with the evolution of the German Army machine's components and encipherment procedures.

At the end of the War, on 19 April 1945, Britain's top military officers were told that they could never reveal that the German Enigma cipher had been broken because it would give the defeated enemy the chance to say they "were not well and fairly beaten.

II. STREAMS OF CRYPTOGRAPHY

a. RAIL FENCE CIPHER

The rail fence cipher is a very simple, easy to crack cipher. It is a transposition cipher that follows a simple rule for mixing up the characters in the plaintext to form the ciphertext. The rail fence cipher offers essentially no communication security, and it will be shown that it can be easily broken even by hand.

Although weak on its own, it can be combined with other ciphers, such as a substitution cipher, the combination of which is more difficult to break than either cipher on its own.

WORKING

To take an example, suppose user want to encrypt the message “this is a test” using a Rail Fence Cipher. In a Rail Fence Cipher, after removing the spaces from the original message, user would write the characters in the message in the following zig-zag pattern, where the message is written along the "rails" of a fence.

t i e

h s s t s

i a t

To encrypt, we construct the ciphertext by reading across the (3) rows that result.

Plaintext: **this is a test**

Ciphertext: **TIE HSSTS IAT**

ADVANTAGE
They are arranged in zigzag manner rather then transposition cipher where they are arranged in vertical columns.

DISADVANTAGE
One can easily break the encrypted text as they are not many possible answers.

b. TRASPOSITION CIPHER (COLUMNAR CIPHER)
The Columnar Transposition cipher is a very simple cipher and very easy to implement. In transposition cipher characters are mixed in plaintext to form the ciphertext.

As this cipher is weak it can combine with another cipher such as with substitution cipher which makes it more difficult to crack.

WORKING
In Columnar transposition cipher all the plain text is written in the row of a specific length and after that it is read out in column by column .For example the key for the columnar transposition is a keyword example -INSERT, The row length should be same as the length of keyword. Here is the example to encrypt:

wolf of wallstreet

write it in according the numbers of rows (keyword here is INSERT)

I N S E R T

w o l f o f

w a l l s t

r e e t x x

in the above table, the plain text is fitted in a rectangle. This is known as Columnar transposition .as it becomes more difficult as their empty characters left. Now the column is reordered such that the letters in the key word are ordered alphabetically.

E I N S R T

f w o l o f

l w a l s t

t r e e x x

Now the cipher text is ready along the column

Fltwwroaelleosxftx

Advantages
This cipher can be combined with other techniques like evaluation method, for example columnar transposition cipher can be combined with substitution cipher which makes it difficult to break.

Disadvantages
This cipher takes more effort and time and complex than simpler cipher

c. PLAYFAIR CIPHER
The Playfair cipher is a digraph substitution cipher. It employs a table where one letter of the alphabet is omitted, and the letters are arranged in a 5x5 grid. Typically, the J is removed from the alphabet and an I takes its place in the text that is to be encoded. Below is an unkeyed grid.

WORKING

A	B	C	D	E
F	G	H	I/J	K
L	M	N	O	P
Q	R	S	T	U
V	W	X	Y	Z

To encode a message, one breaks it into two-letter chunks. Repeated letters in the same chunk are usually separated by an X. The message, "HELLO ONE AND ALL" would become "HE LX LO ON EA ND AL LX". Since there was not an even number of letters in the message, it was padded with a spare X. Next, you take your letter pairs and look at their positions in the grid.

"HE" forms two corners of a rectangle. The other letters in the rectangle are C and K. You start with the H and slide over to underneath the E and write down K. Similarly, you take the E and slide over to the H column to get C. So, the first two letters are "KC". "LX" becomes "NV" in the same way.

"LO" are in the same row. In this instance, you just slide the characters one position to the right, resulting in "MP". The same happens for "ON", resulting in "PO". "EA" becomes "AB" in the same way, but the E is at the far edge. By shifting one position right, we scroll around back to the left side and get A.

"ND" are in a rectangle form and beomes "OC". "AL" are both in the same column, so we just move down one spot. "AL" is changed into "FQ". "LX" is another rectangle and is encoded as "NV".

The resulting message is now "KC NV MP PO AB OC FQ NV" or "KCNVMPPOABOCFQNV" if you remove the spaces.

Manually break apart double letters with X (or any other) characters. Some people break apart all doubles, others break all doubles that happen in the same two-letter chunk. This encoder requires neither in order to be more flexible. Manually make the message length even by adding an X or whatever letter you want. If you don't, the encoder will automatically add an X for you.

All non-letters are ignored and not encoded. The one letter that you select to share a square in the cipher is translated. Numbers, spaces, and punctuation are also skipped. If you leave two letters together in a two-letter chunk, they will be encoded by moving down and right one square ("LL" becomes "RR") where as traditional Playfair ciphers will automatically insert an X for you.

This particular cipher was used by the future U.S. President, John F. Kennedy, Sr. He sent a message about a boat going down.

ADVANTAGES

This cipher has very great advantages on monoalphabetical cipher.

DISADVANTAGES

it's a quite a weak cipher, being better than a simple substitution cipher by only using digraphs instead of monographs.

d. CEASER CIPHER

Caesar cipher comes under substitution method. It was said to be used by

Julius Caesar for communication with his army.

Caesar cipher is also known as the shift cipher. In this crypto graphical

algorithm each letter in plaintext replaces its position down to another letteraccording to its key.

WORKING

Good points of the Caesar cipher is that it is very simple to use. All a person has to do is to write out his message and then referring to his cipher, rewrite his message again, now encrypted. To give the recipient the key, one can just tell them for example “move back 3” so ‘c’ would be represented by ‘z’, and ‘d’ would be represented by ‘a’. No machines or devices are needed to decode it. Only maybe a paper and pen for convenience. This is called a Brute Force Attack.

Bad points are that due to the nature of the cipher, an encrypted text has only 26 possiblities, 25 not including the given text. within 5 minutes, an experienced cryptobreaker could crack the code. Anyone else could crack the code in 10 minutes. With the revolvable cipher, anyone could crack the code in 4-5 minutes. the key could be obtained through trial and error.

An alternative and quicker way to guessing/trial and error is through observing the frequency of the letters. For example, if a certain letter ‘z’ for example is noticed to be repeated very oftenly, you could start off by guessing that ‘z’ represents e, the most commonly used letter. then you can from there subsequently the rest of the letters.

ADVANTAGE

It is very easy to learn.

DISADVANTAGE

It is easy to decrypt the encrypted text.

We can use maximum of 25 keys to encrypt the text.

III. COMPARITIVE ANALYSIS

Name of cipher	Rail fence cipher	Playfair cipher	Transposition cipher	Caesar cipher
Key required	Minimum key or height required is 2	A keyword is given which should be remembered	Both the width of the rows and the permutation of the columns are usually defined by a keyword.	25 possible shift (each possible shift of the alphabet) 25 possible shift
Size of table/column/row	Minimum height required is 2 and length depends on size of plain text	Table is of 5x5 Size (J is arranged along I in same box and if there is j in keyword it is replaced by I)	Keyword defines the width of table	No table
Type of Arrangement	Zig zig way of arrangement in table according to key	5X5 horizontal arrangement	Vertical column table arrangement	No table

IV. CONCLUSION

The use cryptography is to ensure that the message or data is confidentially transmitted and not be altered. The data or message is only available to those who have decipher key. According to mentioned analysis Play fair cipher is more secure than any other cipher mentioned above to transmit a message.

V. REFERENCE

[1]. J. Omole in, O. A. C. and A. O. Bajeh, "The Complexity of 4-Row Rail Fence Cipher Encryption Algorithm," International Journal of Mathematical Science, vol. 1, no. 1, pp. 8-14, 2009.

[2]. J. O. Omolehin, O. C. Abikoye and R. G. Jimoh, "Development of Data Encryption and Decryption Algorithm Using 4-Row Rail Fence Cipher," Jounal of Nigerian Association of Mathematical Physics, vol. 13, pp. 411-416, 2008.

[3]. J. A. Dar, "Humanizing the Security of Rail Fence Cipher Using Double Transposition and Substitution Techniques," International Journal of Science and Research, vol. 3, no. 9, pp. 1787-1791,

[4]. Singh, Simon (2000). The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. ISBN 0-385-49532-3.

[5]. S .Maret," Cryptography Basics PKI ", First Edition. Dimension Data SA, ., (1999):, Switzerland

[6]. W .Stallings, " Cryptography and network security, Principles and practices ", Fourth Edition. Pearson Prentice Hall, (2006):, USA.