JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A Review on Hybrid Vigenere - Polybius Cipher with XOR operation for Enhanced Cryptography

[1]Miss. Pradnya Patil ,[2]Prof. S.S. Redekar

[1]Student,Computer Engeneering, [2]Head,Computer Engeneering

[1,2]Ashokrao mane Group Of Insttitution ,vathar.

Abstract : All Today's reality Sensitive information is progressively utilized in correspondence over the web. Accordingly Security of information is the greatest worry of web clients. Best arrangement is utilization of some cryptography algorithm which scrambles information in a few code (cipher) and moves it over the web and again decoded (decrypt) to original information. The area of cryptography manages the strategy for passing on data safely. The objective is to permit the planned beneficiaries of a message to get the message appropriately while intrude on overhang droppers from understanding the message. Cryptography incorporates a bunch of strategies for scrambling or camouflaging information so it is accessible just to somebody who can reestablish the information to its unique structure. In current PC frameworks, cryptography gives a solid, prudent reason for keeping information arranged and for checking information outrage. While our customary cryptography strategies, such for AES (encryption) and RSA (marking), function admirably on frameworks which have sensible handling power and memory capacities, these don't scale well into a world with inserted frameworks and sensor organizations. Hence, lightweight cryptography strategies are proposed to beat a significant number of the issues of regular cryptography. This work decides to add to the overall assemblage of information in the space of traditional cryptography by fostering another cross breed method of encryption of plaintext. The cryptosystem plays out its encryption by scrambling the plaintext utilizing Vigenere Cipher and further utilizing the ciphertext to encode the plaintext again utilizing Polybius.

IndexTerms - : Encryption, Cryptography, Algorithm, Ciphers.

I. INTRODUCTION

A Cryptography is a procedure that arrangements with getting information and is firmly associated with data hypothesis, PC security, and designing. Notwithstanding, with the presence of enemies that utilizes strong PCs, the need to expand the intricacy of cryptographic methods emerges. This paper utilized and hybridized the two usually involved codes in the writing, in particular the Polybius square and the Vigenere figure, to guarantee safer information. To build the strength of the crossover figure, the ciphertext produced by the Polybius square is XORed. Reproduction results uncovered that the proposed technique produces a one of a kind ciphertext that shows not race of any example from the plaintext thus devoid of being assaulted by recurrence investigation or by bruteforce.

Necessity of Cryptography

To be secured, information need to be hidden from unauthorized access (confidentiality), protected from unauthorized change(integrity), and available to an authorized entity where it is needed(availability). The implementation of these three security goals is made possible through cryptography. Cryptography is the discipline that embodies the principles, means and methods for the transformation of data in order to hide its content, establish its authenticity, prevent its undetected modification or unauthorized use. Cryptographic techniques enable users to protect the privacy of their data (financial or personal records, for example), whether the data are in storage or in transit. Cryptographic techniques also allow users to determine whether someone has altered data —whether, for example, a hacker who has broken into medical records has altered any element of them. They also enable users to determine with confidence the identity of a person or device at a distance, not least by establishing the authenticity of a given document.

II. LITERATURE SURVEY

In paper [1] presents another crossover security figure by consolidating the two most significant Ciphers like Polybius Cipher and Vigenere Cipher. This cross breed encryption figure gives more prominent security as looked at to exemplary codes.

In [2] the security for web keeping cash, account passwords, messages accounts secret word, and so forth requires content insurance in automated media. It shows the security other than; strain for the data with the move encryption standard. The period of key has been finished with the help of the Polybius square. The expansion in number of rounds it will require progressively computational hypothesis and will wind up annoying for the computer programmer to break the framework.

This paper[3] utilized and hybridized the two normally involved codes in the writing, specifically the Polybius square and the Caesar figure, to guarantee safer information. To build the strength of the half and half code, the ciphertext produced by the Polybius square is XORed. Reenactment results uncovered that the proposed strategy produces a remarkable ciphertext that shows no hint of any example from the plain text, hence, without being assaulted by recurrence investigation or by savage power.

In [4] Cryptography is the specialty of safeguarding data by changing it into a mixed up design. It is tied in with building and examining conventions that keep outsiders or general society from perusing private message. Caesar figure is a replacement figure that executes mono-alphabetic replacements. It is an extremely old encryption strategy and significant impediment of caesar figure is the rehashing idea of its keys. In this paper a high level encryption calculation is proposed which works on the security of caesar strategy by consolidating customary playfair approach and an advanced code technique like stream figure. While applying the proposed technique, three different key is utilized which makes the calculation more solid.

In [5] this paper we propose a high level encryption calculation which works on the security of Vigenere technique by joining it with current code strategy like Stream figure, Stream figure somewhat views as strong technique, and it utilizes parallel structure (rather than characters) where the Plaintext, Ciphertext and the Key are series of pieces.

III. EXISTING SYSTEM

The Vigenere Cipher is an encryption plot which was concocted in the sixteenth century by French Blaise De Vigenere. The plan is propelled by the Caesar Cipher in that it utilizes a polyalphabetic substitution matrix " that consolidates at least two alphabetic tables. The Vigenere encryption conspire depends on a catchphrase as its key alongside the polyalphabetic replacement table to encode and interpret a message. For example, to encode the message utilizing a Vigenèrecipher table which is in fig, by utilizing the key will do the accompanying; first the key is rehashed successively until the length of the message and adjusted together. Then, at that point, the words are interpreted by finding the lines and sections of each position in the watchword and plaintext in polyalphabetic replacement table gave beneath to get the scrambled code text. A similar key is then used to unscramble the message to uncover a similar message by utilizing the opposite cycle

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

Figure 1: Polyalphabetic Table

IV. PROBLEM STATEMENT

Cryptographic System had organized, plan, produced and carried out new form of secure Ciphers for embodying message and information now and again with at least few changes. Be that as it may, Every Single New codes goes in two scales, for example, -

- Simple or Complicating: This Cipher are made for sub little framework for less worth security reason yet figures development in any part as immediate basic or confusing with utilization of numerous subsystem inside it.
- Time or Cost Consuming: This Cipher is made and afterward bring about tedious rationale for Ciphers as execution of interaction of unraveling.
- Independent Ciphers Demeritsare
    - Easy to Attack
    - New ways development to handle the line of safety
    - Fault advancement
    - Key can be gotten through sub manual cycle
    - Easy catching and Jamming of framework

In this way, we can get to realize that different code and calculation in the event that It is utilized, It can be broken or a change unwittingly with various sorts of assaults in framework during communication.

V. OBJECTIVES

- Design and implementation by considering of the research network for the up-gradation, refinement and enhancement of data privacy and security.
- Design and Analyze the proposed approach by executing security attacks and performance analysis on messages.

VI. PROPOSED WORK

Lightweight cryptography as Ciphers is taken for thought for System. Two renowned old style figures are utilized for the Defined arrangement to do Combination of Cipher in the System, for example,

I. Vigenere Cipher

Vigenere Cipher is a strategy for scrambling alphabetic text. It utilizes a basic type of polyalphabetic replacement. A polyalphabetic figure is any code in view of replacement, utilizing different replacement letters in order .The encryption of the first text is finished utilizing the Vigenère square or Vigenèretable. This makes the code less powerless against cryptanalysis utilizing letter frequencies. Blaise de Vigenère created what is presently called the Vigenère figure in 1585. He utilized a table known as the Vigenère square, to encipher messages.

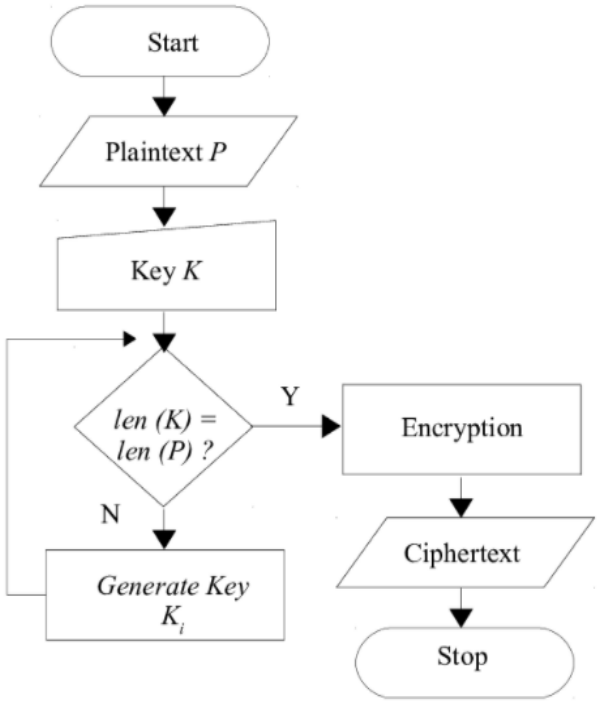

Figure 2 Flowchart

VII. CONCLUSION

Cryptography is the generally utilized technique for the security, privacy, confidentiality and reliability of data. Single classic ciphers are cryptographic techniques that are viewed as least complex and most vulnerable because of numerous impediments, restriction, and smooth system. One of the famous ciphers is Vigen`ere Cipher but it also has few drawbacks. To conquer the impediments of Vigen`ere cipher, A new technique is present an upgraded variant as a combination of Polybius cipher and Vigen`ere that is a lot more secure against attacks like Active, passive, Kasiski and Friedman assaults (attacks).

Cryptanalysis, recurrence examination, men in middle attacks, frequency analysis, fault analysis attacks, design expectation and brute force attacks on the proposed strategy are likewise much troublesome because of the utilization of product tables for encryption. The altered hybrid combination of the Caesar Cipher and Vigen`ere Cipher, that's the result in as a high level of complexity, scattering, distribution, and confusion in the algorithm that creates them making it an exceptionally solid cipher and hard to break.

REFERENCES

[1] Shivam Vatshayan, Raza Abbas Haidri, Jitendra Kumar Verma,"Design of Hybrid Cryptography System based on Vigenere Cipher and Polybius Cipher" 2020 International Conference on Computational Performance Evaluation (ComPE), North-Eastern Hill University, Shillong, Meghalaya, India. July 2–4, 2020.

[2] Puneet Kumar, Shashi B. Rana, Development of modified AES algorithm for data security, Optik - International Journal for Light and Electron Optics, Volume 127, Issue 4, 2016, Pages 2341-2345, ISSN 0030-4026, http://dx.doi.org/10.1016/j.ijleo.2015.11.188. (http://www.sciencedirect.com/science/article/pii/S0030402615018215).

[3] Jan Carlo T. Arroyo, Allemar Jhone P. Delima "A Hybrid Caesar-Polybius Cipher with XOR Operation for Enhanced Cryptography", International Journal of Advanced Trends in Computer Science and Engineering, 9(3), May – June 2020, 2961 – 2967.

[4] Md. Ebrahim Hossain. Enhancing the Security of Caesar Cipher Algorithm by Designing a Hybrid Cryptography System. International Journal of Computer Applications 183(21):55-57, September 2021.

[5] Fairouz Mushtaq Sher Ali, Falah Hassan Sarhan. Enhancing Security of Vignere Cipher by Stream Cipher. Published by International Journal of Computer Applications (0975-8887), Volume-100, No. 1, August 2014.

[6] O.E. Omolara, A.I. Oludare and S.E. Abdulahi (2014). Developing a Modified Hybrid Caesar Cipher and Vigenere Cipher for Secure Data Communication. Published by Computer Engineering and Intelligent Systems. ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online), Vol.5, No.5, 2014.

[7] Fairouz Mushtaq Sher Ali (2014). Enhancing the Security of Playfair Cipher by Stream Cipher. Published by Journal of AL Qadisiyah for Computer Science and Mathematics, Volume-6, No-2, Year-2014.

[8] Self-Study: ASCII Symbol of non-printable characters. URL: https://en.wikipedia.org/wiki/C0_and_C1_control_codes#SOH. Retreived Date: 15 July, 2021.

[9] https://www.researchgate.net/publication/342625483 A Hybrid Caesar Polybius Cipher with XOR Operation for Enhanced Cryptography.

[10] Chaudhari, Swapnil. (2018). A Research Paper on New Hybrid Cryptography Algorithm.

[11] Jakimoski, Kire, "Security Techniques for Data Protection in Cloud Computing" International Journal of Grid and Distributed Computing 9.1 (2016): 49-56.

[12] https://en.wikipedia.org/wiki/Vigen%C3%A8rer cipher

[13] https://en.wikipedia.org/wiki/Polybius_square

[14] Image source from https://www.britannica.com/topic/Vigenere-cipher