SN Social Sciences

Design and Implementation of Hybrid Cryptographic Technique for Secure Communication System

--Manuscript Draft--

Manuscript Number:	
Full Title:	Design and Implementation of Hybrid Cryptographic Technique for Secure Communication System
Article Type:	Original Article
Section/Category:	Education
Funding Information:	
Abstract:	Security had become a biggest concern for most of the people especially for the users who using the internet. Statistics also shows a huge increase in hacking and breaching ones personal data from commonly through gadgets like mobiles and IOT devices during global pandemic because of covid-19. Internet usage has increased a lot and also people using devices without having knowledge of how these attacks may happen. It is our responsibility to protect their data and keep it secured, for this reason cryptography is introduced. By using different techniques and methods in cryptography one can secure the data accordingly by converting their data from one form to another also known as encryption and share it with the others. But many of these techniques are broken eventually and failed to protect the data. so, we choose to combine two cryptography techniques known as vigenere cipher and Polybius cipher making a hybrid cipher in order to provide a better security compared to other classic ciphers and make the hackers difficult to retrieve the original data back from the encrypted data. This is further followed by hashing technique which ensures the data integrity provided.
Corresponding Author:	Hanish Chalicham, B.Tech VIT University INDIA
Corresponding Author Secondary Information:	
Corresponding Author's Institution:	VIT University
Corresponding Author's Secondary Institution:	
First Author:	Hanish Chalicham, B.Tech
First Author Secondary Information:	
Order of Authors:	Hanish Chalicham, B.Tech
	Akhil G.S.S.R, B.Tech
	Sai Kuldeep Kancherla, B.Tech
	Mugelan R K
Order of Authors Secondary Information:	
Author Comments:	Dear Editor, We wish to submit the article for further consideration and evaluation at your esteemed journal. The submitted manuscript is original and is not under consideration else where. Thankyou for your time and consideration.

Design and Implementation of Hybrid Cryptographic Technique for Secure Communication System

Chalicham Hanish
Elec & Communication Eng
VIT University
Vellore, India
chalichamhanish@gmail.com

G.S.S.R.Akhil
Elec & Communication Eng
VIT University
Vellore, India
akhilakhi828@gmail.com

Kancherla Sai Kuldeep
Elec & Communication Eng
VIT University
Vellore, India
kancharlakuldeepsai@gmail.com

Dr. R.K.Mugelan
Elec & Communication Eng
VIT University
Vellore, India
mugelan.rk@vit.ac.in

ABSTRACT

Security had become a biggest concern for most of the people especially for the users who using the internet. Statistics also shows a huge increase in hacking and breaching ones personal data from commonly through gadgets like mobiles and IOT devices during global pandemic because of covid-19. Internet usage has increased a lot and also people using devices without having knowledge of how these attacks may happen. It is our responsibility to protect their data and keep it secured, for this reason cryptography is introduced. By using different techniques and methods in cryptography one can secure the data accordingly by converting their data from one form to another also known as encryption and share it with the others. But many of these techniques are broken eventually and failed to protect the data. so, we choose to combine two cryptography techniques known as vigenere cipher and Polybius cipher making a hybrid cipher in order to provide a better security compared to other classic ciphers and make the hackers difficult to retrieve the original data back from the encrypted data. This is further followed by hashing technique which ensures the data integrity provided.

KEYWORDS: Cryptography, Cipher text, Vigenere Cipher, Polybius Square Cipher, Hashing, Encryption, Decryption

INTRODUCTION

Cryptography is the study of techniques of hidden writing and message hiding. Billions of people around the world use cryptography to secure data and information, with the widespread use of electronic communication systems, although most of the users do not know that they are using it. Cryptography is a known technique to safeguard the data.

With the increase In data transmission through the internet : via emails, chats , etc… , privacy and security become the biggest concern since the data can be bagged or hacked in many ways , though cryptography helps us to encrypt the data before sending it over the internet , many techniques are being broken with the increase in crypto analytical skills (cybercrime activities). In order to continue the protection of data we need to evolve and invent new cryptographic techniques and here comes hybrid cryptographic algorithms, which are formed by combining two or more cryptographic algorithms making them difficult to crack. There few hybrid cryptographic algorithms, which are also called as conventional cryptographic algorithms. But these are difficult to implement with the smaller IOT devices and etc. since they require a lot of computation power and time. So lightweight cryptography can be used to overcome these drawbacks in some areas. we know that vigenere cipher is most popular because of its simplicity and resistance to frequency analysis test of letters and widely using in 18th century

.But with increase in cryptanalytic skills , vigenere cipher is became one of the non secure ciphers and became unpopular. The main reason for this is because of the repeated words using as a key streams in vigenere cipher causes repetition of certain patterns in cipher texts at intervals same as the length of the keyword used. Cryptography plays a crucial role in hiding the information from unauthorized persons. Only the authorized or intended persons can able to read the message that is shared.

The basic terms used in cryptography are:

Plain text – actual message that user wants to send.

Cipher text—a non readable message that gets transmitted after applying certain techniques to the plain text

Encryption—It is a process of converting plaintext into a cipher text

Decryption—it is a process of converting cipher text into a plain text or also called as reverse process of encryption

Key – It is the numeric or alphanumeric text used for the encryption of plain text and decryption of cipher text.

The main objectives of the Cryptography is to provide authentication, integrity, access control, Non repudiation.

Cryptography is basically classified into two types depending upon the key:-

1) Symmetric key algorithms are mostly used algorithms, it uses same key for both encryption and decryption of plaintext and cipher text respectfully.

2) Asymmetric key algorithms slow in working and not suggestable to use them to encrypt huge data.

It uses two keys named as public key and private key. The public key is available to everyone but after the data encrypted using this key of any user can only be decrypted by using private key of that particular user. In this paper we shows that the Polybius cipher offers several security measures and lobby strength when modified and used with vigenere cipher followed by hashing to provide data integrity.

Vigenere Cipher

Vigenere cipher provides an ingenious way of representing mappings from letter to letter in a matrix form. The process starts with the input message into the vigenere cipher algorithm which is a polyalphabetic substitution cipher. Each letter in the input plaintext processed one letter at a time across the columns in the matrix. The key text which is a reference text tells us which row to look at the mapping. The key text affects the input message text in replacement of the letters in the input text. In addition, the keystream should be as long as plaintext. The first letter in the input plaintext is validated with a row combining with the first letter of the key text which is checked at the column of the matrix. By mapping the plaintext letter and the key text letter in the matrix the encrypted letter results as output. Similarly, all the other letters in the input plain text get processed resulting in an encoded message.

In decrypting the encoded message is systematically compared in the matrix table with an instance of the key text. The first letter of the keystream and first letter of the encrypted text is verified with the matrix resulting from the decryption of the original plaintext letter. Similarly, the other letters in the encoded text are decrypted and the exact input plaintext is seen in the output.

	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

Fig: Matrix of Vigenere Cipher for mapping key and plain text

Polybius Square Cipher

Polybius Square Cipher translates letters and represents them in the form of numbers. It is occupied with a table that can be randomized and shared with the recipient permits to change letters into numbers. To make the 26 letters of the alphabet into the 25 cells made in the table, the letters ‘i’ and ‘j’ are commonly bound into a single cell. Originally there has been no such trouble as the ancient greek alphabet has 24 letters

Encryption and Decryption:

During encryption, considering the row and column position of the alphabet present in the table the encoded output results in the form of numbers. Similarly, the same process continues for each letter in the plaintext resulting an encrypted message with a series of numbers. While in Polybius decryption, requires knowledge of the grid and replacing the corresponding letter in the grid as per the coordinates.

Hashing

Hashing algorithm converts data into a compressed format with a certain length. The result is either in numerical or hash value. The output depends on the type of hashing technique we use where the length of output ranges from 160 to 512 bits. It is designed in one way that transforms the data computational, infeasible to invert and verify the integrity of data. The hashing algorithm takes the input of any size and gives the result of fixed length which means, where a large data can be compressed as small as a password and ensures to be strongly collision-free.

PROCESS

The process follows as per the flow chart shown in the figure. The input plain text is encrypted in a combination of Vigenere cipher and Polybius square cipher. A random key text is taken

with the input plaintext and processed in the Vigenere cipher. The output text from the Vigenere cipher turns into an input text for the Polybius square cipher. The Polybius square cipher processes the input cipher text and converts it into a numerical format which is more secure than using a single algorithm. Here the letter 'J' is assigned in a separate box as per our convenience, so as not to get bonded with the letter "I". Description of the text can do in the reverse order of this process to find the original plaintext. To make the encrypted data more computational and secure for one-way communication the output from Polybius square cipher is sent into hashing algorithm which results in a compressed numerical or hash value.

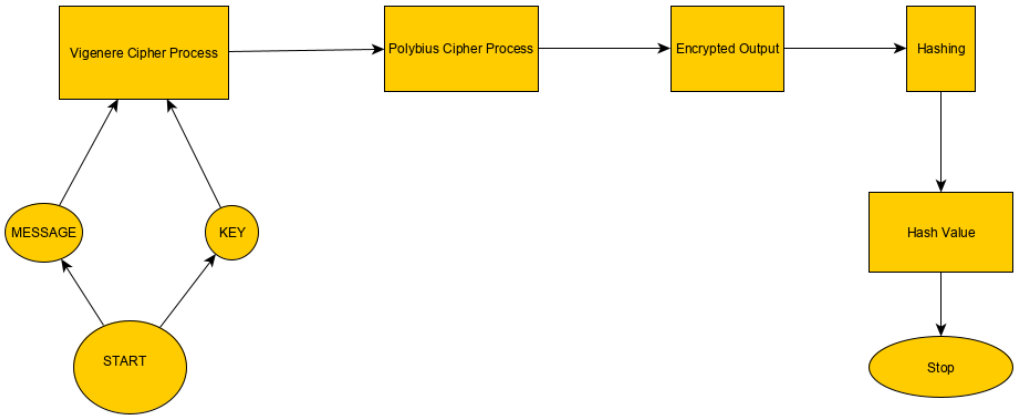

Fig: Flowchart of Hybrid Algorithm

Step-1: The input message is sent into the Vigenere algorithm matrix along with a key text where the text proceeds in columns and a key text in rows. The algorithm finds the encrypted letter by mapping the input message letter with the key text letter and results in an encrypted output.

Step-2: The encrypted output from the Vigenere process is sent into Polybius chipper algorithm which converts the text into numerical form. The output from this is seen in numerical format.

Step-3: The numerically encrypted output is sent into the hashing algorithm which is a one-way algorithm that converts the message into a compressed hash or numerical value and is difficult to decrypt.

A program is executed using python and where the functions returns the encrypted message which is generated with the help of the key that we assign.

RESULTS

Encryption output:

Keyword = "MUMBAI"

```
Ciphertext : YOSFLIZLW
Original/Decrypted Text : MUGELANRK
                                                    # Vigenere cipher

 »» Enter your text - YOSFLIZLW

 »» The result of the text is: ««
45 43 34 12 13 42 55 13 25
                                    # Polybius square cipher
```

The input text MUGELANRK is sent into the Vigenere cipher algorithm in a alphabetical for mat with the key text “MUMBAI” which resulted an unformatted distributed cipher text. The cipher text is sent as input to the Polybius square cipher algorithm resulting the output in a nu merical format.

Decryption Output:

```
 »» Enter your text - 45 43 34 12 13 42 55 13 25

 »» The result of the text is: ««
YOSFLIZLW                                  # Polybius square cipher
```

keyword = "MUMBAI"

```
Originaltext : MUGELANRK
CipherText : YOSFLIZLW
                                                  # Vigenere cipher
```

Decryption takes place in the same way but in the reverse direction of the encryption process. In decryption the text is first sent into the Polybius square cipher and then the Vigenere cipher. This makes hard to the attackers to decrypt the text as it confuse and makes difficult to get exact original message.

Hashing output:

Input text: 45 43 34 12 13 42 55 13 25

```
Hash Value : 34158ac36819808cb577028b939237a0
                                                        #Hashing
```

The outcome of encrypted data from Polybius square cipher is sent into a hashing algorithm. It takes input data of any size and results in a fixed length of the output. The above process makes the data more secure and can be used for the integrity of data. Thus the hybrid cryptographic implementation for encryption and decryption of message is done by a combination of Vigenere, Polybius square and hashing algorithms written in Python code acts as a shield to protect the data during the transmission of messages from sender to receiver and the hashing algorithm makes the data infeasible and computational. This hybrid method can be considered as simple and secure to encrypt or decrypt the message without losing any data.

CONCLUSION:

This paper briefly gives an overview and usage combination of cryptographic algorithms where the transmitted data from the sender side is encrypted with a variety of encrypting algorithms resulting in the output at the receiver side and vice-versa. Despite being common cryptographic algorithms with being weakest and simplest when using a single algorithm, Vigenere, Polybius and hashing still perform tasks very effectively in securing the data when combined with other algorithms, and these laid to the betterment encrypting the data and security performance. Although there are limitations and sharing of cells in the Polybius square and secret key absence in encryption, improvements, and modifications are done in the recent works. However, there are still many approaches and require research for genuine consideration in updations and enhancement of security. In the future, our motto is to find out the various cryptographic strategies and propose the approaches for enhancement of data privacy and security by performing security attacks on messages.

REFERENCES

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

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

[3]https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher

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

[5]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)

[6] Encryption. Wellesley college Computer Science Department lecture note retrieved from : http://cs110.wellesley.edu/lectures/L18-encryption/.

[7] Classical cipher, Transposition ciphers, Retrieved from

http://en.wikipedia.org/wiki/Classical_cipher

[8] Transposition ciphers, columnar transposition Retrieved from http://en.wikipedia.org/wiki/Transposition_cipher

[9] C. Sanchez-Avila and R. Sanchez-Reillo, "The Rijndael block cipher (AES proposal): a comparison with DES," in Security Technology, 2001 IEEE 35th International Carnahan Conference on, 2001, pp. 229-234.

[10] Q.-A. Kester, "A cryptosystem based on Vigenère cipher with varying key," International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), vol. 1, pp. pp: 108-113, 2012.

[11] C. Bhardwaj, "Modification of Vigenère Cipher by Random Numbers, Punctuations & Mathematical Symbols," Journal of Computer Engineering (IOSRJCE) ISSN, pp. 2278-0661, 2012

[12] F. H. S. Fairouz Mushtaq Sher Ali, "Enhancing Security of Vigenere Cipher by Stream Cipher," International Journal of Computer Applications, vol. 100, pp. 1-4, 2014

[13] P. Gutmann, ―Cryptographic Security Architecture: Design and Verification‖. Springer-Verlag,2004.

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

[15] M. Abror, "Pengertian dan Aspek-Aspek Keamanan Komputer," 2018. [Daring]. Tersedia pada:https://www.ayoksinau.com/pengertian-dan-aspekaspek-keamanan-komputer-lengkap/. [Diakses: 01-Okt-2018].

[16]V.Beal.(2009,Encryption.Available:Http://www.webopedia.com/TERM/E/ encryption.html