iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** VII **Month of publication:** July 2023

DOI: https://doi.org/10.22214/ijraset.2023.54819

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VII Jul 2023- Available at www.ijraset.com

Design and Improvement of Caesar Cipher

Dhairya Savla[1], Prof. Ruchi Rautela[2]
[1]*Post-Graduation Student in the Department of MCA, VESIT Mumbai, India*
[2]*Mentor and Assistant Professor, Department of MCA, VESIT Mumbai, India*

Abstract: Cyber security is the application of technologies, processes and controls to guard systems, networks, programs, devices and data from cyber-attacks.
Cryptology is the study of securing Computer systems that allow only sender and receiver to read it.Cryptology comes from Greek word 'Kryptos' which means 'hidden' and 'logos' means 'to study of'. Even though security is important, numerous applications have been created without considering fundamental points of data security that is confidentiality, authentication, and availability. As we depend more on the internet, security issues and problems will also increase. To prevent alteration or access of data by unauthorized persons, cryptography is required. A methodology is proposed to increase the efficiency of the Caesar cipher which is the simplest cipher. This research introduces a new hybrid secure Caesar cipher by combining the three most important Ciphers (Caesar Cipher, Vigenère Cipher, Polybius Cipher) and Diffie-Hellman technique This hybrid encryption cipher provides better security as compared to normal Caesar ciphers.

I. INTRODUCTION

Data privacy and security presently compose one in every of the most important features of an individual's life. One cannot communicate securely anymore as there's always some eavesdropper or an opportunity of leak of data. Cryptography deals with helping to create data safer.
Cryptography together with protection of knowledge from theft or alteration, can also be used for user authentication.
There are two types of cryptographic techniques symmetric key cryptography and public key cryptography.
Symmetric key cryptography is the method where the identical key is used for both the encryption phase and therefore the decryption phase. Public key cryptography is that the method where just one key is used for encryption process and another different secret is used for the decryption process.

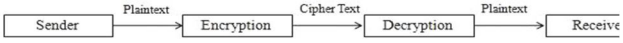


Fig 1. Process of Cryptography

A. Caesar Cipher

The Caesar Cypher technique is one of the oldest and simplest encryption techniques. This particular type of substitution cipher replaces each letter in a text with a letter that is shifted a predetermined number of positions down that alphabet. For instance, with a shift of 4, C would change to G, D to H, and so on. The name Caesar cipher was derived from Julius cypher, who used this method to communicate with his soldiers.
Due to its simplicity, the Caesar cypher algorithm is the fastest. However, the algorithm is extremely simple to crack with the help of a frequency analysis attack. This is because, during this algorithm, each character of a message is usually replaced by the same fixed character that has been predetermined.

B. Diffie-Hellman

Diffie-Hellman is a method of generating a shared secret between two parties in such a way that the secret cannot be seen by simply observing the communication. This is especially helpful because you can use this method to generate an encryption key with another person before beginning to encrypt your traffic with that key. And regardless of whether the traffic is captured and subsequently analyzed, there is no way to determine what the key was, even though the exchanges that produced it will have been visible.

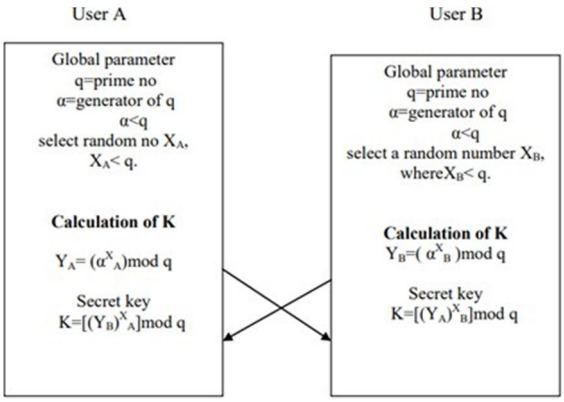


Fig. 2. Diffie – Hellman key exchange protocol.

C. *Vigenère Cipher*

The Vigenère Cipher is a method of encrypting alphabetic text. A straightforward polyalphabetic substitution cipher is used. A polyalphabetic cipher is any substitution-based cipher that employs multiple substitution alphabets. The original text is encrypted with the Vigenère square or Vigenère table.

	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. 3. Vigenère table.

D. *Polybius Cipher*

The Polybius square, also known as the Polybius checkerboard, is a device invented by the ancient Greeks Cleoxenus and Democleitus and popularized by the historian and scholar Polybius. The device is used to fractionate plaintext charactersso that they can be represented by a smaller set of symbols, which is useful for telegraphy, steganography, and cryptography. Therefore, the proposed system will combine various ciphers and encryption methods to improve and further the security of the Caesar cypher. The Vigenère, Polybius, and Diffie-Hellman ciphers will all be used together in this system.

II. RELATED WORK

1) Title: Design of Hybrid Cryptography System based on Vigenère Cipher and Polybius Cipher Year: 2020

Author: Shivam Vatshayan, Raza Abbas, Jitendra Kumar Verma

Methodology: The strategy utilizes a mixture of Vigenère cipher and Polybius Square Cipher in its encryption process. The ciphertext will initially be worked on utilizing the Vigenère cipher. A picked key of arbitrary size will start the method. Toward the finish of the method, the next ciphertext then turns into a key for the Polybius Square Cipher process. The secret's accustomed work on the message which is that the plaintext to make the last ciphertext. This process will finish up making the last ciphertext progressively hard to be broken utilizing existing cryptanalysis processes.

Decryption will be done by the receiver in reverse order for retrieval of a message from the sender.

2) Title: An Enhanced Cipher Technique Using Vigenère and Modified Caesar Cipher
Author: Deepanshu Gautam, Parth Sharma, Poonam Saini,
Chandan Agarwal, Dr. Munish Mehta Year: 2018
Methodology: There are a unit numerous cipher techniques out there for encrypting the messages like verman cipher, mono-alphabetic cipher, poly-alphabetic cipher, etc. one in every of the foremost fashionable cipher techniques is that of the Vigenère cipher. It's a poly-alphabetic cipher technique that uses the Vigenère table for the strategy of coding of alphabets. This paper extends the Vigenère table with numerical knowledge, that the numbers are also encrypted exploitation this method. It combines the coding method of Vigenère and Modified Caesar Cipher for obtaining the cipher text from the given plaintext and key.

3) Title: Innovative enhancement of the Caesar cipher algorithm for cryptography
Author: Shreyank N Gowda Year: 2016
Methodology: This paper proposes an enhancement to the existing algorithm by making use first of a simple Diffie-Hellman key exchange scenario to obtain a secret key and later using simple mathematics to ensure the encryption of data is much safer. Once a private shared key is obtained by making use of the Diffie-Hellman method, the key is subject to the mod operation with 26 to obtain a value less than or equal to 26, then the current character is taken and to this the key value obtained is added to obtain a new character. For any character in the 'x' position the key is simply first multiplied with 'x' and then mod is done to obtain the encrypted character. So, 2nd character of the message is multiplied with 2, the third character with 3 and so on. This enhances the security and also does not increase the time of execution by a large margin.

4) Title: A Complex Polyalphabetic Cipher Technique Myanmar Polyalphabetic Cipher
Author: Dr. Tun Myat Aung, Ni Ni Hla Year: 2019
Methodology: The proposed technique is that the original Vigenère cipher is developed by combining Vigenère cipher with Affine cipher. This proposed technique is also considered as a complex transformation technique from Affine cipher known as a monoalphabetic cipher technique to polyalphabetic cipher technique that is called Vigenère-Affine cipher which based on the combination of Vigenère cipher with Affine cipher

III. METHODOLOGY

A. Proposed Algorithm

1) Use the Diffie-Hellman algorithm to get a shared secret.
2) Use 26 to modulate the shared secret.
3) Use the Caesar cipher and the XOR function rather than shifting.
4) Use the Vigenère encryption and the XOR function instead of shifting.
Implement the Polybius cipher.

B. Implementation

The Differ Hellman key exchange procedure will be used in the suggested paradigm to first obtain a shared secret. This shared information will now serve as the Caesar Cipher's key. An XOR function will be applied to Plain text instead of shifting with n places.

For example,
1) Key is 5 and letter to be encrypted be h which has position as 7
2) XOR key with 26 and 7 (position of h) which is 5 XOR 7 XOR 26=24 so the 24th position is of y.
3) h will be replaced by y.
4) After encryption of all the letters, the text will be again encrypted with our shared secret key in which we will use Vigenère ciphers mechanism.
5) We will implement Polybius ciphers mechanism on the output it
6) The final output will be a number For more complexity six more Greek alphabets would be added in our dataset {Γ, Δ, Θ, Λ, Π, Σ} {Gamma, Delta, Theta, Lambda, Pi, Sigma}

For Example: A=0|B=1|C=2|D=3|E=4|F=5|G=6|H=7|I=8|J= 9|K=10|L=11| M=12|N=13|O=14|P=15|Q=16|R=17|S=18|T =19|U=20|V=2 1|W=22|X=23|Y=24|Z=25|Γ=26|Δ=27|Θ=28| Λ=29|Π30|
Σ=31

For Polybius Cipher

	1	2	3	4	5	6
1	A	B	C	D	E	F
2	G	H	I/J	K	L	M
3	N	O	P	Q	R	S
4	T	U	V	W	X	Y
5	Z	Γ	Δ	Θ	Λ	Π/Σ

➢ *Imagine ALICE AND BOB Key Generation*

- Alice chooses 5 as private key
- Bob chooses 6 as private key
- Alice and Bob accept 10 as a public key
- Alice sent private*public (5*10=50) to Bob
- Bob sent private*public (6*10=60) to Alice
- Alice multiplies the 60 sent by bob with its private key (60*5=300) 300
- Bob multiplies the 50 sent by Alice with its private key (50*6=300) 300
- 300 is our shared secret key between Alice and bob

➢ *Encryption*

- First step is to find k=300mod26 which is 14
- Let's now encrypt hi with our secret key H=7|I=8

k XOR h XOR 26
14 XOR 7 XOR 26=19
19th position is t so h will be replaced by t

- For next iteration q=300//14(floor division)
  =21

- And k =k+qmod26
- K= (300+21) mod26=321mod2
- K=9 I=8

So, k XOR I XOR 26 9 XOR 8 XOR 26=27
27= Δ
So, i will be encrypted as Δ So, hi will be encrypted as t Δ

- Now t Δ will use the initial shared secret key which was 30
- So, t Δ will used Vigenère mechanism
- T=19|Δ=27| it will use 300 only 30 will be used
- T XOR 3 and Δ XOR 0 19 XOR 3=16

27 XOR 0= 27
Now tΔ is encrypted as qΔ

- Using Polybius cipher Q=41 Δ=53
- Final cipher is 4153

- *Decryption:* Cipher text is 4153

- First, we have to use Polybius cipher, with the help of table We will first take two digits of cipher text (first digit being the row and second digit the column andthe intersection will be our text)
- So, 41=Q and 53=Δ
- The shared key is 300 we have to XORits first and second digit with Q position and Δ position and XOR will be 26 Q=16 Δ=53
- 16 XOR 3 =19
- 27 XOR 0 =27
- 19=t 27=Δ
- Now k=300mod26=7 Now 7 position is h
- Now k= (300+300//14(floor division)) mod26
- K=9
- So now 9 XOR 27 XOR 26=8
- 8th position is i.
- Final Text is hi

We have successfully decrypted the text.

IV. CONCLUSION

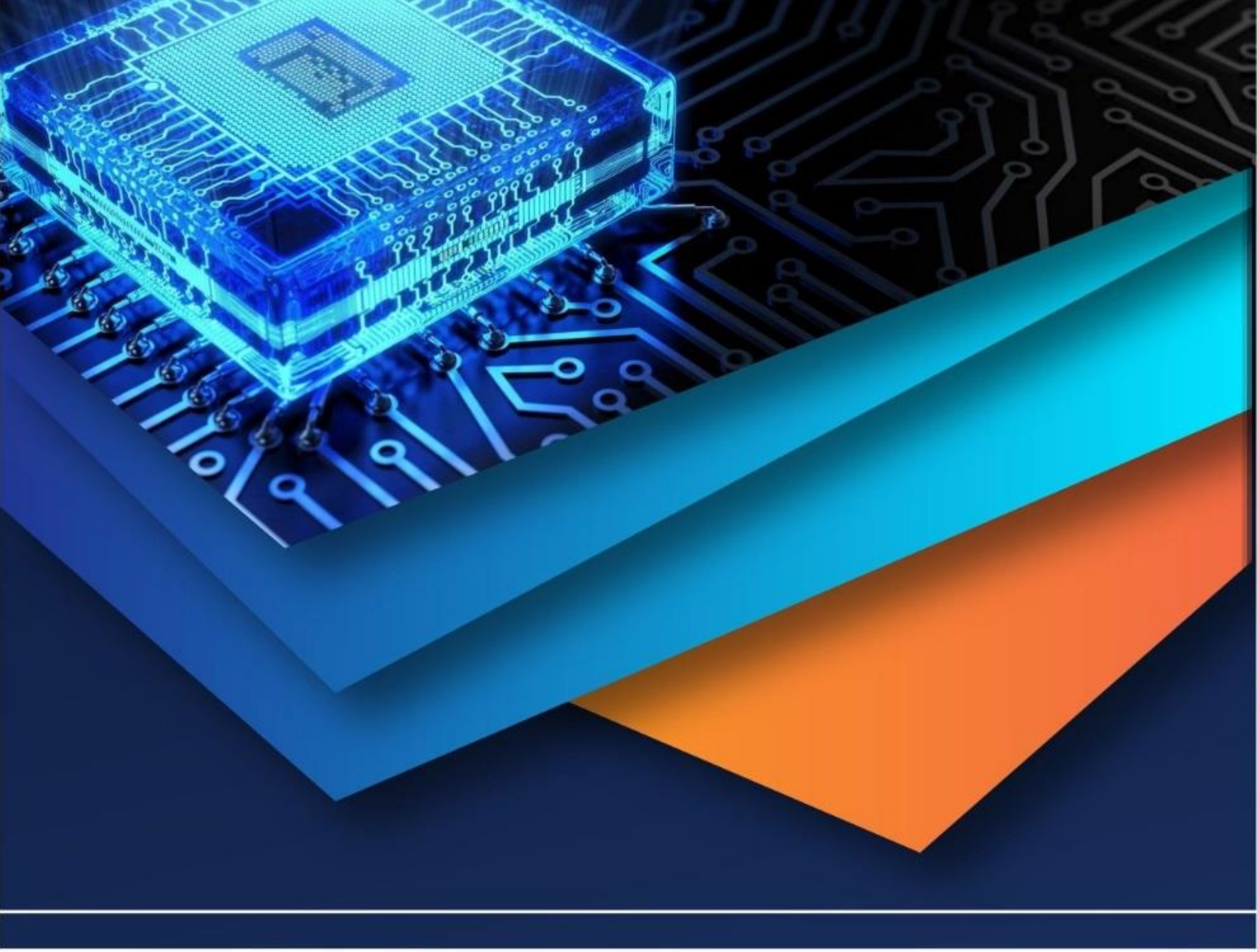
The suggested algorithm will improve file security that needs to be sent. It will secure the file's content from malicious actors. The file's integrity will be carefully maintained. Additionally, it will guarantee data confidentiality. We can achieve high data security in this way.

V. FUTURE SCOPE

The proposed algorithm is still in the planning stages. The speed and complexity of the algorithm can be increased. We have additional options for protecting the private keys we'll be using from bad actors.

REFERENCES

[1] Abhishek Mishra, Abhishek Rai, Dheeraj Gurjar, “Design of Hybrid Cryptography System based on Vigenère Cipher and Polybius Cipher”, IJARSCT, https://ijarsct.co.in/Paper4133.pdf
[2] Aditi Saraswata, Chahat Khatria, Sudhakara, Prateek Thakrala, Prantik Biswasa, “An Extended Hybridization of Vigenere and Caesar Cipher Techniques for Secure Communication ”, ICCC, https://www.sciencedirect.com/science/articl e/pii/S1877050916316465
[3] Enas Ismael Imran, “Enhancement Caesar Cipher for Better Security”, IOSR, https://www.iosrjournals.org/iosr-jce/papers/ Vol16-issue3/Version-5/A016350105.pdf
[4] Dr. Tun Myat Aung, Ni Ni Hla, (2019), “A Complex Transformation of Monoalphabetic Cipher to Polyalphabetic Cipher”, IJMLC, http://www.ijmlc.org/vol9/801-ML0065.pdf



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY