International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 1 Jan 2022, pp: 184-199 www.ijaem.net ISSN: 2395-5252

Triple Layered Fibonacci Caesar Cipher Hybrid

Shivam Sharma, Shubh Gaur, Harsh Vardhan, Pronika Chawla, Madusudhan Mishraa

FacultyofEngineeringandTechnology ManavRachna International Instituteof Research and Studies Faridabad, India
FacultyofEngineeringandTechnology ManavRachna International Instituteof Research and Studies Faridabad, India
FacultyofEngineeringandTechnology ManavRachna International Instituteof Research and Studies Faridabad, India
FacultyofEngineeringandTechnology ManavRachna International Instituteof Research and Studies Faridabad, India
FacultyofEngineeringandTechnology ManavRachna International Instituteof Research and Studies Faridabad,India

Submitted: 01-01-2022 Revised: 05-01-2022 Accepted: 10-01-2022

ABSTRACT— The amount of people that use computer, laptops and mobile platforms daily is staggering. Out of those people, everyone needs internet one day or another which can lead to the discovery of a wonderful amount of content at the disposal oftheir fingertips. The biggest drawback of using these devices and the internet is threat of a cyberattack. Here we try to build an encryption algorithm that's never been attempted before where we remove the drawbacks of their former selves and improve upon it by combining them. This encryption algorithm will certainly help protect more people from the threat ofcyberattacks and secure their privacy and data.

Keywords— cryptography, cryptanalysis, encryption,decryption.

I. INTRODUCTION

Cryptographyistheartofhidingmessages/data/information from any third party without the proper authentication or authorization. These kinds of techniques have been used since ancient times like this Caesar Cipher used by emperor Julius Caesar to hide messages sent and received by the royalty from opposing kingdoms, bandits, spies and also people within the kingdom of Rome that were conspiring against him. In the modern world cryptographic techniques have been used in the cyberspace that is the digital world which is paramount to the way the world works and the biggest stepping stone to the future. Ancient techniques like the Caesar cipher are obsolete in the modern era as it is very easily broken by simple brute forcingtechniques.Thesekindsofcipherscouldbedeciphered easily even by humans so they are absolutely useless against the humongous processing power that the machines of today possess. These days the ciphers we use are So complex that theycan'tbedecipheredbyahumanThroughnormalmeansas it could take an indefinite amount of time Which could be larger than the span of multiple human lives. Some examples are-DES dddesaesrsa blowfish etc.

Ciphers are basically reversible techniques implemented through different mathematical functions to achieve

Cryptographic algorithms are generally classified into two types –

A. SymmetricKeyAlgorithms

This kind of encryption involves using a single key for the processofencryptingamessage,whichisusedforboth encryption and decryption. It generally gives a smaller or the samelengthoftextwhencomparetotheoriginalplaintextfile. This technique is old but it is fast and is also used to transfer large amount of data and it also works on low utilization of resources.

This kind of method is the inverse of the technique known as asymmetric encryption which uses different keys for the process of encryption and decryption. Symmetry Ki cryptography is based on a single share key that all parties are aware of and can use to encrypt and decrypt data.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 1 Jan 2022, pp: 184-199 www.ijaem.net ISSN: 2395-5252

It is the simplest kind of encryption technique and is also knownassecretkeycryptographyorprivatekeycryptography. Its most common example would be DES, DDDES, AES.

This technique provides less security as there is only one key in use and if it falls into the hands of an attacker, it could ruin the whole encryption process and could result in catastrophic damage to an organization's assets, intellectual properties and so on.

It only provides us with confidentiality for the given data but it cannot provide us the assurance of integrity and authenticity.

In specific cases it is very useful for example someone wants to connect to network that is close via VPN, so during the establishment of the connection the client and server will have to exchange keys, if the keys are symmetric the process will be much faster and smoother and the transfer of data will become much easier and the same cannot be said for a symmetric key encryption.

B. AsymmetricKeyAlgorithms

This kind of encryption involves using two keys for the purposeofencryptionordecryption,Itisalsocalledpublickey encryption because thekey isused forencryption or thepublic key and the private key. We use a public key for encrypting a message and a private key for decrypting a message.

It generally gives larger or the same length of text as the original plain text. This technique is modern what is it is not fast and cannot be used to transfer huge amounts of data as it has higher utilisation of resources.

This metal isthe inverse of the technique that is symmetric key encryption which uses the same key for the process of encryption and decryption. A symmetric key cryptography is basedontwokeyswhereeachpersonhasaseparateprivatekey todecryptmessagesandpublicyeartoencryptthosemessages. It is a more complex and newer technique and its most commonexamplesareRSA,DiffieHellmankeyexchangeand DSA.

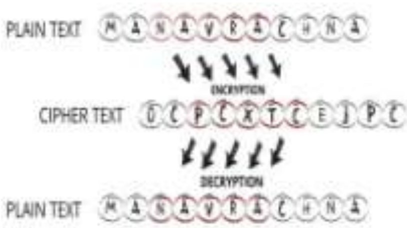
Thismethodofencryptionprovidesuswithconfidentiality, integrity and authenticity for the given data. This method is very useful for broadcasting on multicasting secret messages over a network as only those people who have the proper private key can decrypt the message in corrupted by other specific public key.

Theencryption/decryptionoftheletterisperformedbyfirst converting the letters into numbers, according to the scheme A=0, B =1, C =2,…..,X=23, Y=24, Z=25 and performing a modular arithmetic.

TheAlgorithmcanberepresentedasfollows:

Encryption: C = E(K,P) = (P + K)mod26

Decryption: P = D(K,C) = (C - K)mod26



II. LITERATUREREVIEW

A. CaesarCipher

Caesar Cipher is a basic encryption technique used since the ancient and medieval times. It is an old school encryption technique that was famous for its usage by Emperor Gaius Julius Caesar of the ancient Roman Empire. He is known for leading the Roman armies in many wars and governed the nation as a dictator. He was secretly dispatched during his reign.

The technique that we use in Caesar cipher is a simple monoalphabetic substitution that comprises of shifting our givenstringofcharacters(theplaintext)byacertainnumberof times through a fixed key generally provided by the user.We basically perform a shift with each individual character by N number of times assuming N is the key.

TheformulausedfortheEncryptionwouldbe–` CT = (PT + key) (mod 26)

CTistheCipherTextalphabetnumber

PT is the Plain Text alphabet number (provided by the user).

Keyisthenumberof shiftsneededtobedone(providedby the user).

Mod26 isusedto taketheremainderafterdividingthekey by 26.

The process for decryption is similar to encryption except thefactthatitistheoppositeofit.Weshiftthecharactersb

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 1 Jan 2022, pp: 184-199 www.ijaem.net ISSN: 2395-5252

ack by the number of characters as given in the key for each character in the string and get the desired information, that is, the plain text which we hid successfully.
Theformulausedfordecryptionwouldbe– PT = (CT – key) (mod 26)
CTistheCipherTextalphabetnumber. PT is the Plain Text alphabet number.
Keyisthenumberofshiftsneededtobereversed(provided by the user).
Mod26 isusedto taketheremainderafterdividingthekey by 26.
ForExample:
PlainText: HelloWorld Key : 3
CipherText: KhoorZruog

Another use of Caesar cipher is the ROT 13 which means shift or rotate the alphabets by 13, generally used in learning around the world, though, it has a wide variety of uses where we could see it in different pop culture even going as far as concealing offensive language or other antics such as hiding a responseorsolvingariddle.Therepositioningofthealphabets or units of the strings is deliberately chosen to be 13 to fulfil a few objectives. Since shifting the units of the string twice brings it back to the original text which is useful for easily deciphering the text without building a separate algorithm or programforthedecryptionprocess.Afunctionbysimilarname is also found in python which further illustrates the fame and variety that Caesar cipher hasgarnered over a course of a long time.

B. PlayfairCipher

This is a stronger encryption technique when compared with Caesar cipher which is just a simple mono alphabetic substitution cipher, this cipher encrypts a pair of alphabets called diagraphs.

It was invented by Charles Wheatstone, who is also known for his work with the famous Wheatstone bridge used to measure electrical resistance with a current that is not known.

Wheatstone Bridge is generally taught to high school students and has a very important role in understanding the fundamentalsofelectricalengineering.Itwasinventedin1854 but still isn'tknownbythenameof Charles Wheatstonethisis because Lord play fair brought it out to the world and made it famous in the world of cryptographic techniques.

In this we create a 5×5 matrix Which we call the grid of letters. Wecan createa simplematrix with alphabetsfrom a to Z whereinwe skiponeparticularalphabet aswehave to create a 5X5 matrix which has 25 characters so generally we skip an alphabetorweplacetwoalphabetsinasinglecell.Wecanalso take a key from the user or assume one and inserted alphabets in the beginning of the matrix and then insert the remaining alphabetsin the matrix to improve itscomplexity so it can'tbe easilybrokenbyusingsimplebruteforcingtechniquesorother methods to decipher or decrypt the message.

Wethendividetheplaintextintopairsandstart encrypting themthroughthematrixthatwejustcreated.Wetakeeachpair and encrypt it according to certain set of rules. If both the letterslieinthesamecolumn,weshiftthembyonecharacterto downwards.
If they're in the same row we save them by one character right and if both these conditions are not true then they must form the corners of a rectangle or a square and we encourage thembyereplacingthemwiththeoppositecornersofthe given rectangle or the square. If the number of alphabets aren't even innumberthenweaddaletterwithitsowecanformapairfor examplewecanaddXtoasinglecharactertoformapair, also we use this method in case we have two same letters in a pair and we replace one of them withx asthisimproves thequality of encryption and makes the ciphertext much more difficult to decipher.
In case of decryption, we do the opposite of encryption as usual.First,wetaketheciphertextAnddividedintopairs.Now we take each pair and decrypted according to the same set of rules that we used to encrypt the plaintext. If both the letters line the same column, we shift them One character upwards.
If they're in the same row we shift them one character to theleft.Ifnoneoftheseconditionsoccur,theyformthecorners of a rectangle or a square and we decrypted by taking the oppositecornersofthesamerectangleorthesquareformedby the two characters. After that we check the plaintext that we deciphered for replacement characters like X and replace it with the appropriate character or none depending on the plaintext as we use X to either replace to same characters in a pair or to form a pair if there is only a single character present in a pair.
Thecryptanalysisofthistechniquesuggestitismuchbetter and complex than simple mono alphabetic substitution ciphers like Caesar cipher and is also stronger than other polyalphabetic substitution cycles like the Vigenère cipher.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 1 Jan 2022, pp: 184-199 www.ijaem.net ISSN: 2395-5252

C. Vigenèrecipher

The Vigenère cipher belongs to the class of polyalphabetic Ciphers.Anotherexampleofitwouldbetheenigmamachine. The firstmentionof thisexemplary cipher wasmade in1553. Itwentontobeindecipherableforanother300yearsthrough whichitgarneredthereputationoftheindecipherable cipher.

This cipher particularly requires a secret key to be used effectively.Westartbytakingtheplaintextfromtheuser followed by the key. Then we created 26 x 26 matrix (Vigenère square, Vigenère table or tabula recta).

Wecheckourplaintextandthekeyandifourkeyisnotoft he same length as the plain text we repeat the characters of the key until it is of the same length as the plaintext. The 26 x 26 matrix that we create contains all the alphabets from a to Z in the first row and column. After that, we start mapping the letter according to the letters in the rows and columns. First, we check the alphabet in the plain text and then we check the alphabet in the key and accordingly, we select the specific character in the cell mapped to the letters found in the plain text and the cipher text.

We check to see in the Matrix where is the element is found andthatelementreplacesthegivenalphabetintheplaintext.

Wecontinuethisprocesstillwecome totheendofthe plaintext.

In 1553 its working was shown by Giovan BattistaBellaso whoalsoinventedit.ItwasnamedafterBlaisedeVigenère after Credit went to him wrongfully and not to its original inventor who did so three centuries ago Thecipherbecameindecipherablebecauseitusedakey which could be a phrase or a word and could be easily replacedwhich made the cryptanalysis process difficult in the mediaeval times when it was used by the rulers and nobles as there was no specific study related to cryptography at that time.

III. PROPOSEDALGORITHM

In our approach, we are trying to combine three encryption algorithmstogethertogeneratea**hybridcipher**which willnot be easy to crack because not only we are combining the three algorithms but also modifying the working of two encryption algorithms used and using the third encryption as it is in our hybrid cipher.

The three encryption algorithms used in the proposed approach are:

VigenèreEncryption

Caesar Cipher used in conjunction with Fibonacci Series. [MODIFIED]

PlayfairCipher6x6.[MODIFIED]

Inourapproach,thetextwillbeencryptedonebyoneusing each of the encryption algorithms mentioned above and in the same order as above.

By modifying the existing algorithms of Caesar cipher and Playfair cipher, we are trying to overcome their limitations which ensures that the cipher text generated is highly enforced and not easy to crack using conventional methods.

The limitations of Caesar cipher and Playfair cipher are summarized below: -

In Caesar cipher, a numeric key(n) is required in the range (0-

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 1 Jan 2022, pp: 184-199 www.ijaem.net ISSN: 2395-5252

25)andthenthatnumerickeyisusedtoshifteachcharacter bythatnumberofplacestotherightusing thealphabetictable.

Now,
ALPHABETICTABLE

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

A. LIMITATION1:

Thisisoneofthelimitationsofthistechnique,asJandIare considered equal,thereisnowaytofind outduring decryption whether the character that has just been decrypted was J or I which leads to inconsistency.

If we consider J as I in the Playfair matrix, then after decryption wherever Jwaspresentintheplain text,I wouldbe there.

If we consider I as J in the Playfair matrix, then after decryption whereverI waspresentintheplain text, Jwouldbe there.

After constructing the Playfair matrix, the next step is to splittheplaintextinpairsoftwo,suchthatifanyletterappears

Encryptionwithkeyn,canmathematicallybewrittenas:

$$E_n(x) = (x + n) mod\ 26$$

Similarly,

Decryptionwithkeyn,canmathematicallybewrittenas:

$$D_n(x) = (x - n) mod\ 26$$

Note:

Xrepresentseachcharacterfromthemessagetakenone ata time.

MOD 26 is taken so that (x-n) and (x+n) always remain in the range of 0-25.

UsingtheoldtraditionalCaesarciphertechniqueisobsolete as one can easily decipher it using brute-forcing, as there are not a wide range of keys available. At any time, key will be in the range of 0-25 only and the same key will be used to shift each character of the plain text.

InPlayfairCipher,themessageisencryptedusingdigraphs approach(takingtwocharacterstogetheratatime)insteadofa single letter using a 5 X 5 matrix generated using the key, commonly known as the Playfair matrix.

In this technique, a 5 X 5 matrix (Playfair matrix) consisting of alphabets is generated using the key provided such thatno character isrepeated. As there are only 25 cells in a5X5matrix so JandIareconsidered equalandresidein the same column and J is always considered as I or vice versa.

ForExample,

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 1 Jan 2022, pp: 184-199 www.ijaem.net ISSN: 2395-5252

If the key is **ATHENS**, then Playfair matrix would look like the following:

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

twice (side by side), put X at the place of second occurrenceandalso,ifasinglecharacterremainsatthee nd,pairitwithX.
ForExample,JAZZcanbesplitas:
First pair: JA Second Pair: ZX Third Pair: ZX Digraph:JAZXZX

B. LIMITATION2:

ThisarisesthesecondlimitationofPlayfaircip her,
If X is present side by side in the text that we want to encrypt, then we won't be able to pair it with another X as it willgenerate the same resultand will also lead to the violation of the rule that no two characters can be together.
ForExample, HEXXXO
Splittinginto pairs:
FirstPair:HE
SecondPair:**X**X(RuleViolation) Third Pair: **X**X (Rule Violation) Fourth Pair: **X**O
Now, when we decrypt the cipher text that was generated using this technique, we need to remove all the occurrences of X from the result, so that we get the final plain text because "X" is the character that we appended for the scenario explained above.

C. LIMITATION3:

ThisgivesrisetothethirdlimitationofPlayfairCipher,
Suppose X was present in the string that we wanted to encrypt.
After encryption,if wetry to decryptthen wemustremove all the occurrences of X from the result we got as "X" is also the character that we use for appending to letters for making digraphs.
Thiswouldleadtolossofinformationasthereisnowayto know which X was used for appending and which X was already present in the ciphertext.
ForExample,
PT:HEXO(tobeencrypted) Key: YU
Ciphertext generatedafterencryption,

CT:DFTR
Now,ifwetrytodecryptit,wewillgettheresultasHEXO and according to the rule we must also remove X from it as X isusedforappending, sothefinal resultwouldbe **HEO**which is not the result we expected as the plaintext contained X in it.

So, the modifications proposed by us aim to correct these limitations as well as create a brand-new three-layered **hybrid encryption technique** which could be used in the future for protecting digital data confidentiality.

D. ModifiedCaesarCipherusingFibonacciSeri es

Inthistechnique,charactersinastringareshiftedbasedo n their position and the corresponding number in the Fibonacci series.
Only alphabets can be encrypted using the following technique.
Alphabetic Table is used to rotate the character which is shown below:

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 1 Jan 2022, pp: 184-199 www.ijaem.net ISSN: 2395-5252

ALPHABETICTABLE

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Working:

Message:	A	T	T	A	C	K
Position in Message:	1	2	3	4	5	6
Fibonacci Sequence:	1	1	2	3	5	8
Rotation:	1	1	2	3	5	8
Result:	B	U	V	D	H	S

In the above depiction we are encrypting ATTACK using the proposed approach.
Wefirstmarkthepositionsofeachcharacterinthemessage and then based on that position find the Fibonacci term corresponding to that position and shift that character by the value of that number to the right.
TheMathematicalformulacanbesummarizedasbelow:
CT=(X+Fibonacci(i))MOD26 where,
X=Character
I= Position of X in the string
Fibonacci(n)=nthFibonacciNumber
Using this approach to encrypt text using the traditional Caesar cipher technique, we do not require a key and it also overcomesthelimitationoforiginalCaesarcipheralgorithm whichwasthatitshiftseachcharacterinthestringbythesame amount, but here, every character in the string to be encrypted isshiftedbyadifferentnumberwhichisgivenbytheFibonacci sequence, thus, enforcing it.

E. PlayfairCipher6x6

The original Playfair encryption used a 5 X 5 matrix generated using an alphabetic key due to which we had to considerIandJtobesameandtherewasnowaytodistinguish I and J from each other after decryption.
Inthismodifiedapproach,insteadofusing5X5matrixwe are using a 6 X 6 matrix to so that there are enough places for all the alphabets to fit in. There are in total 36 places in the matrix, out of which 26 are occupied by alphabets and the remaining 10 are occupied by numbers from 0-9.
Also, we have modified the pairing approach in which the character used for pairing is always a number which can be decidedusingthekeywhichresolves thelimitations2and3of the original Playfair technique as explained above.
WORKINGEXAMPLE
Encryption
Step1:CreatingaPlayfairmatrixusingthekey. Key: JIGNESH
The Playfair matrix according to the given key can be constructed as below:

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 1 Jan 2022, pp: 184-199 www.ijaem.net ISSN: 2395-5252

J	I	G	N	E	S
H	A	B	C	D	F
K	L	M	O	P	Q
R	T	U	V	W	X
Y	Z	0	1	2	3
4	5	6	7	8	9

Step2:Calculatethepairingcharacter.
Thepairing character can becalculated by summing up the asciivaluesofeachcharacterinthekeytaketheone'sdigit of the sum obtained as the pairing character
ForExample:

Character	J	I	G	N	E	S	H
ASCII	74	73	71	78	69	83	72

Sum=74+73+71+78+69+83+72 Sum=520
PairingCharacter=SumMOD10 Pairing Character= 520 MOD10
PairingCharacter=0
Step3:Splittheplaintextintopairs. PT: HEXXXG

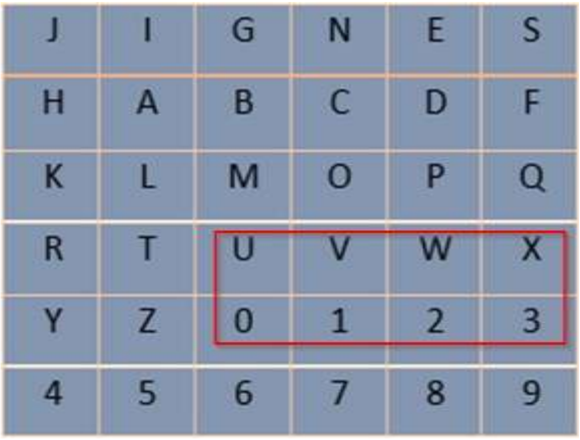
Pair1: HE
Pair2: X0
Pair3: X0
Pair4: XG
We can clearly see that none of the pairs are violating any of the pairing rules of the Playfair technique.

Step4:Usingtheplaintextpairsgeneratedaboveto generate pairs of ciphertext.
Pair1: HE

J	I	G	N	E	S
H	A	B	C	D	F
K	L	M	O	P	Q
R	T	U	V	W	X
Y	Z	0	1	2	3
4	5	6	7	8	9

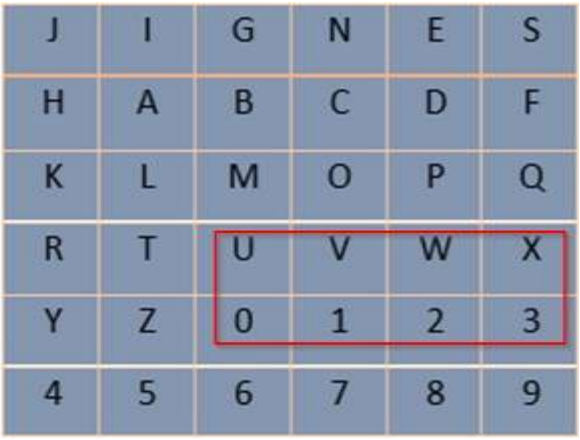
Pair1CT:DJ Pair 2: X0

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 1 Jan 2022, pp: 184-199 www.ijaem.net ISSN: 2395-5252



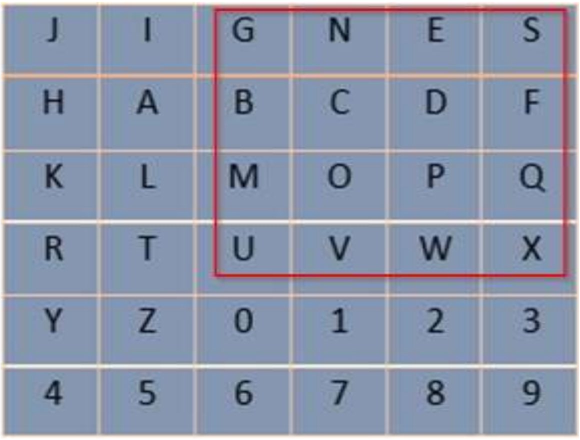
J	I	G	N	E	S
H	A	B	C	D	F
K	L	M	O	P	Q
R	T	U	V	W	X
Y	Z	0	1	2	3
4	5	6	7	8	9

Pair2CT:U3 Pair 3: X0



J	I	G	N	E	S
H	A	B	C	D	F
K	L	M	O	P	Q
R	T	U	V	W	X
Y	Z	0	1	2	3
4	5	6	7	8	9

Pair3CT:U3 Pair 4: XG



J	I	G	N	E	S
H	A	B	C	D	F
K	L	M	O	P	Q
R	T	U	V	W	X
Y	Z	0	1	2	3
4	5	6	7	8	9

Pair4CT:US
Step5:Combiningalltheciphertextpairstogetherto generate ciphertext.
CT=Pair1+Pair2+Pair3+Pair4 CT= DJ + U3 + U3 + US
CT=DJU3U3US

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 1 Jan 2022, pp: 184-199 www.ijaem.net ISSN: 2395-5252

Decryption

Step1:CreatingaPlayfairmatrixusingthekey. Key: JIGNESH

ThePlayfairmatrixaccordingtothegivenkeycanbe constructed as below:

J	I	G	N	E	S
H	A	B	C	D	F
K	L	M	O	P	Q
R	T	U	V	W	X
Y	Z	0	1	2	3
4	5	6	7	8	9

Step2:Calculatethepairingcharacter.

Thepairing charactercanbe calculatedby summingup the ascii values of each character in the key take the one's digit of the sum obtained as the pairing character

ForExample:

Character	J	I	G	N	E	S	H
ASCII	74	73	71	78	69	83	72

Sum=74+73+71+78+69+83+72 Sum=520

PairingCharacter=SumMOD10 Pairing Character= 520 MOD10

PairingCharacter=0

Step3:Splittheciphertextintopairs. CT: DJU3U3US

Pair1: DJ

Pair2: U3

Pair3: U3

Pair4: US

Step4:Usingtheciphertextpairsgeneratedaboveto generate pairs of plaintext.

Pair1: DJ

J	I	G	N	E	S
H	A	B	C	D	F
K	L	M	O	P	Q
R	T	U	V	W	X
Y	Z	0	1	2	3
4	5	6	7	8	9

Pair1PT:HE Pair 2: U3

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 1 Jan 2022, pp: 184-199 www.ijaem.net ISSN: 2395-5252

J	I	G	N	E	S
H	A	B	C	D	F
K	L	M	O	P	Q
R	T	U	V	W	X
Y	Z	0	1	2	3
4	5	6	7	8	9

Pair2PT:X0 Pair 3: U3

J	I	G	N	E	S
H	A	B	C	D	F
K	L	M	O	P	Q
R	T	U	V	W	X
Y	Z	0	1	2	3
4	5	6	7	8	9

Pair3PT:X0

Pair4: US

J	I	G	N	E	S
H	A	B	C	D	F
K	L	M	O	P	Q
R	T	U	V	W	X
Y	Z	0	1	2	3
4	5	6	7	8	9

Pair4PT:XG

Step 5: Combining all the plaintext pairs together and remove the pairing character from the result to generate plaintext.
Result=Pair1+Pair2+Pair3+Pair4 Result= HE + X0 + X0 + XG
Removingallthe0'sfromtheresulttogetPT
PT=HEXXXG

Therefore,ourmodifiedapproachforPlayfaircipherisable to handle all the limitations of the original Playfair encryption technique.
After overcoming the limitations of the encryption techniques discussed before, now we are ready to consolidate the algorithms that we had discussed to create a brand-new hybrid encryption and we will

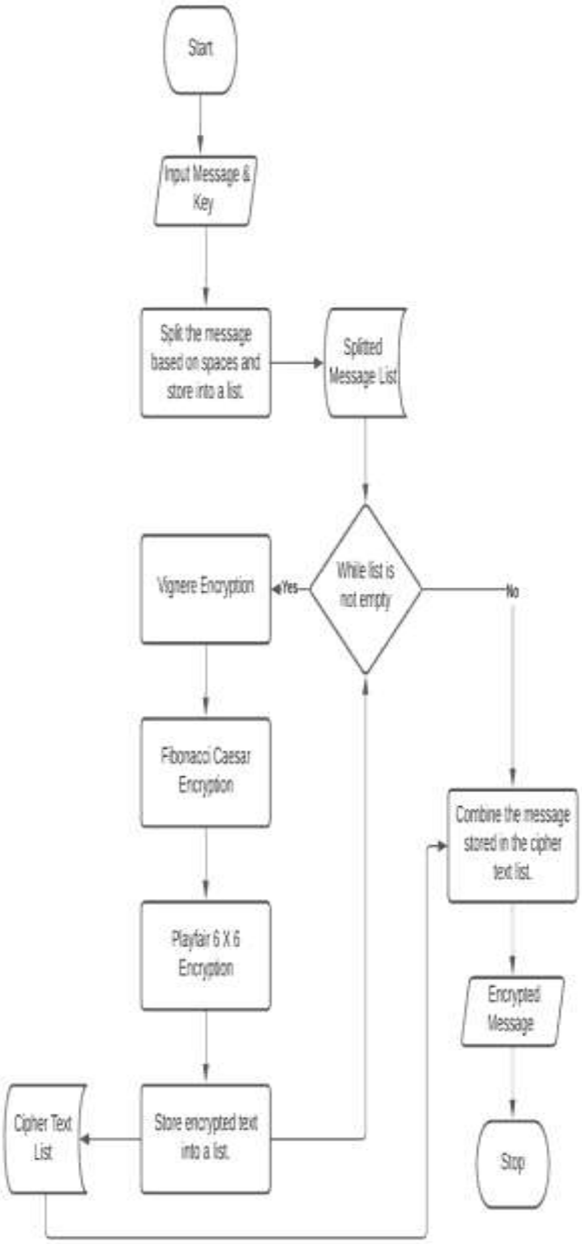
International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 1 Jan 2022, pp: 184-199 www.ijaem.net ISSN: 2395-5252

call it **3LFibCaesar**.

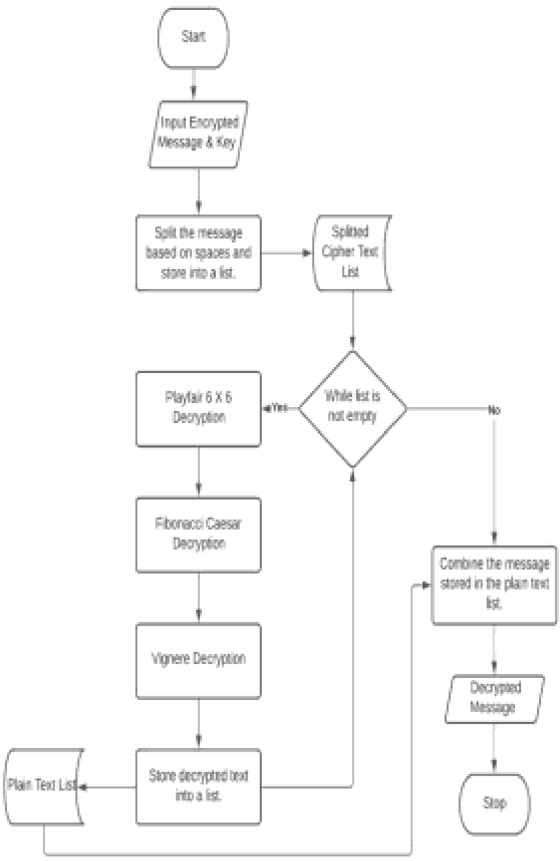
IV. WORKING

We will proceed according to the flowcharts given below for encryption as well as decryption.

A. EncryptionFlowchart:



Let us walkthroughthestepsmentionedinthe flowchart using a simple example:
Step 1: Input message to be encrypted and the key used to encrypt it.
Message:MANAVRACHNA Key: MRIIRS
AsFibonacciCaesardoesnotrequireakey,thiskeywill be used for Vigenère and Playfair 6 X 6 encryption.
Step 2: Split the message based on spaces and store into a list.
B. DecryptionFlowchart:
Split1:MANAV
Split2:RACHNA
List:[“MANAV”,”RACHNA”]
Step 3:Iterateon the split listand encrypt each word in the order as shown in the flowchart.
VigenèreEncryptionFor0thListElement:
Text:MANAV Key: MRIIRS
CipherTextGenerated:YRVIM For 1st List Element:
Text:RACHNA
Key:MRIIRS
CipherTextGenerated:DRKPES
Step 4: Encrypt each cipher text generated in the previous step using Fibonacci Caesar encryption.
FibonacciCaesarEncryptionFor 0th List Element:
Text:YRVIM
CipherTextGenerated:ZSXLR For 1st List Element:
Text:DRKPES
CipherTextGenerated:ESMSJA
Step 3: Encrypt each cipher text generated in the previous step using Playfair 6 X 6 encryption.
Playfair6X6Encryption For 0th List Element:
Text:ZSXLR Key:MRIIRS
CipherTextGenerated:1RUPIZ For 1st List Element:
Text:ESMSJA
Key:MRIIRS
CipherTextGenerated:FIRAOM
Step 3: Combine the cipher texts generated in the previous step to get the final encrypted cipher text.
CipherText=1RUPIZFIRAOM



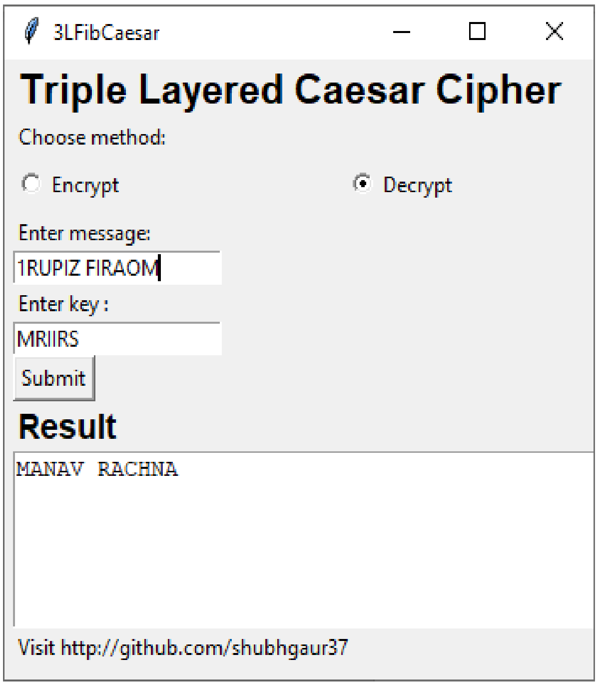
International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 1 Jan 2022, pp: 184-199 www.ijaem.net ISSN: 2395-5252

Let us walkthroughthestepsmentionedinthe flowchart using the example used in the encryption phase:
Step 1: Input message to be encrypted and the key used to encrypt it.
EncryptedMessage:1RUPIZFIRAOM Key: MRIIRS
AsFibonacciCaesardoesnotrequireakey,thiskeywill be used for Vigenèreand Playfair 6 X 6 encryption.

Step2:Splittheencryptedmessagebasedonspacesand store into a list.
Split1:1RUPIZ
Split2:FIRAOM
List: [“1RUPIZ”,”FIRAOM”]
Step 3:Iterateon the split listand decrypt each word in the order as shown in the flowchart.

Playfair6X6Decryption For0^{th}ListElement:
EncryptedText:1RUPIZ Key: MRIIRS
PlainTextGenerated:ZSXLR For 1^{st} List Element:
EncryptedText:FIRAOM Key: MRIIRS
PlainTextGenerated:ESMSJA
Step4:Decrypteachplaintextgeneratedintheprevious step using Fibonacci Caesar decryption.

FibonacciCaesarDecryptionFor 0^{th} List Element:
EncryptedText:ZSXLR
PlainTextGenerated:YRVIM For 1^{st} List Element:
EncryptedText:ESMSJA
PlainTextGenerated:DRKPES
Step3:Decrypteachplaintextgeneratedintheprevious step using Vigenère decryption.
VigenèreEncryptionFor0^{th}ListElement:
EncryptedText:YRVIM Key: MRIIRS
PlainTextGenerated:MANAV For 1^{st} List Element:
EncryptedText:DRKPES
Key:MRIIRS
PlainTextGenerated:RACHNA
Step 3: Combine the plaintexts generated in the previous step to get the final decrypted plain text.
Decryption



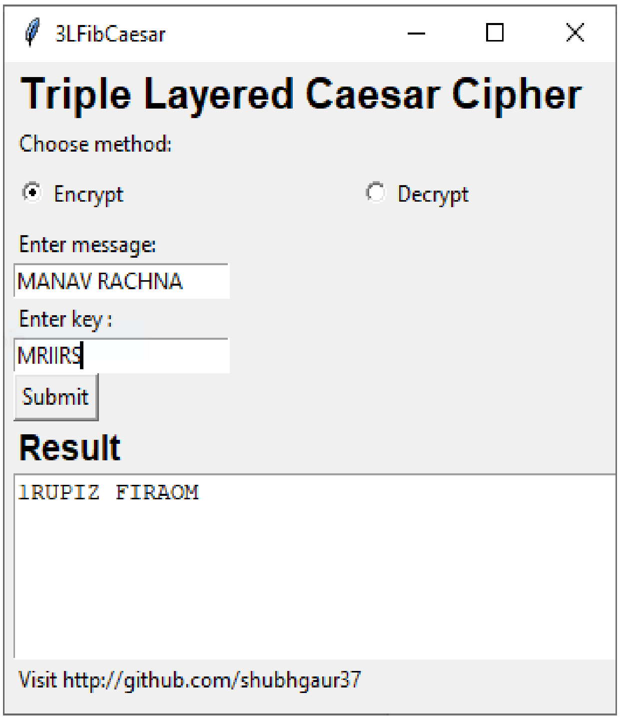
International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 1 Jan 2022, pp: 184-199 www.ijaem.net ISSN: 2395-5252

VI.CONCLUSION

PlainText=MANAVRACHNA

V.IMPLEMENTATION

Encryption



Our project started from the Caesar Cipher and ended up becoming a triple layered encryption algorithm with its basic architecturebeingtheCaesarcipher,thePlayfaircipher andthe Vigenère cipher. We aimed to create an encryption algorithm that would be hybrid and better suited to providing confidentiality, integrity and authenticity of the data that the user wants to encrypt.

The algorithm we created is extremely difficult to crack, albeit near impossible because of the number of permutation and combinations one would have to try to hope to crack the algorithm and get to the critical information.

Our algorithm is new and absolutely original, no one has been able to or tried to cover up the limitations of the existing encryption algorithms while turning them into a unique hybrid like this one.

VII.FUTURE SCOPE

Our project aims to help people by giving them the opportunity to step into the inconceivable huge field of cryptography. This project shall be about giving people a new option to encrypt their data and store it securely.

The project shall have a huge scope of improvement, be it related to adding more cryptographic algorithms in the already existing hybrid algorithm or improvement of the UI and frontend.

It would prove to be most useful to teachers, professors, students and cybersecurity enthusiasts who aim to teach and learn the ways of cryptographic algorithms and the processes involved in it. The field of cryptography should be filled with peoplewhoarewellinformedandaimtoimprovethecurrently existing architectures and procedures.

Thus, our project's idea is simple but an efficient way to givebacktothecommunitywithalotofscopeofimprovement in the sustainable future.

ACKNOWLEDGEMENT

This research paper wouldn't have been possible without the support of our project guide, Ms. Pronika Chawla, who helped us where we needed and acted like our guiding light. We would also like to thank the other staff at our university including the HOD, Dr. Tapas Kumar for their continuous support.

REFERENCES

[1] Han Fet al (2014)Ageneral transformation fromKP-ABEto searchableencryption. Future GenerComputSyst 30:107–115

[2] Rachmawati Dian and Candra Ade 2015 Implementation of thecombinationofCaesarCipherandAffineCipherfortextdatasecurity Informatics Research and Education Journal (JEPIN)

[3] Ariyus D. 2008 Introduction to Cryptography: Theory, analysis andimplementation (Yogyakarta: Andi)

[4] Basuki, Paranita and Hidayat 2016 Design of Layered CryptographyApplications Using Caesar Algorithms, Transpositions, Vigenere andBlock Cipers Based on MobileNational Seminar on Information andMultimedia Technology. STMIK AMIKOM (Yogyakarta,)

[5] Bellare, M., Desai, A., Jokipii, E., Rogaway, P.: A concrete securitytreatment of symmetric encryption: analysis of the DES modes ofoperation. In: Proceedings of the 38th Symposium on Foundations ofComputer Science. IEEE (1997)

[6] K. Senthil, K. Prasanthi and R.Rajaram, "A modern avatar of JuliusCaesarandVigenerecipher",ComputationalIntelligenceand Computing Research (ICCIC) 2013 IEEE International Conference, pp.1-3,2013.

[7] ChampakamalaB.S,PadminiKandRadhikaD. K2014LeastSignificantBit Algorithm for Steganography Int. J. of Advance ComputerTechnology

[8] Emam, Marwa M, Aly Abdelmgeid A and OmaraFatma A 2016 AnImproved Image Steganography Method Based on LSB Technique withRandom Pixel Selection Int.l J. of Advanced Computer Science andApplications 7 17-22

[9] Inan, Y. (2019). Analyzing the Classic Caesar Method Cryptography.4th International Conference on Computational Mathematics andEngineering Sciences(pp. 213-220)

[10] Monika,A.,&Pradeep,M. (2012). A Comparative Survey on SymmetricKey Encryption Techniques.International Journal on Computer Scienceand Engineering (IJCSE), 877-882.

[11] Senthil, K.,et al. (2013). A modern avatar of Julius Caesar and Vigenerecipher. IEEE International Conference.Computational Intelligence andComputing Research (ICCIC)

[12] Verma, O.P et al. (2011). Performance Analysis Of Data EncryptionAlgorithms. IEEE.Delhi Technological University India

[13] Atish,J.,et al.(2015).Enhancing the Security of Caesar CipherSubstitution Method using a Randomized Approach for more SecureCommunication. International Journal of Computer Applications,129(13),6-11.DOI: 10.5120/ijca201590706

[14] Sahai A, Waters B (2005) Fuzzy identity-based encryption. In: Annualinternational conference on the theory and applications of cryptographictechniques. Springer, Berlin, Heidelberg