The hour glass method for encryption and compressing any encrypted text into a singlecharacter, using the fundamentals of power arithmetic function to reduce space complexity

BasimNajimAL-DinAbed[a]Dr.SalamAbdulkhaleqNoaman[b]Dr.BelalAbuAta[c]Dr.AhmadM.Manasrah[d]

[a]Principal i/c, Research Director &Assistant professor of computer science, University of Diyala /Iraq
[b]Assistant Professor of computer science, University of Diyala / Iraq
[c]Associate Professor of computer science,Yarmouk University / Jordan
[d]AssociateProfessorofcomputerscience,Yarmouk University / Jordan

Abstract: Encryption is the science of concealing data, and because researchers seek to find the best way to hide data fromunauthorized persons to access it, and due to competition in this field, it became necessary to find methods that are difficult forattackers to break the cipher text and know its content, in this research paper a new method was proposed that we called it The "hour glass or sand clock method", which mainly depends on reducing the size of any message, regardless of its size, to becomeeight-bit size only, in addition to hiding all characters of the messagewith only one character using the principle of arithmeticpower function, and it is the first method that relies in its work on the principle of compressing a complete message to become
Onlyonecharacter.Whichposesarealchallengeinfrontofallmethodsofbreakingtheciphertextasitwilldealwithonlyonecharacter.By using differentcryptanalysismethods,the proposedmethod'sstrengthandeffectiveness have beenprovenincounteringall types ofattacks.
Keywords:sandclock,hourglass,power function,singlecharacter,compression

1. Introduction

Hourglassorsandclock

The hourglass is a clock that consists of two glass containers, an upper and lower connected, open in themiddle and placed in the upper part of sand, and when the sand reaches the hole between them, the passage of sandbecomesone atomafteranother untilitaccumulatesa second time inthelowerpartfigure(1).

Figure1:hourglassorsandclock

Theencryptionandcompressionintheproposedmethodbehaveasinthesandintheuppercontainer,andthedecryption processanddecompressionbehaveasthegroupingofthesand atomsinthelower container.

Powerfunction:Thepowerfunctioninmathematicscanbedefinedas$f(x)=a^x where a.x\in R$,therearetwo typesofpowerfunction whichisthe odd functionand even functionasshowninthefigures(2) &(3)

Figure2:evenfunctiontype

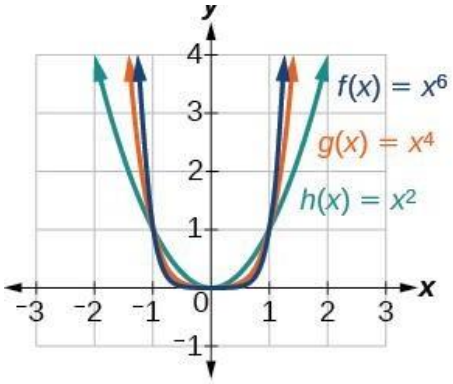
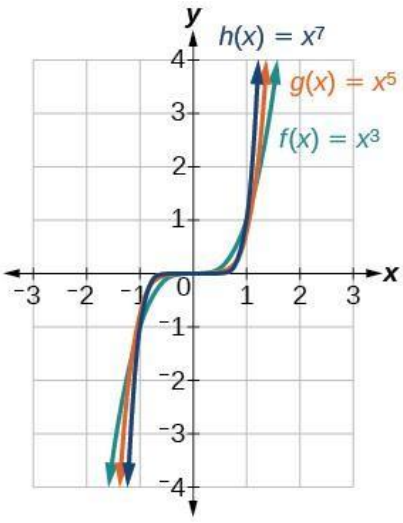


Figure3:oddfunctiontype



the power function behave mathematically according to the value of the power ,which means when thepower of the basis start from 0 to $n\in R$, the value of the power function will increase accordingly, the powerfunctionrepresenttheproductofthebasisbyitselftimesnumberaccordingtothepowerofthebasis$a^n=a\times a\times a\times ...ntimes$

alsothereisexponentialfunctionandpowerfunctionforthebasis10,asanothertypesofpowerfunction(**Zaka,A.,Akhter, A. S., &Jabeen, R. (2020)**)

Cryptography

Cryptographyisthesciencedealswiththecryptographicsystems.
Cryptanalysisisthetechniquesofbreakingthecryptographicsystems.
Cryptography is one of the fields of computer science & mathematics that focuses on all techniques that made a securecommunicationbetweentwopersons(**Alice &Bob**)
Thefourprinciplesofcryptographyare:

Confidentiality:Definesasetofthebasisthatlimitsaccessand/oraddsrestrictiononthecertaininformation.

DataIntegrity:dealswiththe consistencyand theaccuracyofthedataalongitslife-cycle.

Authentication : it confirms the truth of theattribute of a datum whichis cleared to be "True"through usingsomeentity.

Non-Repudiation : To ensures the inability of theauthor of thestatement resp. which is the piece of theinformation to bedenied. today there are two different schemes , which isthe symmetric schemes ,based on bothAlice and Bob need to obtain the same key to encrypt and decrypt their communication .So, they need to share the keyinitially.Onotherside,DiffieandHellman'swasinvitethekeyexchangeidea,sotheconceptofasymmetricschemes which isAlice & Bob have two keys, the private and public key. The public key can be shared with anyperson or any one , this public key can used byBob to encrypt the secret message and send it for Alice. In the otherhandonly Alicecan use the corresponding private key to decrypt the cipher text from Bob. (**Barakat, M., Eder, C.,&Hanke,T. (2018)**)

2.SignificanceOfTheStudy

Most of the secret messages can be breaking through the difference types of the cryptanalysis methods , andall of these messages has the same number of the characters , that make the guessoperation very simple by compereeach character with the equivalent character in the secret message , but in this new method all message characters willbe gathering into one character , this property make the knowing of the original message very difficult, so all thecryptanalysiswillfailto guess thecorrectnumber ofthecharacter and doesn'tdecipher themessage.

3.ReviewOfRelatedStudies

Kumari, M., & Tanti,J.(2020)proposeda Public Keyusingthe blockCryptography matriceswithgeneralized Fibonacci sequence. That show first themultiplicative commutatively of the generalized matrices thatconstructed through using the generalized Fibonacci sequences, then they developed an cryptographical scheme ,theyalsodiscussed theefficiency &thestrengthoftheproposedschemeinthecontextoftheblock matrices.

Abed, B. N., et.al (2020) proposed a new cryptosystem through using the 3ed order equation "cubic equation" and useCardano's method , the purpose is to add more secrecy and complexity to the proposed cryptographic algorithm,whilethere is four different keys and different formulas of the equation . **Noaman, S. A., et . al(2020)** , presents the methodof data encryption / decryption. The proposed method used the Taylor series through choosing the constant andTaylor formula as two secret keys. the first key substitutes the plain text in the Taylor. Where in Decoding phasecomputetheTaylorinversion.manyattacks, areused inorder to evaluate theresultsofthealgorithm.

Najim al-din, B., &Shaban, S. A. (2017) proposed the cryptosystem to encrypt Arabic text throughthe principle ofintegration to producebetter security as well asincreasing the complexity of predicting the secret keys and know thetrueplaintext.the resultsshowthat theproposed cryptosystemwasinevitabletocryptanalysisprocess.

Abed, B. N. A. D., &Noaman, S. A. (2019) presents a new method to develop the techniques of encryption , throughthe McLaurin series considering as a new cryptosystem ,by using different cryptanalysis techniques with differentdecoding tools , the proposed algorithm was inevitable against all these different attacks , in addition its proved as aone way function . **Al-din,B. N.,et.al. (2020)** proposes an algorithm known as wolf algorithm, through classifyingcharacters of the plain textinto manygroups and thenexchange the keys between all thesegroups in the wolfcommunication process to construct an authentication secret keys between the groups , many different cryptanalysistechniquesusedtoevaluatethe proposed newalgorithm.

4.ObjectivesOfTheStudy

- tofindanewmethodthatcanhidetheinformationofthesecret message
- tocompressthemessageintoonecharacter
- todecriesthe memoryusagethroughsendonecharacterinsteadofcompletemessage
- tomakethecryptosystemverycomplexanddifficult forbreaking

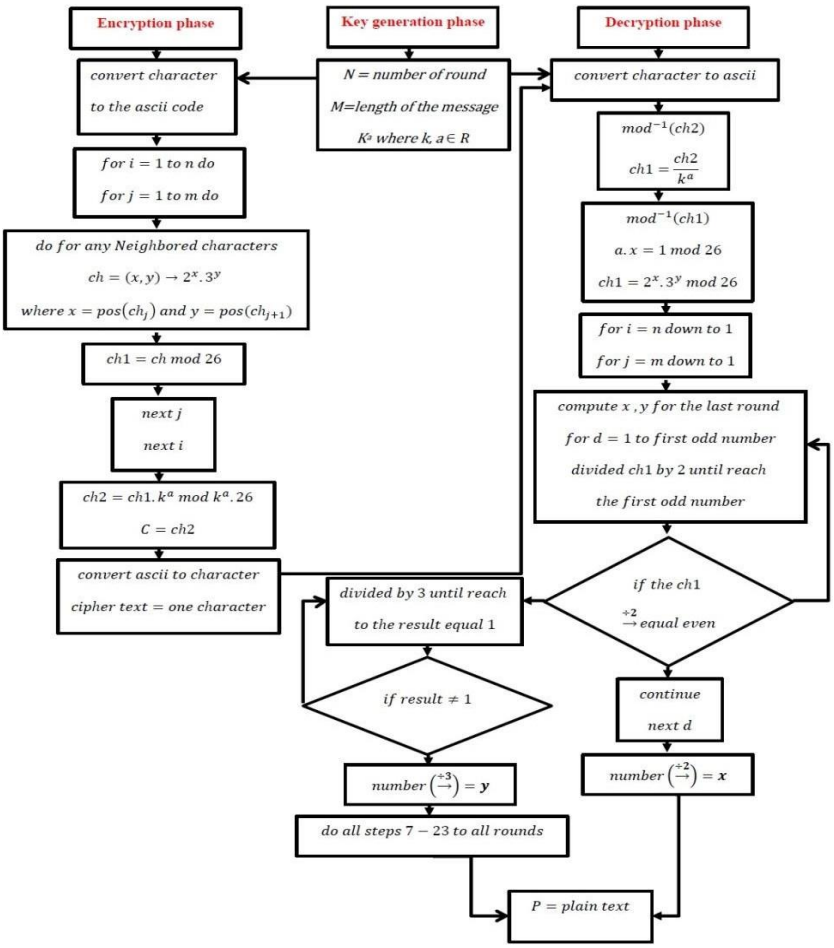
5.HypothesesOfTheStudy

- thereisnocryptosystemhidethemessageinverysecure wayforever
- thereisnocryptosystemhidethemessageinonecharacter
- thereisnocryptosystemcompressthe secret messageinorder todecriesthememoryusage

6.Methodology

In this section, three algorithms are presented that represent the three aspects of thecryptographic andcompression system, which are the key generation phase, the encryption phase, and the decryption phase. These threeaspects are illustrated in the flowchart of the proposed method.In addition to listing all these algorithms in detail . andmaking an implementation of the proposed method in order to list the complete details of the methodpractically andmathematically to add reliability totheproposed method.And as shown in the practical example in this section andthe results achieved theoretically and practically to reach the encrypted text,which is represented by only onecharacter, which is at the same time compressing the size of a message to a much smaller size, which represents onlyone byte, which will reduce the storage space consumed in addition to increasing security And the biography of thetransmitted data via the Internet.

Figure4:flowchartoftheproposedmethod



Keygeneration

$n$isthenumberofthestepsthatexecutethealgorithm
$m$isthelengthofthemessage
k^aisthethirdsecretkeywherk,$a \in R$

Encryption

convertcharactertotheasciicodefor
i=1tondo
forj = 1tomdo
doforanyNeighboredcharacters
$ch=(x,y)\rightarrow 2^x.3^y$where$x=pos(ch_j)andy=pos(ch_{j+1})$
$ch1=ch mod 26$
$next$j
$next$i
$ch2=ch1.k^a mod k^a.26$
$C=ch2$
convertasciitocharacter
ciphertext=onecharacter

Decryption

convertcharactertoascii
$mod^{-1}(ch2)$
$ch1=\frac{ch2}{k^a}$
$mod^{-1}(ch1)$
$a.x=1 mod 26$
$ch1=2^x.3^y mod 26$
fori=ndownto1
forj=mdownto1
computex,yforthelastroundford=
1to firstoddnumber
dividedch1by2untilreachthefirstoddnumberifthec
h1dividedby2equalevennumber
$continue$
$nextd$
$elsestop$
thenumberofthedividedby2isthexvalue
iftheresultofdividedby2equaloddnumberthenfor
l=1to theresultequal1
dividedby3untilreachtotheresultequal1ifther
esult notequal1$continue$
$elsestop$
thenumberofthedividedby3istheyvalue
$nextl$
$doallsteps 7-23 toallrounds$
$nextm$

$nextn$

$P=plaintext$

7.Implementation

Inthisalgorithmwewilladoptnewalphanumeric valuesthatdifferfromtheASCIIcode,asshowninthetable below

Figure5:thealphabettable

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
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

$Key\ generation$

$n=4 where n is the number of round for encryption$

$m=11 where m is the length of the message$

$k^a=2^2 where a=2\ ,k=2 the third secret key$

Encryption

$P=$"GOODMORNING" $//where P is the plaintext$

$P=$ 7 15 15 4 13 15 18 14 9 14 7// Ascii

$code in the first round$

$(7,15)\rightarrow 2^7.3^{15}=1836660096 mod 26=24$

$in the same method(15,4)=24,(13,15)=2,(18,14)=4,(9,14)=6, and 7$

$the result of the first\ round is: 24242467 in$

$the secound round$

$(24,24)=14,(2,4)=12,(6,7)=10$

$the result of the secound round is: 141210 in the t$

$hir round$

$(14,12)=4,10$

$the result in the third round is:$

$410 in the fourth and final round$

$(4,10)=22=V$

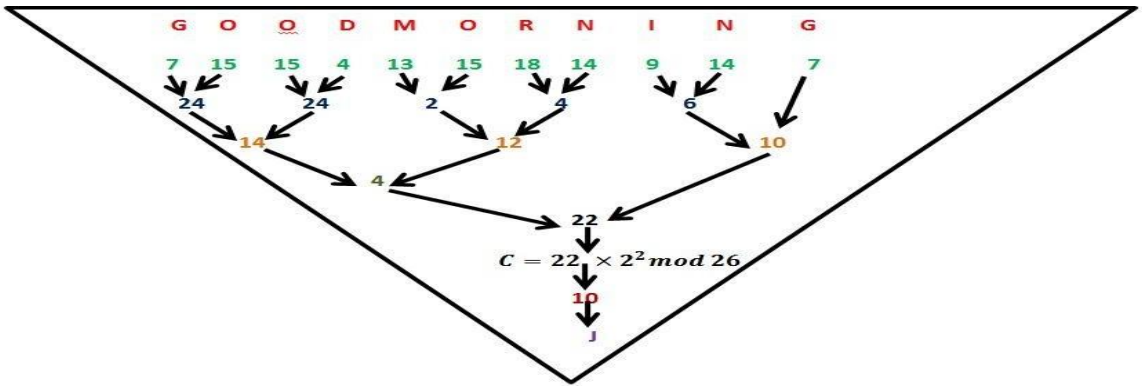
$C=2^2.22 mod 26=10$

$C(10)=J$

$ciphertext=J$

thefollowingchartrepresent"thehourglass"methodforencryptionandcompression

Figure6:encryptionprocesses



Decryption

$J=10$

$mod^{-1}(10)=22$

$mod^{-1}(22)=944784$

i$nthelastroundandcomputex,yvalues$

$944784 \xrightarrow{\div 2} 472392 \xrightarrow{\div 2} 236196 \xrightarrow{\div 2} 118098 \xrightarrow{\div 2} 59049$ $isoddstopthenxvalue$

$=4 \quad (numberofdividedby2 \xrightarrow{\div 2})$

$59049 \xrightarrow{\div 3} 19683 \xrightarrow{\div 3} 6561 \xrightarrow{\div 3} 2187 \xrightarrow{\div 3} 729 \xrightarrow{\div 3} 243 \xrightarrow{\div 3} 81 \xrightarrow{\div 3} 27 \xrightarrow{\div 3} 9 \xrightarrow{\div 3} 3 \xrightarrow{\div 3} 1 theresultisonestopthenyvalue$

$=10(numberdivideby3 \xrightarrow{\div 3})$

$theresultfromthereverse$ firstroundis:410

$theresultfromthereversesecoundroundis$:141210

$theresultfromthereversethirdroundis$:24242467

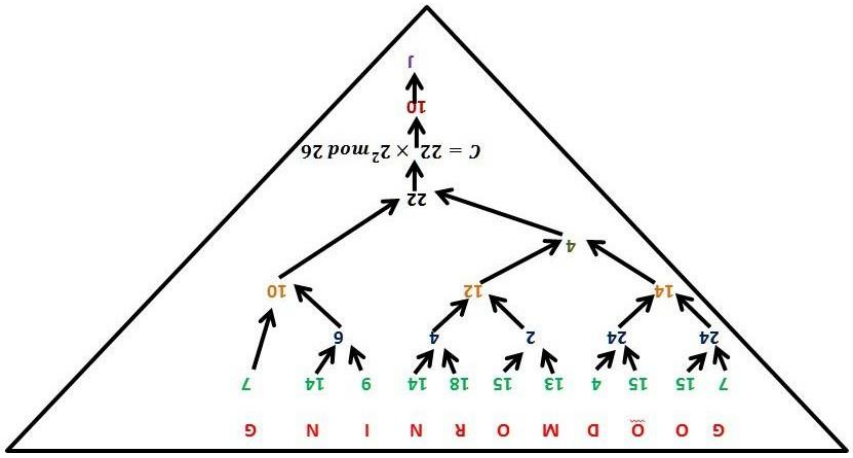
$theresultfromthereversefourthroundis$:715154131518149147

$throughconvertasc$iit$othecharacterwillbe:GOODMORNING$

$P=GOODMORNING$

Thechartbelowrepresentthedecryptionanddecompressionprocesses

Figure7:decryptionprocesses



8.Resultanddiscussion

In order to prove that the proposed method is efficient and effective, a set of crypt analysis methods havebeenadoptedthat willprovewhetheritisabletoguessandpredicttheexplicittextand thekeyusedintheencryptionprocess,whichare asfollows:

When applying frequency analysis to the encrypted text consisting of only one character, this method provedits inability to break the encrypted text as it showed that the cipher text is treated as only one character, which is "J" inthis example, so it is difficult for this method to know the real number of characters, and what are the contents of thismessageasinthe figures(8), (9)

Figure8:frequencyanalysis

Frequencies:

Single letters:

J	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
100%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%

Bigrams:

AA	AB	AC	AD	AE	AF	AG	AH	AI	AJ	AK	AL	AM	...
0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	...

Guesses (clear guesses):

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

Figure9:frequencycomparission

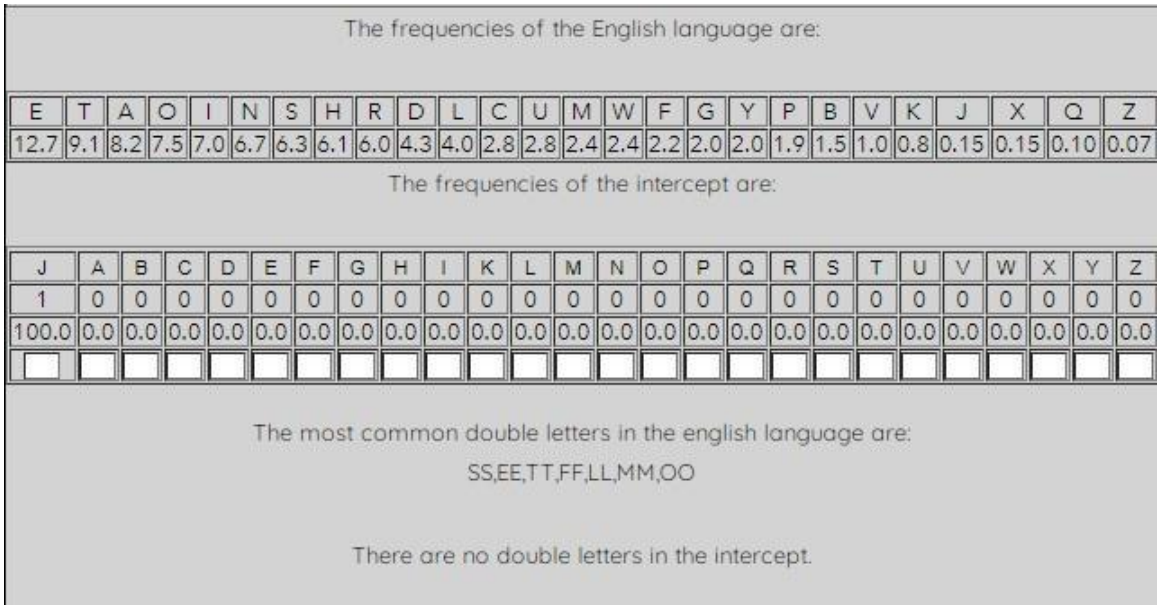
E	T	A	O	I	N	S	H	R	D	L	C	U	M	W	F	G	Y	P	B	V	K	J	X	Q	Z
12.7	9.1	8.2	7.5	7.0	6.7	6.3	6.1	6.0	4.3	4.0	2.8	2.8	2.4	2.4	2.2	2.0	2.0	1.9	1.5	1.0	0.8	0.15	0.15	0.10	0.07

The frequencies of the intercept are:

J	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
100.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0

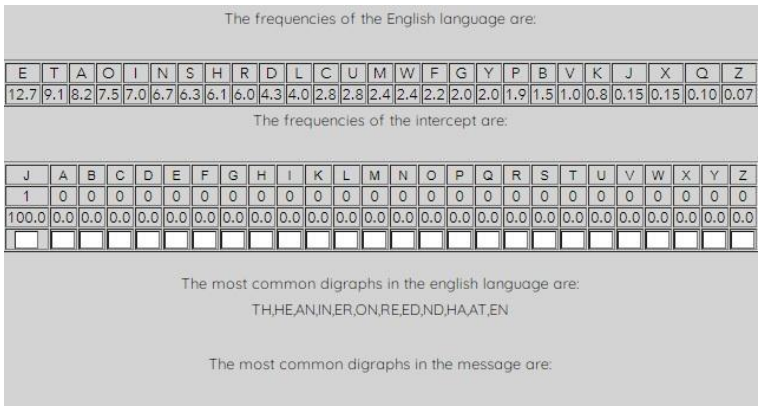
Inadditiontotheinabilitytodeterminethemostcommondoublelettersasisrecognizedintheenglishletters,astheresultsshowed thatitwas notpossibleto specifyanydoubleletter asshowninFigure(10)

Figure10:themostcommondoubleletters



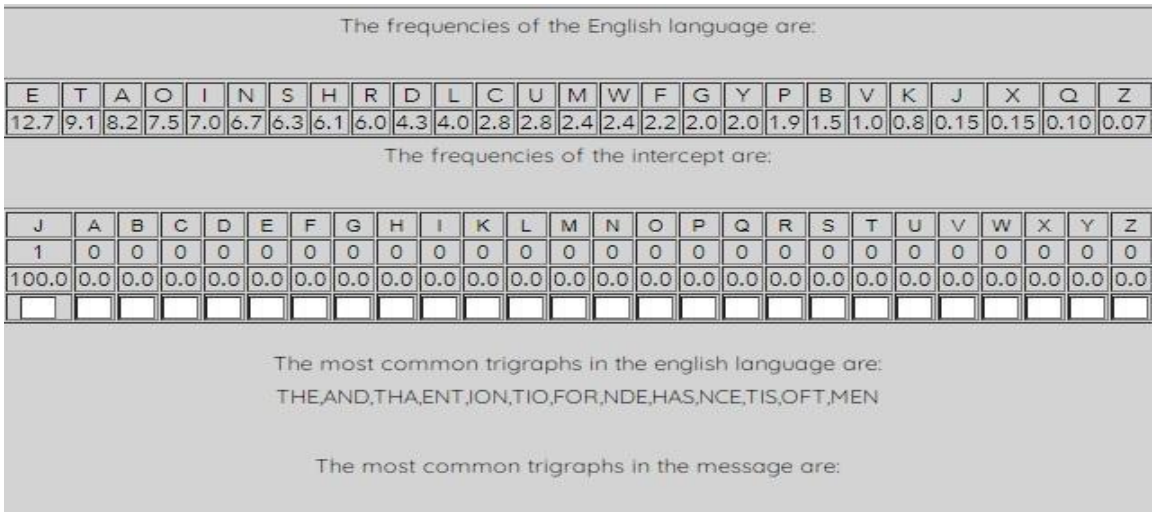
Likewise,theinabilitytodeterminethe mostcommondigraphscharactersasitis knowninEnglishlettersorwhat is known conventionally, as the results showed that it was not possible to specify any digraphs as shown inFigure(11)

Figure11:themostcommondigraphs



thesamethingforthethreeletters..asitprovedthatthemostcommonthreeletterscannotbeidentifiedasitis known in the English letters or what is known conventionally trigraphs , as the results showed that it was notpossibletospecifyanythree lettersasshowninFigure (12)

Figure12:themostcommontrigraphs



The frequencies of the English language are:

E	T	A	O	I	N	S	H	R	D	L	C	U	M	W	F	G	Y	P	B	V	K	J	X	Q	Z
12.7	9.1	8.2	7.5	7.0	6.7	6.3	6.1	6.0	4.3	4.0	2.8	2.8	2.4	2.4	2.2	2.0	2.0	1.9	1.5	1.0	0.8	0.15	0.15	0.10	0.07

The frequencies of the intercept are:

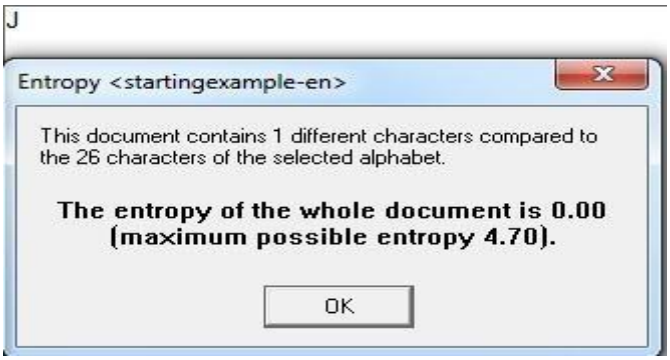
J	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
100.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0

The most common trigraphs in the english language are:
THE,AND,THA,ENT,ION,TIO,FOR,NDE,HAS,NCE,TIS,OFT,MEN

The most common trigraphs in the message are:

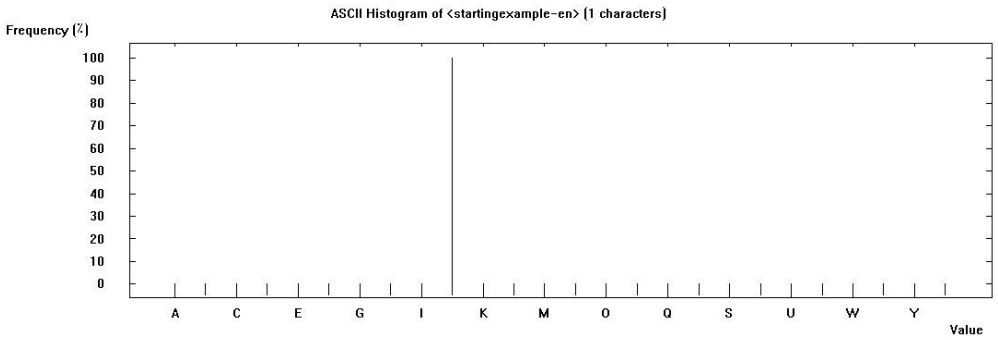
Also,theentropyoftheencryptedtextshowedtheprobabilityofappearingfortheletterwithavalueof0.0becausethem essagecontainsonlyonelettercomparedto 26letters, asinthe figure(13)

Figure13:theentropy



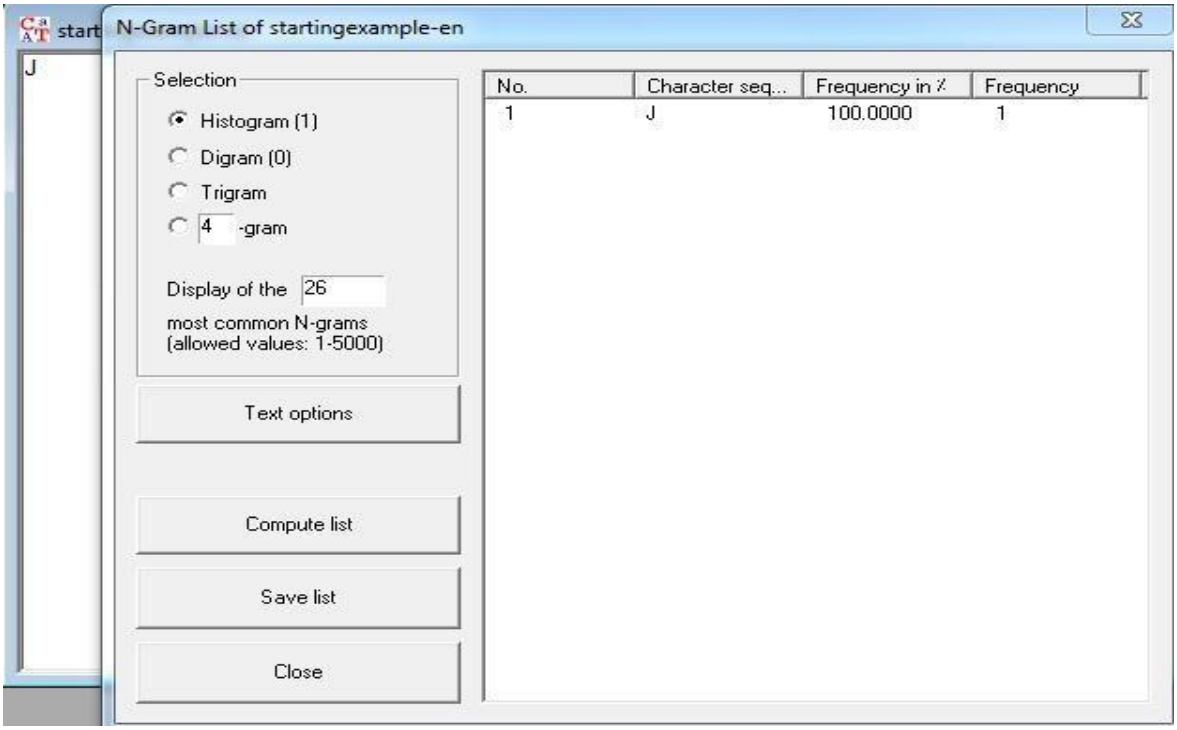
And the analysis of the histogram revealed the presence of the frequency ratio, which is also due to thepresenceofonlyoneletter intheletter,whichmakestheprocessofdeterminingtheproportionsoftheotherlettersdifficultandasshowninthe histograminFigure (14)

Figure14:thehistogram



Likewise, the N-Gram analysis showed that the frequency of the letter J is 100%, and this indicates that itdealswiththeencodedtextas onlyoneletter,andthisis notidenticaltorealityasthenumber oflettersinthistestis11 lettersand notoneletter,sothisanalysis failedAlso inknowingthe explicittextasinthefigure (15)

Figure15:N-Gram



From all of the above mentioned tests that were done on the encrypted text, all the methods dealt with theencryptedtextonthebasisofasinglecharacter,andthisprovesthatanyothermethod willdealinthesamewaywiththe encrypted text, which makes the process of analyzing and decrypting the cipher text very complicated or seemimpossible.For thismethod.

Thespacecomplexityofanyalgorithmisthetotalamountofcomputermemorythatrequired byanalgorithmin order to complete its execution. If the amount of the space that required by the algorithm increasing with theincrease of the input value, as a resultthe space complexity is “Linear Space Complexity”. And if the algorithm thatrequires a fixed amount of space,for all the input values , the space complexity is a “Constant Space Complexity”.(**Queiroz, S., Silva, W., Vilela, J. P., &Monteiro, E. (2020), Can, T., Krishnamurthy, K., & Schwab, D. J. (2020,August)**)

The time complexity of any algorithm is said to be the total amount of thetimethat required by thealgorithm in order to complete program execution. And if the program requires the fixed amount ofthe time for alltheinputvaluesisleadtosaythatthetimecomplexityis“ConstantTimeComplexity”.Whereiftheamountoftimethat required by any algorithm increasing with the increase of the input value, the time complexity is “ Linear TimeComplexity”. So the time complexity for the key generation algorithm is O(1) and space complexity is O(1) whichthebestandthetimecomplexityforencryptionanddecryptionalgorithms isO(n),and spacecomplexityisO(n).

Wealsocomparedtheproposedmethodwiththemethodsintheliteraturereviewintermsofreducingthesizeofthemes sage andintermsofthekeys, asinTable No. (1)

Table1:compressiontable

method	Number ofkeys	Reduce thesize	compressed	efficiency	Number ofCiphertext characters
Kumari,M.,&Tanti, J. (2020)	2	No	No	Yes	Equalplain
Abed,B.N.,et.al(2020)	3	No	No	Yes	Equalplain
Noaman,S. A., et. al (2020)	2	No	No	Yes	Equalplain
Najimal-din,B.,&Shaban,S.A. (2017).	2	No	No	Yes	Equalplain
Abed,B.N. A.D.,&Noaman, S. A.(2019)	3	No	No	Yes	Equalplain
Al-din,B.N.,Manasrah,A.M., &Noaman,S. A.(2020)	2	No	No	Yes	Equalplain
Propsedmethod	3	Yes	Yes	Yes	Onecharacter

9.Conclusion

In this research paper, a method called the hourglass methodwas proposed to build a highly efficientencryption system based on the principle of data compression, which is also an effective method of pressure thatachievestheleastpossiblespace,whichsaveslargestoragespaceandreducesthespacecomplexityverysignificantly, in addition to security and confidentiality. The high level of this system, which will preserve the dataagainst various types of attacks, thus providing a safe way to transfer data. The great contribution made by this methodin the field of data security science and its compression will open great horizons for researchers, and many methods ofcryptanalysis have been applied on The proposed system and the results proved the strength and effectiveness of thismethod and the inability of the cryptanalysis methods to break it, in the future work we can apply this method tocompressandsteganography's the imagesandvideosand otherresources.

References

Abed,B.N.A.D.,&Noaman,S.A.(2019,September).McLaurinseriesasanewtechniqueto improveencryptionprocess.InJournalofPhysics:ConferenceSeries(Vol.1294,No.4, p.042008).IOPPublishing.

Abed,B.N.,Kamil,B.Z.,Hameed,M.A.,&Abdullah,J.N.(2020,November).UsingCardano's methodforsolvingcubic equation in the cryptosystem to protect data security against Cyber attack. In 2020 2nd AnnualInternationalConferenceonInformationandSciences(AiCIS)(pp.127-131).IEEE.

Al-din,B.N.,Manasrah, A.M.,&Noaman,S.A.(2020).ANovelApproachbyUsingaNewAlgorithm:WolfAlgorithmasaNewTechnique in Cryptography.Webology, 17(2),817-826.

Barakat, M., Eder, C., &Hanke, T. (2018). An introduction to cryptography. TimoHanke at RWTH AachenUniversity, 1-145.

Can,T.,Krishnamurthy,K.,&Schwab,D.J.(2020,August).Gatingcreatesslowmodesandcontrolsphase-spacecomplexityinGRUsandLSTMs.In MathematicalandScientificMachineLearning(pp.476-511).PMLR.

Kumari, M., & Tanti, J. (2020). A model of public key cryptography using multinacci matrices. arXiv preprintarXiv:2003.08634.

Najim al-din, B., &Shaban, S. A. (2017). A NEW ALGORITHM FOR ENCRYPTING ARABIC TEXT USING THEMATHEMATICALEQUATION.DIYALAJOURNALOFENGINEERINGSCIENCES,10(1).

Noaman, S. A., Abed, B. N. A. D., & Abdul-Kader, S. A. A. (2020, July). A New Mathematical Model to ImproveEncryptionProcessUsingTaylorExpansion.In20201st.InformationTechnologyToEnhancee-learningand OtherApplication(IT-ELA(pp.35-40).IEEE.

Queiroz, S., Silva, W., Vilela, J. P., &Monteiro, E. (2020). Maximal spectral efficiency of OFDM with indexmodulationunderpolynomialspacecomplexity.IEEEWirelessCommunicationsLetters,9(5),679-682.

Zaka,A.,Akhter,A.S., &Jabeen,R.(2020).TheexponentiatedgeneralizedPowerfunctiondistribution:Theoryandreallife applications.Adv.Appl. Stat,61,33-63.