ISSN 2278-3091
Volume 9, No.3, May - June 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse72932020.pdf
https://doi.org/10.30534/ijatcse/2020/72932020

A Hybrid Caesar-Polybius Cipher with XOR Operation for Enhanced Cryptography

Jan Carlo T. Arroyo[1], Allemar Jhone P. Delima[2]
[1]College of Computing Education, University of Mindanao, Davao City, Davao del Sur, Philippines
[2]College of Engineering, Technology and Management, Cebu Technological University-Barili Campus, Cebu, Philippines
jancarlo_arroyo@umindanao.edu.ph[1], allemarjpdjca@yahoo.com[2]

ABSTRACT

Cryptography is a technique that deals with securing data and is closely affiliated with information theory, computer security, and engineering. However, with the presence of adversaries that uses powerful computers, the need to increase the complexity of cryptographic techniques arises. This paper employed and hybridized the two commonly used ciphers in the literature, namely the Polybius square and the Caesar cipher, to ensure more secure data. To increase the strength of the hybrid cipher, the ciphertext generated by the Polybius square is XORed. Simulation results revealed that the proposed method generates a unique ciphertext that shows no trace of any pattern from the plain text, thus, devoid of being attacked by frequency analysis or by brute force.

Key words: Caesar cipher, cryptography, data security, hybrid ciphers, polybius square

1. INTRODUCTION

Due to the tremendous growth in communication technology today, security becomes one of the top priorities wherein data security is still a challenge. For most organizations, crucial data are very important and must not be changed or used for illegal purposes. In defense, data security is prioritized. The unauthorized broadcast of data in the defense system is extremely disastrous and can cause damage. Likewise, data in banking systems must be adequately secured where authentic data under no circumstances, should go to perpetrators [1].

One way to secure data is by converting it into a non-readable form and revert it to its original format once the data reaches the appropriate receiver. The technique of concealing data so that only an authorized person can read the file is called cryptography. Cryptography is the technique and science of hiding information that uses mathematics to cipher[2]. A cipher is a pair of algorithms that transform plain text into an incomprehensible format called the encryption process with a reversing decryption process that transforms ciphertext back into its original plain text format [3].

Cryptography is divided into two types: symmetric and asymmetric key cryptography. In symmetric-key cryptography, the same key is shared between the sender and receiver that is instrumental for both encryption and decryption process. As opposed to symmetric cryptography, the concept of public and private keys handling is introduced in the asymmetric key cryptography, where every user is assigned a pair of keys. One key is used for encryption, and another key is used for decryption [4].

The graphical representation of the types of cryptography is shown in Figure 1, while the encryption and decryption process in ciphers is shown in Figure 2.

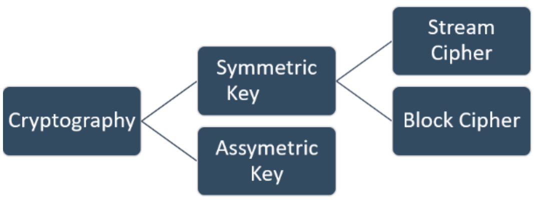

Figure 1: Types of cryptography

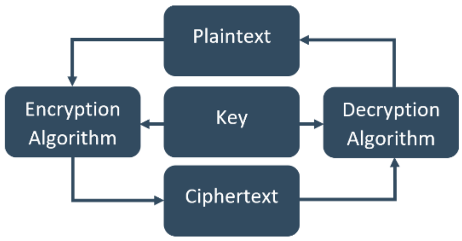

Figure 2: Encryption and decryption process

Ciphers such as Caesar cipher [5]–[7], Playfair cipher [8]–[10], ADFGVX cipher [11]–[13], Polybius square cipher [14]–[18], and Railfence cipher [19], [20] are some of the commonly used ciphers in the literature. Despite the number of known ciphers, security issues still persist, and different organizations use different cryptographic methods to protect their data online. However, perpetrators are keen on trying to break the cryptographic techniques by any means. With this, there is a continued quest to hybrid different cryptographic methods for better data security; hence, this study. In this paper, the extended version of the Polybius square [21] and the standard Caesar cipher is hybridized. The hybrid methodology addresses the drawbacks of the abovementioned ciphers since ciphertext generated using both ciphers show patterns and is prone to attacks [22]. To realize, the plaintext is ciphered using the Polybius square, where keys to be used will be generated using the Caesar Cipher. To ensure a more secure cryptosystem, the ciphertext from the Polybius square is XORed.

2. METHODOLOGY

2.1 Extended Polybius Square

The standard Polybius square with a 5x5 grid matrix is expanded into an 8x8 grid to include symbols and numbers. The expansion has paved the way for more efficient message encryption as data with characters, symbols, and numbers can now be encrypted. Further, the concept of adding keywords inside the grid was introduced to shift characters in the matrix. The keyword is placed on the top cells. Any remaining letters that are not used in the keyword are placed in the cells in alphabetical order. The special symbols are positioned according to their ASCII code equivalent, while the numbers are arranged in ascending order [21]. Given the keyword "JCTA0123", a sample Polybius square is shown in Table 1.

Table 1: Extended Polybius square

	1	2	3	4	5	6	7	8
1	J	C	T	A	0	1	2	3
2	B	D	E	F	G	H	I	K
3	L	M	N	O	P	Q	R	S
4	U	V	W	X	Y	Z	4	5
5	6	7	8	9		!	"	#
6	$	%	&	'	(	)	*	+
7	,	-	.	/	:	;	<	=
8	>	?	@	[	\	]	^	_

2.2 Caesar Cipher

One of the most widely known cipher algorithms is the Caesar cipher. This substitution type of cipher replaces every letter in the plaintext with a letter from a fixed number of positions down the alphabet. The encryption is represented using modular arithmetic, where thorough discussion is found at [23]. For the encryption, every character looks up each letter of the text message in the plaintext and writes down the corresponding letter in the ciphertext. Decryption is done by reversing the process, with a right shift of 3, as shown in Table 2 below.

Table 2: Caesar cipher table

Caesar Cipher	ZYXWVUTSRQPONMLKJIHGFEDCBA
Shifted Caesar Cipher	WVUTSRQPONMLKJIHGFEDCBAZYX

2.3 Proposed Cipher Process

The proposed process is anchored on the concept of [4] but differs on the cipher algorithms used. The Caesar cipher presented in this paper includes digits aside from the traditional Latin alphabets. For the Polybius cipher, the proposed method uses a 6x6 matrix to plot the alphabets "a" to "z" and digits "0" to "9," which are sorted in the grid depending on a given key.

To perform encryption using the proposed process, the following steps are executed as follows:

a. Identify two keys for encryption and decryption. The first key can be any digit, and the other key is a lettered word or group of words. For example, the first key is "24," and the second key is "SPEECH."
b. The first key is used to construct the Caesar cipher table by shifting the elements several times based on the key value. The result is shown in Table 3 after 24 shifts are made to the initial Caesar cipher table.

Table 3: Shifted Caesar cipher table

First key:	24
Caesar Cipher	ABCDEFGHIJKLMNOPQRSTUVWXYZ 0123456789
Shifted Caesar Cipher	YZ0123456789ABCDEFGHIJKLMNOPQ RSTUVWX

c. The Caesar cipher is performed on the second key to generate a new key that is used to construct the Polybius square. This is used to translate the plaintext using the Polybius cipher into bigrams. Using the shifted Caesar cipher table, the second key "SPEECH" is translated to "GD2205," as shown in Table 4. The newly generated key is used in the Polybius square, as shown in Table 5, which also shows that repeating characters,i.e., "2", in the new key, are disregarded. For instance, the plaintext "CRYPTOGRAPHY" is translated into the ciphertext "22 43 54 41 45 36 11 43 16 41 25 54," as shown in Table 6.

Table 4: New key generation

Second key:	SPEECH
Shifted Caesar Cipher	YZ0123456789ABCDEFGHIJKLMNOPQ RSTUVWX
New key:	GD2205

Table 5: Polybius square with the new key

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

Table 6: Plaintext conversion

Plaintext:	CRYPTOGRAPHY
Ciphertext:	224354414536114316412554

d. After converting the plaintext into bigrams based on the previous step, the first key is converted to its binary equivalent, and it will be XORed with the binary equivalent of the first bigram of the generated ciphertext. In this case, the first key "24" and its binary equivalent "11000" is XORed with the first bigram "22" and its binary equivalent "10110" resulting in "1110" as shown in Table 7.

Table 7: XOR operation on first key and first bigram

First key:	24
Binary equivalent:	11000
Polybius ciphertext:	224354414536114316412554
Binary of first bigram 22:	10110
⊕XOR of the first key and first bigram	1110

e. The corresponding output is XORed with the binary equivalent of the succeeding bigram of the ciphertext until it reaches the end of its length. Results after each XOR iteration is presented in Table 8. The table also shows the ASCII equivalent after the XOR operation as the final ciphertext value.

Table 8: XOR operation on succeeding characters

Polybius ciphertext:	22 43 54 41 45 36 11 43 16 41 25 54
Binary equivalent of the Polybius ciphertext after all XOR operations:	1110 100101 10011 111010 10111 110011 111000 10011 11 101010 110011 101
Decimal equivalent of the Polybius ciphertext after all XOR operations:	14 37 19 58 23 51 56 19 3 42 51 5
ASCII equivalent of the Polybius ciphertext after all XOR operations:	\x0e % \x13 : \x17 3 8 \x13 \x03 * 3 \x05 ---*or*--- %:38 *3

f. Converting the binary equivalents (after the XOR operations) to ASCII equivalents results in non-readable characters. The XOR results of the bigrams may produce equivalent decimal values that fall between 0 – 31 (which are not printable ASCII characters). To remedy, each group of bits is added by 100000 (Decimal: 32). This ensures that only printable characters, based on the ASCII table, are generated when translating into the final ciphertext. For instance, the Polybius ciphertext "2243 54 41 45 36 11 43 16 41 25 54" is converted to".E3Z7SX3#JS%," as shown in Table 9.

Table 9: XOR operation on succeeding characters

Polybius ciphertext:	22 43 54 41 45 36 11 43 16 41 25 54
Binary equivalent of the Polybius ciphertext after all XOR operations:	1110 100101 10011 111010 10111 110011 111000 10011 11 101010 110011 101
Decimal equivalent of the Polybius ciphertext after all XOR operations:	14 37 19 58 23 51 56 19 3 42 51 5
ASCII equivalent of the Polybius ciphertext after all XOR operations:	\x0e % \x13 : \x17 3 8 \x13 \x03 * 3 \x05 ---*or*--- %:38 *3
Binary equivalent of the Polybius ciphertext after all XOR operations and 100000 addition:	101110 1000101 110011 1011010 110111 1010011 1011000 110011 100011 1001010 1010011100101
Decimal equivalent of the Polybius ciphertext after all XOR operations and 100000 addition:	46 69 51 90 55 83 88 51 35 74 83 37
ASCII equivalent of the Polybius ciphertext after all XOR operations:	.E3Z7SX3#JS%

To decrypt ciphertext using the proposed method, the process is done in a reverse manner wherein the following steps are executed:

a. Provide the first key (number) and the second key (letter)
b. Convert the first ciphertext character to its equivalent binary code and deduct 100000 (Decimal: 32).
c. Perform XOR operation on the resulting binary equivalent from the previous step with the binary equivalent of the first key to retrieve the first bigram.
d. The binary equivalent of the resulting bigram is XORed with the binary equivalent of the succeeding character of the ciphertext deducted by 100000 (Decimal: 32). This process is done subsequently until it reaches the end of its length to retrieve all the bigrams.
e. Perform the Caesar cipher on the second key using the first key shift to generate a new key.
f. Construct a Polybius square using the newly generated key and match each of the bigram results from previous steps to retrieve the plaintext.

3. RESULTS AND DISCUSSION

In order to assess the viability of the proposed method, it is tested using a variety of plaintext and keys. The following test cases are shown in Tables 10-12.

Table 10: Test case 1

Sample Plaintext (Size: 2169 bytes)			
Ofcourseinonesensethefirstessentialforamanbeingagoodcitizenishisposs essionofthehomevirtuesofwhichwethinkwhenwecallamanbytheemphatic adjectiveofmanlyNomancanbeagoodcitizenwhoisnotagoodhusbandanda goodfatherwhoisnothonestinhisdealingswithothermenandwomenfaithful tohisfriendsandfearlessinthepresenceofhisfoeswhohasnotgotasoundheart asoundmindandasoundbodyexactlyasnoamountofattentiontocivilduties willsaveanationifthedomesticlifeisunderminedorthereislackoftherudemil itaryvirtueswhichalonecanassureacountryspositionintheworldInafreerep ublictheidealcitizenmustbeonewillingandabletotakearmsforthedefenseof theflagexactlyastheidealcitizenmustbethefatherofmanyhealthychildrenA racemustbestrongandvigorousitmustbearaceofgoodfightersandgoodbree derselseitswisdomwillcometonaughtanditsvirtuebeineffectiveandnoswe etnessanddelicacynoloveforandappreciationofbeautyinartorliteraturenoc apacityforbuildingupmaterialprosperitycanpossiblyatoneforthelackofthe greatvirilevirtuesButthisisasidefrommysubjectforwhatIwishtotalkofisthe attitudeoftheAmericancitizeninciviclifeItoughttobeaxiomaticinthiscount rythateverymanmustdevoteareasonableshareofhistimetodoinghisdutyint hePoliticallifeofthecommunityNomanhasarighttoshirkhispoliticalduties underwhateverpleaofpleasureorbusinessandwhilesuchshirkingmaybepar donedinthoseofsmallcleansitisentirelyunpardonableinthoseamongwhom itismostcommoninthepeoplewhosecircumstancesgivethemfreedominthe struggleforlifeInsofarasthecommunitygrowstothinkrightlyitwilllikewise growtoregardtheyoungmanofmeanswhoshirkshisdutytotheStateintimeof peaceasbeingonlyonedegreeworsethanthemanwhothusshirksitintimeofw arAgreatmanyofourmeninbusinessorofouryoungmenwhoarebentonenjo yinglifeastheyhaveaperfectrighttodoifonlytheydonotsacrificeotherthings toenjoymentratherplumethemselvesuponbeinggoodcitizensiftheyevenvo teyetvotingistheveryleastoftheirdutiesNothingworthgainingisevergained withouteffortYoucannomorehavefreedomwithoutstrivingandsufferingfo ritthanyoucanwinsuccessasabankeroralawyerwithoutlaborandeffortwith outselfdenialinyouthandthedisplayofareadyandalertintelligenceinmiddle ageThepeoplewhosaythattheyhavenottimetoattendtopoliticsaresimplysa yingthattheyareunfittoliveinafreecommunity			
First key:	18	Second key:	message
Ciphertext			
[CV?1]0'8\5QF+<X5"LVAYF*G)>S>)M#<7UM$HC +O_HW3*!8Q8.;$JUZM)6[A^3Y0]0'J'8Q5\D*0'=T7 SL N@W:SKF\CVLAV8"=Y85/8\QFSX:XS0;_O:TNYN-G]V8'29/OXM# <OX1)JA%G2V?\W3&-IYNE\5\J_@.1>)M@Z3,A%L")0Y0&<2_OD 6=YOD]4]KSX6,;WZ@)6[?V8"K/8U;$@ZE(>)"@_;"OB]3)@.4#O,;_ T0&+B!6RJA^0*2<^0YC\1)EZM)?RY=+3$/C!6[6)M#9.D(?RE!4#JR HW:"K\1<&OU^3W>PI NE(AO+='0;W92_68\J)6RDO+=6[2<XN^7!TC7<)G%P[6R;0S:4P>W OD*DS7YF/K%LYF5*H^P>!6[VI+I$/\K@$/A^7SLT: 7!H+<Q? 5WHPGX5;_I^2QN*=+B.@ZM!6)D&-8Y0(F\K')?(KT6)GL U&9U;5"OBXGRHC!H,;.%AJ'JD(?4!HF"L U8R;VI'8Q5*N :- I%GQN*!9UBU9.DJZ8'2\FQNXOD&3,B]RE!BL!O_H!ER_@"@_;") M[P@"5[2\W6!*F%HP9U;!6 7/8\1&OW9#4,NE\K?4!O-XS>PJ]BTCH*? NQ^I-N@-CSD*0'?4Z@W;RJ)"F3)>5W9#VCYF$2^I-&JATC .C-=*G)E,HQZ>([D]4X1?RM#@N#M]JA-&3$MUL%LZB]D^0'K&-I			

_F/FP@,;,:-A,;Y4#<R?2-@V?\QN,N[2QF(A%. 9#MF"4+E([D(FH_OXG#4,4#6XG4#(LZ>W:7 7Y=*G*!ESER0/:1$Q5\>W$3+B.%AW\6\0'2-&HW>Z3+;,')G2-IB.@) E'8VA-&HF*=Y0%.DOZE+^F/CS]B 6)MTZ0SX6!MRY;Q=T9SD(7Y,92V<U8UJZ8MF(A%2*C/A[L.%0Q 8 NTCZ6!*D7(D[9.]B.@NY4$*D*0/B]0;VI_HP<U6U MCS3$1_G.BOU^0/"=PJ$M#(J+BZE(F\K@.@_1?)>WO!;,'DS? 5>ZOP>!.9]B&3,_@U7(0'8V?1(2\2[K\W#<U6=SLYF"LVI$1XV2\0E +1:TC0'K>]V2Q_2\J].G)>5YNE(A%.>\K&<7[L%='8U;$GP>WA(7SJ PO"4:T!>Z4.9S:XG)6#(J(7/8QI'=*?V5VX<#M8\5V]9#(EN"=$>P>W: ?S2(7Z0Y;$JU@K)?1_@W:4PFQ=0*!OX+<P:XOD-5_=*!LB.9P<,"O P4#N#(LZWMR0'JDQK&<#O.1UL/$QAV<7[M$@WA^:TN'J]4,A") K)<^IB&KT:%H_;UJ&1S&(L&-AW>ZQA#4+O!;R?(#@)MTYC*IV 8'J)@-CV?\?V2-I'=*@W>T6!,6_2%0/CVX;V83WBU8!>MZ4.9ZB.9. 8Q2-I'=*G)EKRK)>&O#A^FQN*G.6=QZ7YCTA(K(&B]3F_3ZW:T= SIV2S? 9#M/ZE+&9[9[D%2? MZC/FK%L 7.%I_1+<I .JS0;_6.MZQ5XUO&KQN"C.4+FP^0E+B,6!L")GPO+EZ9.G_5")<+ M]JU1(A%G2[?(>)0\K\Q8T9.@ZQ5[AV5>ZWM$JP^3^D[7V;$JU1_ @#4]EHC/$=QFM#@K/Z3+BL CT0/K[U8'CT9T=Q8 IG+^79]D'0TYC*!MZJ]9W>ZM)I UJ.7UJREN#MW@5/$W@K!6ZBU@.B]D^0^7!HWO&B U;!6CU<X1_29,@_GXMZ3]GP<RHW3*G)@W3S:O,;_1]V8"5Y3Q_ <+E_H+FQ3@W:4^7SCTK/6/F/9,3]BMZ>SLT: 7BU&1U&O!6CT:I NQ5,3^0*=NY5@"5>S=TL"8/0\JD*5"O+B,6)MTY0\2(1:%A^:#<QF5 "NW\C'0&+4Z@)'I^F^7[5@)'29]9P3Z6!;0CTL 7 6_<1.@Z3=S>P<#PO+29]K&(0(?SL(1)@,3]3)"F3ZTAJ.#<X5;.;,A,'JA QZ>_H$M!*HCN;,@MR<&OA/MFV?SX<*=%=T8V[D*0YW9TC!9 /8\CH*5Q$MC-7<XN :-;$I#AJ?VNE)>5#V]9/$FQ=SL(FQ3QNW@$1&9]>!7!CT_FQ?%2X O&L.94.G*!T: +E+1&SIB1&B+E+4W@.GL"L[?)G.D-OP>!4YR>)D[8R0E(#VI-4Z @K%KQF38TCM)1.@.G%:I^A%.6ZMZO&E&(LS=H
Runtime: 0.10591490000000015 ms

Table 11: Test case 2

Sample Plaintext (Size: 1275 bytes)			
IhavemyselffullconfidencethatifalldotheirdutyifnothingisneglectedandifthebestarrangementsaremadeastheyarebeingmadeweshallproveourselvesonceagainabletodefendourIslandhometorideoutthestormofwarandtooutlivethemenaceoftyrannyifnecessaryforyearsifnecessaryaloneAtanyratethatiswhatwearegoingtotrytodoThatistheresolveofHisMajestysGovernmenteverymanofthemThatisthewillofParliamentandthenationTheBritishEmpireandtheFrenchRepubliclinkedtogetherintheircauseandintheirneedwilldefendtothedeaththeirnativesoilaidingeachotherlikegoodcomradestotheutmostoftheirstrengthEventhoughlargetractsofEuropeandmanyoldandfamousStateshavefallenormayfallintothegripoftheGestapoandalltheodiousapparatusofNaziruleweshallnotflagorfailWeshallgoontotheendweshallfightinFranceweshallfightontheseasandoceansweshallfightwithgrowingconfidenceandgrowingstrengthintheairweshalldefendourIslandwhateverthecostmaybeweshallfightonthebeachesweshallfightonthelandinggroundsweshallfightinthefieldsandinthestreetsweshallfightinthehillsweshallneversurrenderandevenifwhichIdonotforamomentbelievethisIslandoralargepartofitweresubjugatedandstarvingthenourEmpirebeyondtheseasarmedandguardedbytheBritishFleetwouldcarryonthestruggleuntilinGodsgoodtimetheNewWorldwithallitspowerandmightstepsforthtotherescueandtheliberationoftheold			
First key:	14	Second key:	encryption
Ciphertext			
M/7A^5MFY3S3F,FI$H(KQN"-2F$<H+KS9SI$P2-N='R&^=]1\(J)E$ GL ?^4+$POUM!;X8L.1(7<HP#PH$EZ1.B6=%VI": ?',X:%]E6)0/L A*2(7!>5WO%O!R?IV;N=6)C5*!L /0(IQ2^F_5*^3)6VI%?R'T7<VN"8Z7\C7Z)JPO"W#W5*!U8K M-;#PH$>J'J?K!B4+_="IV:"-2_?K3@X4X C#OP_@K@X+S3^-UJR!*I)EZUJAJR!YA+F*5-YA-U&>JU!C[/LGQ 3+_IVN="C.M!@4Y-^&R?%H<^F2QZ.LS ?4Y3EZ7W5V]6.JU^*RY8U#<O#HW;OP&9J2YA-@ T6)B6TL8[P$FYO,F,A!OW$N-5^A-YA-7C!>RJ>]0\(JUL?\(K@"=V8[(7/CY-OP0C\0?].1_*3Y:5_<P9&<H%D[/MR!B.Z8'D78 U^AY5/L T6)J9UJUOY:P: ?_@,6B/[9&<#;O-Y;$G4X@4W!>5X;QI*0S?^AYV4Y-OP#I*C\=P='(E.]E_@K?R&D[.Z1\W#N.Z8'D7<H;$H)]? VI%Q3^+J(BZ)HW#PHG38U5*_,A/0(D^5-A9T>$<PJ*2Y4AJA5-YF M/7A^>&L&9U8K 8@ 8R8[7C.Z8'F5V8U5A#<]BI=%K&>RHP:P$FY4.M			

U^F(F^-5A4?R2^F;X+^4+=")KS9S?R&F,4U8K+3P:,38ZB(B#N#O;V" @_@,6 ?4VN$N.M,N:Y5U&>R]BTK@":P:Z9X:N#O;YFMRJAY5/BMRJ&-;$ /MU?U5V7U!7T B#P=+H$EJ'K+HRM!.1)E_>M 6U9XS'TK'F2P3_+IVN-^HW\>&L&<#C\0*G2A")C[7-;YA5*\C0D&9 6[P$OW/6)? +IQ;Q1R3Q%H$P2-4+3<^AJ\CH*2X2R1P2F+G3QN$<PJ)E$E6[.BX SEZQ3+A+K(I+_<P$FY9ZE/5>&JP3_+IV])ZEZ.%3,'E]7]=^?])J&R0/ M.D.%3,'E]7]1.XG4?J9JU9#<OW;!>HW;X8.L/ B!;V:W#C.]E.C(7[/6)C ?IV"@#(K@*2^D)ZB(0C"=SK8L!A"V@_,38MT0E$<HWMU9#(\D7 A"N/[9&J'R!>U;X+4-2J'KQ%GXSLT_G4_@ZB.4U 8KQNTM5A#<%V5A")K+A^A5#N;QKD\/\$I%Q3,'S U4U? U9M.D'K*G]V7Z7-Y:QN:XG+4"4Y*@ZL/[9!K!B6=S>(7D\0*A"C!U ^*5[P0].Z8L!U7([DO@5*2^D0RM'D]B1)]>S?R2F$;V<&
Runtime:0.05620280000000033 ms

Table 12: Test case 3

Sample Plaintext (Size: 969 bytes)			
WhenIconsiderthemagnitudeofthesubjectwhichIamtobringbeforetheHousesubjectinwhichtheinterestsnotofthiscountrynorofEuropealonebutofthewholeworldandofposterityareinvolvedandwhenIthinkatthesametimeontheweaknessoftheadvocatewhohasundertakenthisgreatcausewhenthesereflectionspressuponmymindititisimpossibleformenottofeelbothterrifiedandconcernedatmyowninadequacytosuchataskButwhenIreflecthoweverontheencouragementwhichIhavehadthroughthewholecourseofalongandlaboriousexaminationofthisquestionandhowmuchcandourIhaveexperiencedandhowconvictionhasincreasedwithinmyownmindinproportionasIhaveadvancedinmylabourswhenIreflectespeciallythathoweveraverseanygentlemanmaynowbeyetweshallallbeofoneopinionintheendwhenIturnmyselftothesethoughtsItakecourageIdeterminetoforgetallmyotherfearsandImarchforwardwithafirmerstepinthefullassurancethatmycausewillbearmeoutandthatIshallbeabletojustifyupontheclearestprincipleseveryresolutioninmyhandtheavowedendofwhichisthetotalabolitionoftheslavetrade			
First key:	11	Second key:	cipher
Ciphertext			
X8!*K\6=3RJS?3SJ#6)"CO":#IS_?&(ES1(?3@ AV6WB+'M[7V]BTMW=QHD$=]7ZTMXV;-OVAM,'T4UB".NW6=1 (D]S_QZ0<VL@ AOX2_TX4AJ L&<%H$NAXM)CHQG*&LVZ:#P0Z>'T>R6.;0(BXW=3?&J+'RG+2 SX6\8VOWBIQ"B[P1=]<7TAMA!86#JS_>WN$/#CZ)0%FMTZT>$(HQD\2XOZVO<\6VCM +3*FJ_<%."B#-2^GR^I\1?&U5,'+KR\E)0*NW@L-GLBM!868UZ0;R' N/$<]Q0>_69S]S2$@YC)E,5>TXT>$=$@V<0P\E)E$>_F^K@XO%. 9 LG^FS_6C)ZQ0;.6/D)<+^R86[L,95 .M[6:I)0;Z6/5QH_S3Y*3]D(BIE%<%.9S>RGXA(1:6E%DS3R2'IP0% =1Q=W:%EI)0C#I-4#I$HF_5/:^4? 5>&BWA+G&L!/6BW>_TAM,FM'=1Q0>U8!/#B(#6=%E/\5XO/8-&> T9U4TA/6/[TM!@YRE\DQZB"H;,FM#BUY8RY9,"CH_3*?1(0C".N/ $M8R!*C")1P[T8R]7[W6\WBL-MX6/:"LYRE\D%.G2VCU?R>0C#:1 P<%?[BUY@NAXO.;_;NB"7;[1B[5,@U;"N@YLG2-4?3WN'29PE0;Q "4-XAM>')I\8\I-I_F,6\WN$+JA JA +'G^GLT'G^U48U92[. 9]GK!-MTZCO/E(7W[U48-NW@*G+>!8YAXTM!H)";7]G-A^GK^:^ 7B($D]1+2'KEP[C"K^2%E_5Y*?SK8YU5 :[7^G+%)0?^UY9 :W3WBLB/CV]JS_?*&O:-8U[B1P4PF_J&OV<Q]HC[W7".OA!4P4";. 8\EI#A,".OU MB(#/OVA%<)E\R^Q=\W@!.JS]D*3_*F_Q;_2>_5>_T=H(=6."B[N J9 8!*2XB1Q0'G&($D]Q;7"FSE/K*&G-&LVZ:#-I\2+'K^F_			
Runtime: 0.03848779999999863 ms			

Findings show how completely varied, and unintelligible the generated ciphertext from the sample plaintext in the Tables 10-12 are. It also shows that the runtime varies according to the plaintext size; the longer the plaintext, the longer is the encryption process. Further, there are no apparent patterns to determine the cipher used in the encryption. To support this, a frequency analysis was performed to test the efficacy of the proposed method. Discussed in[24]are the most frequent letters in the Latin alphabet shown in Figure 3. Cryptanalysts use this knowledge to count the use of letters and guess the ciphertext [22].

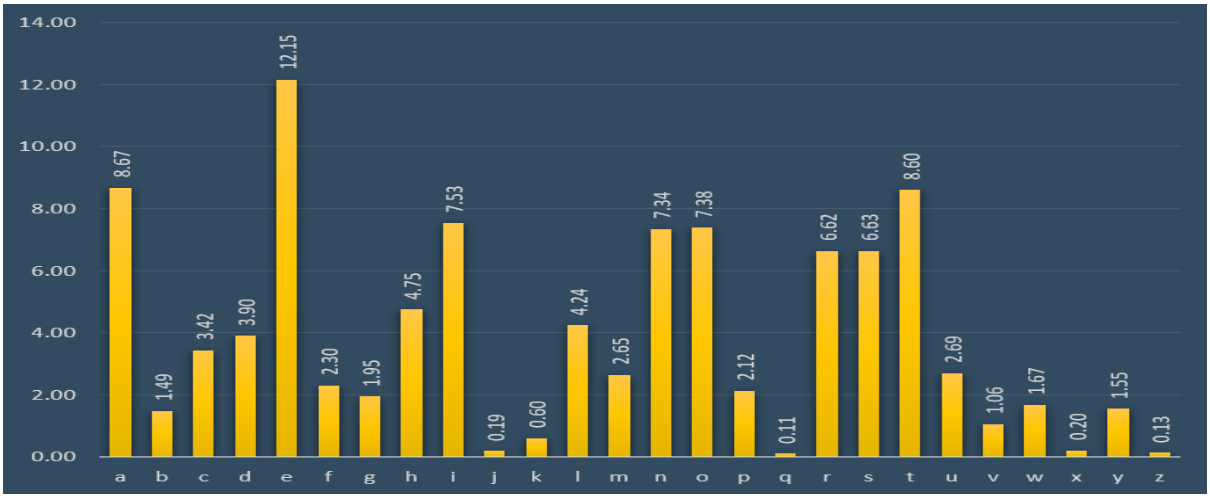

Figure 3: Latin alphabet frequency

The results of the frequency analysis on the test cases using the proposed hybrid method are shown in Figures 4-6. Simulation results revealed that there is minimal difference in the frequency distribution of characters. Further, no obvious patterns are depicted as opposed to the study of [24] since the use of characters in the ciphertext is generally distributed equally. Thus, making the proposed method more secure and difficult to break compared to traditional substitution ciphers.

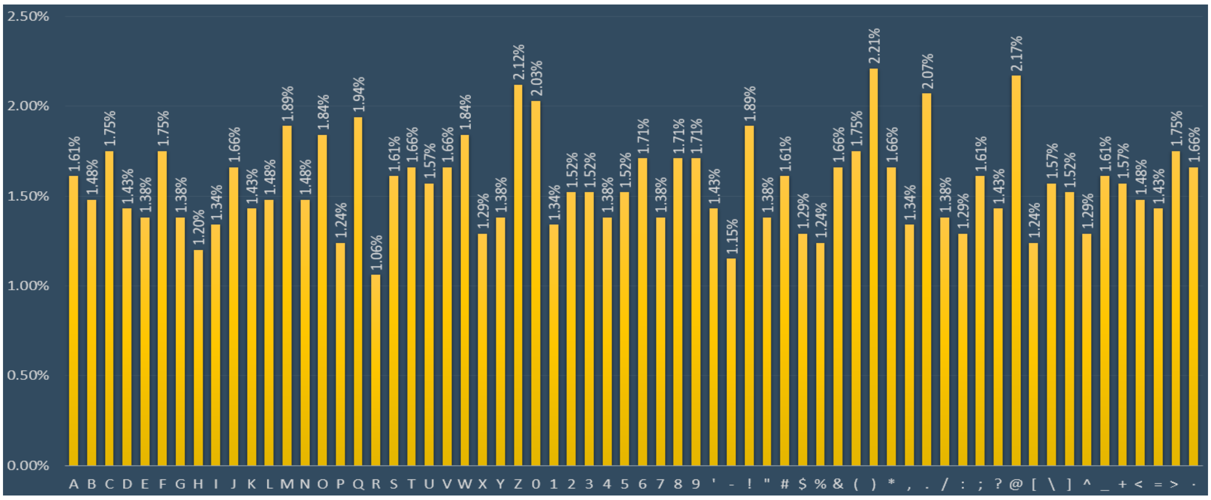

Figure 4: Test case 1 frequency count

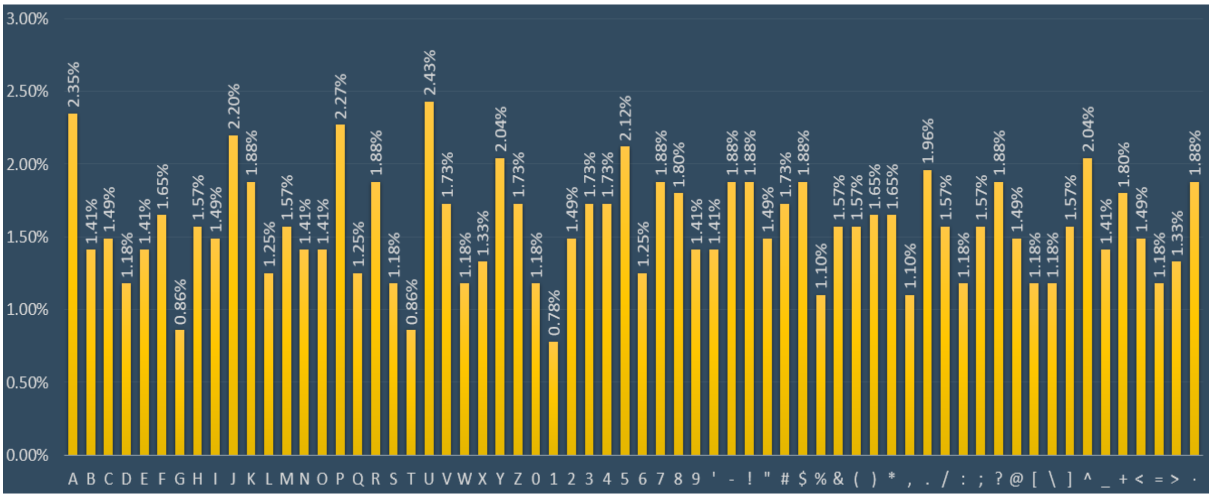

Figure 5: Test case 2 frequency count

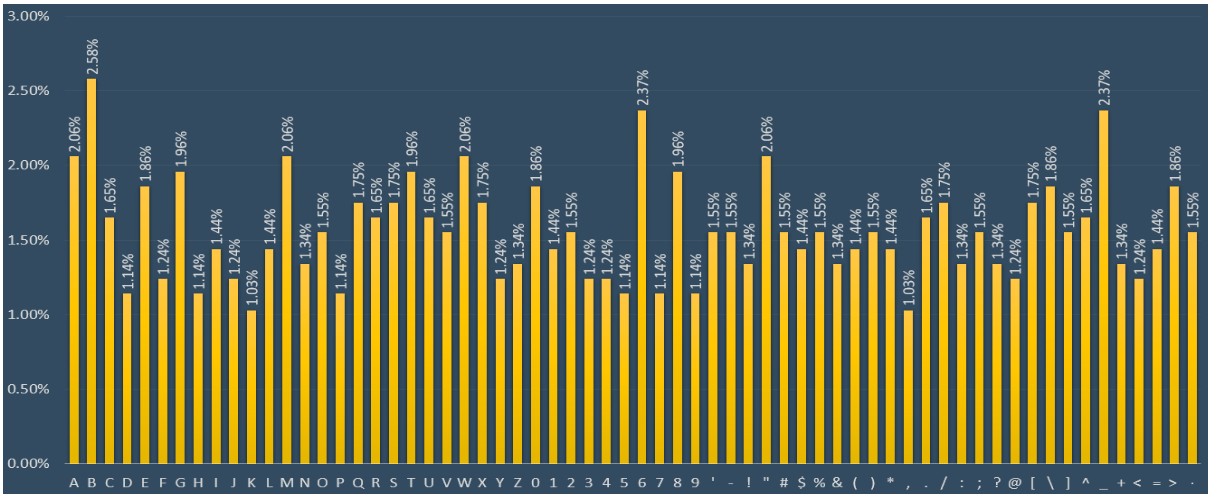

Figure 6: Test case 3 frequency count

4. CONCLUSION

In this paper, the two different ciphers, namely the Polybius and Caesar ciphers, are combined to ensure an unbreakable encryption process from standard cryptographic attack. With the inception of the XOR process, the weakness of both Polybius and Caesar ciphers has been addressed. The frequency analysis shows that the proposed method is resilient to attack when applied to some known plaintext as characters from the ciphertext show no repetition of pattern with minimal difference in its occurrence.

REFERENCES

[1] S. Dey, J. Nath, and A. Nath, "An Integrated Symmetric Key Cryptographic Method – Amalgamation of TTJSA Algorithm, Advanced Caesar Cipher Algorithm, Bit Rotation and Reversal method: SJA Algorithm," *Int. J. Mod. Educ. Comput. Sci.*, vol. 4, no. 5, pp. 1–9, 2012. https://doi.org/10.5815/ijmecs.2012.05.01

[2] W. Stallings, *Cryptography and Network Security Principles and Practices*. Prentice Hall, 2015.

[3] M. S. Hossain Biswas *et al.*, "A systematic study on classical cryptographic cypher in order to design a smallest cipher," *Int. J. Sci. Res. Publ.*, vol. 9, no. 12, pp. 507–11, 2019. https://doi.org/10.29322/IJSRP.9.12.2019.p9662

[4] O. E. Omolara, A. I. Oludare, and S. E. Abdulahi, "Developing a Modified Hybrid Caesar Cipher and Vigenere Cipher for Secure Data Communication," *Comput. Eng. Intell. Syst.*, vol. 5, no. 5, pp. 34–64, 2014.

[5] A. Singh and S. Sharma, "Enhancing Data Security in Cloud Using Split Algorithm, Caesar Cipher, and Vigenere Cipher, Homomorphism Encryption Scheme," in *Emerging Trends in Expert Applications and Security*, 2019, vol. 841, pp. 157–166.

[6] I. Gunawan, Sumarno, H. S. Tambunan, E. Irawan, H. Qurniawan, and D. Hartama, "Combination of Caesar Cipher Algorithm and Rivest Shamir Adleman Algorithm for Securing Document Files and Text Messages," *J. Phys. Conf. Ser.*, vol. 1255, 2019.

[7] D. Gautam, C. Agrawal, P. Sharma, M. Mehta, and P. Saini, "An Enhanced Cipher Technique Using Vigenere and Modified Caesar Cipher," in *2nd International Conference on Trends in Electronics and Informatics, ICOEI 2018*, 2018. https://doi.org/10.1109/ICOEI.2018.8553910

[8] R. Deepthi, "A Survey Paper on Playfair Cipher and its Variants," *Int. Res. J. Eng. Technol.*, vol. 4, no. 4, pp. 2607–2610, 2017.

[9] M. Syahrizal, M. Murdani, S. D. Nasution, M. Mesran, R. Rahim, and A. P. U. Siahaan, "Modified Playfair Cipher Using Random Key Linear Congruent Method," in *International Seminar: Research, Technology and Culture*, 2017.

[10] R. Rahim and A. Ikhwan, "Cryptography Technique with Modular Multiplication Block Cipher and Playfair Cipher," *Int. J. Sci. Res. Sci. Technol.*, vol. 2, no. 6, pp. 71–78, 2016.

[11] I. B. Venkateswarlu and J. Kakarla, "Password security by encryption using an extended ADFGVX cipher," *Int. J. Inf. Comput. Secur.*, vol. 11, no. 4–5, pp. 510–523, 2019. https://doi.org/10.1504/IJICS.2019.101938

[12] R. Mahendran and K. Mani, "Generation of Key Matrix for Hill Cipher Encryption Using Classical Cipher," *2nd World Congr. Comput. Commun. Technol. WCCCT 2017*, pp. 51–54, 2017. https://doi.org/10.1109/WCCCT.2016.22

[13] G. Lasry, I. Niebel, N. Kopal, and A. Wacker, "Deciphering ADFGVX messages from the Eastern Front of World War I," *Cryptologia*, vol. 41, no. 2, pp. 101–136, 2017.

[14] H. B. Macit, A. Koyun, and M. E. Yüksel, "Embedding Data Crypted With Extended Shifting Polybius Square Supporting Turkish Character Set," *BEU J. Sci.*, vol. 8, no. 1, pp. 234–242, 2019. https://doi.org/10.17798/bitlisfen.455126

[15] E. V. Haryannto, M. Zulfadly, Daifiria, M. B. Akbar, and I. Lazuly, "Implementation of Nihilist Cipher Algorithm in Securing Text Data With Implementation of Nihilist Cipher Algorithm in Securing Text Data With Md5 Verification," *J. Phys. Conf. Ser.*, vol. 1361, no. 012020, 2019.

[16] G. Manikandan, P. Rajendiran, R. Balakrishnan, and S. Thangaselvan, "A Modified Polybius Square

Based Approach for Enhancing Data Security," *Int. J. Pure Appl. Math.*, vol. 119, no. 12, pp. 13317–13324, 2018.

[17] M. Maity, "A Modified Version of Polybius Cipher Using Magic Square and Western Music Notes," *Int. J. Technol. Res. Eng.*, vol. 1, no. 10, pp. 1117–1119, 2014.

[18] C. Kumar, S. Dutta, and S. Chakraborty, "A Hybrid Polybius-Playfair Music Cipher A Hybrid Polybius-Playfair Music Cipher," *Int. J. Multimed. Ubiquitous Eng.*, vol. 10, no. 8, pp. 187–198, 2015.

[19] A. Banerjee, M. Hasan, and H. Kafle, "Secure Cryptosystem Using Randomized Rail Fence Cipher for Mobile Devices," in *Intelligent Computing - Proceedings of the Computing Conference*, 2019, pp. 737–750. https://doi.org/10.1007/978-3-030-22868-2_52

[20] A. P. U. Siahaan, "Rail Fence Cryptography in Securing Information," *Int. J. Sci. Eng. Res.*, vol. 7, no. 7, pp. 535–538, 2016.

[21] T. S. Kondo and L. J. Mselle, "An Extended Version of the Polybius Cipher," *Int. J. Comput. Appl.*, vol. 79, no. 13, pp. 30–33, 2013. https://doi.org/10.5120/13803-1836

[22] J. F. Dooley, *History of Cryptography and Cryptanalysis*. 2018.

[23] S. G. Srikantaswamy and H. D. Phaneendra, "Improved Caesar Cipher with Random Number Generation Technique and Multistage Encryption," *Int. J. Cryptogr. Inf. Secur.*, vol. 2, no. 4, pp. 39–49, 2012. https://doi.org/10.5121/ijcis.2012.2405

[24] G. Grigas and A. Juškevičienė, "Letter Frequency Analysis of Languages Using Latin Alphabet," *Int. Linguist. Res.*, vol. 1, no. 1, pp. 18–31, 2018. https://doi.org/10.30560/ilr.v1n1p18