ENHANCEMENT COMPLEXITY OF CAESAR CIPHER ALGORITHM USING MATHEMATICAL COMPUTATION

[1]Author: Syawash "Mirzad"
[2]Co Author: Syed Tariq Shah "Waqif"
[3]Assistant Professor: Mr. Ihsanulhaq
[1]Mscs Faculty of Computer Science Bakhtar University, Kabul Afghanistan
[2]Mscs Faculty of Computer Science Bakhtar University, Kabul Afganistan
[3]Faculty of Computer Science Bakhtar University, Kabul Afghanistan.

Abstract: Cryptographic algorithms play an important role in the security domain. In this system, in order to increase the security and complexity of the Caesar cipher, some mathematical calculations and computation are performed on the cipher text in order to make it strong. The proposed of this new system is case sensitive. The encryption and decryption of the plain text is done by making use of the character values and positional values of the corresponding characters and letters as the key. The multistage encryption and computation is imposed on the plain text which indeed improves the security of the plain text and secures it from brute force attack, pattern matching and frequency analysis to an extent. Further discuss the need of the additional methodology to the existing scenario.

***Key words* - Cryptography, Caesar Cipher, Brute Force Attack, Pattern Matching, Frequency Analysis, Encryption and Decryption, Key.**

I. INTRODUCTION

in today's information age, it is impossible to imagine without internet. This modern era is dominated by paperless offices mail messages cash-transactions and virtual departmental stores. Due to this there is a great need of interchanging of data through internet. Now a day when internet provides essential communication between tens of millions of people and is being increasingly used as a tool for commerce, security becomes a tremendously important issue to deal with. One essential aspect for secure communication is that of cryptography.

Cryptography is mainly used in transmitting the text which is sometimes called as the plaintext or the clear text from one end to the other. It includes techniques such as merging the words with some images to securely transmit the text. But in today's computer centric world, cryptography is mainly dealing with the scrambling of the plaintext into a form which is not meaningful and does not reveal any information that is being transmitted called cipher text and then later converting it back to the plaintext. The process of converting plaintext to cipher text is called encryption and then converting the cipher text back to the plaintext is known as decryption. Cryptography not only protects data from theft or alteration, but can also be used for user authentication [2].

II. PROBLEM STATEMENT

In cryptography, many algorithms are available to protecting our online important information which we are transferring from one person or end user to another. One of these algorithms is Caesar cipher that it is verybasic algorithm. Caesar cipher is not case sensitive and hence for one particular shift for a plaintext the corresponding cipher text is always the same [3].(Refer fig. 1)

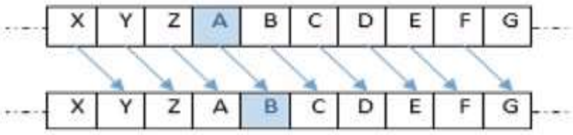


Fig. 1: Basic Caesar cipher with shift +1

The frequency analysis and pattern matching is done by observing the frequency of each occurrence of the letters in the cipher text. If the repetitions of the characters happen, it will be easy for the intruder to guess the plain text and crack it.

And also the Brute force attack requires attempts for each possible keys until crack the massage.Three important characteristics of this problem enabled us to use a brute-force cryptanalysis[10]:

1- The encryption and decryption algorithms are known.
2- The algorithm is used for simple text.
3- There are only 25 keys to try.
4- The language of the plaintext is known and easily recognizable.

III. PROPOSED WORKED

To completely removed repetitions of characters and strong possibilities of more than 161 deferent language letters, numbers, and special characters. Strong security against frequency analysis and brute force attack to find one letter or character need to attempt every possible key on more than 161 peace of cipher text to crack. In order to achieve this, the proposed worked is capable of handling case sensitive plaintext. Frequency Analysis Attack reduced in proposed work and no need for key distribution.

IV. DESIGNED OF PROPOSED SYSTEM

The main focus of this system is to increase the security of the basic Caesar cipher in terms of pattern matching, frequency analysis and brute force attack[6]. In order to achieve this, the proposed system is capable of handling case sensitive plaintext. Since the classical Caesar cipher is not case sensitive and hence for one particular shift for a plaintext the corresponding cipher text is always the same. Whereas in this system, if one toggles with the upper or the lower case letters in one plaintext, the corresponding cipher text will be different hence covering a wide range of plaintext cases. In the encryption side, we have used 3 stages of encryption.

The first stage of encryption is based on the basic Caesar cipher algorithm with shift + 1 as the substitution [8]. We are using character values and position values in our further computation where character values are the values assigned to a particular character say, A-1, B-2, Z-93, a-12, b-13….z-79…*-32, %-10, &-11, $-9, ….etc. Fig 4.

These Character values are fixed for the corresponding character or letter. The position values are assigned based on the position of the corresponding letter or character in the plain text [6]. In the second stage, we assign character and position values to each individual letters of the stage 1 encrypted text. The sum of the obtained character values is also been calculated. The stage 2 encrypted text is obtained by subtracting the character values from the sum which was calculated earlier. The third stage encryption is done by multiplication the positional values from the stage 2 encrypted text to obtain the final cipher text which is sent to the receiver along with the sum of the face values as the key.

The decryption also includes 3 stages. In the first stage, the position values are divided to the obtained cipher text. In the second stage the above obtained stage 1 decrypted text is subtracted from the key as received from the sender. The result will be the character values of the corresponding letters or characters which is the stage 2 decryption. These character values are converted back to its corresponding fixed character. The third stage decryption uses the basic Caesar cipher algorithm with shift -1 as a substitution technique. Hence the plain text is obtained. (Refer fig. 2)

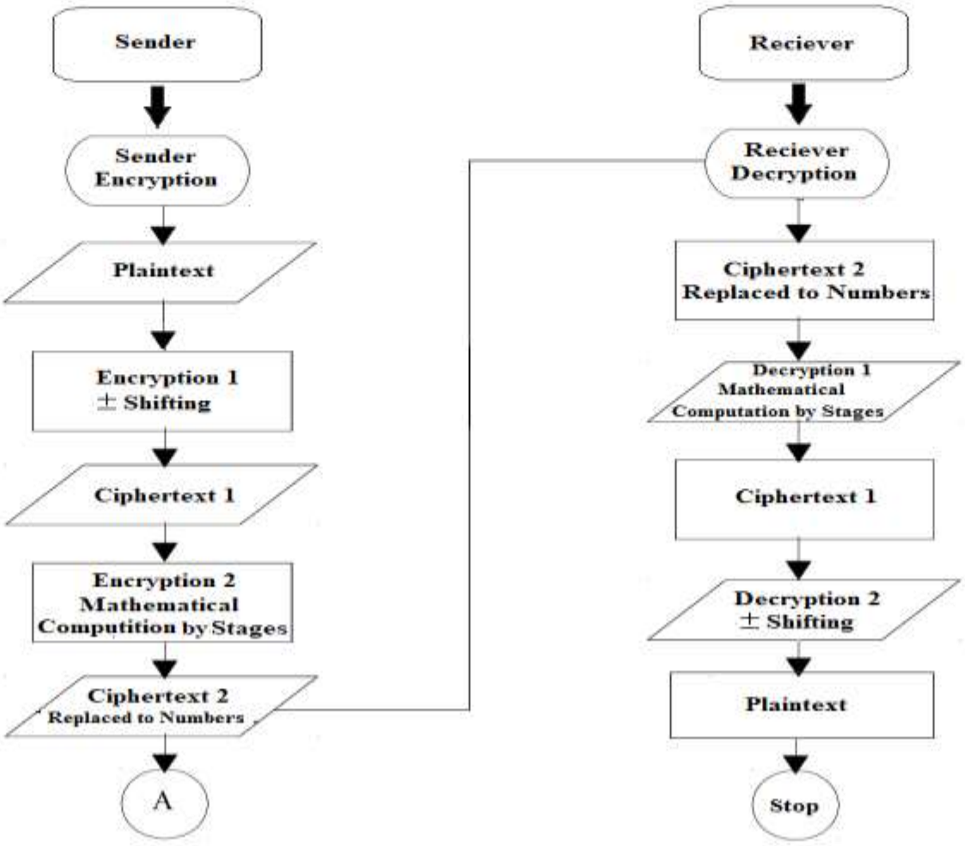

Sender
Sender Encryption
Plaintext
Encryption 1 ± Shifting
Ciphertext 1
Encryption 2 Mathematical Computition by Stages
Ciphertext 2 Replaced to Numbers
A
Reciever
Reciever Decryption
Ciphertext 2 Replaced to Numbers
Decryption 1 Mathematical Computation by Stages
Ciphertext 1
Decryption 2 ± Shifting
Plaintext
Stop

Fig. 2: Enhancement Complexity of CCA Using Mathematical Computation Flow Chart.

1.RESEARCH DESIGN

A. The Encryption Algorithm:

1. Transform the plain text using basic Caesar cipher algorithm.
2. Use the cipher text obtained from step (1) and do the following:
   - Assign character values and position values to each individual letters or characters in the cipher text.
   - Sum up the individual character values of all the letters and characters in the cipher text.
   - Subtract the individual face value of each letter of the cipher text from the above obtained sum.
   - Now, multiply the position values of each of the corresponding letters and characters of the cipher text obtained in step (2c).
3. The obtained cipher text is sent to the receiver along with the sum of face values as a key.

B. The Decryption Algorithm:-

1. Do the following on the received cipher text:
   - Divide the position values of each corresponding letter and character from the cipher text as received from the sender.
   - Subtract each corresponding values obtained from step (1a) from the sum received as a key along with the cipher text to get the character value.
   - Transform the obtained character values to its corresponding alphabets and character.
2. Apply the basic Caesar cipher decryption to obtain the plain text.

2. Implementation: The steps involved in the implementation of the proposed system is as follows –

A. Encryption –

The plain text chosen for the encryption is (**@gmail.com**) Initial step is to make use of the basic Caesar cipher to convert the given plaintext into its corresponding stage 1 cipher text havingdisplacement +1. (Refer fig. 3)

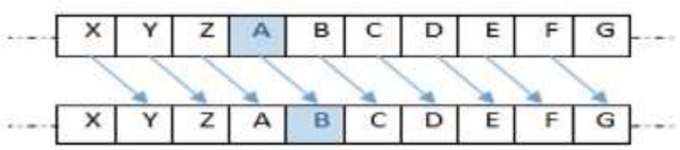
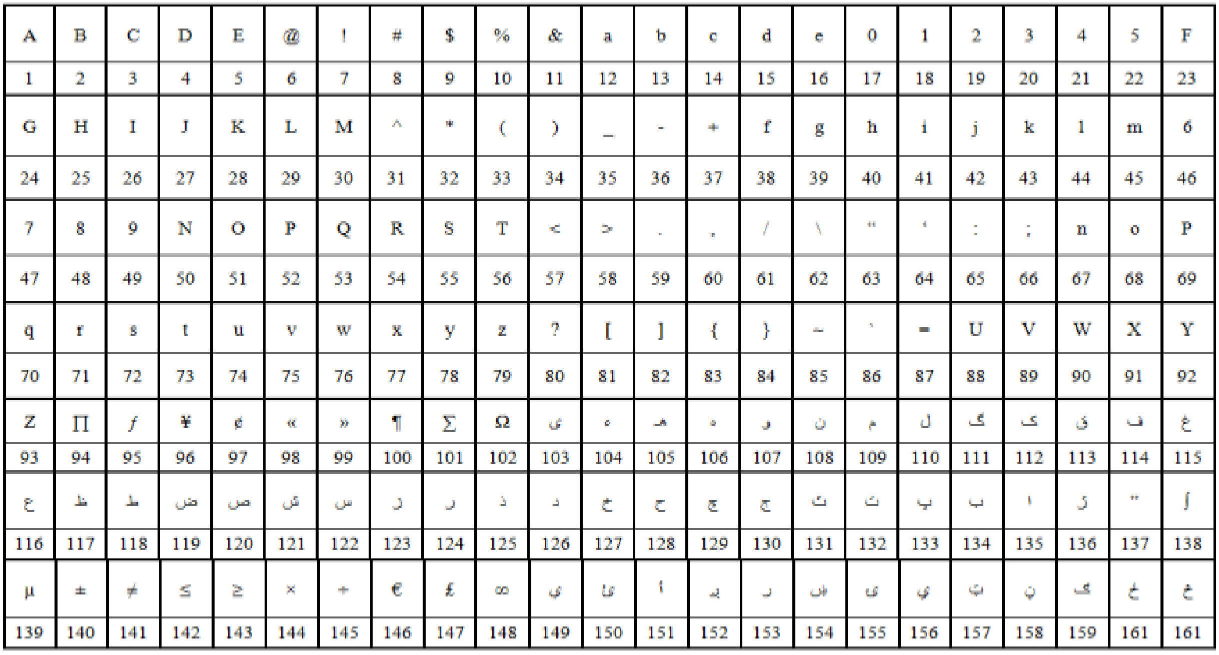


Fig. 3: Basic Caesar cipher with shift +1

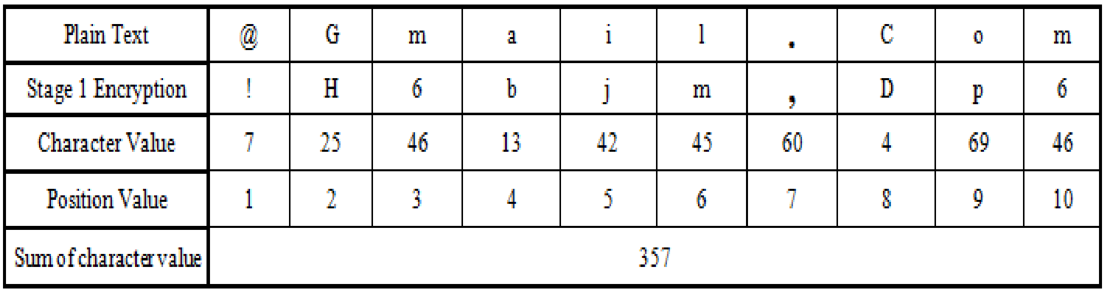
The position values are assigned corresponding to each letter and character of the plain text.The character values are assigned to each letter of the stage 1 cipher text (Refer fig. 4)



A	B	C	D	E	@	!	#	$	%	&	a	b	c	d	e	0	1	2	3	4	5	F
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
G	H	I	J	K	L	M	^	*	(	)	_	-	+	f	g	h	i	j	k	l	m	6
24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46
7	8	9	N	O	P	Q	R	S	T	<	>	.	,	/	\	"	'	:	;	n	o	P
47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69
q	r	s	t	u	v	w	x	y	z	?	[	]	{	}	~	`	=	U	V	W	X	Y
70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92
Z	∏	ƒ	¥	¢	«	»	¶	∑	Ω	ى	ه	ـه	ه	و	ن	م	ل	گ	ک	ق	ف	غ
93	94	95	96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115
ع	ظ	ط	ض	ص	ش	س	ز	ر	ذ	د	خ	ح	ج	چ	ث	ت	پ	ب	ا	ژ	"	∫
116	117	118	119	120	121	122	123	124	125	126	127	128	129	130	131	132	133	134	135	136	137	138
µ	±	≠	≤	≥	×	÷	€	£	∞	ي	ﻘ	أ	ﯾ	ـر	ﻬ	ﻰ	ي	ﺜ	ﭘ	ﮐ	ﻐ	ﻏ
139	140	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159	161	161

Fig. 4: Character value of each character and letters

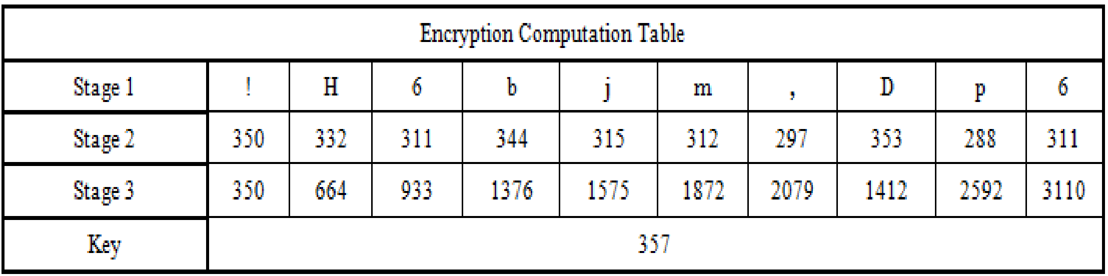
Find the sum of character values (Refer fig. 5)



Plain Text	@	G	m	a	i	l	.	C	o	m
Stage 1 Encryption	!	H	6	b	j	m	,	D	p	6
Character Value	7	25	46	13	42	45	60	4	69	46
Position Value	1	2	3	4	5	6	7	8	9	10
Sum of character value	357									

Fig. 5: Plaintext Having Character Values, Position Values and Sum of the Character Value

Subtract each character value from the sum to get the stage 2 cipher text. Than multiply the position values in the stage 2 cipher text to get the final stage 3 cipher text (Refer fig. 6).



Encryption Computation Table										
Stage 1	!	H	6	b	j	m	,	D	p	6
Stage 2	350	332	311	344	315	312	297	353	288	311
Stage 3	350	664	933	1376	1575	1872	2079	1412	2592	3110
Key	357									

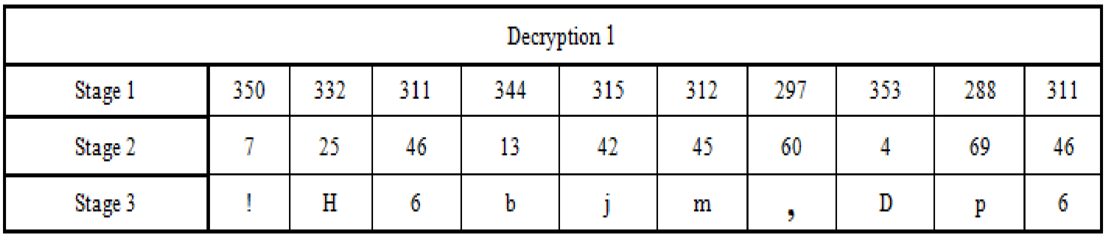
Fig. 6: Result of Deferent Stages of Encryption.

The cipher text obtained from stage 3 encryption is sent to the receiver along with the sum as the key.

B. Decryption –

Take up the cipher text and the key from the sender. Divide the position values of each corresponding letter and characterfrom the cipher text as received from the sender to get stage 1 decryption.

The above obtained stage 1 decrypted text is subtracted from the key as received from the sender to get the character values which forms the stage 2 decrypted texts. Transform the obtained character values to its corresponding letters and characters. (Refer fig. 7)



Decryption 1										
Stage 1	350	332	311	344	315	312	297	353	288	311
Stage 2	7	25	46	13	42	45	60	4	69	46
Stage 3	!	H	6	b	j	m	,	D	p	6

Fig. 7: Result of Deferent Stages of Decryption.

Now, apply the basic Caesar cipher algorithm with substitution as -1 (Refer fig. 8). Thus the plain text is obtained (Refer fig. 9).

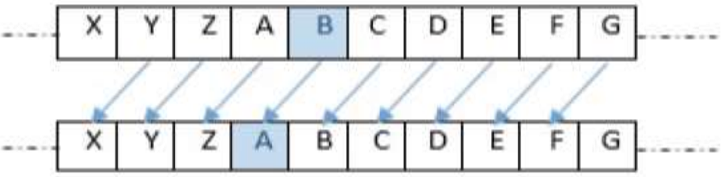
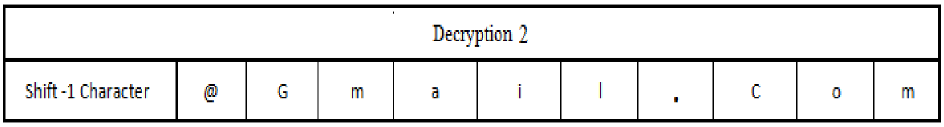


Fig. 8: Basic Caesar cipher with shift -1



Decryption 2										
Shift -1 Character	@	G	m	a	i	l	.	c	o	m

Fig. 9: Result of Deferent Stages of Decryption.

V. RESULTS AND DISCUSSION

Caesar cipher is prone to brute force attack, frequency analysis and pattern matching. The earliest known use of a substitution cipher, and the simplest, was by Julius Caesar. The Caesar cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet. In order to overcome to these problems occurring in the cipher text some modifications is been added with multi stage encryption technique

The frequency analysis and pattern matching is done by observing the frequency of each occurrence of the letters and characters in the cipher text. If the repetitions of the characters happen, it will be easy for the intruder to guess the plain text and crack it.

The attacker tries every possible key on a piece of cipher text until an intelligible translation into plaintext is obtained. On average, half of all possible keys must be tried to achieve success.

In this system as the plain text is been converted into numbers, and then upon carrying out some computations stage by stage on the obtained numbers, the chances of getting the same number for the corresponding letter and character is very rare. In addition to this the system is case sensitive and so a wide range of plain text combinations can be covered. All these features provide security to the data transmitted that using the insecure channel connecting the sender side and receiver side.

VI. CONCLUSION

The proposed system provides more security and it is capable of protecting the transmitted data from brute force attack by using stage by stage computation for encryption. The cipher text generated after the different stages of encryption is in the form of numbers along with a key which is also a number. The chances of guessing the plaintext from those numbers is difficult and so frequency analysis, pattern matching and brute force attack are not possible to an extent and crack the transmitted data. We can also make the displacement dynamic instead of fixing it as ±1. Allowing the spaces between the words and character can also be added as a future enhancement. Using the various data structures in C, like linked list, stack, queue, tree graph etc, [1] the modified Caesar cipher algorithm can be combined with any one the above mentioned data structures so that the cipher code has strong security and harder to crack. In this way an extra measure can be taken to send the private message and data safely from the sender side to the receiver side.

REFERENCES

[1]. SonaliKulkarni,"Cryptographic algorithm using data structure using c concepts for better security", International Conference on Pervasive Computing (ICPC), 2015.

[2]. WillianStallings,"Cryptography and Network", Prentice Hall of India.

[3]. B.A.Forouzan,"Cryptography & Network Security", Tata- McGraw Hill Book Company

[4]. S G Srikantaswamy, Dr. H D Phaneendra,"Improved Caesar Cipher with Random Number Generation Techniqueand Multistage Encryption", International Journal on Cryptography and Information Security (IJCIS). Vol. 2, No. 4. pp. 39-49, December 2012.

[5]. AkankshaMathur,"A Research paper: An ASCII value based data encryption algorithm and its comparison with Others ymmetric data encryption algorithms", International Journal on Computer Science and Engineering (IJCSE). Vol. 4, No. 09. pp. 1650-1657, September 2012.

[6]. VinodSaroha, SumanMor, AnuragDagar,"Enhancing Security of Caesar Cipher by Double Columnar Transposition Method", International Journal of Advanced Research in Computer Science and Software Engineering. Vol. 2, Issue 10. pp. 86-88, October 2012.

[7]. Gaurav Sharma, Ajay Kakkar,"Cryptography Algorithms and approaches used for data security", International Journal of Scientific & Engineering Research, Vol. 3, Issue 6, 2012.

[8]. [Online] Available: http://www.cs.trincoll.edu/~crypto/ historical/caesar.html. Last visited on 15-09-2015

[9]. Ayushi,"A Symmetric Key Cryptographic Algorithm", International Journal of Computer Applications (0975 - 8887), Vol. 1, No. 15, 2010.

[10]. ShyamNandanKumar,"Review on Network Security and Cryptography", International Transaction of Electrical and Computer Engineers System, Vol. 3, No. 1, pp. 1-11, 2015.