SIGNIFICANCE OF NUMBER THEORY TO DEVELOP SECURITY OF CAESAR CIPHER METHOD

Ahmad Shah Noori[1] and Abdullah Abid [2]
[1]Designation, Department of Mathematics, Urozgan Institute of Higher Education, Afghanistan
[2]Designation, Department of Mathematics, Shaikh Zayed University, Afghanistan
[1]Noorimath2018@gmail.com
[2]abdullahmangal579@gmail.com

Abstract

Cryptography is a discipline of converting the basic text communication into non readable form. the wide progress of technology increases the necessity of electronic data protection than ever before. Cryptography performance a significant role in data safety techniques. Cryptography has raised as a clarification which performances a dynamic function in data safety arrangement against malevolent attacks. Number Theory plays significant role in the encryption process. Caesar cipher is an earliest and basic cryptographic method of transforming initial text communication in to non-readable to keep the text from opponents. Caesar cipher is an arm of substitution method so we shall underwrite this technique in the range of traditional cryptography through delivering of an escalating and traditional form for Caesar cipher by means of information of mathematics and Computer science to growth the stability of the encryption. I Considered Caesar ciphers as agents and improved form of Traditional method with numerous characters key, that encrypted plaintext is approximately difficult to decrypt.my purposes is to present the utilization of Number Theory in Caesar Cipher Cryptography. We drive quick conversation around the knowledge of encryption in Caesar ciphering and several connected tools in Number Theory.

Keywords: Number Theory, Cryptography, Plaintext, Cipher text, Caesar Cipher

1. Introduction:

In today's technical and scientific nature, it is difficult to visualize without web or internet This up-to-date era is overcome by paperless communications in workplaces by means of usage of E-mail, E-cash trades, etc. on the other hand we study Number theory so we have to observe that each Number Theory's tool performances a significant

function in cryptography to encrypt and decrypt a communication text. Due to this there is an excessive necessity of exchanging of information over online channels. In different commerce and business-related areas, there may be private communication such as banking trades, credit information, governmental communication and personal text messages is transmitted in excess of web using E-mails, social network etc... To keep this category of private data from not permitted persons, there is a huge necessity of safety techniques to progress a system that guarantees to keep the data from the aggressor. One of the schemes to keep online secret information from unlicensed revelation is to transform the online information to non-readable. Cryptology is at center of running such warranty. The expression of Cryptology has been for more than 2000 years. This word had taken from two Greek expressions: kryptos, which means "secret or hidden" and logos, which means "description". Cryptology includes double contra services – privacy and resolution. The function of Privacy is named cryptography. The target of cryptography is to present a communication test unintelligible to the unapproved person. Cryptography is some time named "code making." The outcomes quantity of cryptology is named cryptanalysis. Cryptanalysis is often called "code breaking".

Cryptography is the knowledge of developing latest strong and useful encryption and decryption schemes. It distributes with the methods for transmission of communication text with a stable and secure manner. The fundamental purpose of cryptography is to permit the planned receivers of a communication to have the text correctly whereas avoiding eavesdroppers from comprehension the communication. Cryptography guarantees that the communication being referred at one end be secret and must be obtained just by the proposed receptionist at the other end. Cryptography transforms the primary communication in to non- readable design, then refers the communication through an exposed canal. The persons who is not allowed to know the communication have attempt to disruption the non-readable communication however it is difficult to do so. The allowed body has the ability to transform the not readable communication to understandable one. We have dual methods for transforming information into non readable document.

a.**Transposition technique**

b. **Substitution technique**

The cryptography is separated into two basic types dependent on the category of safety keys handled to encrypt/decrypt the text message. These double classes are: Asymmetric and Symmetric encryption methods.

i) Symmetric Encryption: In symmetric key cryptography similar hidden key is applied for encryption and decryption. The

encryption algorithm provide a key and then guide it to receptor portion somewhere decryption takes position. It is significantly valuable and faster than asymmetrical key cryptography.

ii) Asymmetric Encryption: Asymmetric key cryptography which some time called as shared key cryptography. It plays with double keys: i.e public key and private key. Public key is consumed for encryption. And only the user knows about private key and is used for decryption. These both keys are connected to each other by any mathematical channel.

iii) Cryptography Terminology

a) Plain Text: the primary text Communication or the real secret Text which somebody wants to forward to another person. We will denote byP.

b) Cipher Text: It is the production of encryption algorithm. Cipher text Communication couldn't be recognized by invader as in not readable layout. We will denote by C.

c) Encryption Algorithm: The process which transform a plaintext into cipher text with usage of a key

d) Key: This is likewise assumed as enter to encryption algorithm It might be numeric or alpha numeric text or might be a particular sign.

e) Decryption Algorithm: It is a contrary technique of encryption algorithm. Which the primary communication is recovered from the cipher text. Encryption algorithm occurs at the writer end and Decryption algorithm occurs at the recipient end.

1-1. Caesar Cipher (Substitution technique):

The Caesar cipher is very classical division of ancient cryptography its titled after the Roman Emperor Julius Caesar, who conforming to Suetonius consumed shift cipher through a steady left shift of 3 to encrypt essential armed text communication in combat. Therefore, it is likewise called as shift cipher, Caesar's cipher or Caesar shift. Substitution method plays an important rule to develop the encrypted text.

For the explanation we will consider the example

Plain text: ZYXWVUTSRQPONMLKJIHGFEDCBA

Cipher text: WVUTSRQPONMLKJIHGFEDCBAZYX

While encrypting, a separate consider every character of the text communication in the "plain text" and inscribes the matching letter in the "cipher text". Deciphering is precisely a reverse Process, by shifting of three positions.

This might be similarly illustrated by consuming Numerical arithmetic by converting the letters into numbers, we will explain on the time. Currently, if we want to encrypt a letter (x),it is

equation is $E(x) = (x + n) mod\ 26$, and the decryption is presented by : $D(x) = (x - n) mod\ 26$. The substitution of letters is similar for whole text message which is encrypted.

The main downsides of Caesar cipher is it can simply be cracked, even in cipher-text only situation. Several techniques have been discovered which break the cipher text by consuming regularity analysis and pattern texts. This is achievable since here we have just restricted number of conceivable transferals. (26 in English).

The circulation of letters in a archetypal model of English linguistic text message has different and expected form. A Caesar shift "replaces "this circulation, and it is achievable to establish the shift by testing the resulting frequency graph. This is the simplest method to breakdown Caesar cipher.

If we think through a text communication which is encrypted through a key of 1260356.The encryption method is Caesar cipher. Now suppose an aggressor obtains an encrypted cipher text but doesn't identify the key. Therefore, to create a plaintext he attempts several cryptanalysis methods on the cipher text. Assume, he applies frequency analysis method to breakdown it then its frequency circulation graph attained by analyzing the cipher text will be much different than actual.

Underneath the plain text letter, the substitution alphabet for Caesar cipher is given by

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

For instance: NUMBER THEORY IS EASY is converted in to QXPEHU WKHRUB LV HDVB by the benefit of congruence theory Caesar cipher could be simply explained. Any plaintext is first presented arithmetically by altering the character of the text into digit by means of particular communication for instance.

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

Now for every Plaintext, we will alternate the cipher text C, so we get the congruence

$C \equiv P + 3(\mathrm{mod}26)$, We shift with three positions, so we have $C = E(3, P) = (P + 3) mod 26$

In above equation C is the cipher text letter, E is the encryption of 3 which is the key and P is the sing of plaintext letter

Generally, with Caesar Cipher algorithm we can shift from 1 to 25 positions, it can be some digit between1 to 25, so we name that digit K,therefore we have

$$C = E(K, P) = (P + K)\text{mod}26$$

At the present we will effort for the alteration of encrypted information into its initial shape which is named Decryption. It deciphers the encrypted data therefore that an authoritative operator can just decrypt the information so decryption necessitates a top-secret key or password, to get back the plaintext we have the following equality

$$P = D(K, C) = (C - K)\text{mod}26$$

We see the planned algorithm and its operation is explained with the assist of instance. The algorithm is used to encrypt as well as decrypt the plaintext

For example: HELLO WORLD YO.

We are to concern the Caesar cipher text to the plaintext, we will consider the key as$K = 3$, for encryption we have

$$C = E(3, P) = (P + 3)\text{mod } 26.$$

We see that first letter in plaintext is H, whose representative number in the above table is 7. So, we have

$$C = E(3,7) = (7 + 3)\text{mod } 26$$
$$C = 10 \text{ mod } 26$$

As we see that $26 > 10$, according the rule of congruence the remainder is 10, that is C=10, which 10 is the representative number of K, so the cipher text for H is K.

Similarly, for E, which is the second letter of "HELLO" we get

$$C = (4 + 3)\text{mod } 26$$
$$\Longrightarrow C = H$$

Similarly, when we want to encrypt an arbitrary number let us say y,so y represented number of 24, so we have

$$C = E(3,24) = (24 + 3)\text{mod } 26$$
$$C = 27 \text{ mod } 26$$
$$C = 1$$

So, the cipher latter for the letter y would be B.

So, for the final cipher text of the above plaintext is

Plain text: HELLO WORLD YO

Cipher text: KHAAR ZRUOG BR

Now for the decryption process we have $P = D(K, C) = (C - K)\text{mod } 26$

Our key is $K = 3$, so let decrypt, first for the letter K we have

$$p = D(3,10) = (10 - 3)\text{mod } 26$$
$$P = H$$

For the second letter H we have

$$P = D(3,7) = (7-3) \bmod 26$$
$$P = 4 = E$$

So, after decryption of all the letters we get our plaintext back

1-2. Playfair Cipher:

Playfair cipher is a special form of classical cipher, it deals with a square of matrix of 5X5 alphabetical letters organized in a proper method. We can choose a key and put it in the matrix .the waiting letters of English alphabet are then one by one located in the matrix of Playfair cipher, the plain text is cracked in to couples and if a couple has identical script then they are disjointed by presenting a putty letter such as „x", in addition, if couples are dissimilar alphabetical letters and inhabit in the identical line of matrix at that time every letter is restored by the letter forward of it. If the couple of letters are in similar column of matrix then every letter is restored by the letter under it, while the couple of letters are not in similar column nor in similar row afterward, they substituted by the letter in their row that inhabits at the connection of combined letters. Inverse process is concerned to get the answer.

For example,

Plain text: enemyattackstonight (we use z to pad empty location). And consider the key:31452

Step 1: arrange the considered text column by column.

1	2	3	4	5
e	n	e	m	y
a	t	t	a	c
k	s	t	o	n
i	g	h	t	z

Step 2: Reschedule the columns

3	1	4	5	2
e	e	m	y	n
t	a	a	c	t
t	k	o	n	s
h	i	t	z	g

Step 3: Consider the matrix column by column, we het the Cipher text: ettheakimaotycnzntsg

The main downside of simple columnar transposition cipher is that to decipher it, the receptionist must Consider the column segments by sharing the segment of cipher text by the key segment. Then he can write the cipher text out in columns again and then re-order the columns by restructuring the key term to get the plain text.

1-3. Vigenere Cipher:

When we match this cipher beside Caesar provides particular rank of safety with the overview of a keyword; this keyword is

recapped to covering the size of the plain text that is to be encrypted we will consider the example

KEY: f a u z a n f a u z a n

P.T: c r y p t o g r a p h y

Cipher: H R S O T B L R U O H L

In the example, “fauzan” is our keyword, “cryptography” is plaintext, and its encrypted form is “HRSOTBLRUOHL”. which is done by Vigenere table which includes characters in method of rows and columns left most column designates keywords and top most row designates plaintext and at the intersection of dual alphabetic letters resides our replacement and behind separately altering each letter we obtain an encrypted text message.

1-4. Proposed Modified Caesar algorithm

In this approximate, in place of instable the typescripts linearly, they are shifted arbitrarily by handling the replacement and combination box methods which are applied in recent encryption methods such as blowfish, DES, etc. Subsequently, replacement box is to be generated by applying the method of affine ciphers (i.e. $\text{Cipher text} = (\text{Plaintext} * \text{key1}) + (\text{Key2})$. The typescripts are then substituted by its corresponding rates connect to the replacement box. In Addition, challenge the cipher message to conceal the characteristics of the language by with combination methods (i.e. by chance altering the places of characters in the cipher text). Combination of cipher text is completed by consuming dual columnar substitution on the cipher text. The planned algorithm could encrypt the area of typescripts which the Caesar cipher could not encrypt, i.e. ASCII and Extended ASCII characters.

2. Discussion:

This part explains connected investigated work done to make effective Caesar cipher Encryption Algorithm.

1. Goyal has recommended an alteration to the classical Caesar cipher wherever he holds the key length stable as single. However, replacement he tests the index of character set, if the index is even then he improves the key rate by a single more, if the index is odd then he reduces the key rate by single unite
2. Singh et al. has projected a method to join Caesar cipher along with Rail fence substitution method to remove essential weak points of Caesar cipher in addition to generate a cipher text message it is difficult to breakdown.
3. Omolara et al has propositioned an improved connection of Caesar cipher and Vigenere cipher to enhance the dissemination and destruction properties of cipher text by including methods as of up-to-date ciphers similar to xoring key to the initial

letter of plain text, xoring initial letter of the plain text to next (second) letter and so on.

4. Disina has propositioned a technique of encryption that belong to the location of the bit in the text communication. The writer will transfer the bits in the communication by instable the typescripts in the odd place to the leftward and typescripts in the even place to the right-hand side.
5. Purnama has projected an improved Caesar cipher technique wherever she practices a technique of encryption that the cipher text created is readable therefore creating it fewer doubtful to the cryptanalyst that the text message has been encrypted.

3. Acknowledgment:

Safety is one of the significant standpoints in calculating. In information transmission, safety should be minded as one of the techniques applied to confirm safe information transmission. Information transmission is shifting data from a position to another position, or waitperson. To have a protected information transmission, this could be utilized, and one of them is encryption of information, formulate it to be shifted in encrypted manner and decrypted after the information need to be consumed.

As the significance and the importance of replaced information throughout the Internet or other channels are growing, the investigate for the greatest answer to approach the essential safety in opposition to the information burglars' strikes along with arranging these facilities below timely way is one of the best effective issues in the safety linked societies

4. CONCLUSION:

In this manuscript we comprehend that each number theory instrument performance a significant function in cryptography to conceal text communication for the safety of information, the congruencies have played important task in Caesar ciphering key cryptography. We derive that the cipher manuscript generated by this technique can be sing correctly, this of definite factions wouldn’t be doubtful of text communication which is encoded. Alongside the resultant cipher manuscript be able to state, this technique can select the cipher text that can be state and basically as necessary, this technique had the key word that is on the script turnaround outcome (root) which be able to exert by the handler as necessary, since the outcomes of this reformation are a specific replacement, then the technique is similarly simply answered by cryptanalyst beside the cipher text solution not doubtful by cryptanalyst of convinced factions.

REFERENCES

[1] *Ramandeep Sharma, Richa Sharma and Harmanjit Singh "Classical Encryption Techniques" published in International Journal of Computers & Technology. Volume 3. No. 1, AUG, 2012.*

[2] *O.P Verma, RituAg arwal, DhirajDafouti and ShobhaTyagi, "Peformance Analysis of Data Encryption Algorithms", IEEE, Delhi Technological University India, 2011.*

[3] *William Stallings, "Cryptography and Network Security", Fourth Edition, Prentice-Hall -pp.80-81.*

[4] *Stallings, W. (2006), Cryptography and Network Security 4/E., Pearson Education India.*

[5] *Atul Kahate (2009), Cryptography and Network Security, 2nd edition, McGraw-Hill*

[6] *Behrouz A Fourouzan, Debdeep Mukhopadhyay (2010), Cryptography and Network, 2nd edition, McGraw-Hill.*

[7] *Senthil, K., K. Prasanthi, and R. Rajaram. "A modern avatar of Julius Caesar and Vigenere cipher." Computational Intelligence and Computing Research (ICCIC), 2013 IEEE International Conference on. IEEE, 2013.*

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

[9] *Hamdan.O.Alanazi, B.B.Zaidan and A.A.Zaidan, "New Comparative Study Between DES, 3DES and AES within Nine Factors", JOURNAL OF COMPUTING. Vol.2, Issue 3. Pp.152-157, MARCH, 2010.*

[10] *Jason Crampton, "Time-Storage Trade-Offs for Cryptographically-Enforced Access Control", Lecture Notes in Computer Science, Springer, 2011, Vol. 6879/2011, pp. 245-261.*

[11] *Jiannong Cao, Lin Liao, Guojun Wang, "Scalable key management for Secure Multicast Communication in the Mobile Environment" Pervasive and Mobile Computing Vol. 2, pp.187–203, 2006.*

[12] *Stalling, William."Cryptography and Network Security: Principles and Practice". 5th ed, Prentice Hall, 2006.*

[13] *"Classical-Encryption Techniques", mrajacse.files.wordpress.com/chapter-2.*

[14] *Sinkov A., "Elementary "Cryptanalysis-A mathematical Approach", Mathematical Association of America, 1966.*

[15] *Jason Crampton, "Time-Storage Trade-Offs for Cryptographically-Enforced Access Control", Lecture Notes in Computer Science, Springer, 2011, Vol. 6879/2011, pp. 245-261.*

[16] *Stalling, William."Cryptography andNetwork Security: Principles andPractice". 5th ed, Prentice Hall, 2006.*

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

[18] *Sinkov A., "Elementary "Cryptanalysis-A mathematical Approach", Mathematical Association of America, 1966.*

[19] *Kraft, J. S., & Washington, L. C. (2018). An introduction to number theory with cryptography. CRC press.*

[20] *Koblitz, N. (2000). A survey of number theory and cryptography. In Number Theory (pp. 217-239). Hindustan Book Agency, Gurgaon.*