



Secure Message Transmission using Caesar Cipher and Residue Number System

Damilola David Popoola; & Prof Kazeem Alagbe Gbolagade

Department of Computer Science, Faculty of Information and Communication Technology, Kwara State University, Malete

Abstract

Secure communication across a digital medium is ensured by data security. The data should be guided against availability by unrecognised users and communicated to the right recipient in a secure and confidential manner. Although the cipher text can make data difficult for a third party to interpret, the irregular representation given to it acts as a means of drawing an attacker's attention to such data. As a result, through the design of a character swap table to swap characters to numbers and the use of RNS to convert the numbers to residues, this research proposes a scheme that integrates additional phases to the standard Caesar cipher. The proposed system was able to generate the cipher text as residues, ensuring that the message remains undetectable and difficult to crack.

Keywords: *Residue, Number System, Caesar Cipher, Cipher-Text, Communication*

Introduction

With so many internet-based professions, digital communication has become an important aspect of two-party collaboration currently. Communication with a high level of confidentiality is essential. As a result, the security of data

exchanged between the parties is a critical issue that extends to the integrity and confidentiality of the message, necessitating implementation of safeguards against unauthorized access and use. Cryptography, which is an act of

encrypting and decrypting a message using some sort of mathematics, was born out of the need for secure communication between two closures. Cryptography gives room for storage and forwarding of data across a network (example is the world wide web) in such a way it is unknown by anybody other than real receiver of such data (Badoni & Jain, 2014). As a result, the cryptosystem may be thought of as a collection various algorithm that are used with specific keys that convert the real message (plain-text) to the encrypted message (ciphertext) (Al-Hazaimeh, 2013). The illustration of the concept was made by Barakat et al (2018), who needed Alice to send a message securely to Bob in the presence of Eve or Mallory, where Alice represents the sender, Bob represents the receiver, Eve represents the eavesdropper, and Mallory represents the Man-in-the-middle attack, as shown in Figure 1.1.

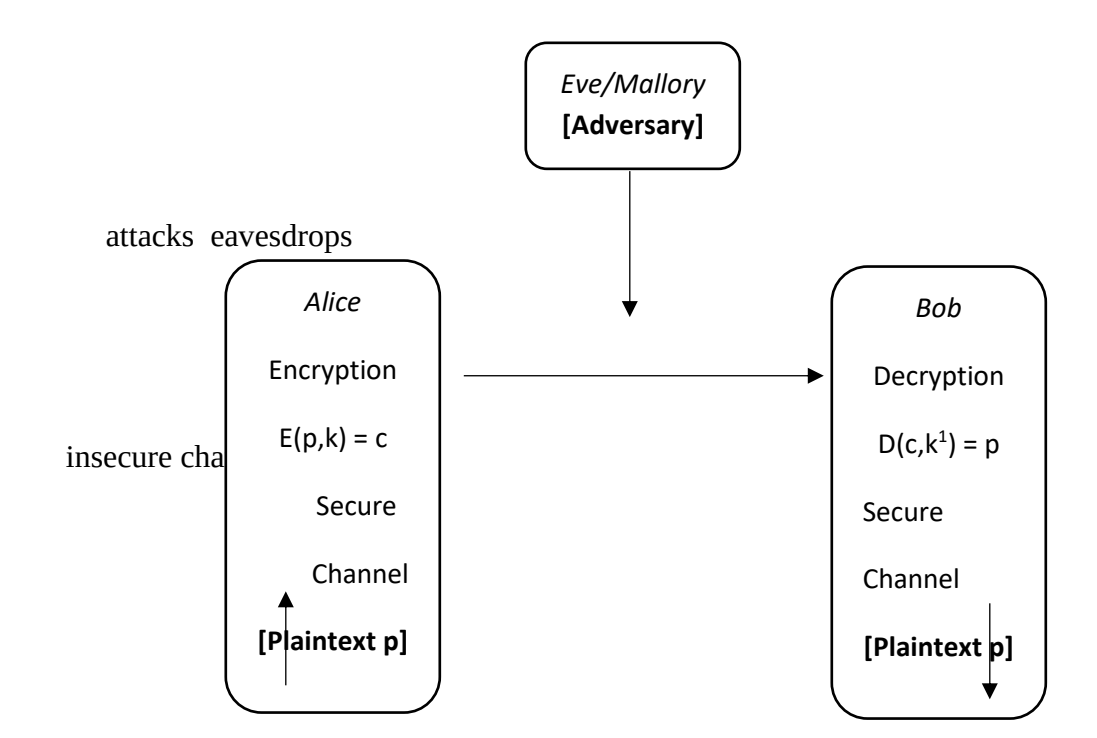


Figure 1: Pictorial representation of cryptography (Source: Barakat et al, 2018)

Cryptography is made up of sophisticated numerical formulas that govern the instructions for converting ordinary text to cipher text and the other way round. symmetric and asymmetric algorithms are employed, which involves the use of a single key or a two separate keys (Private and Public) respectively (Deepak & Parveen, 2017).

Plain text is any message that can be understood without the need for further explanation. Encryption is a technique for altering the representation of data with the goal of concealing its content. When you encrypt plaintext, you get cipher text, which is an unreadable and difficult-to-understand representation. Encryption helps to make data inaccessible to anyone who isn't supposed to see it, including those that have access to the data that has been encrypted. On the other hand, the process of reversing the action to turn the text to its initial form known as decryption.

Transposition and substitution are techniques employed in encryption. The transposition approach involves making modifications to plaintext to alter its appearance. In substitution, the plaintext is replaced with various characters.

A message must be transferred from the sender to the receiver over a transmission channel, which is controlled by a set of protocols, as shown in Figure 1.2. The sender is the source of the message to be conveyed, the receiver is the intended recipient, the medium of transmission is the channel by which the message moves from one end to the other. The rules that governs the transmission process is the protocol.

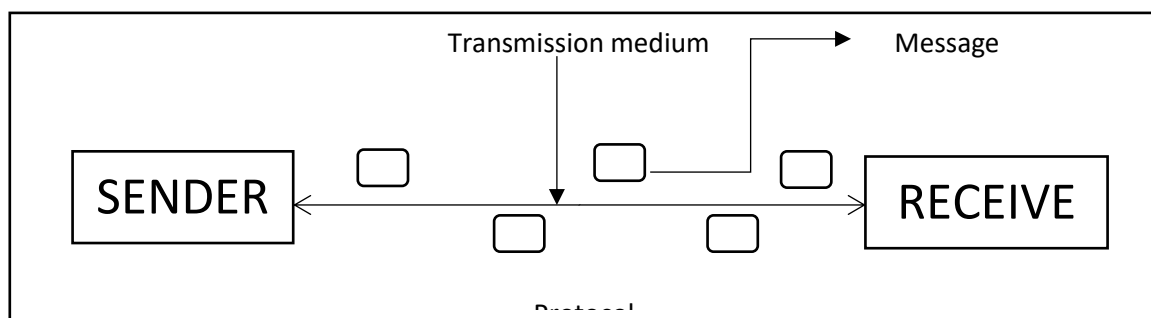


Figure 2: Data transmission process

The important aspect of any cryptography approach is for enhanced security level which makes it difficult for an outside body to perceive the data.

A number system, known as Residue Number System (RNS) is used to aid equalize, convey free expansion, receive free deduction, and increase in a single step without missing any items. In RNS, data conversion is typically based on the Chinese Remainder Theorem (CRT) or the Mixed Radix Conversion (MRC), to reverse a number from its residue form to decimal (Aremu & Gbolagade, 2017).

A shift cypher, also known as Caesar cipher algorithm, was devised by Julius Caesar. The approach uses the third letter set to one side of the start letters in order to address every letter in order in the message with another letter in order. Because interlopers may surely give a shot each coded message and effortlessly get at the end of what the

first message is, the Caesar cipher algorithm is considered as a fragile algorithm due to the ease with which it can be executed. As a result, various methodologies have emerged in order to ensure that data communicated over a digital medium is difficult to decipher by an outside body. Based on findings Hercigonja and gimnazija (2016), symmetric algorithms perform better than asymmetric algorithms. Despite various improvements that has been achieved on these algorithms over time, the cipher-text still appears in the traditional jargon structure. As a result, to ensure safe communication, this research introduces a methodology that will maintain the message's personality while also acquainting greater complexity through the use of RNS to change the structure of the cipher-text.

Most communications takes place through the internet, which has clearly opened up a channel through which attackers can obtain information about what is being transmitted. Although the many encryption methods in use appear to handle this issue, it is limited to the way a cipher-text creates a road for doubt with its depiction as a result of the substitution or transposition strategy.

The Caesar cipher technique, which is a replacement approach for encrypting data, has the problem of being vulnerable to attack because the first message may be easily deduced if an attacker tries every possible combination of movements for each of the 26 letters. Despite recent efforts to mitigate these problems by adding special characters and symbols and employing a transposition and substitution strategy, they still give characters that indicate some type of manipulation of the transmitted message, rendering it suspect.

As a result, a plan is needed that would make the encrypted data unobvious to attackers and also make the message tedious to discern by completely transforming the appearance of the message.

Literature Review

Lubis et al (2017) presented Combination of Caesar Cipher Modification with Transposition Cipher, which combines substitution cipher with transposition cipher. It adds three encryption stages: first, Caesar modification; subsequently, the resultant ciphertext was done using transposition. The resultant of the process was further encrypted with another Caesar modification. The shift of letters in the Caesar cipher modification made use of the ASCII table, original text gets the addition some

characters before being divided into two, the text to be encrypted and the text to be left constant. The key that is used dynamically is the third modification.

Verma et al (2017) proposed a new improved Caesar cipher algorithm in which encryption is not limited to alphabets. The Caesar cipher is a versatile cipher that can encrypt symbols, letters, and numerals. In addition, a new character value table is proposed, which specifies the symbol, character, and digit places in the table. Furthermore, the Caesar cipher is made more complex using the matrix concept, making it difficult for brute force attackers to find the key value.

Pinheiro and Saraf (2016) present a system in which case sensitive characters are recognized. The plain text is encrypted and decrypted by using the face values and positioning values of the respective characters as the key. The plain text is subjected to multistage encryption, which improves its security and protects it from brute force attacks, pattern matching, and frequency analysis to some extent.

The system described by Jain et al (2015) provides an expanded and modified version of the Caesar cipher employing mathematical and computer science knowledge. The algorithm proposed uses the ideas of transposition ciphers, affine ciphers, and randomized substitution techniques to construct a cipher text that is very tedious to decipher in order to improve the strength of this conventional encryption technology. In addition to alphabets, it expands the range of characters that the Caesar cipher Algorithm can encrypt by including all ASCII and expanded ASCII characters. To ensure increased security, a complicated key generation mechanism is used that generates two keys from a single key.

Purnama and Rohayani (2015) suggested a strategy that modifies the Caesar cipher method to produce cipher-text that can be read while looking for a better way to improve the Caesar cipher algorithm. When the cipher text can be read, cryptanalysis is unconcerned with the cipher text. The Caesar cipher was modified by splitting the alphabet into two halves, replacing the vocalists with the alphabet vocals, and replacing the consonant alphabet with a consonantal alphabet. However, some alphabet consonants are not substituted, owing to the fact that the alphabet's frequency is rarely utilized in an Indonesian text. A cipher-text that can be read was derived from the test results.

Imran and Abdulkareem (2014) proposed a way in which information will be encrypted to make it difficult to read and secure in their approach. Each letter in the plaintext is replaced with a specified number of positions down the alphabet using one

of three approaches. The end result of this project is encrypted data that can be decrypted into readable form.

Srikantaswamy and Phaneendra (2012) presented a method to improve Caesar cipher key generation operations using a random number generation mechanism. Alphabets, digits, and symbols have all been added to the Caesar cipher. Only alphabets were allowed in the original Caesar cipher. The key for Caesar Substitution was derived using a Modulo 94-restricted key Matrix Trace value. The Matrix elements are created using a recursive random number generation equation, whose output is solely determined by the seed value used.

Abraham and Shefiu (2012) made some significant enhancements to the traditional Caesar cipher algorithm, totally eliminating its flaws. First, it removes spaces from the cipher-text, and second, the Improved Caesar Cipher (ICC) involves two processes in the creation of the cipher-text, such that even if it is decoded, the output is gibberish.

Deepak and Parveen (2017) presented a technique using ASCII and binary operations the cryptography to improve security and make it more difficult for attackers to decrypt the original message delivered over the network.

Dey (2016) introduced a new cryptographic strategy for removing repeating phrases from a message before encrypting it, making it nearly hard to recover or predict the original message from the encrypted message. The approach used the SD-AREE cryptography method to remove repetitive phrases from an encrypted message. The repeating bits / characters are deleted in the SD-AREE approach, and there is no evidence of any repetition in the message.

Al-Hazaimeh (2013) suggested a method called "A New Approach for Complex Encrypting and Decrypting Data," which maintains the security of communication channels by making it difficult for attackers to predict a pattern while also increasing the speed of the encryption/decryption scheme. The scheme's algorithm is made up of a hybrid system's public key infrastructure and the RC6 algorithm for confusion and diffusion operations.

Methods and Materials

A new strategy was developed to improve the present system by giving a better means of ensuring secure communication from one end to the other and to overcome the limitations of the Caesar cipher algorithm. There are two stages to the plan. The first stage entails exchanging each letter in the message for decimal numbers, and the

second stage entails using the RNS technique to transform the decimal numbers to residues, which are then sent to the target recipient.

Character swapping and forward conversion

The first stage of the transposition involves performing the swapping of each of the characters to decimal numbers using a formulated character table (see figure 3.1). The table formulated will ensure that other characters such as alphabets, symbols and numbers are also catered for.

Numeric value	Character	Numeric value	Character	Numeric value	Character
1	a	23	w	45	(
2	b	24	x	46	)
3	c	25	y	47	-
4	d	26	z	48	-
5	e	27	0	49	+
6	f	28	1	50	=
7	g	29	2	51	[
8	h	30	3	52	]
9	i	31	4	53	{
10	j	32	5	54	}
11	k	33	6	55	\
12	l	34	7	56	
13	m	35	8	57	;
14	n	36	9	58	:
15	o	37	!	59	,
16	p	38	@	60	"
17	q	39	#	61	<
18	r	40	\$	62	>
19	s	41	%	63	.
20	t	42	^	64	/
21	u	43	&	65	?
22	v	44	*	66	*

Figure 3: Characters swapping table

The forward conversion takes place for each of the characters using a moduli set e.g $\{2^{2n}-1, 2^{2n}, 2^{2n}+1\}$. A numeric value is assigned to n in the moduli set in order to compute the moduli. Using the moduli set, it is expected that for each character, three residue numbers will be computed. From the computed residue numbers, a matrix is formed and this in turn becomes the cipher-text with each character of the original message occupying a row of the matrix.

The transposition is achieved using;

$$x = m_i[x/m_i] + |x|_{m_i}$$

where m is the moduli and x is the number to be transposed.

Algorithm

A. Encryption

- i. Read all characters
- ii. Swap each character with its numeric equivalent using the character table
- iii. Choose a moduli set to be used
- iv. Set value for n for the computation of your moduli

- v. Compute the forward conversion of the Use the computed moduli to generate residues for each of the numbers.

Decryption process

For the decryption process, the residues generated for the encryption process will undergo backward conversion using Chinese Remainder Theorem.

This theorem is used in converting RNS to decimal. Given the residue representation $\{r_1, r_2, \dots, r_n\}$ of c , the CRT makes it possible to determine $|c|_m$, provided the gcd of any pair of moduli is 1. Such moduli are called pairwise relatively prime.

The CRT is given by

$$|x|_m = \left| \sum_{j=1}^N \hat{m}_j \left| \frac{r_j}{\hat{m}_j} \right|_{m_j} \right|_m$$

where

$$\hat{m}_j = \frac{M}{m_j}, \quad M = \prod_{j=1}^N m_j$$

and

$$\gcd(m_j, m_k) = 1 \text{ for } j \neq k$$

$$X = |x_1|_{m_1} |\hat{m}_1|_{m_1} + |x_2|_{m_2} |\hat{m}_2|_{m_2} + |x_3|_{m_3} |\hat{m}_3|_{m_3}$$

The procedure for the decryption is stated below;

1. Read all residues, one row at a time.
2. Using the Chinese Remainder Theorem, perform a reverse conversion on the residues based on the moduli set $\{2^{2n}-1, 2^{2n}, 2^{2n}+1\}$.
3. Substitute each of the numbers generated from the reverse conversion to Yoruba character based on the numeric character table.
4. Substitute each of the Yoruba characters to English alphabets using the Yoruba character table.

Results and Discussions

To check the performance of the scheme, a text file was supplied (see fig 4.1) as the original message. A value of 1 was for n using the moduli set $\{2^{2n}-1, 2^{2n}, 2^{2n}+1\}$ to achieve the encryption process. The resultant ciphertext(residues) is given as output.

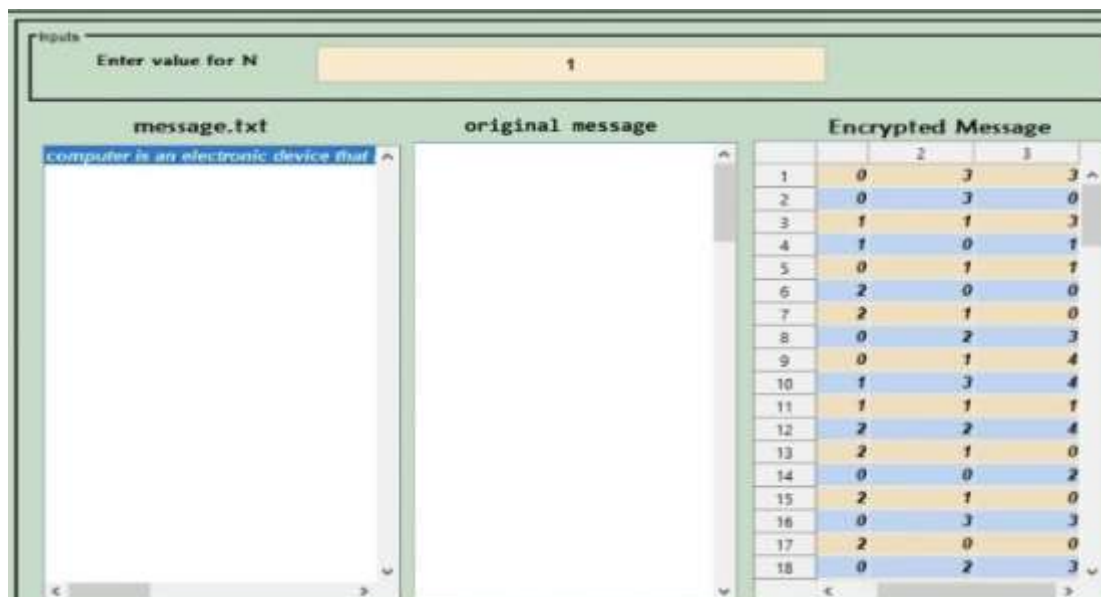


Figure 4: Encryption Process

The decryption of the ciphertext(residues) to plain text can be done by using the same key the Chinese reminder theorem using the moduli set and the same value for n. figure 4.2 shows the decryption process.

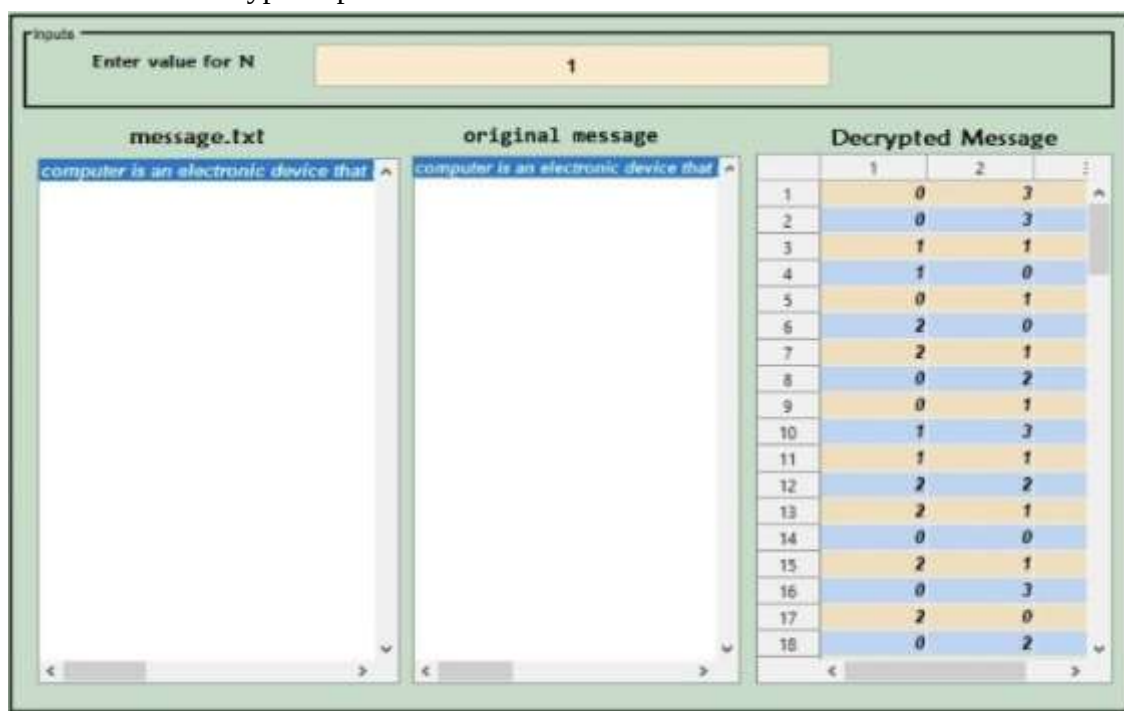


Figure 5: Decryption Process

Now, assume an attacker gets this encrypted cipher text, the knowledge of what it is will be a burden. If eventually, the attacker figures out it is a message, the moduli set will have to be determined as well as the value assigned for n .

Comparison

The proposed scheme is further compared with the traditional Caesar cipher to show the distinction in both schemes. Table 4.1 shows the comparison

Table 4.4: Comparison of Traditional Caesar cipher with proposed scheme

<i>TRADITIONAL CAESAR CIPHER</i>	<i>PROPOSED SCHEME</i>
It shifts all characters linearly by a constant key.	Swaps each character to a decimal equivalent on the character table
It retains a language's qualities.	It uses residues which total changes the representation of the message
It's incredibly simple to put into action.	It is relatively tough to put into practice.
Using brute force, it just takes 26 key combinations to crack it.	It takes knowing the moduli set, value of n and the character table to break the scheme

Conclusion

The proposed scheme has provided a better means of sending messages securely over a network while the message maintains a high level of secrecy, proving to outperform its predecessors in terms of secrecy attached to the message, the stages and complexity involved while attaining a maximal result. The result of cipher-text produced in the proposed scheme is very tedious owing to trial of many possibilities such as: finding the of algorithms employed, determining moduli set, determining the value of n for the moduli set and determining the character table.

Recommendations

For the purpose of further enhancement and providing a more efficient way of sending message securely using this approach, it is important to evaluate this research using the following experiments;

- i. Use of Mixed Radix conversion with Caesar cipher algorithm.
- ii. Use of another moduli set for the scheme
- iii. Use of New Chinese Remainder Theorem with Caesar cipher algorithm

REFERENCES

- Abraham, O., & Shefiu, G. O. (2012). An improved Caesar Cipher (ICC) algorithm. *International Journal Of Engineering Science & Advanced Technology*, 2(5), 1198–1202.
- Alhassan S & Gbolagade K.A (2013). Enhancement of the Security of a Digital Image using the Moduli Set $2n-1, 2n, 2n+1$. *International Journal of Advanced Research in Computer Engineering & Technology*, 2(7).
- Al-Hazaimah, O. M. (2013). A new approach for complex encrypting and decrypting data. *International Journal of Computer Networks & Communications*, 5(2), 95-103.
- Aremu, I. A., & Gbolagade, K. A. (2017). An overview of Residue Number System . *International Journal of Advanced Research in Computer Engineering & Technology*, 6(10), 1618-1623.
- Ayushi. (2010). A Symmetric Key Cryptographic Algorithm. *International Journal of Computer Applications*, 1(15), 1-4.
- Badoni, V. D., & Jain, M. A. (2014). Chip Implementation of Text Encryption and Decryption Algorithms. *Journal of Computer Engineering*, 56-61.
- Barakat, M., Eder, C., & Hanke, T. (2018). An Introduction to Cryptography.
- Deepak, & Parveen. (2017). Modern Encryption and Decryption Algorithm based on ASCII Value and Binary Operations. *International Journal of Computer Applications*, 172(1), 30-34.
- Delfs .H and Knebl .H (2015). Introduction to Cryptography. *Springer Berlin Heidelberg*, 49 106.
- Dey, S. (2016). A New Modified Caesar Cipher Cryptographic Method Along with Bit-Manipulation to Exclude Repetition from a Message to be Encrypted. *Global Journal of Computer Science and Technology Network, Web & Security*, 90-94.
- Doshi, R., Jain, P., & Gupta, L. (2012). Steganography and Its Applications in Security . *International Journal of Modern Engineering Research*, 4634-4638.
- Ajao, J., Olufemi, O. D., & Odetunji, O. O. (2018). Offline Yoruba Handwritten Character Recognition using Freeman Chain Code and K-Nearest Neighbor Classifier. *Jurnal Teknologi dan Sistem Komputer*, 6(10), 129-134
- Gbolagade K.A (2009). A Shorter Algorithm for Efficient Residue to Decimal Conversion, *Advances in Computer Science and Engineering*, 3(2) ,147-156.
- Gbolagade K.A. and Cotozana S.D (2009). An efficient rns to binary converter using the moduli set $\{2n+1, 2n, 2n-1\}$. *Conference on Design of Circuits and Integrated Systems*.
- He .D and Zeadally S. (2015). An analysis of RFID authentication schemes for internet of things in healthcare environment using elliptic curve cryptography. *IEEE internet of things journal*, 2(1), 72-83.
- Hercigonja, Z., & gimnazija, D. (2016). Comparative analysis of cryptographic algorithms. *International Journal of digital technology & economy*, 127-134.
- Imran, E. I., & abdulkareem, F. a. (2014). Enhancement Caesar Cipher for better security. *Journal of Computer Engineering*, 1 - 5 .
- Jain, A., Dedhia, R., & Patil, A. (2015). Enhancing the security of Caesar cipher substitution method using randomized approach for more secure communication. *International Journal of Computer Applications*, 129(13), 6 - 11.
- Lubis, F. I., Simbolon, H. F., Batubara, T. P., & Sembiring, R. W. (2017). Combination of Caesar Cipher Modification with Transposition Cipher. *Advances in Science, Technology and Engineering Systems Journal*, 2(5), 22-25.
- Mohammad A. A, Abdelfatah A.T and Omaira N.A (2014). Cryptography Based Authentication Methods. *World Congress on Engineering and Computer Science*, 1(1)Vol, 6-8.
- Pinheiro, G., & Saraf, S. (2016). Improved Caesar Cipher Algorithm using multistage encryption. *International Journal of Computer Science and Technology*, 117 - 119.
- Purnama, B., & Rohayani, H. (2015). A new modified Caesar cipher cryptography method with legible Cipher-text from a message to be encrypted. *International Conference on Computer Science and Computational Intelligence*, 195 - 204).
- Siewobr H, Gbolagade K.A. (2012). An Area Efficient RNS-to-Binary Converter for the Moduli Set $\{2n, 2n+1-1, 2n-1\}$. *International Conference on Adaptive Science and Technology*, 104-107.

- Siewobr H, Gbolagade K.A, and Cotofana S.D (2014). An Efficient Residue-to-Binary Converter for the New Moduli Set $\{2n/2\pm 1, 22n+1, 2n+1\}$. *International Symposium on Integrated Circuits*.
- Srikantaswamy, S. G., & Phaneendra, D. H. (2012). Improved Caesar Cipher with random number generation technique and multistage encryption. *International Journal on Cryptography and Information Security*, 294), 39 - 49.
- Verma, P., Gaba, G. S., & Miglani, R. (2017). Diversified Caesar Cipher for Impeccable Security. *International Journal of Security and Its Application*, 11(3), 33 - 40.