ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1654

Transposition Cipher as a Solution for a Better Bank Verification Number (BVN) Security in Communication Channel

Umar, M[1]; Hassan, A[2;] Abdullahi, I[3]; Muhammad Shehu, Z[4]
[1,3,4]Department of Mathematics, Sokoto State University, Sokoto, Nigeria
[2]Department of Mathematics, Federal University Birnin Kebbi, Kebbi, Nigeria

Abstract:- BVN stands for Bank Verification Number, which is a biometric identification used in Nigeria to verify identity of bank customers, a transposition cipher is an encryption method that recognizes data sent via a communication channel in such a way, no one but the intended receiver can understand the original message. As we increasingly rely on digital channels to share and store information, it becomes crucial to prioritize information security to safeguard against unauthorized access, data breaches and cyber threats. This paper explores the principles, goals and intended outcomes of utilizing transposition ciphers as a data security measure, shedding light on its applications and benefits in protecting digital information. The data will be encrypted in two phases, in phase I, the stack method will be used and in phase II, the transposition will be applied on the data in phase I, the transposition is by using a newly constructed algebraic structure (G_p) which makes encryption and decryption possible using mathematical functions before sending the data over the communication channels, the resulted ciphertext after applying the transposition is more complex for the intruders but very simple for the intended receiver to decrypt, and the method that will be adopted is the construction of a function that can allow encryption and decryption of the data.

Keywords:- *Encryption, Decryption, Transposition, Cipher, BVN, Non Deranged Permutation.*

I. INTRODUCTION

BVN is a system of identifying people using their unique physical characteristics such as the fingerprints and face marks. BVN is an acronym for Bank Verification Number, it is a biometric identification employed throughout Nigeria in checking the true identity of bank customers to mitigate or [control] frauds "it is a 11- digit number that combines the customer's biometric data (such as his fingerprints or facial features) There have been some controversies about the security implication of having all bank accounts in different banks linked to one number, but the BVN has come to stay. Issues arose where fraudsters attempted to use the launch of the system to phish for customers' bank details. With the increasing incidents of compromise on conventional security systems (password and PIN), there is a high demand for greater security on access to sensitive or personal information in the Banking system. The BVN gives each Bank customer a unique identity across the Nigerian Banking industry that can be used for easy identification and verification at Point of Banking operations. Biometrics refers to identification of an individual based on physiological attributes- fingerprint, voice, facial features etc. To address existing challenges with identity management, the Central Bank of Nigeria, in collaboration with all Nigerian banks launched a centralized biometric identification system tagged Bank Verification Number (BVN). BVN was extensively studied by [9],[10],[24].

The Central Bank of Nigeria, in partnership with the Bankers Committee, joined forces and took a proactive approach to enhance the banking infrastructure. This brings about the initiative to create a unified bank verification system and hence introduced the Bank Verification Number (BVN) in February, 2014 in order to strengthen the banking sector and promote financial security. As part of a detailed approach to enhancing "Know Your Customer" (KYC), The BVN assigns a unique identity to each bank customer across the entire banking industry. The BVN uses the biometric authentication of a person's physical characteristics such as fingerprints , facial recognition, voice recognition or retinal scans to verify and identify individuals. The BVN system has been widely adopted in security applications across various organizations due to its superior advantages over traditional security measures like password and PINs (Personal Identification Number) which has limitations and vulnerabilities. For Nigeria's bank customer identification program, fingerprints and facial recognition have been chosen to be the preferred primary identification methods for customers with a minimum age limit of 18 years for BVN registration. However, banks managing accounts for minors or undergraduate under 18 years of age can collect necessary information to issue a BVN to these account holders as long as they comply with legal regulations and ensure data privacy and security. The Central Bank of Nigeria (CBN) has put in place a regulatory framework that outlines the rules and guidelines for BVN operations in Nigeria, these includes guidelines for standard operating procedures and a framework for managing watch-lists within the Nigerian financial system.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1654

- The Standard Operating Guidelines (SOG), provides a framework for banks to manage customers data which includes collection, updates, linking, storage and usage by banks.
- The Watch-list serve as tool to identify and track customers with a history of fraudulent activities. The watch-list serve as a centralized database keeping track record of bankcustomers identified by their BVN.
- The CBN Regulatory Framework provides a structured approach to manage the BVN system in Nigeria. These regulatory frameworks govern the activities of various stakeholders which are categorized into five (5) groups.

- *Central Bank of Nigeria (CBN)*
- *Nigeria Inter-Bank Settlement System (NIBSS)*
- *Deposit Money Banks (DMBs);*
- *Other Financial Institutions (OFIs) and*
- *Bank Individual Customers*

And each group has the role for which it'll be responsible for which are listed below categorically

- *Central Bank of Nigeria (CBN): The CBN is Responsible for:*

- Setting the Regulatory Framework and Standard Operating Guidelines for the BVN system
- Authorizing access to the BVN database for eligible users.
- Ensuring the full implementation and successful achievement of the BVN initiative objectives.
- Overseeing the operations of NIBSS, Deposit Money Banks (DMBs) and Other Financial Institutions (OFIs) regarding BVN.
- Monitoring all stakeholders to guarantee compliance.

- *Nigeria Inter-Bank Settlement System (NIBSS): The NIBSS is Responsible for:*

- Collaborating with stakeholders to develop and review the standard operating guidelines for the BVN system.
- Initiating reviews of guidelines as needed, subject to CBN approval.
- Ensuring hitch-free operation of the BVN system.
- Maintaining and managing the BVN database
- Controlling access to the database for approved
- Directing request for BVN information to the CBN.
- Furnish CBN, DMBs and OFIs with regular reports on customers on the watch-list
- Ensuring the protection and storage of BVN information.

- *Deposit Money Banks (DMBs) and the Other Financial Institutions (OFIs): The DMBs and OFIs are Responsible for:*

- Accurate BVN data capture and validate same before linking it to customer accounts.
- Ensuring all operated accounts are associated with the correct owner's BVN.
- Identifying and reporting suspicious BVN activity to NIBSS for updates to the central watch-list database.

- *Bank Customers:*

Bank customers are required to adhere to the rules and operating guidelines governing the Bank Verification Number (BVN) system and the watch-list for the Nigerian financial system.

- *The BVN Processes/Procedures*

These are as listed below:

- Enrollment: This is the initial step where individuals undergo biometric and demographic data capture, which is then stored in the central BVN database, and a unique identification number known as the Bank Verification Number (BVN) is created for each individual.
- Identification: This involves verifying an individual's biometric data against the existing biometric data of all enrolled customers in the database to avoid duplicate enrollment and ensure a unique BVN is issued.
- Verification: This is the process of checking if a customer's biometric data matches the data stored in the database. It involves 1:1 comparison of an individual's biometric data with the biometric data of the enrolled customers associated with the same BVN, to confirm their identity and ensure that the person is indeed the owner of the BVN.
- Associating a customer's unique ID with all their bank accounts: This process involves using the unique ID generated during enrollment to link all the customer's bank account regardless of the bank where the account is held. This facilitates the sharing of information between banks to detect report and prevent fraudulent activities.
- Offline Authentication: This process enables the verification of a customer's identity using their biometric data (fingerprints or facial geometry) stored on their e-identity card without requiring an internet connection, making it possible to authenticate customers even in areas with limited or no network coverage.
- Fraud Management: This process utilizes a unique and traceable customer identifier to track, prevent, detect and minimize the risk of financial fraud in the industry.
- Customer Information Update: Is the process by which customers can make changes to their personal details such as address, phone number, or biometric data in the central identity database, to ensure that their records remain accurate and up to date.
- Credit Check: This is the evaluation of a borrower's creditworthiness to ensure they can repay a loan. Banks are required to regularly report credit information to the credit bureau, including details of loan granted to customers and other relevant credit data, in accordance with approved credit rating guidelines in order to prevent lending risks.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1654

- In mathematics, the term permutation has two distinct meanings:

✓ A specific ordering or sequencing of the elements in a set, where each element is arranged in a particular linear order.
✓ The process of rearranging the elements of an already ordered set. Permutation was studied by [22],[20],[12],[7],[18] and many discoveries and findings were been developed.

To highlight the first meaning, we can see that the concept of permutations is exemplified by the six permutations (orderings) of the set {1, 2, 3}: written as tuples, they are (1, 2, 3), (1, 3, 2), (2, 1, 3), (2, 3, 1), (3, 1, 2), and (3, 2, 1). Anagrams of a word with distinct letters are also a type permutation, as they rearrange the original letters to form a new ordering. The letters in the original word are already in a specific order and the anagram reorganizes them to create a new arrangement.

Permutations of finite sets are explored Combinatorics , which deals with counting and arranging objects and Group theory, which explores symmetry and transformations. Permutations are a fundamental concept with versatile applications, influencing a wide range of mathematical areas and scientific fields, including statistics, computer science, biology and more. In computer science, permutation are valuable tool used to assess the efficiency of sorting algorithms, in quantum physics, to describe the states of particles at the atomic and subatomic level, and in biology, to analyze and understand the sequences of RNA molecules. The number of permutations of n distinct objects is n factorial, usually written as n!, which means the product of all positive integers less than or equal to n. Under the second definition, a permutation of a set S is a one-to-one correspondence between S and itself. That is a bijective function from that maps each element of S to exactly one other element in S serving as the image of exactly one other element. Such a function $\sigma: S \to S$ is equivalent to the rearrangement of the elements of S in which each element is replaced by the corresponding $\sigma(1)$. For example, the permutation (3, 1, 2) is described by the function σ defined as $\sigma(1) = 3,\ \sigma(2) = 1,\ \sigma(3) = 2$ The set of all possible permutations of a given set forms a mathematical structure called the symmetric group. The group operation combining two permutations is the composition of functions (rearranging elements according to one permutation and then rearranging them according to another permutation), which results in another function. The properties of permutations are invarientto the type of elements being permuted, and only depend on the cardinality (size) of the set being permuted regardless of the elements nature or identity, so one can consider the standard set $S = \{1,2,3, \ldots n\}$. In basic combinatorics, an n-permutations, or partial permutations, refers to a specific ordering or sequence of n-unique elements chosen from a larger set, where the order of the selected elements matters. When the number of the selected elements (n) is equal to the total number of elements in the set, these permutations become the same as the previous permutations. Permutations called hexagrams were used in China in the I Ching (Pinyin: Yi Jing) as early as 1000 BC. In Greece, Plutarch wrote that Xenocrates of Chalcedon (396–314 BC) discovered the number of different syllables possible in the Greek language. This would have been the first attempt on record to solve a difficult problem in permutations and combinations. Al-Khalil (717–786), an Arab mathematician and cryptographer, wrote the Book of Cryptographic Messages. It contains the first use of permutations and combinations, to list all possible Arabic words with and without vowels. The rule to determine the number of permutations of n objects was known in Indian culture around 1150 AD. The Lilavati by the Indian mathematician Bhāskara II contains a passage that translates as follows: The product of multiplication of the arithmetical series beginning and increasing by unity and continued to the number of places, will be the variations of number with specific figures. In 1677, Fabian Stedman described factorials when explaining the number of permutations of bells in change ringing. Starting from two bells: "first, two must be admitted to be varied in two ways", which he illustrates by showing 1 2 and 2 1. Then explains that with three bells there are "three times two figures to be produced out of three" which again is illustrated. His explanation involves "cast away 3, and 1.2 will remain; cast away 2, and 1.3 will remain; cast away 1, and 2.3 will remain". Then moves on to four bells and repeats the casting away argument showing that there will be four different sets of three. Effectively, this is a recursive process. He continues with five bells using the "casting away" method and tabulates the resulting 120 combinations. At this point he gives up and remarks: Now the nature of these methods is such, that the changes on one number comprehends the changes on all lesser numbers, ... insomuch that a complete Peal of changes on one number seem to be formed by uniting of the complete Peals on all lesser numbers into one entire body, Stedman widens the consideration of permutations; he goes on to consider the number of permutations of the letters of the alphabet and of horses from a stable of 20. A first case in which seemingly unrelated mathematical questions were studied with the help of permutations occurred around 1770, when Joseph Louis Lagrange, in the study of polynomial equations, observed that properties of the permutations of the roots of an equation are related to the possibilities to solve it. This line of work ultimately resulted, through the work of Évariste Galois, in Galois theory, which gives a completed description of what is possible and impossible with respect to solving polynomial equations (in one unknown) by radicals. In contemporary mathematics, numerous problems across various areas of study require examining specific permutations to gain insight and understanding in unraveling complex mathematical concepts and resolving related issues. Permutations played a vital role in the cryptanalysis, for instance the Enigma machine used permutations to scramble messages, but cryptal analyst like Alan Turing and his team were able to understand and exploit these permutations to break the code giving the Allies valuable insights into Nazi communications and contributing to the war's outcome. In particular, one important property of permutations, namely, that two permutations are conjugate exactly when they have the same cycle type, was used by cryptologist Marian Rejewski to break the German Enigma cipher in turn of years 1932-1933. Cryptography was studied by many researchers

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1654

such as [1],[2],[3],[4],[5],[6] and many dimension was introduced such as symmetric key cryptography and asymmetric key cryptography and also [8],[14],[15],[16],[17],[18] discovers many applications of cryptography that can be used to secure an information.

Cryptography was derived from two Greek words "Kryptos" which means "Hidden or Secret" and "Graphein" "to write" which is the art and science of making communication. Cryptography is a method or technique by which a message can be altered so that it becomes meaningless to anyone else but the intended recipient. This is done primarily in two basic ways, one is to change the position of letters or words in a message known as "Transposition" and the other is by substituting letters or words by different ones, known as "substitution" respectively. The science of encryption and decryption can be traced back all the way to year 2000BC in Egypt. In 2010, using the concept of Catalan numbers the scheme for prime numbers $(p \geq 5)$ was developed. They defined the generating function for $\boldsymbol{G_p} = \{w_1, w_2, \dots, w_{p-1}\}$ for $p \geq 5$ such that $w_i = \left((1)(1+i)_{mp}(1+2i)_{mp} \dots (1+(p-1)i)_{mp}\right)$ where $m_p \coloneqq modulo_p$. Many algebraic properties of $\boldsymbol{G_p}$ was been investigated.

In this paper, application of $\boldsymbol{G_p}$ was used in order to make the BVN more secure over the communication channel such as social media, emails, etc. Cryptography is divided into two types, Symmetric key and Asymmetric key cryptography. In Symmetric key cryptography single key is used between the sender and receiver, while the Asymmetric key cryptography each user is assigned a pair of keys, a public key and a private key, the public key is made known to all members, while the private key is hidden by the user (sender), the sender uses the public key to encrypt the message, while the receiver uses his own hidden (private) key to decrypt the message. In this work, we consider Symmetric key cryptographic approach.

II. PRELIMINARIES

Let Ω be a non-empty subset of ℕ, totally ordered and finite. Let $\boldsymbol{G_p} = \{w_1, w_2, \dots, w_{p-1}\}$ be a setting in which each w_i is obtained from the arbitrary set Ω for any prime number $p \geq 5$, given by:

$$w_i = \left((1)(1+i)_{mp}(1+2i)_{mp} \dots (1+(p-1)i)_{mp}\right)$$

Thus, each w_i is called a cycle and the elements in each w_i refers to successors and are distict.

➢ *Example*

Using the above setting, if p=11, then we have $\boldsymbol{G_{11}}$ as $\boldsymbol{G_{11}} = \{w_1, w_2, \dots, w_{10}\}$ where Since 0 and 5 in modulo5 are equivalent, thus instead of using 0 in $modulo_p$ we will be using p.

- Cipher: - Is a method of transforming a message to conceal its meaning.
- Encryption: - Is the process of encoding an information in such a way that only intended parties can access the meaning of the coded text (ciphertext).
- Decryption: - is the process of transforming the ciphertext into a plaintext.
- Plaintext: - is the original text from the sender's end.
- Padding: - padding is the addition of characters in the encryption process if the letters are scarce, the padding letter is usually X.
- KEY: - a key is a relatively small logical amount of information that is used by an algorithm to customize the transformation of a plaintext into the ciphertext and vice versa during the encryption and decryption process.
- TRANSPOSITION CIPHER: - ciphertext is obtained by interchanging the position of each or some of the letters of a plaintext.
- Example of transposition cipher is as follows.
- Plaintext: COMPRESSING

Table1: Plaintext

1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
C	O	M	P	R	E	S	S	I	N	G

Table 2: Cipher Text

1	**3**	**5**	**7**	**9**	**11**	**2**	**4**	**6**	**8**	**10**
C	M	R	S	I	G	O	P	E	S	N

➢ *The Ciphertext is "CMRSIGOPESN".*

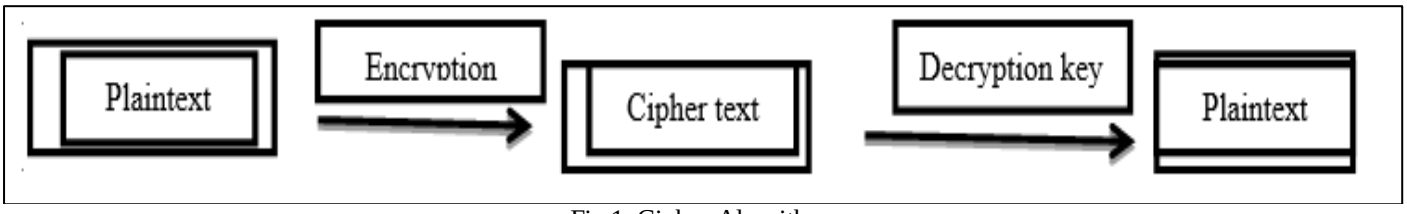

Fig 1: Cipher Algorithm

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1654

The above diagram represents Encryption and Decryption process of a Symmetric key cryptography.

➢ *Experimental Result*

- Let PT be a plaintext
- Let C_n be the ciphertext (n=1,2)
- Let i be the key

➢ *The Encryption Process will take the Following Steps.*

- Stack PT to produce C_1
- Apply encryption function of G_p on C_1 to produce C_2, where the C_2 is the ciphertext to be sent to the receiver.
- The encryption function is given by
  $C_2: w_1 \rightarrow w_{1+i}$, $i < p-1$,.

➢ *The Decryption Process will use the Following Steps.*

- Apply the decryption function of G_p on C_2 to produce stacked ciphertext (C_1).
- The decryption function is given by
  C_1: $w_{1+i} \rightarrow w_1$
- Reverse the stacking process to produce PT.

III. ILLUSTRATION

Let:
PT: 22214546780

Where PT is a plaintext containing a BVN of which the encryption is to be apply to.

➢ *Encryption Stage:*

- Stack PT to produce C_1. where C_1 is 08764541222
- Applying encryption function of Gp on w_1 (p=11, number of characters and *p* is always a prime,)

$$G_{11} = \{w_1, w_2, w_3, \dots, w_{10}\}$$

Where

$$w_1 = (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11)$$
$$w_2 = (1\ 3\ 5\ 7\ 9\ 11\ 2\ 4\ 6\ 8\ 10)$$
$$w_3 = (1\ 4\ 7\ 10\ 2\ 5\ 8\ 11\ 3\ 6\ 9)$$
$$w_4 = (1\ 5\ 9\ 2\ 6\ 10\ 3\ 7\ 11\ 4\ 8)$$
$$w_5 = (1\ 6\ 11\ 5\ 10\ 4\ 9\ 3\ 8\ 2\ 7)$$
$$w_6 = (1\ 7\ 2\ 8\ 3\ 9\ 4\ 10\ 5\ 11\ 6)$$
$$w_7 = (1\ 8\ 4\ 11\ 7\ 3\ 10\ 6\ 2\ 9\ 5)$$
$$w_8 = (1\ 9\ 6\ 3\ 11\ 8\ 5\ 2\ 10\ 7\ 4)$$
$$w_9 = (1\ 10\ 8\ 6\ 4\ 2\ 11\ 9\ 7\ 5\ 3)$$
$$w_{10} = (1\ 11\ 10\ 9\ 8\ 7\ 6\ 5\ 4\ 3\ 2)$$

$$C_2: w_1 \rightarrow w_{1+i},\quad i < p-1,\quad i = 2.$$
$$C_2: w_1 \rightarrow w_3$$
Where w_1 is the stack PT

Table 3: The Table Below Shows the Permutation Values of w_1

1	2	3	4	5	6	7	8	9	10	11
0	8	7	6	4	5	4	1	2	2	2

Table 4: The Table Below Shows the Permutation Values of w_3

1	4	7	10	2	5	8	11	3	6	9
0	6	4	2	8	4	1	2	7	5	2

The ciphertext to be sent to the receiver is 06428412752_2

➢ *Decryption Stage:*

- Apply the decryption function of **Gp on** the C_2 to produce C_1
  $C_1: w_{1+i} \rightarrow w_1$
- Reverse the stacking process to produce *PT*

IV. RESULT AND DISCUSSION

Encryption and decryption process goes through 2 processes, in the encryption stage, the original text(plaintext) will be encrypted twice with the stacking process and a special transposition cipher is then been applied to the stack result there by producing a ciphertext which is more complex for Brute force attackers but simply be decrypted for the intended recipient.

➢ *Mathematically the Process of Encryption and Decryption are as Follows.*

- C_1: is the stacked PT
- C_2: $w_1 \rightarrow w_{1+i}$, $i < p-1$,, Encryption state of **Gp.**
- C_1: $w_{1+i} \rightarrow w_1$, $i < p-1$,, Decryption stage of **Gp.**

REFERENCES

[1]. Pooja S and Pintu S. (2017), Enhancing security of Ceaser cipher using "Divide and Conquer Approach". *International Journal of Advance Research in Science and Engineering*. 06(02):144-150.

[2]. Fahrul I, K., Hassan F, S., Toras P and Rahmat W. (2017), Combination of Ceaser Cipher Modification with Transposition Cipher. *Advances in Science Technology and Engineering Systems Journal* .2(5): 22-25.

[3]. Rajput Y., Naik D. and Mane C. (2014), An improved cryptographic technique to encrypt text message using double encryption. *International Journal of Computer Applications* 86(6):24-28.

[4]. Shahid B. D. (2014), Enhancing the security of Ceaser cipher using double substitution method. *International Journal of Computer Science and Engineering Technology*.5:772-774.

[5]. Kashish G and Supriya K.(2013) Modified Ceaser Cipher for a Better Security Enhancement. *International Journal of Computer Application.*73:26-31

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1654

[6]. Mishra A. (2013), Enhancing security of Ceaser cipher using different methods. *International Journal of Research in Engineering and Technology.* 2(09):327-332.
[7]. Garba A. I and Ibrahim A. A. (2010), A new method of constructing a Variety of Finite Group Based on some succession scheme. *Internal Journal of Physical Science.* 2(3):23-26.
[8]. Massoud S., Sokouti B. and Saeid P. (2009), An Approach in Improving Transposition cipher System. *Indian Journal of Science and Technology.*2(8):9-15.
[9]. Clement, Adewole & Muna, Cynthia & Odumu, Victor. (2022). bvn regulatory framework and banking system stability in nigeria. International Journal of Innovative Research in Social Sciences and Strategic Management Techniques. 9. 62-79. 10.48028/iiprds/ijirsssmt.v9.i1.07
[10]. Olumayokun, Akindutire & Adewumi, Ayodeji & Oluseyi, Oniwura. (2023). Bank Verification Number and Fraud Prevention and Detection in Nigerian Banks. International Journal of Research and Innovation in Social Science. VIII. 1727-1745. 10.47772/IJRISS.2023.7934.
[11]. Ayodeji, Adewumi & Oluwamayokun, Akindutire & Oluseyi, Oniwura. (2023). Bank Verification Number and Fraud Prevention and Detection in Nigeria Banks.. 7. 10.47772/IJRISS.20.
[12]. Audu M.S. (1986), Generating Sets for Transitive Permutation groups of prime-power order. The Journal of Mathematical Association of Nigeria Abacus, 17(2), 22-26.
[13]. Ibrahim A. A. (2006), Correspondence between the Length of some Class of Permutation patterns and Primitive Elements of Automophism Group modulo n, Abacus. The Journal of mathematical Association of Nigeria, 33:143-154.
[14]. Alhassan, M. J; Hassan, A; Sani, S. and Alhassan, Y. (2021). A Combined Technique of an Affine Cipher and Transposition Cipher *Quest Journals Journal of Research in Applied Mathematics Volume 7. Issue 10 (2021) pp: 08-12*
[15]. Hassan, A; Alhassan, M. J; Alhassan, Y. and Sani, S. (2021). Cryptography as a Solution for a Better Security International Journal of Advances in Engineering and Management (IJAEM :3(12). pp: 849-853
[16]. Azzam A and Sumarsono (2017), A Modifying of Hill Cipher Algorithm with 3 Substitution Ceaser Cipher. Proceedings International Conference of Science and Engineering, Indonesia.1: 157-163.
[17]. Garba A. I, Yusuf A and Hassan A. (2018), Some Topological Properties of a Constructed Algebraic Structure. Journal of the Nigerian Association of Mathematical Physics, 45:21-26.
[18]. Garba A. I, Zakari, Y. and Hassan, A. (2019), on the fuzzy nature of constructed algebraic structure Gp. Bayero Journal of Pure and applied sciences, 12(1):146-150.
[19]. A. Hassan, A. Garko, S. Sani, U. Abdullahi and S. Sahalu (2023) Combined Techniques of Hill Cipher and Transposition Cipher. Journal of Mathematics Letters, 2023, 1, 822 www.scipublications.org/journal/index.php/jml DOI: 10.31586/jml.2023.822
[20]. Rejewski, Marian (1980). "An application of the theory of permutations in breaking the Enigma cipher". Applicationes Mathematicae. 16 (4): 543–559. doi:10.4064/am-16-4-543-559. ISSN 1233-7234.
[21]. https://www.cbn.gov.ng/out/2017/ccd/circular% 20and%20exposure% 20draft% 20on% 20the% 20framework% 20for%20bvn% 20operations%20and%20watchlist.pdf
[22]. Bacher, A.; Bodini, O.; Hwang, H.K.; Tsai, T.H. (2017). "Generating Random Permutations by Coin Tossing: Classical Algorithms, New Analysis, and Modern Implementation" (ACM Trans. Algorithms 13(2): 24:1–24:43 ed.). pp. 24–43.
[23]. Zaks, S. (1984). "A new algorithm for generation of permutations". BIT Numerical Mathematics. 24 (2): 196–204. doi:10.1007/BF01937486. S2CID 30234652.
[24]. Akyuz, M. Tony, L. W & Opusunju M. I (2019) Impact of bank verification number (BVN) on corrupt business practices in united bank for Africa in Abuja, international Journal of Management Studies and Social Science Research, 1(6), https://wwwresearchgate net / publication/338078769