ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1655

Permutation of National Identification Number for a Better 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,

Abstract:- This study proposes a new method to enhance the security of transmitting national identification number via various communication channels like SMS, email, and Box office. It introduces a permutation technique utilizing the Gamma 1 Non-Deranged Permutation group, ensuring the confidentiality of the information. By employing 11 factorial (11!) permutations, the national identification number is transformed into a mixed format for unintended recipients, yet remains easily decrypted by the intended recipient. This approach mitigates concerns regarding data interception and unauthorized access, providing a robust solution for secure information transmission across diverse media channels.

Keywords:- *NIN, Permutation, Cryptography, Factorial, Non Deranged Permutation.*

I. INTRODUCTION

National Identity Management Commission (NIMC) as a national body in Nigeria is responsible for allocating the national identity number (NIN), an 11-digit number code (e.g.: 41134789082) designed and given to Nigerians and legal residents by government irrespective of their ages. The issuance of National identification Number, a National Identity or National Insurance Number by Nigerian government is in line with the global best practices in keeping a good track record of its citizen and those who resides both in permanent and temporary basis serving government in a variety of functions. The study of identification was extensively conducted by [8],[9],[10],[11].

The distribution and allocation of National Identification Number may vary among countries but the issuance of identification number is mostly done to citizens when they reach certain legal age or at the point of birth. Unlike non-citizens whom will be given identification upon entrance of a particular country or when a permanent or temporary resident permit is obtained. In some countries the purpose of issuing such numbers may be singular but in the long run the numbers may serve a National Identity. In United State of America, for example, the use of (SSN) i.e. Social Security Number system had been introduced in order to distribute and manage social security benefits. But over time a significant expansion of the widespread use of the SSN is recorded beyond its original purpose leading to the wide range of activities such as opening bank accounts, getting credit cards, driving permit to mention but a few. However, in some countries the use of Tax Identification Number is necessary before any overseas payment procedure can be consummated; unlike in US where parameters like date of birth could serve without demanding for other nations' Tax Payer Identification Number. In countries where an established nationwide number failed to exists, the need to create their own number for each individual arise and the risk of mismatching people identity could be high.

In [6],[5],[4],[2] the study of cryptography was conducted, 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 $\boldsymbol{G_p} = \{w_i : i \in p-1\}$ such that $w_i = \left((1)(1+i)_{mp}(1+2i)_{mp} \ldots (1+(p-1)i)_{mp}\right)$ where $m_p \coloneqq modulo_p$. Permutation of Gp was studied by [7],[12],[13],[14],[15]

In this research $\boldsymbol{G_p}$ permutation group was employed to secure NIN over the communication channel such as social media, emails, box office, etc. Cryptography is divided into two, Symmetric key cryptography 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.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1655

II. PRELIMINARIES

Let $\boldsymbol{G_p} = \{w_i : i \in p-1\}$ be a structure such that each w_i is generated from the arbitrary set for any prime $p \geq 5$, using the scheme

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

Then each w_i is called a cycle and the elements in each w_i are distinct and called successors.

➢ *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 $modulo_5$ 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.
- Decryption: - Is the process of converting a data into its original form.
- Plaintext: - Is an unencrypted information pending input into cryptographic algorithms.
- KEY: - A string of characters used within an encryption algorithm for altering data so that it appears random.
- TRANSPOSITION: The process of changing objects from one position to another.
- TRANSPOSITION CIPHER: - Is an encryption technique that rearranges the position of characters without altering the characters themselves.
- Example of transposition cipher is as follows.
- Plaintext: GOVERNMENT

Table 1: Plaintext

1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
G	O	V	E	R	N	M	E	N	T

Table 2: Transposition

1	3	5	7	9	10	2	4	6	8
G	V	R	M	N	T	O	E	N	E

The resulting transposition will be "**GVRMNTOENE**". The cipher process is given by the figure below:

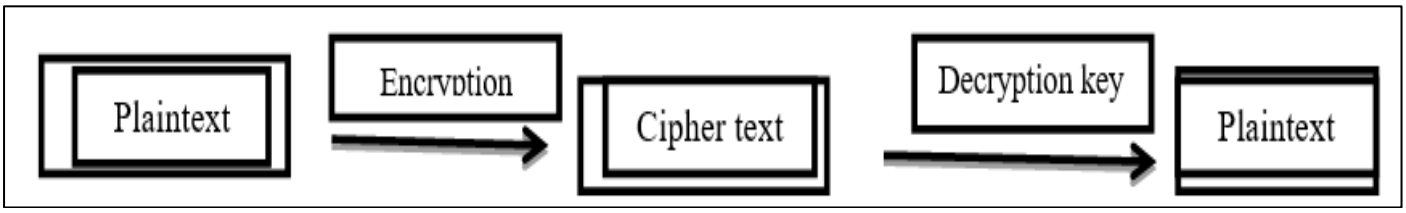

Fig 1: Cipher Algorithm

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

➢ *Experimental Result*

- Let PT be a plaintext
- Let **C** be the ciphertext
- Let i be the key

➢ *The Encryption Procedure to Take the Following Stages.*

- Applying encrypted function of G_p on PT will yield C, where the C is the ciphertext to be sent to the receiver.
- The encrypted function obtained is given by

$$C: w_1 \rightarrow w_{1+i}, \quad i < p-1$$

➢ *The Decryption Procedure to Take the Following Stages.*

- Reverse the encrypted function of G_p on C to obtain stacked ciphertext PT.
- The reversed function obtained is given by

$$PT: \quad w_{1+i} \rightarrow w_1$$

By producing the PT the receiver can then use the national identification number used.

III. ILLUSTRATION

Let:
PT: **35789426315**

Where PT is a plaintext containing the NIN in which the encryption algorithm is to be applied.

➢ *Encryption Stage*

Applying encryption function of G_p 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

$$w_1 = (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11)$$
$$w_2 = (1\ 3\ 5\ 7\ 9\ 11\ 2\ 4\ 6\ 8\ 10)$$
$$w_3 = (1\ 4\ 7\ 10\ 2\ 5\ 8\ 11\ 3\ 6\ 9)$$
$$w_4 = (1\ 5\ 9\ 2\ 6\ 10\ 3\ 7\ 11\ 4\ 8)$$
$$w_5 = (1\ 6\ 11\ 5\ 10\ 4\ 9\ 3\ 8\ 2\ 7)$$
$$w_6 = (1\ 7\ 2\ 8\ 3\ 9\ 4\ 10\ 5\ 11\ 6)$$
$$w_7 = (1\ 8\ 4\ 11\ 7\ 3\ 10\ 6\ 2\ 9\ 5)$$
$$w_8 = (1\ 9\ 6\ 3\ 11\ 8\ 5\ 2\ 10\ 7\ 4)$$
$$w_9 = (1\ 10\ 8\ 6\ 4\ 2\ 11\ 9\ 7\ 5\ 3)$$
$$w_{10} = (1\ 11\ 10\ 9\ 8\ 7\ 6\ 5\ 4\ 3\ 2)$$
$$C: w_1 \rightarrow w_{1+i}, \quad i < p-1, \quad i = 4.$$

$$C: w_1 \rightarrow w_5$$

Where w_1 is the PT

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1655

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

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

Table 4: The Table Below Shows the Permutation Values of w_5

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

The ciphertext to be sent to the receiver is **34591837652₄,** where the subscript ₄ is to be used as a key for the decryption process.

➢ *Decryption Stage*

Reverse the encryption of **Gp** on the C to get PT

$$PT\colon\ w_{1+i} \rightarrow w_1$$

Table 5: The Table Below Shows the Permutation Values of w_5

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

The table above is the table of permutation of NIN digits in which the sender is assumed to receive then use the decryption method and decode the coding process to use the original NIN numbers which was intended for concealing.

➢ *The Decryption Takes Place in Two Forms.*

- Identifying the key
- Using the key to decode the message

From (i) above, the message is **34591837652₄** and the subscript is **4** which is the key used in the encoding process, and then we move to item (ii).

- $PT\colon\ w_{1+i} \rightarrow w_1,$ where $(i = 4)$
- $PT\colon\ w_{1+4} \rightarrow w_1 \vdots\ \ w_{4-1} \rightarrow w_1$
- And w_1 is the final arrangement of the letters.

Table 6: Transposed NIN

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

Table 7: Decoded NIN

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

The above tables indicate the arrangements of the encoded and decoded NIN looks from the sender and receivers end.

IV. RESULT AND DISCUSSION

Encryption and decryption process goes through 2 processes, in the encryption stage, the original text(plaintext) will be encrypted with a special transposition cipher, then, there by producing a ciphertext which is more complex for cyber attackers but its easier for decryption by the intended recipient.

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

- $C\colon\ \ w_1 \rightarrow w_{1+i},\ \ i < p-1,$, Encryption state of **Gp.**
- $PT\colon\ \ w_{1+i} \rightarrow w_1,\ \ i < p-1,$, 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.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1655

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

[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]. Vukašin, G and Sandra, O (2024) Group Processes & Intergroup Relations Active rejection or passive indifference? Mixed-methods evidence on national (dis) identification, *Group Processes & Intergroup Relations.*1–22 DOI: 0.1177/136 84302241229981

[9]. Rajendra K. B, Uzma B, Nupura V, Vidya K, Pramod R. C and Sushma G (2018) Proposing national identification number on dental prostheses as universal personal identification code – A revolution in forensic odontology, *Journal of Forensic Dental Sciences* . Vol 7 / Issue 2 pp:84-89

[10]. Osita, E (2023) Understanding the Mandatory use Of National Identification Number in Nigeria. https://www.Researchgate.net/publication/375963871

[11]. Maya B-W., Ella D., Einat, E. Noga, S and Peter F. T (2024) Values and National Identification in Minority and Majority Youth: Longitudinal Multi-Study Findings. Journal of Youth and Adolescence https://doi.org/10.1007/s10964-024-01965-0 pp:1-18

[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