Mustansiriyah Journal of Pure and Applied Sciences, Print ISSN: 2957-9910. Online ISSN: 2957-9929, Vol. 3, No. 3, 2025, Pages 10-17
DOI: 10.47831/mjpas.v3i3.265

MJPAS

MUSTANSIRIYAH JOURNAL OF PURE AND APPLIED SCIENCES

Journal homepage:
https://mjpas.uomustansiriyah.edu.iq/index.php/mjpas

RESEARCH ARTICLE - MATHEMATICS

New Encryption Systems using Modules and their Application for Affine cipher

Khudhayer.O.Kadem[1]*

[1] *Ministry of Education-Babylon Education Directorate, Babylon, Iraq.*
* Corresponding author E-mail: Khudhayer1981@gmail.com

Article Info.

Article history:

Received
12 July 2024

Accepted
1 August 2024

Publishing
30 June 2025

Abstract

A triple vertex path graph MG(Z_n) Depending on the modules and submodules is the focal point of this work, which uses the affine cipher to construct the hybrid symmetric encryption method. The security level of the suggested MG(Z_n)-Affine symmetric encryption techniques is higher than that of the earlier ES schemes modules and submodules are used in the form of keys depending on the number of characters in the cipherr text. The cipherr text of the plaintext is communicated to the recipient entity as the MG(Z_n) graph in suggested MG(Z_n) systems. The suggested MG(Z_n) schemes' study cases are shown as fresh experimental findings. The suggested MG(Z_n) schemes' security vulnerabilities are identified. The MG(Z_n) systems to offer fresh perspectives on more secure communication.

The official journal published by the College of Education at Mustansiriya University

Keywords: Module, Submodule, Cryptography, Graph theory, MG(Z_n) graph, Security.

1. Introduction

In this work, we will use the graph, modules and their properties as a new beginning for developing some encryption systems. Ustimenko published a paper in 2001 that used graphs as symmetric encryption methods [1]. Also in 2002, the same researcher presented an encryption method similar to the classical linear cipher scheme [2]. In 2009, Jiang, et al., introduced a new encryption method based on public key cryptography and graph coloring. [3]. In 2007, Mittenthal, proposed a special method for finding Latin squares and its applications [4]. In 2012, Selvakumar and Gupta presented a new algorithm for encryption using continuum graphs [5], in the same year, Yamuna,et al, introduced encryption using Hamiltonian path properties [6]. Also, in 2013, Cheema, et al., proposed a network security using the graph theory [7]. Furthermore, in 2013, Yamuna, et al., introduced the encryption of a binary string using the music notes and graph theory [8]. In 2017, Ahmed and Babujee introduced an encryption scheme through the labeled graphs using the strong face bimagic labeling [9]. As of late, within 2019, Ruma Ajeena proposed two research. the first one is her chapter on using other graphs or the sub-graphs H of the graphs G to directly represent a scalar v in elliptic scalar multipliecation vP [10], Additionally, in [11], In her paper, she discussed how to use the graphs to accelerate elliptic scalar multipliecation algorithms. In 2018 clear up Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. More details about the method affine cipher [12]. Also, in 2019. Jaya Shruthy, and V. Maheswari created a twofold encryption method for secret text utilizing the Vigenere cipher and difference labelling of signed graphs [13]. In 2022, H. Ibrahim, et al furnished a starting point for a cyclic near-resolvable (v-1/2)-cycle system of a complete graph and offered a method for a new triple system known as a Butterfly triple system [14]. In 2023, Wanbo and others also used a new encryption method based on a 3D nonlinear system [15]. Furthermore, Huda and others proposed a method to encode color images using DNA [16]. The table was used [17]. As for the modules, a study was conducted by Ameri, R., in 2003 [18]. It was also studied prime sub module by Athab in 1996 [19]. The modules were also studied in more detail by C. P. Lu, in 1997 [20]. In this work, New variants of the hill symmetric encryption techniques are designed using MG($\boldsymbol{Z_n}$) graph as a key point depending on the modules. This work's outline comprises. 2: It includes proposing a new definition for graph encryption based on modules MG($\boldsymbol{Z_n}$). 3: Contains examples to clarify the new definitions of the graphs known as MG($\boldsymbol{Z_n}$) and its application in encryption systems using modules and some of their characteristics. 4: Demonstrates the use of MG($\boldsymbol{Z_n}$) in

* khudhayer1981@gmail.com

hybrid symmetric encryption methods by affine. 5: Displays the security of encryption for the proposed system MG($\boldsymbol{Z_n}$). Finally, displays the conclusions.

2. The Module in a Triple Vertex Graph.

In this work, a new definition of the graph was presented to develop some encryption schemes using modules. We will rely on the values of the English Alphabetic (EAVs) and the ASCII values as follows:

Definition 2.1. Let G (V, E) be a path graph (Z_n) such that Z_n is a module of order n, with n ≥ 3. The Module triple vertex (MG(Z_n)) is a graph whose vertex set V such that two vertices $\{a, b, c\}$ and $\{a', b', c'\}$ are adjacent if and only if $|\{a, b, c\} \cap \{a', b', c'\}| = 2$ and if $a = a'$, $b = b'$ then c and c' have edge in G as follows (odd, c') or (c,odd).

3. The MG ($\boldsymbol{Z_n}$) for symmetric encryption schemes based on (EAVs) and ASCII values.

To apply the idea of define (MG(Z_n)) to propose new encryption systems. Let $K=\{k_1, k_2, \ldots, k_n\}$ is presented in plaintext as an English phrase or word. The shared secret key Z_n between the two parties is chosen based on the module, where the number of letters in the word represents the order of the module n. We find the text or word to be encrypted by $Q_j \equiv k_j + Z_j \ (mod\ 26)$, with j=1, 2, …, n. Where the elements of the module are mentioned according to their rank, which is equal to the number of letters of the word, so that we collect the elements of the module j=1, 2, …, n with the letters of the word or text to be encryption, respectively. The process of sending the code is in the form of a path graph resulting from the cipher text Q_i for j=1, 2, …, n. The encrypted path graph (MG(Z_n)) is generated using Q_i. After the recipient receives the code in the form of a graph (MG(Z_n)), where the recipient selects the vertices of (MG(Z_n)) and takes the encrypted letters from them to form Q_j in a correct way to retrieve the original text using $k_j \equiv Q_j$ - Z_j (mod 26), with j=1,2,…,n. Finally, everything mentioned is applied to on (EAVs) and ASCII values.

Example 3.1. We will encrypt the word (PRIME) using (MG (Z_n)) depending on (EAVs).

$P \rightarrow 15$, $R \rightarrow 17$, $I \rightarrow 8$, $M \rightarrow 12$, $E \rightarrow 4$.

∵ The word consists of 5 letters.

∴ The module corresponding to the word that represents the key
$Z_5 = \{0, 1, 2, 3, 4\}$.

$Q_j \equiv k_j + Z_j \ (mod\ 26)$

In other words,

$Q_1 \equiv K_1 + Z_0 \ (mod\ 26) \equiv 15 + 0 \ (mod\ 26) \equiv 15 \rightarrow P$

$Q_2 \equiv K_2 + Z_1 \ (mod\ 26) \equiv 17 + 1 \ (mod\ 26) \equiv 18 \rightarrow S$

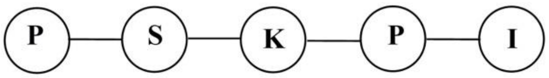
$Q_3 \equiv K_3 + Z_2 \ (mod\ 26) \equiv 8 + 2 \ (mod\ 26) \equiv 10 \rightarrow K$

$Q_4 \equiv K_4 + Z_3 \ (mod\ 26) \equiv 12 + 3 \ (mod\ 26) \equiv 15 \rightarrow P$

$Q_5 \equiv K_5 + Z_4 \ (mod\ 26) \equiv 4 + 4 \ (mod\ 26) \equiv 8 \rightarrow I$

Then Q_j = PSKPI.

The path of PSKPI based on the module Z_5 is given in Figure (1).



Figuer 1. The path Z_5

Now, we find triple vertices resulting from the elements of the module corresponding to the letters Q_j. By using MG(Z_n) we get

Z_5= {P, S, K, P, I}.

PSK, PSP, PSI, PKP, PKI, PPI, SKP, SKI, SPI, KPI.

PSK ∩ PSP = KP☒☑, PSK ∩ PSI = KI☒☒, PSK ∩ PKP = SP☑☑, PSK ∩ PKI = SI☑☒, PSK ∩ PPI = ☒☒, PSK ∩ SKP = PP☒☑, PSK ∩ SKI = PI☒☒, PSK ∩ SPI =☒☒, PSK ∩ KPI = ☒☒.

PSP ∩ PSI = PI☑☒, PSP ∩ PKP = SK☑☒, PSP ∩ PKI = ☒☒, PSP ∩ PPI = SI☑☒, PSP ∩ SKP =PK☒☒, PSP ∩ SKI = ☒☒, PSP ∩ SPI = PI☒☒, PSP ∩ KPI = ☒☒.

PSI ∩ PKP = ☒☒, PSI ∩ PKI = SK☑☒, PSI ∩ PPI = SP☑☑, PSI ∩ SKP = ☒☒, PSI ∩ SKI = PK☒☒, PSI ∩ SPI = PP☒☑, PSI ∩ KPI = ☒☒.

PKP ∩ PKI = PI☑☒, PKP ∩ PPI = KI☒☒, PKP ∩ SKP = PS☒☑, PKP ∩ SKI = ☒☒, PKP ∩ SPI = ☒☒, PKP ∩ KPI = PI☒☒.

PKI ∩ PPI = KP☒☑, PKI ∩ SKP = ☒☒, PKI ∩ SKI = PS☒☑, PKI ∩ SPI = ☒☒, PKI ∩ KPI = PP☒☑.

PPI ∩ SKP = ☒☒, PPI ∩ SKI = ☒☒, PPI ∩ SPI = PS ☒☑, PPI ∩ KPI = PK ☒☒.

SKP ∩ SKI = PI☑☒, SKP ∩ SPI = KI☒☒, SKP ∩ KPI = SI☑☒.

SKI ∩ SPI = KP☒☑, SKI ∩ KPI = SP☑☑.

SPI ∩ KPI = SK☑☒.

The products of the above intersections the MG(Z_5) is given in Figure (2).

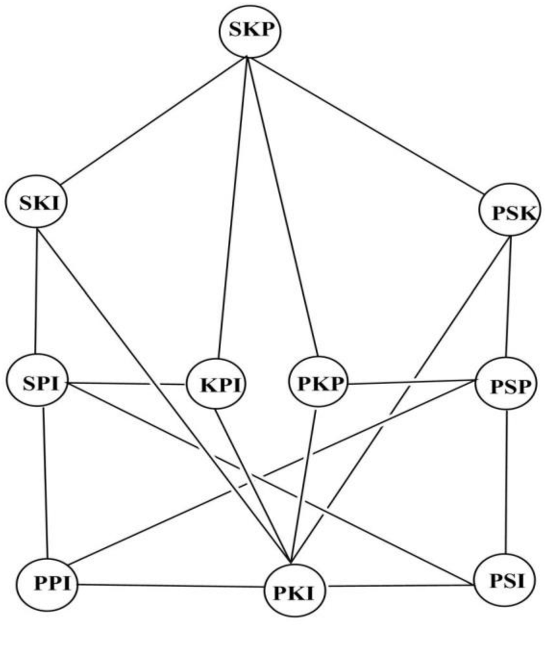


Figure 2 MG(Z_5)

To find the cipher text from above Figure, we note the following vertices PSK, PSP, PSI, PKP, PKI, PPI, SKP, SKI, SPI and KPI. There are many possibilities for choosing the correct text (PSPKI).

To decrypt Q_j = PSKPI.

$K_j \equiv Q_j - Z_j \ (mod\ 26)$

In other words,

$K_1 \equiv Q_1 - Z_0 \ (mod\ 26) \equiv 15 - 0 \ (mod\ 26) \equiv 15 \rightarrow P$

$K_2 \equiv Q_2 - Z_1 \ (mod\ 26) \equiv 18 - 1 \ (mod\ 26) \equiv 17 \rightarrow R$

$K_3 \equiv Q_3 - Z_2 \ (mod\ 26) \equiv 10 - 2 \ (mod\ 26) \equiv 8 \rightarrow I$

$K_4 \equiv Q_4 - Z_3 \ (mod\ 26) \equiv 15 - 3 \ (mod\ 26) \equiv 12 \rightarrow M$

$K_5 \equiv Q_5 - Z_4 \ (mod\ 26) \equiv 8 - 4 \ (mod\ 26) \equiv 4 \rightarrow E$

As a result, the initial message is PRIME.

4. The MG(Z_n) for an Affine Encryptions scheme based on the ASCII.

In this section, we apply the definition of MG(Z_n) in the manner affine cipher using the law $Q \equiv (uh + v)(mod\ 127)$ with the key is (u, v) such that u, v is the smallest two submodules prime numbers from the module Z_n. The decryption is done by $K(h) \equiv u^{-1}(Q - v)\ (mod\ 127)$.

Remark: If the module does not contain at least two submodules, this method of graph and encoding cannot be relied upon.

Example 4.1. We will encrypt the word (Module) using MG (Z_n) for an affine cipher depending on (ASCII).

M→ 77, 0 → 111, d → 100, u→ 117, l→ 108, e→ 101.

∵ The word consists of 6 letters.

∴ The prime submodule of the module Z_6 only (2, 3) whereas the ordered pair represents the key.

$Q(h) \equiv (uh + v)(mod\ 127)$, in other words,

$Q(M) \equiv (2\times77+3)(mod\ 127) \Longrightarrow 157(mod\ 127)=30 \rightarrow$ *record separator*

$Q(o) \equiv (2\times111+3)(mod\ 127) \Longrightarrow 225\ (mod\ 127) \equiv 98 \rightarrow b$

$Q(d) \equiv (2\times100+3)(mod\ 127) \Longrightarrow 203\ (mod\ 127) \equiv 76 \rightarrow L$

$Q(u) \equiv (2\times117+3)(mod\ 127) \Longrightarrow 237\ (mod\ 127) \equiv 110 \rightarrow n$

$Q(l) \equiv (2\times108+3)(mod\ 127) \Longrightarrow 219\ (mod\ 127) \equiv 92 \rightarrow \backslash$

$Q(e) \equiv (2\times101+3)(mod\ 127) \Longrightarrow 205\ (mod\ 127) \equiv 78 \rightarrow N$

Let *record separator* = ɤ

Then Q = ɤ$bLn \setminus N$

The path of ɤ$bLn \setminus N$ based on the module Z_6 is given in Figure (3).

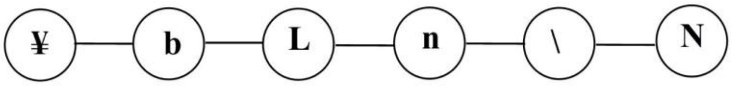


Figure 3. The path Z_6

Now, we find triple vertices resulting from the elements of the module corresponding to the letters Q as in the previous example.

The products of the above intersections the MG(Z_6) is given in Figure (4).

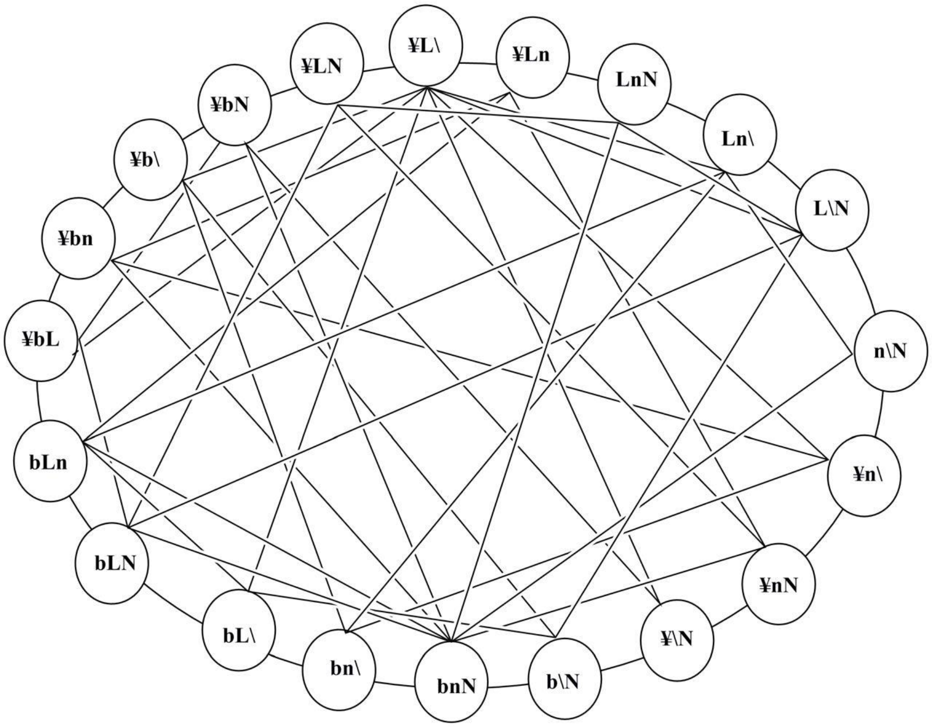


Figure 4. The MG(Z_6)

To find the cipher text from above Figure, we note the following vertices ȣbL, ȣbM, ȣb\, ȣbN, ȣLn, ȣL\, ȣLN, ȣn\, ȣnN, ȣ\N, bLn, bL\, bLN, bn\, bnN, b\N, Ln\, LnN, L\N and n\N. There are many possibilities for choosing the correct text ȣ$bLn \setminus N$

To decrypt Q = ȣ$bLn \setminus N$

$K(h) \equiv u^{-1}(Q - v)\ (mod\ 127).$

$u^{-1} = 2^{-1}(mod\ 127)=64$

$K(record\ separator) \equiv 2^{-1}(30 - 3)(mod\ 127) \equiv 1728(mod\ 127) \equiv 77 \rightarrow M$

$K(b) \equiv 2^{-1}(98 - 3)(mod\ 127) \equiv 6080(mod\ 127) \equiv 111 \rightarrow o$

$K(L) \equiv 2^{-1}(76 - 3)(mod\ 127) \equiv 4672(mod\ 127) \equiv 100 \rightarrow d$

$K(n) \equiv 2^{-1}(110 - 3)(mod\ 127) \equiv 6848(mod\ 127) \equiv 117 \rightarrow u$

$K(\setminus) \equiv 2^{-1}(92 - 3)(mod\ 127) \equiv 5696(mod\ 127) \equiv 108 \rightarrow l$

$K(N) \equiv 2^{-1}(78 - 3)(mod\ 127) \equiv 4800(mod\ 127) \equiv 101 \rightarrow e$

As a result, the initial message is Module.

5. Proposed encryption security using modules and submodules.

A covert creation of a path graph P_C that matches the cipherr text which is represented later views as the primary point of secrecy for the suggested encryption schemes. To choose the correct case that corresponds to a path graph that is encrypted and yields the original plaintext, the attackers must consider a multitude of probability possibilities. Namely, Eve must specifically guess both the shared secret key and the vertices of graph P_C The security of the shared key was increased by not setting a fixed or random key to the text using modules as the key to the cipher text. As a result, There are many possibilities to find the cipherr text from the form MG(Z_n), where the three vertices that contain the correct letters of the text must be chosen, and this requires many possibilities to guess the correct text of the cipher. Moreover, after guessing the correct text, it is necessary Eve to decode the text and calculate other possibilities to predict the key is to obtain the original text. Therefore, this method is a new beginning for more secure systems than previous methods based on modules.

6. Conclusion

This work proposed new graphs which are called MG(Z_n) graphs. The MG(Z_n) graph is used to give new contribution through proposition symmetric encryption schemes. MG(Z_n) schemes rely mainly on modules as an important code for implementing this system. MG(Z_n) schemes are more secure compared to previous schemes.

References

[1] V. Ustimenko, "Graphs as tools for symmetric encryption.," in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, 2001.

[2] V. Ustimenko, ". Graphs with special arcs and cryptography.," *Acta Applicandae Mathematica,* pp. 117-153, 2002.

[3] R. Z. a. B. Z. Z. Jiang, "A software watermarking method based on public-key cryptography and graph coloring," in *In 2009 Third International Conference on Genetic and Evolutionary Computing, pages 433–437. IEEE,* 2009.

[4] M. Lothrop, "Sequencings and directed graphs with applications to cryptography," *In Sequences, Subsequences, and Consequences,Springer,* pp. 70-81, May 31-June 2 2007.

[5] R. S. a. N. Gupta, "Fundamental circuits and cut-sets used in cryptography.," *Journal of Discrete Mathematical Sciences and Cryptography,,* vol. 15, no. 4-5, p. 287–301, 2012.

[6] G. M. S. a. M. K. M. Yamuna, "Encryption using graph theory and linear algebra. .," *International Journal of Computer Application,,* p. 5(2):102–107, 2012.

[7] S. Cheema, J. Kohli, K. Arora, S. Gupta, and S. Ahmed, " Network security using graph theory," *International Journal of Innovation in Engineering and Technology, Vol. 2,* pp. 131–138, 2013.

[8] M. Yamuna, A. Sankar, S. Ravichandran and V. Harish, "Encryption of a binary string using music notes and graph theory," *International Journal of Engineering and Technology,,* vol. 5, p. (3):2920–2925, 2013.

[9] M. A. a. J. Babujee, "Encryption through labeled graphs using strong face bimagic labeling," in *International mathematical Forum*, 2017.

[10] R. Ajeena, "The Graphs for Elliptic Curve Cryptography,”," in applied mathematics, 2019.

[11] R. Ajeena, "“The Graph and its Role for Speeding up the Elliptic Scalar Multiplication Algorithms”," in *2019 2nd international conference on engineering tehnoloy and its applications*,

Al-Najef, Iraq, 2019.

[12] D. Stinson, "Cryptography theory and practice", Chapman and Hall/CRC, 2005.

[13] S. Shruthy, V. Jaya and V. Maheswari, "“Double Encryption, Decryption Process Using Graph Labeling Through Enhanced Vigenere Cipher”," in *International Conference on Physics and Photonics Processes in Nano Sciences*, 2019.

[14] S. Karim, H. Ibrahim and H. aslinda, "“Butterfly Triple System Algorithm Based on Graph Theory”," *Journal of Information & Communication Technology,* vol. vol. 21, p. no.1, 2022.

[15] Y. Wanbo, Z. Qinwu and Z. Qingjian, "chaotic imege incryption method based on three -dimentional nonlinear system," *Mustansiriyah Journal of Pure and Applied Sciences,* vol. 1, pp. 1-27, 2023.

[16] R. Huda, A. Sadiq and A. Anwar, "A New Method for Color Imege Encryption Using Chaotic System and DNA Encoding "*Mustansiriyah Journal of Pure and Applied Sciences, Vol. 1, pp. 68-79, 2023.*

[17] J. H. a. M. Kummel, *“Ascii Table ”,* 2007.

[18] R. Ameri, "“On the Prime Submodules of Multiplication Modules”," *Interratirnal Journal of Maths. And Math. Sci,* vol. 27, pp. 1715-1724, 2003.

[19] A. Athab and A. Eman, *“Prime and Semi-Prime”,* University of Baghdad: M.Sc. Thesis, 1996.

[20] L. Chin , “Unions of prime submodules” *Houston J. Math,* vol. 23, pp. 203-213, 1997.