United International Journal for Research & Technology
Volume 04, Issue 08, 2023 | Open Access | ISSN: 2582-6832

Enhanced 3D Playfair Cipher using Bcrypt and Goldbach Code Algorithms

Johanna Mei T. Caparros[1], Ma. Angelica Joy D. Manzano[2], and Ariel Antwaun Rolando C. Sison[3]

[1,2,3]Computer Science Department, Pamantasan ng Lungsod ng Maynila, Manila, Philippines

***Abstract*—** With the rise in sophisticated cyberattacks and dependence on digital data, ensuring data security has become a significant concern. Cryptography has emerged as an effective method for protecting data, notably passwords, frequently used to authenticate and access sensitive data. Therefore, there is a need for highly secure encryption techniques to protect passwords. The paper proposes enhancing the 3D Playfair Cipher algorithm to address this issue.

The 3D Playfair Cipher is a symmetric encryption scheme that uses a substitution technique and overcomes the limitations of the classical 5x5 Playfair Cipher by utilizing a 4x4x4 matrix. The proposed enhancement further improves the encryption scheme by increasing the matrix size to 16x4x4, integrating Bcrypt hashing algorithm and Goldbach code algorithmr. The avalanche effect evaluation results show a massive improvement from the original 3D Playfair Cipher, increasing from 1.39% to 56.58%. Furthermore, since the proposed algorithm uses a 16x4x4 matrix, there are 256x64x4 = 65536 possible trigraphs, and it would take 3.73605E+94 centuries to break the ciphertext through a brute force attack. This result indicates that the proposed enhancement provides a highly secure password encryption scheme.

***Keywords*—** 3D playfair, bcrypt, cryptography, decryption, encryption, goldbach code compression, XOR.

I. INTRODUCTION

A. Background of the Study

Recently, the interest in cybersecurity increased as Internet users and organizations seek to secure their accounts, Internet, and computers from cybersecurity attacks [1] since applications and websites require users to input sensitive information. One way of securing sensitive information is through authentication systems. Hence, most applications and websites require users to create strong passwords [2]. However, some databases, online tools, and websites store passwords in plaintext format, causing data to become more vulnerable and effortless to hack [3]. Better methods are needed to secure these passwords, such as converting them into an encrypted format, as hackers have mastered password attacks and password-cracking techniques [2].

Password encryption adds another layer of security by protecting passwords stored in a server and as passwords travel across the Internet. Even strong passwords generated by a secure password generator are ineffective without password encryption since anyone with access to a server where passwords are stored can copy and use them for cyberattacks [4].

The 3D Playfair cipher algorithm is a symmetric-key encryption algorithm that uses the same key for encryption and decryption. It was developed by [5] to address the limitations of the traditional Playfair cipher. The 3D Playfair cipher utilizes a 4x4x4 matrix that accommodates 64 characters, including 26 letters of the alphabet, ten numerals, and 28 most-used special ASCII characters. It is a multiple-character or trigraphs encryption cipher encrypting a trigraph of plaintext into its corresponding trigraph of ciphertext. It involves three main processes: key-matrix generation, encryption, and decryption [5].

However, 3D Playfair cipher has the following drawbacks: the algorithm only encrypts 64 characters (26 uppercase letters of the English alphabet, ten numerals, and 28 special characters), being a deterministic algorithm wherein the same output is generated for a specific input, ambiguity of the decrypted ciphertext of the 3D Playfair cipher algorithm, and low avalanche effect.

Hence, this paper aims to enhance the limitations of data security present in the original 3D Playfair cipher.

II. RELATED WORKS

A. Authentication (Signup/Login) Systems

Authentication is a system's most crucial component [7]. Authentication technology provides access control for systems by determining whether a user's credentials match those in a database of authorized users or a data authentication server. Authentication technology ensures secure systems, processes, and enterprise

information security [8]. Hence, most applications and websites require users to create strong passwords [2].

B. 3D Playfair Cipher

Due to the limitations of the traditional Playfair cipher algorithm, the study [5] proposed a block cipher algorithm known as the 3D Playfair cipher algorithm. The 3D Playfair cipher algorithm is an enchantment of the traditional 5x5 Playfair cipher algorithm. It is a multiple-character or trigraphs encryption cipher encrypting a trigraph of plaintext into its corresponding trigraph of ciphertext. Because of this, it uses a 4x4x4 matrix to support all 26 uppercase alphabets, 19 digits, and 28 special characters. It involves three main processes: key-matrix generation, encryption, and decryption.

Like the traditional Playfair cipher algorithm, the 3D Playfair cipher algorithm is a symmetric-key method that uses the same key for encryption and decryption. The Key-matrix generation includes the following steps: First, enter the keyword, which may contain numerals, alphabets, and special characters. Next is the pre-processing of the key by dropping duplicate characters. The secret key is then arranged in the 4x4x4 matrix by floor, row (left to right), and column (top to bottom). Lastly, fill the remaining spaces in the matrix with numerals (0-9), alphabets (A-Z), and special symbols which are not part of the keyword [5].

The 3D Playfair algorithm ignores whitespace when preparing the plaintext. Then, regroup the input plaintext into trigraphs or groups of three characters. Filler letters 'X' and 'Z' are added after the first letter when one letter is left, or if any two letters are the same in a trigraph. On the other hand, the trigraph contains only two letters, the filler letter 'X' is added after the second letter. The 3D Playfair cipher differs significantly from the original Playfair encryption in how plaintext messages are encrypted. Implement the substitution process in a circular fashion wherein each letter within a trigraph gets encrypted by the same row of the letter to be encrypted, the column of its next letter, and the floor of the letter followed by its next letter [5].

To decrypt the ciphertext, reverse the encryption process. To decrypt the ciphertext, reverse the encryption process. Use the substitution technique in trigraphs. In a circular pattern, replace a letter in the trigraph with the letter from the same row, the floor of the following letter, and the column of the subsequent-to-subsequent letter. Filler letters are also dropped from the trigraph to reveal the plaintext message [5].

C. Related Studies

According to [9], it shows that implementing the XOR computation on the 3D Playfair's key and cipher can effectively authenticate the validity of the source. Furthermore, applying Message Digest Algorithm 5 (MD5) to hash the results can validate the integrity of the data.

[10] aimed to improve the efficiency and security of the cipher by utilizing the XOR operation, Left Circular Shift (LCS) method, and employing dual keys. Based on the study's results, integrating the XOR operation and LCS method increases the confusion and diffusion rate.

The study of [6] intends to deliver a more secure secret key and improve the encryption technique of the original 3D (4x4x4) Playfair cipher using the dual Cipher Block Chaining Method (CBC) method. The proposed study utilizes a 4x8x8 matrix that contains 256 ASCII characters in decimal format from 0 – 255 positioned floor by floor, row-wise, and top to bottom. Experimental results demonstrate a substantial improvement in the security performance of the proposed enhancement, surpassing other algorithms with a Strict Avalanche Criterion (SAC) of 54.17%. Furthermore, the proposed modification also passed the three randomness tests - frequency mono bit test, frequency block test, and runs test with a p-value of 0.46521, 0.54358, and 0.56685, respectively.

Based on the study of [11], produced a more secure cipher that is not vulnerable to cryptanalytic attacks using MATLAB and XOR operation. The study uses a 5x5x4 key matrix to store 100 symbols (26 lower case alphabets, 26 upper case alphabets, ten numbers, and 38 special symbols), XOR operation to double-encrypt the plaintext, and uses 'NULL' as a filler character. According to the study's findings, there was an increase in throughput and an avalanche effect of 28.11%. It indicates that the proposed algorithm provides better security against known cryptanalytic assaults.

In the study of [12], suggested a variation that extends the traditional 3D Playfair cipher into a 128x128x4 key matrix to store 65536 Unicode characters. Accordingly, the study can encrypt any language worldwide, including language characters, space, symbols, and special characters. The proposed algorithm was

encrypted and decrypted using the same method. However, a "NULL" filler character was used. The proposed method gets evaluated against cryptanalysis techniques, namely brute force attack and frequency analysis. When performing a brute force attack, the attacker must look for 4,294,967,296 different trigraphs before knowing the original message. Additionally, based on the frequency analysis results of the proposed cipher, there is a 0.0000152 chance that any given character will appear out of 65536 characters.

The study of [13] introduced a 3D generalized Playfair technique. This Playfair method relies on a 3x7x7 matrix, simultaneously encrypting three plaintext letters. The generated cipher is either an alphabetic or symbolic encryption, depending on the parameters chosen. In an alphabetic cipher, one alphabet is substituted for another, while in a symbolic cipher, the alphabet gets replaced with a symbol. When using an alphabetic cipher to encrypt plaintext, letters from the matrices X, Y, and Z will be mapped onto letters from matrices Y, Z, and X, respectively. In a symbolic cipher, if letters appear from matrices Y and Z, they will be mapped to the beneath letters of matrices Z and X. Lastly, for the hybrid cipher text, we take one letter from an alphabetic cipher and the second letter from the symbolic cipher and so on. Findings show that the proposed 3D Playfair cipher has more index shift and tremendous magnitude difference, significantly affecting the cipher's security. In conclusion, the new technique is easier to use, less complicated, and more secure against brute force attacks and frequency analysis.

III. PROPOSED METHODS

The suggested approach expands the 3D Playfair algorithm into a 16x4x4 matrix to hold 256 characters consisting of ASCII control characters, ASCII printable characters, and Extended ASCII characters. The process involves three techniques: key matrix formation, encryption, secret key encryption, and decryption. Fig. 1 shows the general step-by-step key matrix formation and encryption process using the Enhanced 3D Playfair cipher algorithm.

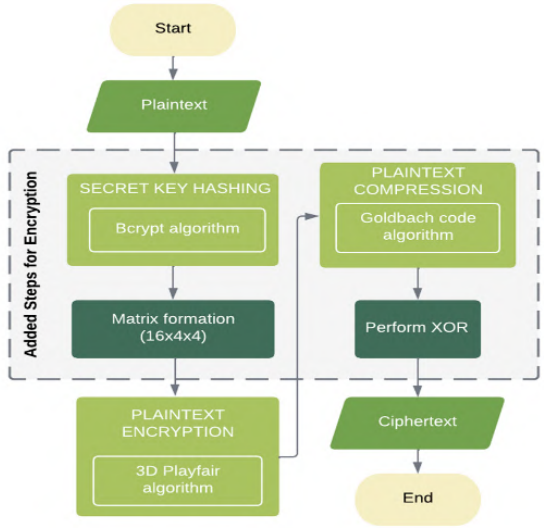

Fig. 1. *Flowchart of the Enhanced 3D Playfair Key Matrix Formation and Encryption Algorithm*

A. Key Matrix Formation of the Enhanced 3D Playfair Cipher

The proposed method uses a 16x4x4 key matrix. This matrix stores the secret key or keyword used in encryption and decryption. The key matrix can hold 256 decimal characters and applies the following rules:

To generate a key matrix, first hash the secret key "16x4x43DPlayfair!" using the Bcrypt algorithm which produces a hash value of "$2a$10$F.NMDJoFxBeWAdMWSvxGL.2bdn/fRYI7lQhm6mYbyvRmaNX9HeX1e". Next, pre-process the hashed secret key by dropping the duplicate letters and convert it into decimal format.

Then, Arrange the keyword in a 16x4x4 matrix by floor, row (left to right), and column (top to bottom).

Lastly, fill the remaining spaces in the matrix with the remaining decimals not part of the keyword.

B. Encryption Process of the Enhanced 3D Playfair Cipher

To encrypt a plaintext using the enhanced algorithm, first convert each "Hello World123!" characters into decimal format. Regroup the decimal format of the plaintext message into trigraphs or groups of three characters. Use the decimal equivalent of the "NULL" character as a filler letter. This process gives a trigraph of [[72, 101, 108], [108, 111, 32], [87, 111, 114], [108, 100, 49], [50, 51, 33]]. Next, use the 3D Playfair cipher to encrypt the plaintext. Encrypt each letter within a trigraph using the same row of the letter to be encrypted, the column of its next letter, and the floor of the letter followed by its next letter, all implemented circularly. This method can be better understood by referring to Table I.

Table I. *3D Playfair Encryption*

Plaintext Trigraph	**Plaintext Trigraph**			**Ciphertext Trigraph**
	1st Letter	2nd Letter	3rd Letter	
1st Letter	Row	Column	Floor	1st Letter
2nd Letter	Floor	Row	Column	2nd Letter
3rd Letter	Column	Floor	Row	3rd Letter

After encrypting using the 3D Playfair, the produced ciphertext was "HelCo.)DDLE7vaEMG"". Then, compress the ciphertext using the Goldbach Code algorithm. To compress the ciphertext, count the times each character appears in ciphertext and arrange the characters in order of frequency and appearance. The character that appears the most frequently should be listed first in the list encoded in G0, denoted by n = 1. To create a codeword for each character, calculate for 2(n+3) and identify two prime numbers representing the sum of two primes. To find the binary counterpart of the codeword, map the two primes to the list of prime numbers greater than 2. List all G0 codes produced based on the ciphertext. Then, group the list into 8 bits and add trailing zeros if the last group is less than 8 bits. Convert each group into its equivalent ASCII character to create the compressed ciphertext of "HelCo.)DDLE7vaEMG"" which is "r¦TGäh¡…¢SPÈDLE". Table II represents the Goldbach compression of "HelCo.)DDLE7vaEMG"".

Table II. *Goldbach G0 Code of "HelCo.)DDLE7vaEMG""*

Character	**Frequency**	**n**	**2(n+3)**	**Primes**	**Codeword**
D	2	1	8	3 + 5	11
E	2	2	10	3 + 7	101
H	1	3	12	5 + 7	011
e	1	4	14	3 + 11	1001
l	1	5	16	5 + 11	0101
C	1	6	18	7 + 11	0011
o	1	7	20	7 + 13	00101
.	1	8	22	5 + 17	010001
)	1	9	24	11 + 13	00011
L	1	10	26	7 + 19	0010001
7	1	11	28	11 + 17	000101
v	1	12	30	13 + 17	000011
a	1	13	32	13 + 19	0000101
M	1	14	34	11 + 23	00010001
G	1	15	36	17 + 19	0000011
"	1	16	38	7 + 31	0010000001

After Goldbach compression, convert the compressed ciphertext and pre-processed secret key to its binary equivalent. Then, perform XOR on the compressed ciphertext and ciphertext length on the pre-processed secret key. The result of XOR encryption is "01010110 10010100 00110101 01110110 11010100 00101110 10001111 11001011 11101111 01100100 10000010 01111111". Lastly, convert the binary output to decimal

and find its equivalent in ASCII character. After converting to ASCII characters, the final ciphertext is “V”5vÔ. Ëïd,DEL”.

C. Decryption Process of the Enhanced 3D Playfair Cipher

The decryption process of the enhanced algorithm is the reverse of the encryption process. Fig. 2 shows the general step-by-step decryption process using the Enhanced 3D Playfair cipher algorithm.

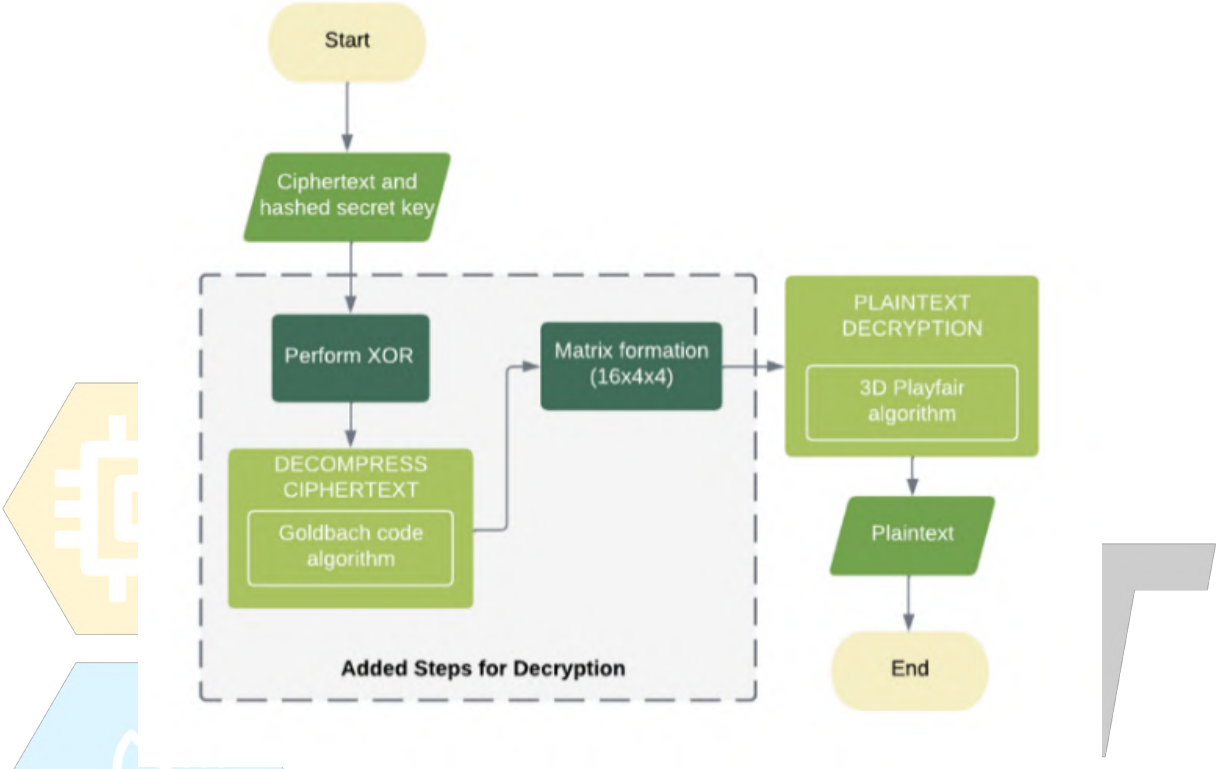

Fig. 2. *Flowchart of the Enhanced 3D Playfair Decryption Algorithm*

To decrypt the compressed ciphertext “V”5vÔ. Ëïd,DEL” first pre-process the hashed secret key, “$2a$10$F.NMDJoFxBeWAdMWSvxGL.2bdn/fRYI7lQhm6mYbyvRmaNX9HeX1e” and remove the duplicates. The pre-processed hashed secret key will result in “$2a10F.NMDJoxBeWAdSvGLbn/fRYI7lQhm6yX9H” Next, perform the XOR decryption process on the compressed ciphertext and pre-processed secret key, ensuring that the secret key has the same bit length as the compressed ciphertext. The XOR decryption will result in “01110010 10100110 01010100 01000111 11100100 01101000 10100001 10000101 10100010 00100000 11001000 00010000” in binary and “r¦TGäh¡…¢SPÈDLE” equivalent in ASCII characters.

After performing the XOR decryption process, decompress the result using the Goldbach Code algorithm. Refer to the Goldbach Code compression in Table II, which the encryption process also used. The decompression will result in “HelCo.)DDLE7vaEMG"” Afterward, convert the ciphertext and the pre-processed secret key into decimal format.

Generate the 16x4x4 matrix using the decimal format of the pre-processed hashed secret key. Arrange the key in the 16x4x4 matrix from left to right and top to bottom. Fill the spaces in the matrix with the remaining ASCII characters in a decimal format, not part of the keyword. Generate trigraphs of the decimal format of the ciphertext and use the equivalent decimal format of “NULL" as a filler letter. The trigraphs generated from the example would be [[72, 101, 108], [67, 111, 46], [41, 68, 16], [55, 118, 97], [25, 71, 34]].

Moreover, implement the 3D Playfair cipher to decrypt the ciphertext. In a circular pattern, replace a letter in the trigraph with a letter from the same row, the following letter’s floor, and the column of the next-to-next letter. This approach is presented in Table III.

Table III. 3D Playfair Decryption

Plaintext Trigraph	Plaintext Trigraph			Ciphertext Trigraph
	1st Letter	2nd Letter	3rd Letter	
1st Letter	Row	Floor	Column	1st Letter
2nd Letter	Column	Row	Floor	2nd Letter
3rd Letter	Floor	Column	Row	3rd Letter

The result from the 3D decryption will be "text." The last step is to convert the decimal format into its corresponding ASCII character value and drop the "NULL" values. Converting it to ASCII produces the original plaintext, "Hello World123!"

IV. RESULTS AND DISCUSSION

A. *Avalanche Effect Results*

The strength of any block cipher cryptographic algorithm is assessed in cryptography using the diffusion or avalanche effect [6]. It measures the notable change in ciphertext when there is a slight change in key or plaintext. Thus, an algorithm must satisfy the avalanche effect to significantly randomize the input and maintain its secrecy [14]. [15] states that "The avalanche effect close to 50% satisfies the Strict Avalanche Criterion (SAC)." The Avalanche Effect can be calculated as follow:

The researchers assessed the proposed enhancement to the 3D Playfair algorithm by comparing it to the research conducted by [18] and [19], as the papers also evaluated the enhancements using the same performance metric. To ensure a more accurate evaluation, the researchers utilized the same dataset. Table IV presents a comparison of the avalanche effect among the three algorithms.

Table IV. Comparison of Avalanche Effect

Content		Avalanche Effect		
Plaintext	Secret Key	Ferrer et al.	Villafuerte et al.	Proposed Algorithm
hello world	pass 123	54.55	51.14	52.50
	Pass 123			
Jane Doe	12345	22.22	48.61	52.08
	11345			
playfair	Secret	50	51.39	54.17
	secret			
cryptography	encrypt	0	51.14	54.17
	dncrypt			
encryption	keyword	40	55.68	55.21
	Keyword			
cryptography	encrypt	33.33	52.27	55.21
	Encrypt			
Playfair	secret	0	45.83	51.39
	secrev			
PLAYFAIR	ENCRYPT	0	52.78	57.14
	DNCRYPT			
Average		25.01	51.11	56.58

Table IV shows that the proposed algorithm gains an average of 56.18, while the work of [18] and [19] has an average of 25.01 and 51.11, respectively. Furthermore, the original 3D Playfair by [5] has a minor result, with only 1.39 [6].

B. *Brute Force Attack*

A brute force attack is a hacking technique that uses trial and error to break encryption keys, passwords, and login credentials [16]. The difficulty of brute-forcing the actual encryption key determines the strength of the encryption algorithm. The attack's success relies on key length, total characters in the set, and calculation speed

[17]. The following calculation is used to compute estimated time frame for the brute force attack:

Since the proposed algorithm uses a 16x4x4 matrix, there are 256x64x4 = 65536 possible trigraphs, so it is more challenging to execute a brute-force attack than the original algorithm. Compared to the original 3D Playfair algorithm by [5], which utilizes a 4x4x4 matrix, there are 64x16x X 4 = 4096 potential trigraphs. Since the enhancement uses a 16x4x4 matrix with a total of 256 characters, if, for instance, the length of a given plaintext is 256 characters without repetition, then there are 256! (8.578177753E+506) possible arrangements, making random guessing practically impossible [17].

The study also estimated the time for a brute-force attack to occur using a device equipped with an Intel Core i3 processor with 2 cores and 8GB of RAM.

Table V. *Result of Brute Force Attack*

Unit	Estimated Time to Crack
Seconds	1.17900E+104
Minutes	1.96500E+102
Hours	3.27500E+100
Days	1.364583E+99
Years	3.73605E+96
Decades	3.73605E+95
Centuries	3.73605E+94

Table V presents the estimated time required for successfully cracking the key using a brute-force attack. In this experiment, the researchers utilized a key length of 17, which indicates that breaking the security would demand a significant amount of time.

V. CONCLUSION AND RECOMMENDATION

The Bcrypt hashing technique and Goldbach Code algorithms are used in this study to improve the 3D (4X4X4) Playfair cipher developed by [5]. The authors expanded the key matrix to support 256 characters, including Extended ASCII, ASCII Printable, and Control ASCII characters. The Bcrypt algorithm's implementation prohibits the same plaintext from being encrypted with the same encryption key. Additionally, the enhanced algorithm successfully eliminates ambiguity by employing the "NULL" character as a filler letter. Based on experimental findings, the performance of the enhanced algorithm has significantly improved, with an Avalanche Effect of 56.58%. It also shows that the improved algorithm outperforms the improved algorithm by [18] and [19] with an increase of 31.57% and 5.47%, respectively. Brute force results also indicate that it would take decades to centuries to decipher the ciphertext produced by the improved algorithm successfully.

The researchers strongly recommend conducting a comprehensive security evaluation to assess the security performance of the proposed approach. Evaluations should encompass an extensive range of security tests, including, but not limited to, common cryptanalysis attacks such as frequency analysis and known-plaintext attacks.

ACKNOWLEDGMENT

The researchers would like to express their sincerest gratitude and extend their heartfelt appreciation to the individuals who have offered invaluable support and played significant roles in the accomplishment of this study. Their support and dedication are genuinely cherished and gratefully acknowledged.

REFERENCES

[1] S. Shea, A. S. Gillis, and C. Clark, “What is cybersecurity? everything you need to know: TechTarget,” Security, https://www.techtarget.com/searchsecurity/definition/cybersecurity (accessed May 27, 2023).

[2] G. Malviya, “Password security: Loginradius blog,” loginradius, https://www.loginradius.com/blog/engineering/password-secure/ (accessed May 27, 2023).

[3] “Dangers of storing and sharing passwords in plaintext,” PassCamp, https://www.passcamp.com/blog/dangers-of-storing-and-sharing-passwords-in-plaintext/ (accessed May 27, 2023).

[4] “What is password encryption and how much is enough?,” TeamPassword, https://teampassword.com/blog/what-is-password-

encryption-and-how-much-is-enough (accessed May 27, 2023).

[5] Kaur, H. Kumar Verma, and R. Kumar Singh, "3D(4 x 4 x 4) - playfair cipher," International Journal of Computer Applications, vol. 51, no. 2, pp. 36–38, 2012. doi:10.5120/8017-1286.

[6] R. S. Villafuerte, A. M. Sison, and R. P. Medina, "An Improved 3d Playfair Cipher Key Matrix With Dual Cipher Block Chaining Method," International Journal Of Scientific & Technology Research , vol. 8, no. 10, pp. 1013–1018, Oct. 2019. doi:https://www.researchgate.net/profile/Ritchell-Villafuerte/publication/338621994_An_Improved_3D_Playfair_Cipher_Key_Matrix_with_Dual_Cipher_Block_Chaining_Method/links/5f60d7b4299bf1d43c0594f8/An-Improved-3D-Playfair-Cipher-Key-Matrix-with-Dual-Cipher-Block-Chaining-Method.pdf.

[7] M. H. Barkadehi, M. Nilashi, O. Ibrahim, A. Zakeri Fardi, and S. Samad, "Authentication systems: A literature review and classification," Telematics and Informatics, vol. 35, no. 5, pp. 1491–1511, 2018. doi:10.1016/j.tele.2018.03.018.

[8] M. E. Shacklett and L. Rosencrance, "What is authentication?," Security, https://www.techtarget.com/searchsecurity/definition/authentication (accessed May 27, 2023).

[9] Kuo, W., Kao, W., Wang, C., & Huang, Y. (2020). 3D-Playfair Encrypted Message Verification Technology based on MD5. https://doi.org/10.1109/asiajcis50894.2020.00028.

[10] Das, A., & Das, N. (2020). Enhancement of 3D-Playfair algorithm using dual key. International Journal of Advanced Intelligence Paradigms, 15(4), 405. https://doi.org/10.1504/ijaip.2020.106036.

[11] Bala, A. (2017). Title: Enhanced 3-D PLAYFAIR Cipher. http://www.ijeam.com/Published%20Paper/Volume%2048/Issue%2001/IJES%2005/IJEAMJune2017_37_43_Anju_Abstract.pdf.

[12] M. Ahmed, S. H. Ahmed, and O. H. Ahmed, "Enhancing 3D-playfair algorithm to support all the existing characters and increase the resistanceto brute force and frequency analysis attacks," 2017 International Conference on Current Research in Computer Science and Information Technology (ICCIT), 2017. doi:10.1109/crcsit.2017.7965538.

[13] E. Elahi, H. Raza, and S. Ali, "A new 3D Playfair based secure Cipher Generation Model," 2017 13th International Conference on Emerging Technologies (ICET), 2017. doi:10.1109/icet.2017.8281719.

[14] H. T. Assafli and I. A. Hashim, "Security enhancement of AES-CBC and its performance evaluation using the Avalanche effect," International Conference on Engineering Technology and its Applications (IICETA), 2020. doi:10.1109/iiceta50496.2020.9318803.

[15] S. D. Sanap and V. More, "Performance analysis of encryption techniques based on avalanche effect and strict Avalanche criterion," International Conference on Signal Processing and Communication (ICPSC), 2021. doi:10.1109/icspc51351.2021.9451784.

[16] "What is a brute force attack?: Definition, Types & How It Works," Fortinet, https://www.fortinet.com/resources/cyberglossary/brute-force-attack#:~:text=A%20brute%20force%20attack%20is%20a%20hacking%20method,to%20individual%20accounts%20and%20organizations%E2%80%99%20systems%20and%20networks (accessed May 27, 2023).

[17] J. C. Arroyo, A. M. Sison, R. P. Medina, and A. J. Delima, "A cryptographic test of randomness, entropy, and brute force attack on the modified Playfair algorithm with the novel Dynamic Matrix," International Journal of Emerging Technology and Advanced Engineering, vol. 12, no. 6, pp. 73–83, May 2022. doi:10.46338/ijetae0622_11.

[18] J.C.C. Ferrer, F.E. De Guzman, K.L.E. Gardon, R.J.R. Rosales, D.M.D.A. Badua, and D.R. Marcelo, "Extended 10x10 Playfair Cipher," in 2018 IEEE 10th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment and Management (HNICEM), 2018, pp. 1-4.

[19] R. S. Villafuerte, A. M. Sison, and R. P. Medina, "I3d-playfair: An improved 3D playfair cipher algorithm," 2019 IEEE Eurasia Conference on IOT, Communication and Engineering (ECICE), 2019. doi:10.1109/ecice47484.2019.8942655.