Journal of Science Engineering Technology and Management Science
Volume 02, Issue 06, June 2025 *ISSN: 3049-0952*
www.jsetms.com *DOI:10.63590/jsetms.2025.v02.i06.pp16-20*

An Innovative Use of Interweaving in an Extended Playfair Cypher on DNA-Encoded Data

P. Vijay[1] and K. Srinivasa Rao[2]
Department of Electronics and Communication Engineering, KL University, Vijayawada
[1]Corresponding Author: Vijayece1223@gmail.com

To Cite this Article
Robert Stewart and Samuel Jack, "An Innovative Use of Interweaving in an Extended Playfair Cypher on DNA-Encoded Data", Journal of Science Engineering Technology and Management Science, Vol. 02, Issue 06, June 2025, pp:16-20, DOI: http://doi.org/10.63590/jsetms.2025.v02.i06.pp16-20

Submitted: 15-02-2025 *Accepted: 10-05-2025* *Published: 12-05-2025*

Abstract*: The advanced field of cryptography makes extensive use of bioinformatics together with other domains as one of its applications. The presented cypher operates by converting messages of all types—including texts and audio files and images—into sequences consisting of single-stranded DNA. A matrix of randomly generated 8x8 codon squares derived from the security key serves to encrypt series of triple codon sequences. The DNA encoding process creates such a significant difficulty that attackers cannot perform frequency analysis despite preserving the original encryption/decryption rules of traditional 5x5 Playfair. An interweaving operation should be added as a step to encrypt the sequence because it enhances unpredictability. Workers who used this approach gained multiple benefits against Playfair cypher modifications because their system encrypted all digital content types without text processing and integrated well for DNA steganography purposes. The proposed technique shows resistant behavior against cypher attacks because the original message and cipher-data bear minimal correlation between them.*

Keywords*: DNA Encryption, Cryptanalysis, Brute Force, Cypher, Codon, Interweaving, Playfair*

I. Introduction

Cryptography describes the scientific methods and procedures developed for ensuring safe communications between three or more parties. The encryption process converts plain text which represents typical information into ciphertext that appears as unintelligible nonsense through a transformation procedure shown in figure 1 [1]. A received unintelligible ciphertext gets converted back to plaintext through the decryption process. In this context the encryption and decryption algorithms known as cyphers are usually grouped together. In addition to algorithms the cipher operates through an undisclosed factor called key. The combination of present-day encryption methods and a secret key exclusive to communicating parties makes it virtually unattackable to intercept specific message content. The classification of traditional cyphers exists between transposition methods that rearrange letter positions and substitution algorithms that apply systematic letter replacements to create new coded language. The Caesar cypher represents a substitution cypher which transforms plaintext letters into different alphabetic letters that lie at specified positions lower imprudence [10].

The two fundamental encryption algorithm types currently used include public key and symmetric-key algorithms. The encryption methods known as symmetric-key cryptography utilize a single key which must be shared by both sender and recipient. Public-key cryptography operates with two different keys which share mathematical connections by using a secret private key together with a public key available for sharing [2]. As a symmetric cipher method, the Playfair uses two letters at once to perform encryption. A ciphering procedure exists with simple rules for use while the technique works through a 5 by 5 table that derives from chosen key words. The Playfair system maintains its basic nature but remains very resistant to cracking attempts that rely on frequency analysis for simple monograph substitution cyphers [11]. When functioning as an encryption method the system does not permit alphabetic characters together with punctuations or numerical symbols. Prior to encryption double-letter digraphs must be managed through space elimination in the pre-processed plain-text. The decryption process becomes complicated when dealing with long ciphertexts due to difficulties understanding the restored plaintext.

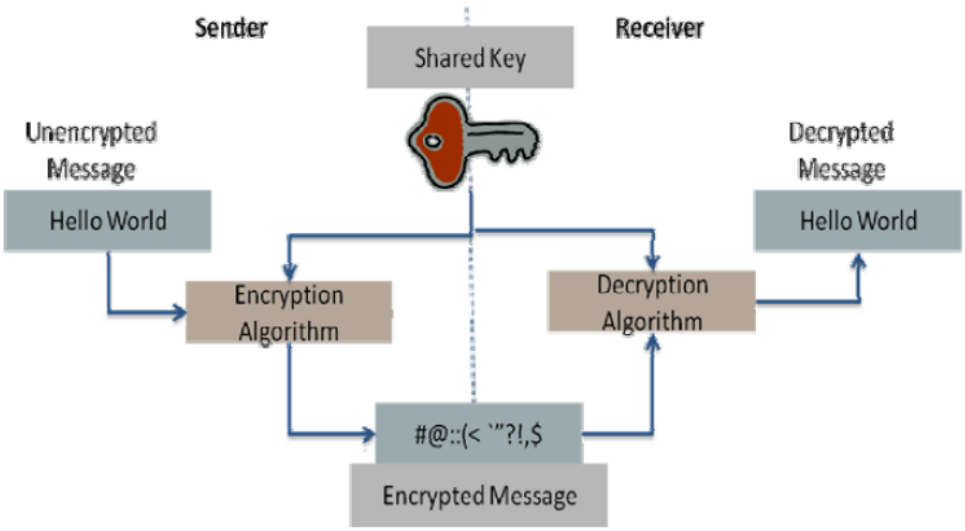


Fig 1: The encryption and decryption processes of a cipher

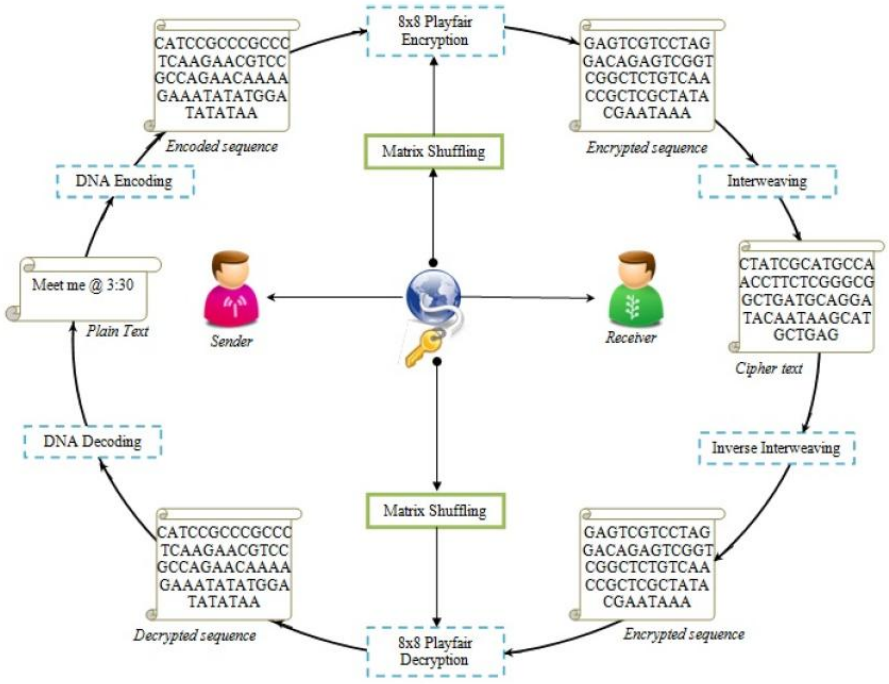
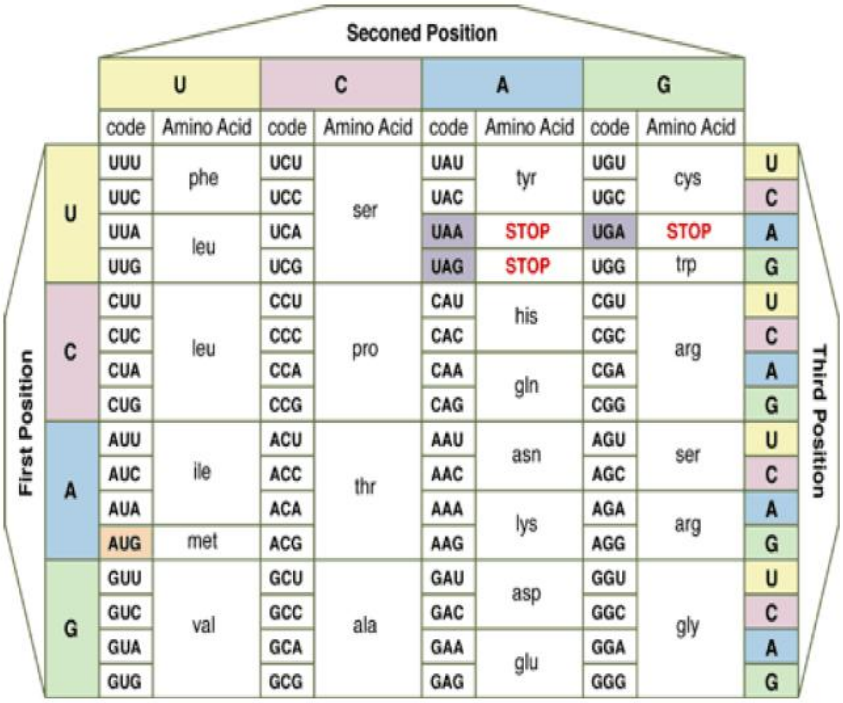


Fig 2: The general scheme of the proposed ciphering system

Additionally, the plain-text preparation phase still affects them. In this work, we suggest a new improvement on the traditional Playfair cypher that allows any type of binary data to be encrypted using the same 5x5 Playfair cypher rules. The suggested method makes it possible for cryptography to heavily utilise certain ideas from the bioinformatics domain. More precisely, the plain and encrypted texts will be handled as DNA sequences. An innovative 8x8 Playfair

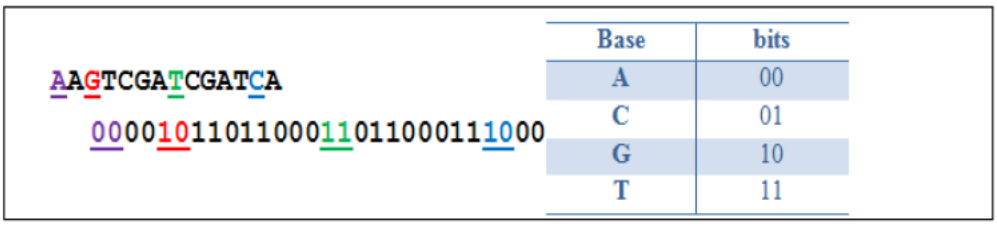
cypher based on codons will be used to encrypt and decrypt these specifically encoded sequences. Figure 2 shows the primary steps of the suggested ciphering scheme [10-11].



	U			C			A			G		
	code	Amino Acid		code	Amino Acid		code	Amino Acid		code	Amino Acid	
U	UUU	phe	U	UCU	ser	U	UAU	tyr	U	UGU	cys	U
	UUC		C	UCC		C	UAC		C	UGC		C
	UUA	leu	A	UCA		A	UAA	STOP	A	UGA	STOP	A
	UUG		G	UCG		G	UAG	STOP	G	UGG	trp	G
C	CUU	leu	U	CCU	pro	U	CAU	his	U	CGU	arg	U
	CUC		C	CCC		C	CAC		C	CGC		C
	CUA		A	CCA		A	CAA	gln	A	CGA		A
	CUG		G	CCG		G	CAG		G	CGG		G
A	AUU	ile	U	ACU	thr	U	AAU	asn	U	AGU	ser	U
	AUC		C	ACC		C	AAC		C	AGC		C
	AUA		A	ACA		A	AAA	lys	A	AGA	arg	A
	AUG	met	G	ACG		G	AAG		G	AGG		G
G	GUU	val	U	GCU	ala	U	GAU	asp	U	GGU	gly	U
	GUC		C	GCC		C	GAC		C	GGC		C
	GUA		A	GCA		A	GAA	glu	A	GGA		A
	GUG		G	GCG		G	GAG		G	GGG		G

Fig 3: The Amino Acid/codons table

This is known as degeneracy, and it indicates that certain amino acids are coded for by many codons [8]. The types of amino acid molecules are actually indicated by three-letter abbreviations like "Phe" and "Leu," as illustrated in figure 3.



Base	bits
A	00
C	01
G	10
T	11

Fig 4: Digital coding of DNA bases

II. The Proposed Algorithm

As previously stated, the suggested ciphering method offers a fresh viewpoint on the extended 8*8 Playfair cypher by utilizing the characteristics of DNA and amino acid codons. The suggested approach begins with a DNA-encoding stage, as illustrated in figure 2, and then builds the substitution matrix that will be utilized to implement the 8x8 Playfair cypher. To further improve the cipher's security, we also included an interweaving step. The steps in the encryption process are obviously reversed in the decryption procedure. In other words, a single-stranded DNA sequence is initially used to encode the binary information. The contents of the encrypted sequence are then revealed by performing the opposite of the interweaving procedure. The 8x8 grid of codons that is created using the secret key

is then used to decrypt the nucleotides of the encrypted sequence once they have been grouped into codon triplets. By converting the decoded nucleotides into their binary form, the original data's contents can eventually be revealed.

GGG	CCA	GAT	ACG	GTA	TGG	ATA	GCT
GCG	AAG	AAA	CCT	TGT	CGT	CGA	GAC
GGA	AGA	CGC	ACA	GCA	ACC	CAC	CTC
TTT	CCG	GAG	TAC	TTA	GTT	GGC	AAT
CTG	ACT	CAA	TGA	AAC	GTC	GGT	TTC
GTG	TCG	CAT	TCT	TTG	ATG	AGC	TGC
AGG	TCA	CGG	CTT	AGT	CTA	ATT	CAG
GAA	ATC	GCC	TAG	CCC	TCC	TAT	TAA

Fig 5: Resultant 8x8 matrix of codons used as a cipher key

III. Random Shuffling of the Substitution Matrix

The 8x8 matrix that will be utilized in the encryption stage must be prepared in this step. In contrast to the traditional Playfair cypher, this matrix has 64 codon-filled places. Additionally, the matrix should be built in a distinctive pattern utilizing a particular key. Using a random permutation function whose seed value is determined by the cypher key, this distributes the codons randomly around the grid. In this instance, there is no need to perform any pre-processing to the key, such as eliminating spaces or omitting any duplicate letters, and the key can be made up of any combination of characters. For instance, the 8x8 matrix of codons depicted in Figure 5 will be created using EgyRev@25Jan as the cypher key[1-2].

IV. Conclusion

Based on the 64 DNA codon table, this research suggested a new 8x8 matrix implementation of the Playfair cypher. The purpose of this improvement was to address the issues with the traditional 5x5 Playfair cypher. The suggested method's ability to cypher any type of digital message, including text, voice, graphics, etc., is a significant advantage over the traditional Playfair algorithm, which only works with English letters. Furthermore, it produces a comprehensive and accurate decrypted message without requiring any pre-processing of the plain-text. Additionally, the cipher-text can be represented in a number of formats, such as DNA and binary. It can thus be viewed as a phase of a more extensive and intricate procedure, such the concealment of information inside DNA sequences. According to a thorough cryptanalysis, the suggested cypher is nearly impossible to decipher using a brute force attack. In other words, uneven mapping between corresponding letter digraphs is provided by encoding binary messages into DNA codons. Additionally, the technique's security is increased by performing an interweaving step to the replacement sequence. Because there are fewer signs that lead to the Playfair cypher, it would be practically hard for an attacker to carry out a frequency analysis[10-11].

References

[1] David K. *The Codebreakers – The Story of Secret Writing*. 1967 New York: Macmillan.

[2] Whitfield D and EH Martin. *Multiuser cryptographic techniques*, in *Proceedings of the June 7-10, 1976, national computer conference and exposition*. 1976, ACM: New York, New York.

[3] Srivastava SS, N Gupta and R Jaiswal. Modified Version of Playfair Cipher by using 8x8 Matrix and Random Number Generation. in *IEEE 3rd International Conference on Computer Modeling and Simulatio*. 2011. Mumbai.

[4] Srivastava SS and N Gupta. A Novel Approach to Security using Extended Playfair Cipher. *International Journal of Computer Applications*. 2011; 20(6): 0975 – 8887.

[5] Sastry VUK, NR Shankar and SB Durga. A Generalized Playfair Cipher involving Intertwining, Interweaving and Iteration. *International Journal of Network and Mobile Technologies*. 2010; 1(2): 45-53.

[6] Amin ST, M Saeb and S El-gindi. A DNA-based implementation of YAEA encryption algorithm. *Computational Intelligence*. 2006: 120-125.

[7] Sabry M, et al., A DNA and Amino Acids-Based Implementation of Playfair Cipher. *International Journal of Computer Science and Information Security*. 2010; 8(3): 129-136.
[8] Crick F, Central dogma of molecular biology. *Nature*. 1970; 227: 561–563.
[9] Department of the Army. *Basic Cryptanalysis, FM 34-40-2, FIELD MANUAL*, 1990: Washington
[10] S, Samuel Johnson. "Design a Smart Active Filter for Solar Power System Using V2G." Journal of Science Engineering Technology and Management Sciences, vol. 2, no. 5, Apr. 2025, pp. 12–19. Crossref, https://doi.org/10.63590/jsetms.2025.v02.i05.pp12-19.
[11] Kuldeep Singh, "I-Slotted Rectangular Microstrip Patch Antenna Design and Analysis for Wireless Applications", Journal of Engineering Technology and Sciences, Vol. 02, Issue 05, May 2025, pp: 27-30, Crossref, http://doi.org/10.63590/jets.2025.v02.i05.pp27-30