**International Journal of Scientific Research in Computer Science and Engineering**
Vol.**12**, Issue.**4**, pp.**08-17**, August **2024**
E-ISSN: 2320-7639
Available online at: www.isroset.org

Research Article

# Examining Cryptographic Primitives and Introducing the Periodic-Shift Cipher

**Padma Sree Uma Nandini Kadavakollu[1], Sony Kumari[2], Srinivasa Rao Gundu[3*]**

[1,2]Dept. of Digital Forensics, Malla Reddy University, Hyderabad, India
[3]Dept. of Computer Sciences, Malla Reddy University, Hyderabad, India

**Corresponding Author: srinivasarao.gundu@gmail.com*

**Received**: 29/Jun/2024; **Accepted**: 31/Jul/2024; **Published**: 31/Aug/2024

***Abstract***— Cryptography is an essential element of modern digital security. It consists of techniques for translating plaintext into ciphertext and back to allow safe communication. It also serves as a foundation for critical applications such as secure internet interactions, electronic business, and data integrity authentication. This work investigates five types of cryptographic primitives: symmetric encryption, asymmetric cryptography, hash functions, and digital signatures, while examining their impact on the CIA Triangle—confidentiality, integrity, and availability. Both classical and modern advances in cryptography are discussed, tracing their evolution from classical ciphers to modern algorithms like RSA, along with the emerging threat of quantum computing. Additionally, a unique encryption technique, the Periodic-Shift Cipher B/I law, is introduced. Designed for educational purposes, it emphasizes simplicity and security, using only odd-numbered shifts and the new "a=z" rule. This article reviews some of the positives and negatives of this architecture and suggests areas for further investigation to enhance pro-cryptography education and better prepare forensic specialists for future security challenges.

***Keywords***— Cryptography, Digital security, Secure communication, Symmetric encryption, Asymmetric cryptography, Hash functions, Digital signatures, RSA algorithm.

## 1. Introduction

Cryptography can be described as the science of encoding and decoding information to ensure its secure transmission. It involves encrypting plaintext messages into codes and code-breaking to allow the appropriate message to be received. Cryptography provides means of protecting data content by using mathematical constructs in the form of keys for confidentiality, integrity, and authenticity. It is used in secure internet interactions, electronic transactions, password protection, and verification of data integrity [1-11].

Contemporary cryptographic concepts include key exchange, cryptographic protocols, post-quantum cryptography, and blockchain technology. Symmetric encryption algorithms like AES are commonly used, while asymmetric encryption employs RSA and ECC for public-key algorithms. Features such as digital signatures are used for message validation, and key exchange protocols facilitate the sharing of security keys.

Post-quantum cryptography addresses vulnerabilities created by quantum computing, while blockchain provides a security solution for transactions and decentralized ledgers.

The organizational principles focus on CIA: Confidentiality, Integrity, and Availability. Cryptography supports these principles by ensuring confidentiality through encryption, maintaining integrity with hash functions and digital signatures, and promoting availability by securing systems and resources.

Cryptography is essential in the modern world where information technology is pervasive and data security is crucial. It protects communication through cipher techniques, ensuring confidentiality, integrity, and authenticity.

This paper aims to discuss cipher techniques, starting from classical methods and progressing to modern approaches. It will differentiate between physical and higher layers, as well as symmetric-key and asymmetric-key ciphers.

### 1.1 Ciphers since ages

Cryptographic primitives play crucial roles in digital information security. Encryption, a key primitive, includes symmetric encryption and asymmetric encryption (using a key pair).

Hash functions, such as SHA-256 and MD5, are essential for data validation and password protection. Message

Authentication Codes (MAC) verify the authenticity of information through a secret key and MAC algorithm; the recipient recalculates the MAC to check for consistency. Electronic signatures, utilizing asymmetric cryptography, authenticate electronic documents or messages.

Ciphers, fundamental to cryptography, transform plaintext into ciphertext and back. Symmetric ciphers use one key for both processes; substitution ciphers map characters based on a fixed key, and transposition ciphers rearrange characters in a set pattern. Fixed-size block ciphers are effective for secure communication by encrypting fixed-size blocks.

Asymmetric ciphers, such as RSA and Elliptic Curve Cryptography (ECC), use separate keys for encryption and decryption, with ECC offering efficient security for low-resource devices. Understanding these techniques and their limitations is crucial for maintaining robust information protection [18-21].

### 1.2 History of ciphers

The use of ciphers dates back centuries and includes the profound evolutionary processes of the Caesar Cipher, Scytale, and Polyalphabetic Cipher, most notably the Vigenère Cipher.

Historically, cryptography was primarily associated with encryption, which involves converting plaintext into ciphertext to secure messages. Early methods, such as frequency analysis, were used with early ciphers, including the Enigma Machine and RSA Algorithm. AES has since replaced other algorithms and now dominates the data encryption field as the most efficient and secure option.

As technology advances, ciphers evolve to provide optimal security, time-efficient computations, and protection against new threats.

In cryptography, ciphers are methods for encrypting and decrypting information using keys. These differences significantly impact the implementation of secure communication protocols and the handling of sensitive data [22-27].

### 1.3. Popular cipher machines

#### 1.3.1. Enigma Cipher Machine

The Enigma series comprised several cipher machines created by the Germans during World War II. They varied in design and compatibility.

#### 1.3.2. Hagelin Cipher Machine

Boris Hagelin developed his first cipher machine in 1921, with the M-209 being the most well-known. His company, Crypto AG, continued to develop numerous models after World War II.

#### 1.3.3. Fialka Cipher Machine

Developed by the Russians shortly after World War II, the Fialka machine improved upon the Enigma design with features like irregular wheel stepping and a built-in printer.

#### 1.3.4. Siemens Cipher Machine

Siemens, like other European companies, developed cipher machines, notably the T-52 or Geheimschreiber, used by the German High Command during World War II [28-35].

#### 1.3.5. Lorenz Cipher Machine

The Lorenz SZ-40 was created by the German High Command during World War II for high-level messages. It posed a significant challenge to Bletchley Park codebreakers and was eventually decrypted using the Colossus machine.

#### 1.3.6. Colossus Cipher Machine

Developed during World War II, Colossus was one of the earliest programmable electronic computers. It was designed to break the Lorenz SZ-40/42 cipher.

#### 1.3.7. Philips Cipher Machine

Philips Usfa, a Dutch defense electronics manufacturer, produced a range of cryptographic machines compatible with NATO standards in the latter half of the 20th century.

#### 1.3.8. NEMA Cipher Machine

Developed by the Swiss during World War II as a replacement for Enigma K machines, NEMA had similarities to and weaknesses inherited from Enigma.

#### 1.3.9. Transvertex Cipher Machine

Produced by a small Swedish company similar to Hagelin machines, the HC-9 was their notable model, designed on a different principle to avoid patent infringement [36-45].

#### 1.3.10. Gretag Cipher Machine

Gretag Data Systems, based in Switzerland, manufactured a variety of commercial, industrial, and military cipher machines over the years.

#### 1.3.11. HELL, Cipher Machine

Rudolf Hell, known for graphical equipment, also built mechanical cipher machines post-World War II under license from Boris Hagelin for the German Army.

#### 1.3.12. OMI Cipher Machine

OMI, an opto-mechanical factory in Italy, developed cipher machines including the OMI Alpha in 1939 and subsequent models like the Cryptograph and Cryptograph-CR [46-49].

## 2. Related Work

The following is a literature survey of various cryptographic techniques and advancements:
Technological Evolution: Advances in science and technology have transformed many aspects of human life, including communication. Traditional methods such as letters, telegrams, and radios have been replaced by digital technologies like the internet, mobile phones, and online chat. Consequently, many traditional encryption techniques have become increasingly vulnerable to attacks due to outdated security standards [50].

An Unpredictable Cipher: The Mercurial Cipher addresses the deficiencies of current encryption algorithms, such as XOR and classical ciphers like the Caesar Cipher or Vigenère Cipher, by incorporating machine information from the sender into the process. This helps avoid key-based weaknesses that attackers could exploit to gain unauthorized access to ciphertext [50].

Poly-Alphabetic Cipher Improvements: For encoding numeric data, the Numeric Data Incorporation to the Classic Vigenère Cipher extends the classic polyalphabetic method, improving its effectiveness and flexibility in data encryption [51].

Layered Cryptographic Technique: The Cyclic Cryptographic Technique (CCT) combines symmetric and asymmetric cryptography methods, outperforming traditional techniques such as the Caesar Cipher or Vigenère Cipher [52].

Advancements in Alphabetic Ciphers: Efforts to improve classical alphabetic ciphers, such as the Vigenère Cipher, address vulnerabilities like Kasiski and Friedman attacks. A hybrid Vigenère-Affine cipher has been introduced for English and Myanmar alphabets [53].

Nonlinear Feedback Shift Register (NFSR): For NFSR-based block cipher systems, a novel ring structure approach has been proposed to enhance data security in electronic storage and transmission for 64-bit block ciphers [54].

Hill Cipher Algorithm: To address weaknesses such as key matrix instability and known plaintext attacks, the Hill Cipher has been enhanced with multiple rounds of encryption, cipher block chaining, and a hexadecimal substitution box [55].

Playfair Stream Cipher: This two-step symmetric key algorithm transforms the traditional 5x5 Playfair cipher into a block cipher and tests its strength against other cryptographic algorithms to improve security [56].

Hybrid Encryption Approach: For securing Short Message Service (SMS) on Android devices, a hybrid approach that uses RC4 for message encryption and the Affine Cipher for key encryption protects data against malicious third-party interception [64].

Lightweight Cryptography for IoT: Lightweight cryptographic solutions are needed to secure IoT-based e-healthcare systems, focusing on efficient data transmission and storage security in remote health monitoring [65].

Securing MQTT Protocol: Payload encryption using lightweight block ciphers and hash functions like SPONGENT ensures data integrity and authenticity, addressing security issues related to the MQTT protocol in IoT environments [66].

Chaotic Stream Ciphers: Robust pseudo-chaotic number generators (RPCNG) are used in designing chaotic stream ciphers for IoT applications, providing secure real-time communication capable of resisting statistical attacks [73].

Power Saving Techniques: Techniques focused on power and area efficiency in cryptic block ciphers, especially for IoT applications, show improved efficiency while maintaining security [60, 68].

Cryptography for Limited Devices: Resource-constrained environments such as RFID and WSN employ SLIM, a lightweight block cipher that performs better than traditional ones [69].

Analysis and Improvement of Classical Ciphers: Research continues to improve classic ciphers like Vernam and Kuznyechik by using multi-level encryption methodologies and power analysis attack countermeasures [70, 71].

AES Efficiency Enhancements: Modifications to AES through non-linear feedback shift operations in CFB or OFB modes aim to speed up the process while maintaining high security levels [72].

This review offers an organized overview of current developments in cryptographic methods, outlining recent progress aimed at addressing security challenges in various application areas [73].

## 3. Research problem

The research aims to address a gap in the existing literature: the development of a simple yet secure cipher technique specifically designed for novice learners in cryptography. Standard cipher techniques often present challenges for beginners due to the complexity of their algorithms, and many simple ciphers sacrifice security. This study focuses on the Periodic-Shift Cipher, a new form of encryption that combines simplicity with security. By using only odd-numbered shifts and incorporating the rule "a=z", the Periodic-Shift Cipher seeks to provide an effective yet straightforward cryptographic tool for individuals unfamiliar with modern cryptography. The study evaluates how well the Periodic-Shift Cipher serves as a user-friendly learning tool, with particular emphasis on its encryption principles and information security.

## 4. Existing cipher techniques and their limitations

### 4.1. Caesar Cipher:

Description: This is a secret code that replaces each letter in the English alphabet with a letter shifted by n positions down the alphabet.

Limitations: The Caesar Cipher can be easily compromised if someone attempts to determine the shift value. Additionally, it does not provide strong security for confidential communication.

**4.2. Substitution Ciphers:**

Description: These ciphers replace characters in plaintext with other characters using specific rules called keys.

Limitations: They can be vulnerable to frequency analysis because some letters in languages appear more frequently than others. If the key is not complex enough, the cipher can be easily broken.

**4.3. Vigenère Cipher:**

Description: This encryption method uses a keyword to perform a series of simple substitutions based on the letters of the keyword.

Limitations: The strength of the Vigenère Cipher depends on the length and complexity of the keyword. A longer keyword offers better protection but may be challenging for beginners to manage.

**4.4. Morse Code:**

Description: Telegraphic messages are encoded using a series of dots and dashes representing individual letters, which are transmitted over telegraph lines.

Limitations: Morse code cannot directly encode alphabetic texts in their entirety because it primarily represents numbers, certain letters, and a limited set of special characters. Users need to have knowledge of Morse code to interpret the messages accurately.

## 5. Proposal of a new cipher: periodic-shift cipher

The Periodic-Shift Cipher is a simple algorithm that encrypts messages in such a way that odd-numbered shifts are made to each letter of the alphabet following the “a=z” rule. Here is how the algorithm works:

1. Input: Plain text message which consists only of letters, either upper or lower case, and maybe spaces on it.
2. Rules: The Periodic-Shift Cipher obeys “a=z” meaning ‘z’ takes the place of ‘a’ and vice versa. Use only odd shift numbers (e.g., 3, 5, 7). The user is allowed to choose any value for the shift.
3. Encryption Process: For every letter in a plain text message:
   - If a letter is equal to ‘a’, then replace it with ‘z’. (This follows the "a=z" rule.)
   - Otherwise, perform an odd number shift based on the selected value for the shift.
   - Do not change the letter’s case from the original form that can be both uppercase and lowercase letters.
4. Output: After encryption this will be called ciphertext as well as encrypted message.

Example: Periodic-Shift Cipher with Shift 3

- Plaintext: HELLO
  - Encryption Process:
  - H (shifted by 3) → I
  - E (shifted by 3) → F
  - L (shifted by 3) → M
  - L (shifted by 3) → M
  - O (shifted by 3) → P
- Ciphertext: IFMMP

Example: Periodic-Shift Cipher with Shift 5

- Plaintext: GOOD MORNING
- Encryption Process:
  - G (shifted by 5) → L
  - O (shifted by 5) → T
  - O (shifted by 5) → T
  - D (shifted by 5) → I
  - M (shifted by 5) → R
  - O (shifted by 5) → T
  - R (shifted by 5) → W
  - N (shifted by 5) → I
  - I (shifted by 5) → D
  - N (shifted by 5) → I
  - G (shifted by 5) → L
- Ciphertext: LTTIRTWIDI

These examples illustrate the Periodic-Shift Cipher's encryption process, showcasing how each letter in the plaintext is transformed using odd-numbered shifts and the "a=z" rule. The shift value can be adjusted to customize the encryption.

## 6. Experimental setup and parameter selection

The experimental parameters for the Periodic-Shift Cipher, including odd-numbered shifts and key lengths, are crucial considerations for both security and educational purposes. Here's a detailed explanation of the chosen parameters:

1. Odd Numbered Shifts:

Rationale:

- To create an extra layer of complexity compared to the most common ciphers which usually have even number shifts, we use odd-numbered ones.
- Offering a unique learning experience for beginners, odd shifts depart from usual cryptographic practices.
- Uncommon nature of the shifts adds unpredictability making it more difficult for potential interceptors to understand the text.

2. Key Lengths:

Rationale:

- In the Periodic-Shift Cipher’s initial implementation, there is no fixed key length stated explicitly. Instead, the key is generated from the user selection of odd-numbered shift values.
- The user during encryption implicitly sets this as determined by the length of their choice of shift values.
- This makes it simpler for beginners so that they can concentrate on basic encryption principles rather than complex mechanisms in case they opt for using our Periodic-Shift Cipher as designed by allowing them to easily use passwords instead of spending time on managing keys that are typically hard to deal with.

3. Customizing Shift Values:

Rationale:

- Odd shift customization gives the users some room for adaptation. They can play around with different shift values to understand how varying shift lengths affect cipher security.
- Customization is aimed at imparting skills to students who would wish to know what is key management in cryptography and its importance in the security of the message being encrypted.

4. Integration of Morse Code into the System:
Rationale:

- For educational as well as security reasons, Morse code has been integrated. This extra coding level helps learners diversify their knowledge acquisition by combining several cryptographic techniques.
- The choice of integrating Morse code fits well with the educational objectives of the Periodic-Shift Cipher since it allows learners to experience different ways of encoding and know more about diversity in terms of cryptography.

In conclusion, this periodic shift cipher's parameters strike a balance between security considerations and educational objectives. The use of odd-numbered shifts, customizable key lengths, and Morse code integration all add up to a simple but flexible instructional tool for basic principles in cryptography.

### 6.1. Examples

Example 1:

Plain text: "HELLO"

Cipher text: "ITCCR" (using Periodic-Shift Cipher with a shift of 3)

In this example, each letter is shifted by 3 positions. According to the Periodic-Shift Cipher rules, "A" is always equal to "Z," and shifts happen only with odd numbers. So, the encryption is done as follows:

- H + 3 = I
- E + 3 = H
- L + 3 = O
- L + 3 = O
- O + 3 = R

Example 2:

Plain text: "GOOD MORNING"

Cipher text: "POOU FTOMDMP" (using Periodic-Shift Cipher with a shift of 5)

Again, applying the Periodic-Shift Cipher rules:

- G + 5 = L
- O + 5 = T
- O + 5 = T
- D + 5 = I
- M + 5 = R
- O + 5 = T
- R + 5 = W
- N + 5 = M
- I + 5 = D
- N + 5 = M
- G + 5 = P

### 6.2. Schematic representation

A schematic representation typically shows the high-level components and how they interact. For the Periodic-Shift Cipher, the main components are:

I. Input text
II. Shift value
III. Encryption process
IV. Output encrypted text
V. Decryption process
VI. Output decrypted text.

Therefore, the schematic representation is shown as given in the below figure. 1.

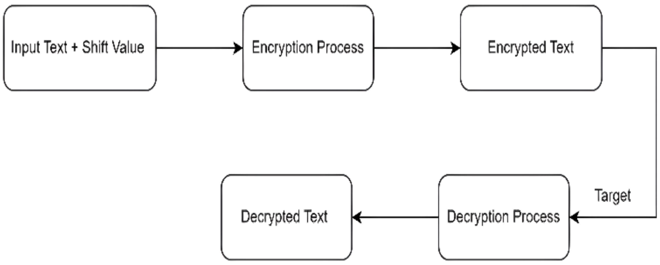


**Figure 1**. Schematic Representation

**Flowchart**

A flowchart will provide a step-by-step visual representation of how the program executes. The flowchart is shown as given below figure 2.

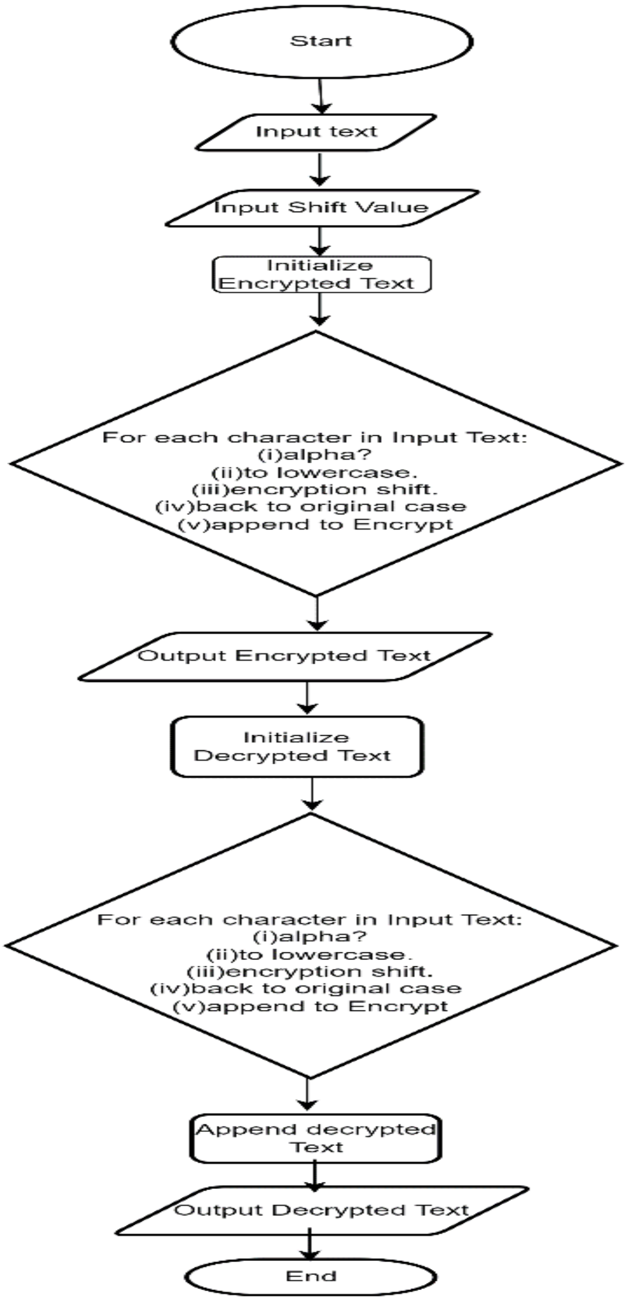


**Figure 2**. Flow chart of step-by-step visual representation of the program execution.

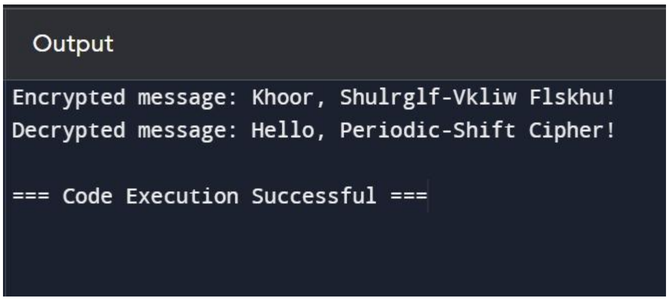
**6.3. Pseudo code:** The psedo code is as given below,

```
function Periodic-Shift Cipher(text, shift):
    encrypted_text = ""
    for each character char in text:
        if char is alphabetic:
            is_upper = check if char is uppercase
            char = convert char to lowercase
                        if char equals 'a':
                char = 'z'
            else:
                shifted = (ord(char) + (shift % 26) - ord('a')) % 26 + ord('a')
                char = convert shifted back to character
                        if is_upper:
                char = convert char to uppercase
                    append char to encrypted_text
        return encrypted_text
# Example Usage:
text = "Hello, Periodic-Shift Cipher!"
shift = 3
encrypted_message = Periodic_Shift_Cipher(text, shift)
print("Encrypted message:", encrypted_message)
# Decryption example:
decrypted_message=
Periodic_Shift_Cipher(encrypted_message, -shift)
print("Decrypted message:", decrypted_message)
```

This pseudocode outlines the encryption and decryption process using the Periodic-Shift Cipher algorithm. It includes the shift operation, handling of uppercase and lowercase characters, and the modular arithmetic necessary for wrapping around the alphabet.

**6.4. Test cases**

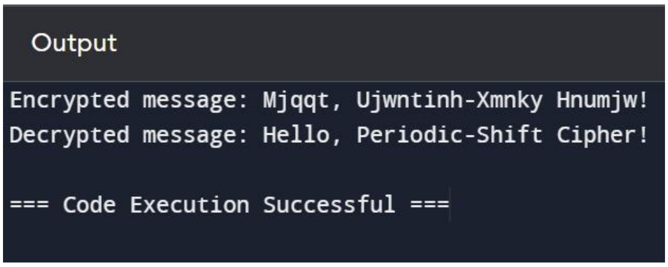
The test cases are shown in the given figures: 1,2,3,4,5,6,7,8,9.



```
Output
Encrypted message: Khoor, Shulrglf-Vkliw Flskhu!
Decrypted message: Hello, Periodic-Shift Cipher!

=== Code Execution Successful ===
```

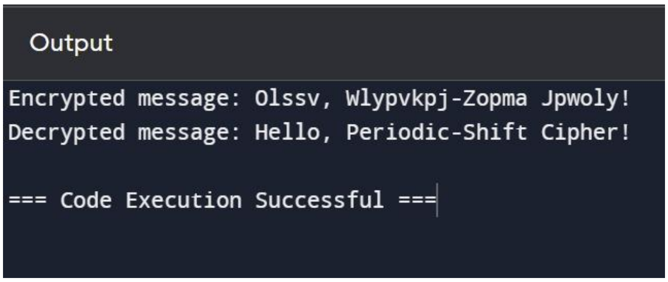
**Figure.3.** Test case screenshot -1



```
Output
Encrypted message: Mjqqt, Ujwntinh-Xmnky Hnumjw!
Decrypted message: Hello, Periodic-Shift Cipher!

=== Code Execution Successful ===
```

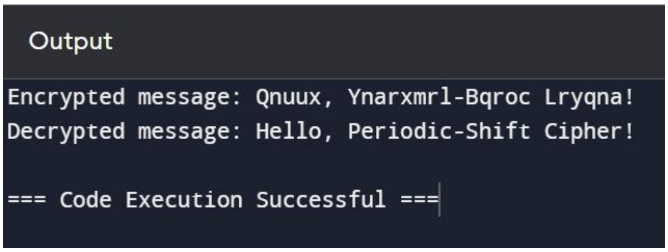
**Figure.4.** Test case screenshot -2



```
Output
Encrypted message: Olssv, Wlypvkpj-Zopma Jpwoly!
Decrypted message: Hello, Periodic-Shift Cipher!

=== Code Execution Successful ===
```

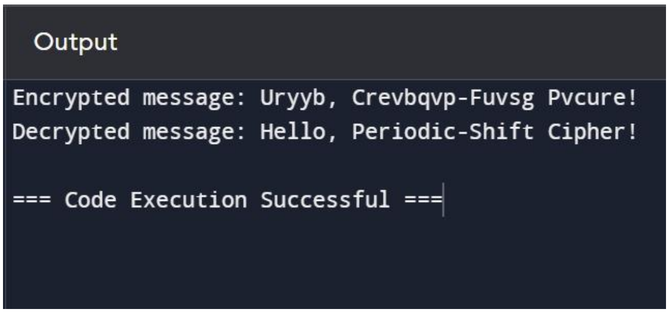
**Figure.5.** Test case screenshot -3



```
Output
Encrypted message: Qnuux, Ynarxmrl-Bqroc Lryqna!
Decrypted message: Hello, Periodic-Shift Cipher!

=== Code Execution Successful ===
```

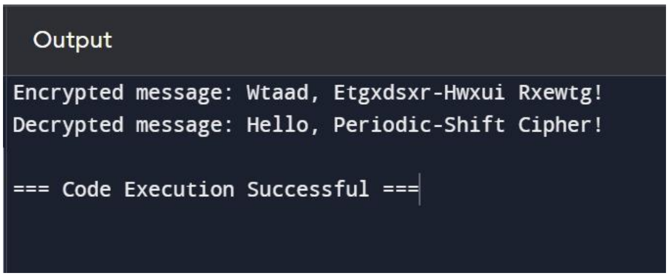
**Figure.6.** Test case screenshot -4



```
Output
Encrypted message: Uryyb, Crevbqvp-Fuvsg Pvcure!
Decrypted message: Hello, Periodic-Shift Cipher!

=== Code Execution Successful ===
```

**Figure.7.** Test case screenshot -5



```
Output
Encrypted message: Wtaad, Etgxdsxr-Hwxui Rxewtg!
Decrypted message: Hello, Periodic-Shift Cipher!

=== Code Execution Successful ===
```

**Figure.8.** Test case screenshot -6

**6.5. Thematic Representation**

For the Periodic-Shift Cipher program using a key, the schematic representation shows the additional component of a randomly generated key:

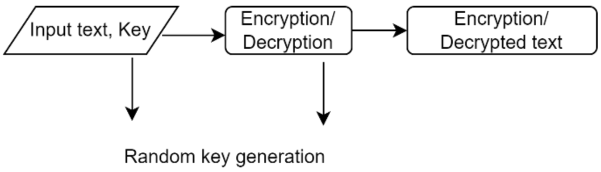


**Figure 9**. Thematic representation

**6.6. Observations**

- The strange thing about the Periodic-Shift Cipher is that it employs odd number shifts and the "a=z" rule which makes a unique pattern for encrypted messages.

- Selecting odd shifts adds one more intricacy that makes it less predictable than ciphers having fixed shifts.
- The "a = z" rule ensures that the first letter in the alphabet always equals the last one, thus forming a consistent pattern in encryption.

The Periodic-Shift cipher on its own may seem complex but not sufficiently secure compared to other contemporary forms of encryption. Its strength and potential weaknesses should be evaluated by further analysis and testing.

**Table .1.** Test cases 1 to 6

| Test Case. | Encrypted Message | Decrypted Message |
|---|---|---|
| 1 | Khoor, Shulrglf-Vkliw Flskhu! | Hello, periodic-Shift Cipher! |
| 2 | Ujqqt,Ujwntinh-Xmnky Hnumjw | Hello, periodic-Shift Cipher! |
| 2 | Olssv,Wlypvkpj-Zopma Jpwoly! | Hello, periodic-Shift Cipher! |
| 3 | Qnuux, Ynarxml-Bqroc Lryqna! | Hello, periodic-Shift Cipher! |
| 4 | Uryyb,Crevbqvp-Fuvsg Pvcure! | Hello, periodic-Shift Cipher! |
| 5 | Wtaad,Etgxdsxr-Hwxui Rxewtg | Hello, periodic-Shift Cipher! |

### 6.7. Salient features of periodic-shift cipher

Periodic-Shift Cipher Features

Simplicity:

- Implements the "a=z" rule and uses only odd shifts.
- Compared to Vigenère type of traditional ciphers, it is easier for beginners.

Security:

- Uses odd shifts for increased security.
- Addresses challenges of basic ciphers by striking a balance between simplicity and improved security.

Accessibility:

- Aims to reduce complexities for new learners while maintaining cryptographic principles.
- Neither complicated nor unsafe, making it suitable for beginners without compromising on safety.

Use Case:

- Designed for newcomers in cryptography and other introductory purposes.
- Distinctive from other high-level ciphers used in real-world scenarios.
- Always "a=z" Rule: Establishes a cyclical nature, requiring users to understand the cyclic nature of the alphabet.
- Shifts Only with Odd Numbers: Restricts shifts to odd numbers, adding an additional layer of unpredictability.
- Customizable Odd-Numbered Shifts: Allows for experimentation and exploration of different encryption scenarios.
- Integration with Morse Code: Reinforces understanding of multiple cryptographic techniques and adds an extra layer of encoding to the encrypted message.

### 6.8. Limitations of periodic-shift cipher

1. Vulnerability to Brute Force:

- Due to its simplicity, Periodic-Shift Cipher may be susceptible to brute-force attacks, where an attacker systematically tries all possible combinations to decrypt the message.

2. Dependence on Odd Numbers:

- The exclusive use of odd-numbered shifts might introduce predictability, making it easier for experienced cryptanalysts to identify patterns and exploit vulnerabilities.

## 7. Future scope

- Multilingual Support: Developing regional languages to make the cipher language-independent.
- Morse Code Integration: Expanding Morse code usage in encryption.
- Adaptive Cipher: Modifying the cipher to change encryption approach based on text parameters.
- Cryptanalysis and Breaking Techniques: Promoting studies to identify flaws and improve protection.
- User-Friendly Tools: Designing user-friendly programs or web applications that incorporate the cipher.
- Quantum Computing Resilience: Analyzing the cipher's security features and vulnerability to quantum computing attacks.
- Odd-Numbered Shifts: Enhancing security by deviating from traditional even shifts.
- Morse Code Integration: Introducing a different encoding system.
- Balancing Security and Education: Striking a balance between security and educational value.
- Variable Shifts: Introducing a mechanism for variable shifts based on a dynamic key.
- Key Management: Developing a robust key management system.
- Enhanced Security Measures: Integrating additional cryptographic techniques.
- Algorithmic Complexity: Exploring ways to increase algorithmic complexity without sacrificing simplicity.
- Integration with Modern Technologies: Adapting the cipher for use in secure messaging applications or cyber security training tools.

## 8. Conclusions

The research introduces the Periodic-Shift Cipher, which is an easy encryption mechanism intended for newcomer students in the field of cryptography. Periodic-shift cipher is somewhat different as the letter ‘a’ is always equivalent to the letter ‘z’ while shifting occurs with odd numbers like 3, 5, 7, and so on. In a way, it is issued in an elementary matter that is more suitable for learning by rookie learners while creating adequate grounds for the understanding of cryptological principles. Periodic Shift Cipher is compared with other existing cipher techniques where the author insists that the technique is simple and was designated for educational purposes only. Teaching aid is one of the keen benefits of the cipher as it creates a perfect scenario in which learners can try encrypting and decrypting messages for themselves without a lot of hassle. The use of Periodic-Shift Cipher is recommendable in certain and specifically confined domains, such as education where one would like to teach basics of encryption, fundamental cryptography training where one wants to lay down a foundation, and for any other person interested in learning the elementary concepts in cybersecurity.

Possible improvements and adjustments that can be made based on the research findings have been determined and these may apply to the development of future aspects of Periodic-Shift Cipher.

## 9. Future Scope

- Security Checks: Evaluate the cipher’s robustness against various cryptographic attacks to better understand its security limits.
- Modern Integration: Explore potential applications of the cipher within contemporary encryption systems to enhance its practical utility.
- Teaching Tools: Develop interactive educational software and lesson plans featuring the cipher to improve its effectiveness as a teaching aid.
- Algorithm Enhancements: Investigate possible modifications to increase the cipher’s complexity and security.
- Comparative Analysis: Compare the Periodic-Shift Cipher with other simple ciphers to assess its relative effectiveness and educational value.
- Specialized Applications: Assess the cipher’s suitability for specific low-security environments or beginner training programs.
- User Feedback: Gather and analyze feedback from educators and learners to refine the cipher and optimize its use in educational settings.
- Quantum Computing Impact: Research how emerging quantum computing technologies might affect the cipher’s security and effectiveness.

### Authors’ Contributions

First Author (Padma Sree Uma Nandini Kadavakollu) has designed and developed this concept, second author (Sony Kumari) has documented and third author (Dr. Srinivasa Rao Gundu) has inspected and guided technological and research & developmental activities.

**Acknowledgements**
We (Padma Sree Uma Nandini Kadavakollu, Sony Kumari) sincerely thank and express a deep sense of gratitude to my Research supervisor Dr. Srinivasa Rao Gundu, who is the Assistant Professor at the School of Science, Malla Reddy University, and Hyderabad.

### Competing Interests

Authors declare that have no competing interest.

**Funding Information**
This study is not funded by any organization in any manner at any stage of this study

### Competing Interests

Not Applicable, all data is provided in side this manuscript.

### Research involving human and /or animals

Not Applicable

### Informed consent

Not Applicable

### Conflict of interest statement

The authors do not have any conflict of interest.

## References

[1] R.I. Masya, R.F. Aji, and S. Yazid, "Comparison of Vigienere Cipher and Affene Cipher in Three-pass Protocol for Securing Image," International Conference in Science and Technology, Vol., pp. 1-5, 2020.

[2] A. Carlson, S.R. Mikkilineni, M.W. Totaro, R.B. Wiells, and R.E. Hiromoto, "Equivalence of Product Ciphers to Substitution Ciphers and their Security Implications," International Symposium on Networks, Computers and Communications, Vol., pp. 1-6, 2022.

[3] S. Vatsayan, R.A. Hydri, and J.K. Verma, "Design of Hybrid Cryptography System based on Vigenère Cipher and Polybius Cipher," International Conference on Computational Performance Evaluation, Vol., pp. 848-852, 2020.

[4] D. Gautam, C. Agrawal, P. Sharma, M. Mehta, and P. Saini, "An Enhanced Cipher Technique Using Vigienere and Modified Caesar Cipher," International Conference on Trends in Electronics and Informatics, Vol., pp. 1-9, 2018.

[5] N. Jain and S.S. Chauhan, "Novel Approach Transforming Stream Cipher to Block Cipher," International Conference on Technological Advancements and Innovations, Vol., pp. 182-187, 2021.

[6] K. Singh, R. Johari, K. Singh, and H. Tyagi, "Mercurial Cipher: A New Cipher Technique and Comparative Analysis with Classical Cipher Techniques," International Conference on Computing, Communication, and Intelligent Systems, Vol., pp. 223-228, 2019.

[7] A. Al-Sabaawi, "Cryptanalysis of Vigenère Cipher: Method Implementation," IEEE Asia-Pacific Conference on Computer Science and Data Engineering, Vol., pp. 1-4, 2020.

[8] R. Dodmane, R. K R, S. Shetty, K.R. N S, B. K, and S.M.N. Islam, "Implementation of NonLinear Feed Back Stream Cipher System through Hybrid block Cipher Mode to Enhance the Resistivity and Computation Speed of AES," IEEE 9th Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering, Vol., pp. 1-6, 2022.

[9] T.M. Aung and N.N. Hla, "A Complex Polyalphabetic Cipher Technique Myanmar Polyalphabetic Cipher," International Conference on Computer Communication and Informatics, Vol., pp. 1-9, 2019.

[10] S. Souror, N. El-Fishawy, and M. Badawy, "SCKHA: A New Stream Cipher Algorithm Based on Key Hashing and Splitting Technique," International Conference on Electronic Engineering, Vol., pp. 1-7, 2021.

[11] T. Ichiki and A. Tsuneda, "Study on Security Enhancement of 64-Bit NFSR-based Block Cipher Systems with Ring Structure," International Conference on Information and Communication Technology Convergence, Vol., pp. 842-844, 2018.

[12] B. Triandi, E. Ekadiansyah, R. Puspasari, L. T. Iwan, and F. Rahmad, "Improve Security Algorithm Cryptography Vigenere Cipher Using Chaos Functions," International Conference on Cyber and IT Service Management, Vol., pp. 1-5, 2018.

[13] A. Sahi, D. Lai, and Y. Li, "An Efficient Hash Based Parallel Block Cipher Mode of Operation," International Conference on Computer and Communication Systems, Vol., pp. 33-40, 2018.

[14] D. Sehrawat, N. S. Gill, and M. Devi, "Comparative Analysis of Lightweight Block Ciphers in IoT-Enabled Smart Environment," International Conference on Signal Processing and Integrated Networks, Vol., pp. 915-920, 2019.

[15] A. Serdano, M. Zarlis, and E. B. Nababan, "Performance of Combining Hill Cipher Algorithm and Caesar Cipher Algorithm in Text Security," International Conference on Artificial Intelligence and Mechatronics Systems, Vol., pp. 1-5, 2021.

[16] A. Al-Sabaawi, "Cryptanalysis of Stream Cipher: Method Implementation," IEEE Asia-Pacific Conference on Computer Science and Data Engineering, Vol., pp. 1-4, 2021.

[17] Joydeep Dey, Sunil Karforma, “A Recent Study on Security Techniques of Information Communication Systems,” International Journal of Scientific Research in Multidisciplinary Studies, Vol.10, Issue.4, pp.77-83, 2024.

[18] Auparajita Krishnaa, Dharmendra Kumar Gurjar, “The Concept of Basic Cipher Text for Enhancing Security in the Algorithms of Cryptography Applications Using Labelled Graphs,” International Journal of Scientific Research in Mathematical and Statistical Sciences, Vol.10, Issue.3, pp.9-13, 2023.

[19] S. Dubey, R. Jhaggar, R. Verma, D. Gaur, “Encryption and Decryption of Data by Genetic Algorithm,” International Journal of Scientific Research in Computer Science and Engineering, Vol.5, Issue.3, pp.47-52, 2017.

[20] M. Rodinko and R. Oliynykov, "Comparing Performances of Cypress Block Cipher and Modern Lightweight Block Ciphers on Different Platforms," IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology, Vol., pp. 113-116, 2019.

[21] C. Bharathi, K. Y. Annapurna, D. Koppad, and K. Sudeendra Kumar, "An Analysis of Stream and Block Ciphers for Scan Encryption," International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control, Vol., pp. 1-5, 2022.

[22] Srinivasa Rao Gundu, T. Anuradha, “Digital Data Growth and the Philosophy of Digital Universe in View of Emerging Technologies,” International Journal of Scientific Research in Computer Science and Engineering, Vol.8, Issue.2, pp.59-64, 2020.

[23] S. A. Thileeban, "Encryption of images using XOR Cipher," IEEE International Conference on Computational Intelligence and Computing Research, Vol., pp. 1-3, 2016.

[24] Dr. G. S. Rao, Dr. P. Charanarur, and Mr. P. Patel, Eds., Cloud Computing and its Service Oriented Mechanism, AkiNik Publications, 2022.

[25] B. P. R. V. Datta and S. K. N, "FPGA Implementation of Different Layers of Present Cipher," International Conference on Intelligent Technologies, Vol., pp. 1-4, 2023.

[26] P. Charanarur, H. Jain, G. S. Rao, D. Samanta, S. S. Sengar, and C. T. Hewage, “Machine-Learning-Based Spam Mail Detector,” SN Computer Science, Vol. 4, No. 6, 2023.

[27] C. Panem, S. R. Gundu, and J. Vijaylaxmi, “The Role of Machine Learning and Artificial Intelligence in Detecting the Malicious Use of Cyber Space,” Robotic Process Automation, Wiley, Vol., pp. 19–32, Aug. 25, 2023.

[28] J. Ge, Y. Xu, R. Liu, E. Si, N. Shang, and A. Wang, "Power Attack and Protected Implementation on Lightweight Block Cipher SKINNY," Asia Joint Conference on Information Security, Vol., pp. 69-74, 2018.

[29] P. Charanarur, S. R. Gundu, and J. Vijaylaxmi, “Decision Making Using Fuzzy Logic Using Multicriteria,” Fuzzy Logic Applications in Computer Science and Mathematics, Wiley, Vol., pp. 1–12, Sep. 15, 2023.

[30] S. G. Garba, A. A. Obiniyi, M. A. Ibrahim, and B. I. Ahmad, "Towards Finding An Optimal S-box For Lightweight Block Cipher," Information Technology for Education and Development, Vol., pp. 1-8, 2022.

[31] J. Cheng, S. Guo, and J. He, "ALLPC: A Lightweight Block Cipher Based on Generalized Feistel Networks for IoT," IEEE International Performance, Computing, and Communications Conference, Vol., pp. 1-8, 2021.

[32] A. Vambol, "The prospects for group-based knapsack ciphers in the post-quantum era," IEEE 9th International Conference on Dependable Systems, Services and Technologies, Vol., pp. 271-275, 2018.

[33] W. -C. Yang and J. -X. Lee, "Implementation of stream cipher service in JCA," International Symposium on Next-Generation Electronics, Vol., pp. 557-561, 2013.

[34] S. R. Gundu, C. Panem, and J. Vijaylaxmi, “A Comprehensive Study on Cloud Computing and its Security Protocols and Performance Enhancement Using Artificial Intelligence,” Robotic Process Automation, Wiley, Vol., pp. 1–17, Aug. 25, 2023.

[35] A. Singh, N. Chawla, M. Kar, and S. Mukhopadhyay, "Energy efficient and side-channel secure hardware architecture for lightweight cipher SIMON," IEEE International Symposium on Hardware Oriented Security and Trust, Vol., pp. 159-162, 2018.

[36] H. Shi, T. Pu, W. Mou, and Y. Chen, "NIST Randomness Tests on the Extended Key of Quantum Noise Random Stream Cipher," International Conference on Optical Communications and Networks, Vol., pp. 1-3, 2019.

[37] C. Oikonomou, C. S. Kouzinopoulos, D. Ioannidis, and D. Tzovaras, "An Encryption Scheme using Dynamic Keys and Stream Ciphers for Embedded Devices," Mediterranean Conference on Embedded Computing, Vol., pp. 1-4, 2022.

[38] K. -M. Ma, T. -B. -T. Cao, and D. -H. Le, "Design of an SoC Based on 32-bit RISC-V CPU and Lightweight Block Cipher PRINCE on FPGA," 9th NAFOSTED Conference on Information and Computer Science, Vol., pp. 25-29, 2022.

[39] I. Aouissaoui, T. Bakir, and A. Sakly, "FPGA Hardware Co-Simulation of a Stream Cipher Image Cryptosystem based on Fixed-Point Chaotic Map," 19th International Multi-Conference on Systems, Signals & Devices, Vol., pp. 1764-1769, 2022.

[40] A. Heuser, S. Picek, S. Guilley, and N. Mentens, "Lightweight Ciphers and Their Side-Channel Resilience," IEEE Transactions on Computers, Vol. 69, No. 10, pp. 1434-1448, 2020.

[41] S. Taha and H. Mostafa, "Accelerated Software Implementation of Authenticated Encryption Stream Ciphers for High Speed Applications," 31st International Conference on Microelectronics, Vol., pp. 27-31, 2019.

[42] J. Gao, L. Gu, and B. Sun, "Power Attack and Protected Implementation on Block Cipher BIG," 5th International Conference on Information Science, Computer Technology and Transportation, Vol., pp. 1-6, 2020.

[43] S. -W. Eum, H. -J. Kim, H. -D. Kwon, K. -B. Jang, H. -J. Kim, and H. -J. Seo, "Implementation of SM4 block cipher on CUDA GPU and its analysis," International Conference on Platform Technology and Service, Vol., pp. 71-74, 2022.

[44] S. Wang, R. Zhao, Z. Yu, and L. Wang, "Optimized implementations of stream cipher ZUC-256 algorithm," 4th International Academic Exchange Conference on Science and Technology Innovation, Vol., pp. 952-956, 2022.

[45] R. S. Mohammed, "Simon Chaotic: An enhancement of SIMON block cipher by using Arnold and Henon chaotic maps," 8th International Conference on Contemporary Information Technology and Mathematics, Vol., pp. 237-242, 2022.

[46] P. Shivapriya and K. N. Meera, "Application for Digraph Substitution Cipher using Graph Labeling Techniques," IEEE 5th PhD Colloquium on Emerging Domain Innovation and Technology for Society, Vol., pp. 1-2, 2023.

[47] G. S. Manoj, B. Sravanthi, G. Thirumal, and S. R. Venishetty, "VLSI Implementation of SMS4 Cipher for Optimized Utilization of FPGA," Second International Conference on Inventive Communication and Computational Technologies, Vol., pp. 1225-1231, 2018.

[48] A. Al-Sabaawi, "Cryptanalysis of Classic Ciphers: Methods Implementation Survey," International Conference on Intelligent Technologies, Vol., pp. 1-6, 2021.

[49] Y. Wang, "A Classical Cipher-Playfair Cipher and Its Improved Versions," International Conference on Electronic Information Engineering and Computer Science, Vol., pp. 123-126, 2021.

[50] K. Singh, R. Johari, K. Singh, and H. Tyagi, "Mercurial Cipher: A New Cipher Technique and Comparative Analysis with Classical Cipher Techniques," International Conference on Computing, Communication, and Intelligent Systems, Vol., pp. 223-228, 2019.

[51] D. Gautam, C. Agrawal, P. Sharma, M. Mehta, and P. Saini, "An Enhanced Cipher Technique Using Vigenere and Modified Caesar Cipher," 2nd International Conference on Trends in Electronics and Informatics, Vol., pp. 1-9, 2018.

[52] S. Gupta, R. Johari, P. Garg, and K. Gupta, "C3T: Cloud based

Cyclic Cryptographic Technique and it's comparative analysis with classical cipher techniques," 5th International Conference on Signal Processing and Integrated Networks, Vol., pp. 332-337, 2018.

[53] T. M. Aung and N. N. Hla, "A Complex Polyalphabetic Cipher Technique Myanmar Polyalphabetic Cipher," International Conference on Computer Communication and Informatics, Vol., pp. 1-9, 2019.

[54] T. Ichiki and A. Tsuneda, "Study on Security Enhancement of 64-Bit NFSR-based Block Cipher Systems with Ring Structure," International Conference on Information and Communication Technology Convergence, Vol., pp. 842-844, 2018.

[55] A. Serdano, M. Zarlis, and E. B. Nababan, "Performance of Combining Hill Cipher Algorithm and Caesar Cipher Algorithm in Text Security," International Conference on Artificial Intelligence and Mechatronics Systems, Vol., pp. 1-5, 2021.

[56] C. Bharathi, K. Y. Annapurna, D. Koppad, and K. Sudeendra Kumar, "An Analysis of Stream and Block Ciphers for Scan Encryption," International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control, Vol., pp. 1-5, 2022.

[57] J. R. Paragas, A. M. Sison, and R. P. Medina, "An Improved Hill Cipher Algorithm using CBC and Hexadecimal S-Box," IEEE Eurasia Conference on IOT, Communication and Engineering, Vol., pp. 77-81, 2019.

[58] N. Jain and S. S. Chauhan, "Novel Approach Transforming Stream Cipher to Block Cipher," International Conference on Technological Advancements and Innovations, Vol., pp. 182-187, 2021.

[59] R. Majumder, S. Datta, and M. Roy, "An Enhanced Cryptosystem Based on Modified Classical Ciphers," International Conference on Advanced Computing and Communication Systems, Vol., pp. 692-696, 2022.

[60] E. B. Kavun, "A Power Reduction Technique Based on Linear Transformations for Block Ciphers," IFIP/IEEE 30th International Conference on Very Large Scale Integration, Vol., pp. 1-6, 2022.

[61] M. R and N. K. V, "Optimized Implementation of S-box and Inverse S-box for PRESENT Lightweight Block Cipher," International Conference on Visions Towards Emerging Trends in Communication and Networking Technologies, Vol., pp. 1-5, 2023.

[62] A. Al-Sabaawi, "Cryptanalysis of Vigenère Cipher: Method Implementation," IEEE Asia-Pacific Conference on Computer Science and Data Engineering, Vol., pp. 1-4, 2020.

[63] E. Jintcharadze, T. Sarajishvili, A. Surmanidze, and D. Khojava, "Implementation and Comparative Analysis of Symmetric Encryption Model Based on Substitution Cipher Techniques," IEEE East-West Design & Test Symposium, Vol., pp. 1-6, 2021.

[64] O. S. Sitompul, Handrizal, N. H. Pasaribu, and E. B. Nababan, "Hybrid RC4 and Affine Ciphers to Secure Short Message Service on Android," International Conference on Informatics and Computing, Vol., pp. 1-6, 2018.

[65] R. R. K. Chaudhary and K. Chatterjee, "An Efficient Lightweight Cryptographic Technique for IoT based E-healthcare System," International Conference on Signals Processing and Integrated Networks, Vol., pp. 991-995, 2020.

[66] S. Iyer, G. V. Bansod, P. N. V, and S. Garg, "Implementation and Evaluation of Lightweight Ciphers in MQTT Environment," International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques, Vol., pp. 276-281, 2018.

[67] O. Jallouli, M. Chetto, and S. E. Assad, "Lightweight Stream Ciphers based on Chaos for Time and Energy Constrained IoT Applications," Mediterranean Conference on Embedded Computing, Vol., pp. 1-5, 2022.

[68] Ali.M., Nazish.M., Ashaq.S., I. Sultan, and M. T. Banday, "Design of Hybrid Glitch-Reduction Techniques for Loop Unrolled SIMON Block Cypher," Smart Technologies, Communication and Robotics, Vol., pp. 1-6, 2022.

[69] Kumar.P., Mishra.Z, and Acharya.B., "High frequency architecture of SLIM lightweight block cipher for resource-constrained IoT applications," International Conference on Microwave, Optical, and Communication Engineering, Vol., pp. 1-4, 2023.

[70] D. G. Brosas, A. M. Sison, and R. P. Medina, "Modified OTP Based Vernam Cipher Algorithm using Multilevel Encryption Method," IEEE Eurasia Conference on IOT, Communication and Engineering, Vol., pp. 201-204, 2019.

[71] E. Maro and V. Girichev, "Power Analysis of Symmetric Block Cipher Kuznyechik," International Conference on Computer Communication and the Internet, Vol., pp. 106-109, 2020.

[72] R. Dodmane, R. K R, S. Shetty, K. R. N S, B. K, and S. M. N. Islam, "Implementation of Non-Linear Feedback Stream Cipher System through Hybrid block Cipher Mode to Enhance the Resistivity and Computation Speed of AES," IEEE 9th Utthar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering, Vol., pp. 1-6, 2022.

[73] F. Dridi, S. El Assad, C. Atamech, W. E. Youssef, and M. Machhout, "Design and Implementation on FPGA Board of a Chaos-based Stream Cipher," International Conference for Internet Technology and Secured Transactions, Vol., pp. 1-5, 2020.

## AUTHORS PROFILE

**Padma Sree Uma Nandini Kadavakollu** is currently a student of B.Sc. (Honors - Digital Forensics), Department of Digital Forensics, School of Science, Malla Reddy University, Hyderabad. She is passionate in Forensic Sciences and Digital Forensics. Her aim is to design and develop a cyber security technique for the current challenges in cyber space.

**Sony Kumari** is currently a student of B.Sc. (Honors - Digital Forensics), Department of Digital Forensics, School of Science, Malla Reddy University, Hyderabad. She is passionate in Forensic Sciences and Digital Forensics. Her aim is to design and develop a cyber security technique for the current challenges in cyber space.

**Dr. Srinivasa Rao Gundu** holds a PhD in computer science and applications. His research work is focused on load balancing in cloud computing, and his research interests are cloud computing, artificial intelligence (AI), and the Internet of Things (IoT). He is the author of Cloud Computing and its Service Oriented Mechanism, Dodecahedron: The Influential Transformations of the Computational Aspects of Artificial Intelligence, Compendia of Reuleaux Tetrahedron, and Robotic Process Automation Design & Development, as well as 30 research papers and book chapters. He is currently Assistant Professor at the Department of Computer Science, School of Sciences at Malla Reddy University, Hyderabad, India.