DrillBit

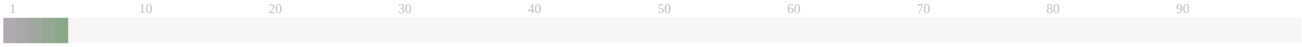
The Report is Generated by DrillBit Plagiarism Detection Software

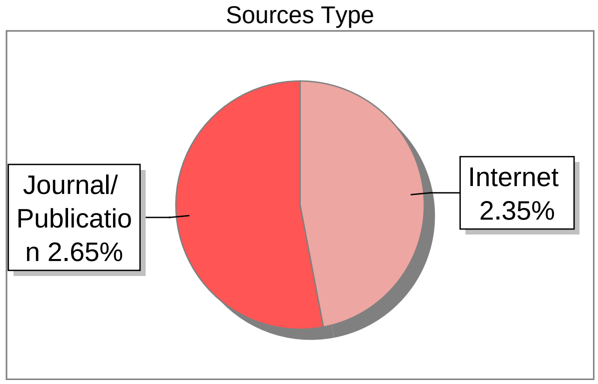
Submission Information

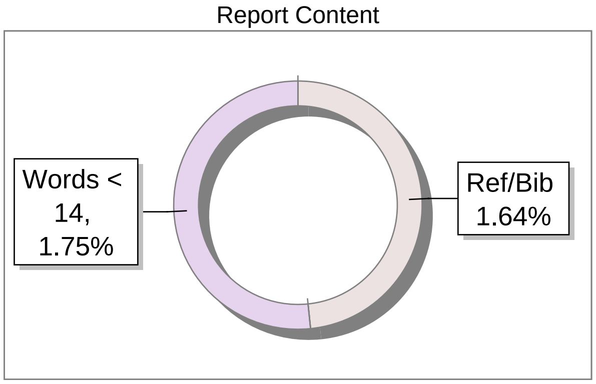
Author Name	saanvi
Title	ins task
Paper/Submission ID	3329085
Submitted by	nnm22is162@nmamit.in
Submission Date	2025-02-13 12:24:07
Total Pages, Total Words	19, 2684
Document type	Assignment

Result Information

Similarity **5 %**







Exclude Information

Quotes	Not Excluded
References/Bibliography	Not Excluded
Source: Excluded < 14 Words	Not Excluded
Excluded Source	**0 %**
Excluded Phrases	Not Excluded

Database Selection

Language	English
Student Papers	Yes
Journals & publishers	Yes
Internet or Web	Yes
Institution Repository	Yes

A Unique QR Code use to View/Download/Share Pdf File

DrillBit

DrillBit Similarity Report

5	7	A	A-Satisfactory (0-10%) B-Upgrade (11-40%) C-Poor (41-60%) D-Unacceptable (61-100%)
SIMILARITY %	MATCHED SOURCES	GRADE	

LOCATION	MATCHED DOMAIN	%	SOURCE TYPE
1	Thesis submitted to shodhganga - shodhganga.inflibnet.ac.in	2	Publication
2	www.freepatentsonline.com	1	Internet Data
3	dannyboston.blogspot.com	<1	Internet Data
4	dochero.tips	<1	Internet Data
5	Beyond Prevention of Influenza The Value of Flu Vaccines, by Resnick, Barbara G- 2018	<1	Publication
6	aiou.academia.edu	<1	Internet Data
7	esjournal.org	<1	Internet Data

INFORMATION AND NETWORK SECURITY

Report on

Comparative Analysis of Classical Encryption Techniques

Submitted by

SAANVI U

NNM22IS133

Submitted to

Dr. JASON ELROY MARTIS

Associate Professor

Dept of ISE

1. Introduction

Encryption methods have played a key role in keeping information safe for centuries. Ancient encryption methods, mainly substitution and transposition ciphers, are the basis for contemporary cryptographic methods. While these methods, now mostly outdated in real-world use, serve as the basis for understanding the development and constraints of contemporary cryptography, they must be learned in order to fully appreciate the history of cryptography.

The classical methods worked in the past as the means of studying the modern encryption standard and basically lay down the principles on which modern-day powerful encrypting algorithms stand. The basic methods also give ideas regarding basic yet crucial principles like confusion and diffusion that are very much the backbone of modern cryptography. While modern encryption has advanced far from these simple techniques, it is these classical ciphers that allow cryptographers and security professionals to examine both the development of the field and the very basics of what makes communication secure.

With the need for secure communication, cryptographers have consistently sought to create more advanced encryption methods. Ancient ciphers like Playfair, Hill, and Vigenère were such landmarks. Though vulnerable, these ciphers have played significant roles in the past in encryption attempts and are well worth learning today for pedagogical and analytical purposes.

This report includes a comparative study of Playfair, Hill, and Vigenère ciphers, analyzes their computational complexity, and discusses their cryptanalysis. A hybrid cipher that utilizes the substitution and transposition methods to provide greater security beyond and above these individual traditional methods is also constructed. The intention of the study is to illustrate the efficacy and weakness of each method through theoretical analysis and application examples.

1.1 Scope and Objectives

The objectives of this analysis are as follows:

- Reviewing the mathematical background of classical encryption methodologies
- An analysis of the computational efficiency and resource requirements
- Evaluation of the degree of vulnerability to various cryptanalytic attacks

- Hybrid implementations: suggestions for improvement
- Mesh into the framework for comparing classical and modern cryptographic methods

1.2 Methodology

The modal methodologies employed by the study are theoretical as well as practical, in which the ciphers are in operation. The methodology includes:

- Mathematical modeling of the encryption and decryption processes
- Implementation of algorithms in the Common Programming Language of use
- Performance tests are performed using all kinds of contexts
- Cryptanalysis using both classical and contemporary methods
- Comparison analysis of outstanding features and vulnerabilities

2. Historical Context

Classical ciphers have been used in military and diplomatic communications for centuries. The Playfair cipher had been a staple in World War I, particularly among British troops, since it was a simple yet effective encrypting method more secure than ordinary monoalphabetic substitution ciphers. Effective during its time, advances in cryptanalysis made it obsolete as frequency analysis methods improved.

The Vigenère cipher, considered unbreakable since it was polyalphabetic, was used extensively in the 16th century. It was later broken, however, with the development of frequency analysis methods like the Kasiski method. The Hill cipher, developed in 1929 by Lester Hill, was one of the earliest linear algebra-based encryption algorithms, leading to later mathematical cryptography.

Cryptography has played a major role in warfare. During World War II, the successful breaking of the German Enigma by Allied cryptanalysts at Bletchley Park influenced Allied victory. It is an important historical lesson in the significance of having sound encryption and the attendant dangers associated with the vulnerabilities in cryptography. Though complex, the eventual defeat meted on the Enigma showcased the deep need for continuous improvement in encryption methods and the associated weakness that comes with subscribing to a single method of encryption.

2.1 Evolution of classical cryptography

The history of classical cryptography can be subjugated into various chronological periods:

Ancient Times (Pre-500 CE):

- Development of simple substitution ciphers
- Use of various tangible devices for encryptions
- More emphasis on concealing messages rather than on mathematically securing them

The Medieval Era (500-1450 CE):

- Founded upon frequency analysis
- Polyalphabetic substitution
- A close involvement with diplomatic correspondence

The Renaissance (1450-1700 CE):

- The introduction of orthodox cryptanalysis
- The design of more sophisticated ciphers
- The appearance of professional cryptographers

Modern History (1700-1900 CE):

- The principles of mathematical introduction
- The development of mechanical encryption devices
- Establishment of cryptography as a formal scientific discipline

3. Analysis of Classical Ciphers

3.1 Playfair Cipher

3.1.1 Computational Complexity

The Playfair cipher employs digraphs (pairs of two letters), depriving monoalphabetic ciphers of the frequency analysis advantage. The encryption procedure involves:

- Constructing a 5x5 key matrix (O(1))

- Substituting each pair of plaintext based on the matrix (O(n), where n is the length of the message)
- Overall complexity: O(n).

3.1.2 Mathematical Formulation

The following encryption rules hold:

- If the two letters are in the same row, replace them with the letters to their immediate right.
- If the two letters are in the same column, replace them with the letters immediately below.
- If neither, replace each letter with the letter in the same row but in the column of the other letter.

Let P1,P2 be a pair of plaintext letters, then the encryption function is:

$$C1, C2 = E(P1, P2)$$

where C1,C2 are letters of ciphertext.

3.1.3 Cryptanalysis

Known Plaintext Attack: If an attacker knows plaintext and corresponding ciphertext, they can reconstruct the 5x5 key matrix by noticing transformations.

Frequency Analysis: Playfair cipher reduces but does not eliminate frequency patterns. Analysis of frequency distribution of digraphs can be utilized to break it.

Advanced Cryptanalytic Techniques:

- Statistical Analysis: Bigram analysis, while less effective than letter frequency, will still allow for the recognition of patterns.
- Pattern Recognition: Plaintext will have repeated phrases, giving the ciphertext a recognizable numeric pattern.
- Multiple Message Attack: The multiplicity of messages encrypted using the same secret key drastically lowers security.
- Brute Force Approach: The combinations of configurations of possible key arrangements are feasible to be tested due to immense computational power.

Example of Cryptanalysis:

Given a ciphertext "GATLMZCLRQTX" and assuming it is a Playfair cipher, an adversary can:

- Identify frequent digraphs in English and notice their transformations.
- Utilize trial decryption by constructing probable key matrices.
- Utilize statistical methods to narrow hypotheses.

3.1.4 Time and Space Complexity

Encryption/Decryption Time Complexity: O(n)
Space Complexity: O(1) because the key matrix is of constant size.

3.1.5 Strengths and Weaknesses

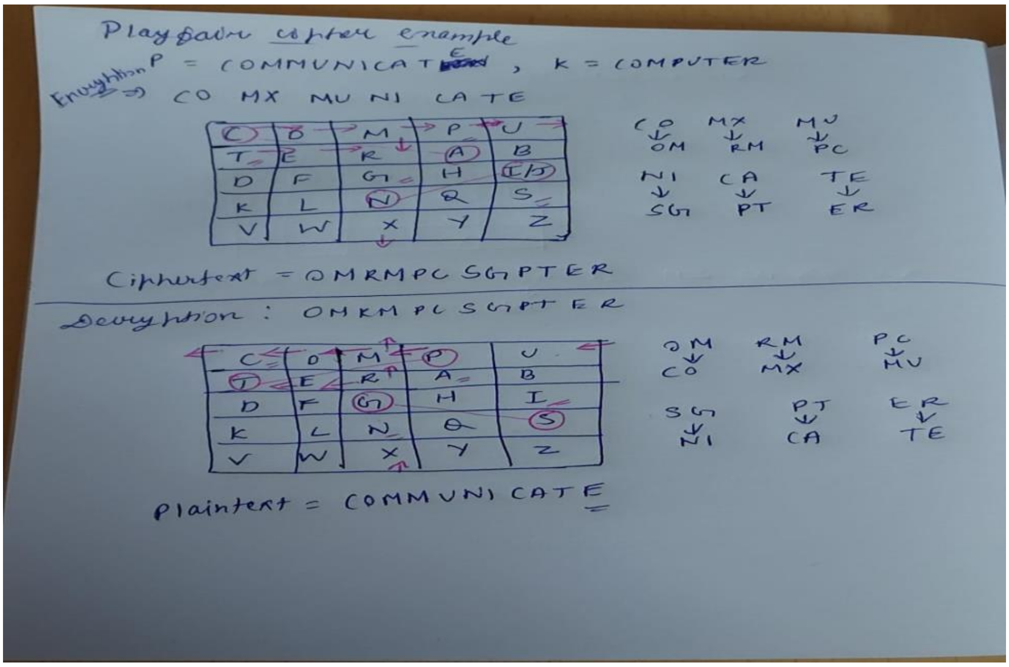
Strengths:

- Resistant to obstructing frequency analysis.
- Quick and effective implementation.
- Suitable for manual encryption.
- The cipher text being a digraph substitution, hence providing security that is not the case for monoalphabetic ciphers.

Weaknesses:

- Limited key space.
- Given revealed letters, the ciphering scheme becomes obvious, rendering it now vulnerable against known-plaintext attacks.
- Content in digraph substitution.
- Limited character set, if not downright excluding J.

3.1.6 Solved Example



Playfair cipher example

P = COMMUNICATE , K = COMPUTER

Encryption ⇒ CO MX MU NI CA TE

C	O	M	P	U
T	E	R	A	B
D	F	G	H	I/J
K	L	N	Q	S
V	W	X	Y	Z

CO ↓ OM   MX ↓ RM   MU ↓ PC

NI ↓ SG   CA ↓ PT   TE ↓ ER

Ciphertext = OMRMPC SGPTER

Decryption : OMKM PC SGPT ER

C	O	M	P	U
T	E	R	A	B
D	F	G	H	I
K	L	N	Q	S
V	W	X	Y	Z

OM ↓ CO   RM ↓ MX   PC ↓ MU

SG ↓ NI   PT ↓ CA   ER ↓ TE

Plaintext = COMMUNICATE

3.2 Hill Cipher

3.2.1 Computational Complexity

- Encryption is matrix-vector multiplication (O(n^3) generally in matrix inversion, O(n^2.376) in optimized code).
- Decryption uses the matrix inverse (O(n^3) generally in cases).
- Total complexity: O(n^3).

3.2.2 Mathematical Formulation

Encryption is given by the formula:

$$C = K.P \; mod \; 26$$

Where:

- C is the ciphertext vector,
- K is the key matrix,
- P is the plaintext vector.

Decryption uses the inverse matrix:

$$P = K^{-1}.C\ mod\ 26$$

Where K^{-1} is the modular inverse of K.

3.2.3 Cryptanalysis

Known Plaintext Attack: If an attacker knows plaintext and the corresponding ciphertext, the attacker can compute the key matrix:

$$K = C.P^{-1}\ mod\ 26$$

Security Considerations:

- Specification of Matrix Size: Larger matrices assure improved security, starting from higher computational complexity.
- Challenges in Key Generation: Not all matrices may be adopted for use as keys; they must be invertible modulo 26.
- Block Size Vulnerability: The static nature of the block size may leak the information regarding the structure of the message.
- Weakness of the System: Linear nature of the cipher opens door for algebraic attacks.

Limitations of Practical Implementations:

- Key matrix requirements-client to ensure that the key matrix is inversible requires some careful selections and validations.
- Error handling afterwards-one being a problem of treating non-invertible matrices and message lengths not divisible by the amount of links in all matrices.
- Heavy computational duty compromises between size of the matrix and the benchmark of performance that needs to be met.
- Memory issues: Operating matrix on very big messages needs employment of techniques that are as efficient as possible.

Example of Cryptanalysis:

Given: $P = \begin{bmatrix} 7 \\ 8 \end{bmatrix}$, C=$\begin{bmatrix} 4 \\ 15 \end{bmatrix}$ and the determinant of modulo 26 is invertible, solving for which gives the encryption key.

3.2.4 Time and Space Complexity

Encryption/Decryption Time Complexity: O(n^3)

Space Complexity: O(n^2)

3.2.5 Strengths and Weaknesses

Strengths:

- Strong mathematical foundation.
- Simultaneous encryption of multiple letters.
- High diffusion properties.
- Resistant to simple frequency analysis.

Weaknesses:

- Key matrix must be invertible.
- Vulnerable to known plaintext attacks.
- Complex implementation
- High computational overhead.

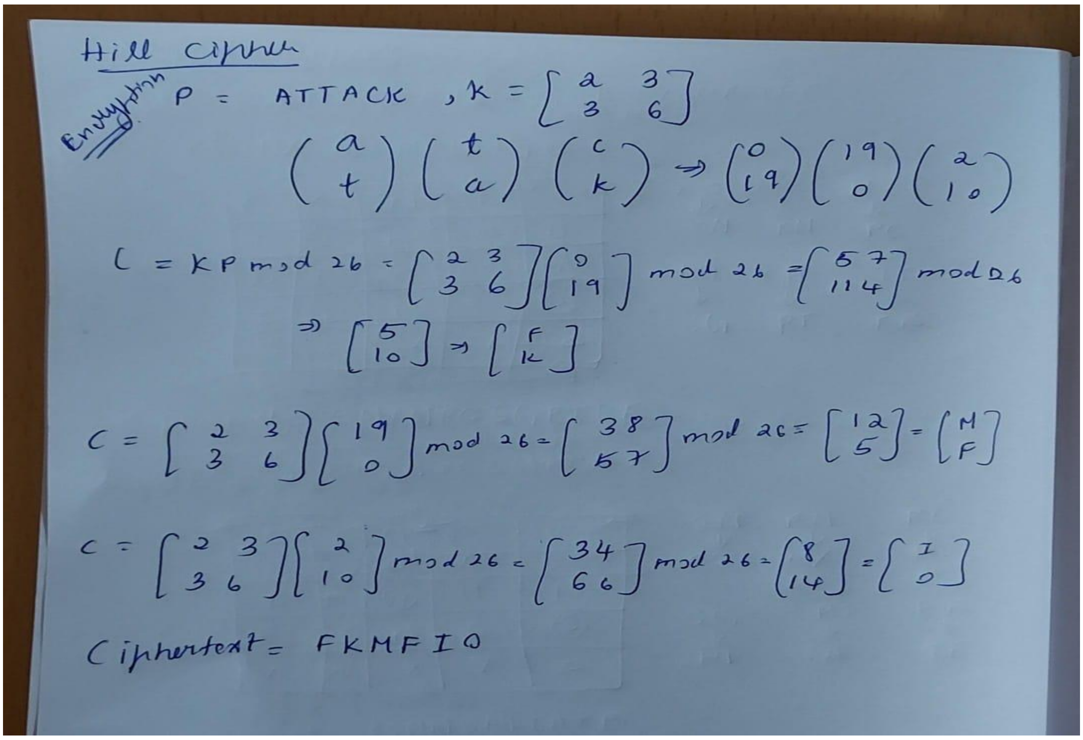
3.2.6 Application in Advanced Areas

The mathematical properties of the Hill cipher make it useful for:

- Using as an Educator's Theory in linear algebra.
- A starting point for growing complex systems.
- Understanding Matrix Operations in Cryptography.
- Growth in the area of Cryptanalysis.

3.2.7 Solved Example

Encryption:



Hill cipher

Encryption

$P = \text{ATTACK}, \quad K = \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$

$$\begin{pmatrix} a \\ t \end{pmatrix} \begin{pmatrix} t \\ a \end{pmatrix} \begin{pmatrix} c \\ k \end{pmatrix} \Rightarrow \begin{pmatrix} 0 \\ 19 \end{pmatrix} \begin{pmatrix} 19 \\ 0 \end{pmatrix} \begin{pmatrix} 2 \\ 10 \end{pmatrix}$$

$$C = KP \bmod 26 = \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix} \begin{bmatrix} 0 \\ 19 \end{bmatrix} \bmod 26 = \begin{bmatrix} 57 \\ 114 \end{bmatrix} \bmod 26$$

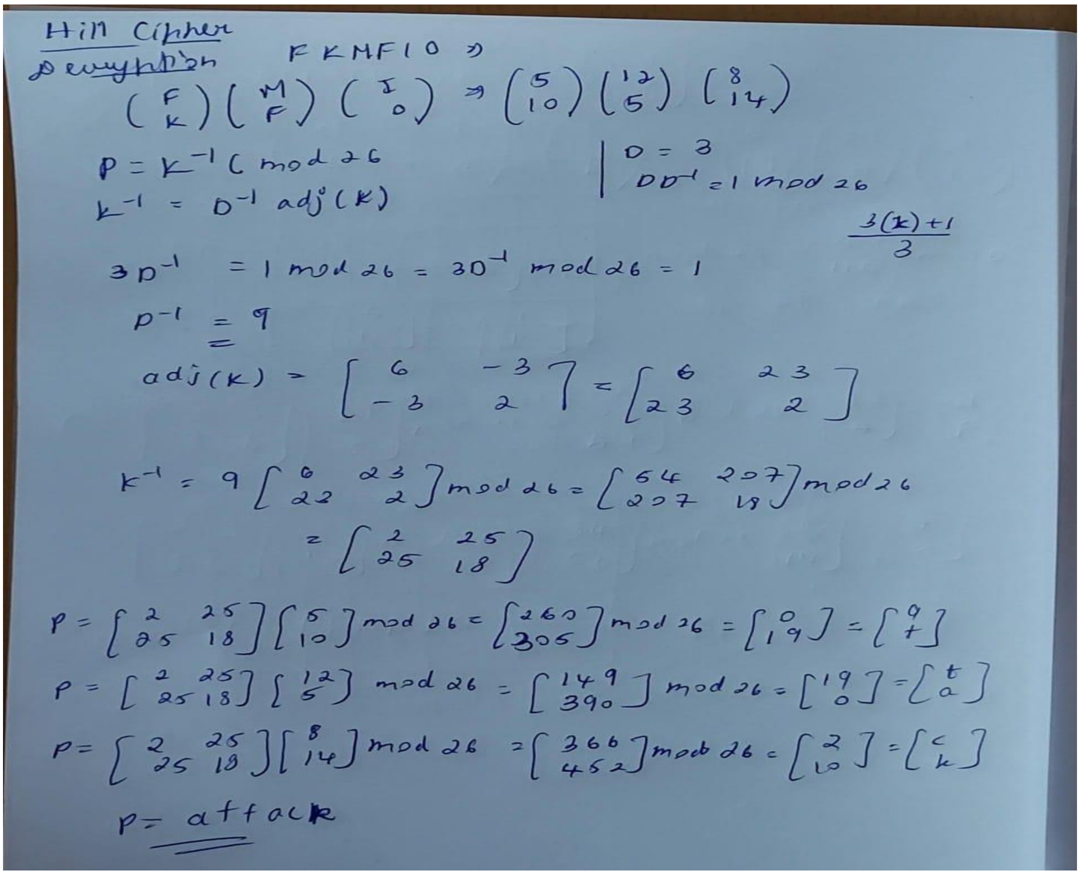
$$\Rightarrow \begin{bmatrix} 5 \\ 10 \end{bmatrix} \Rightarrow \begin{bmatrix} F \\ K \end{bmatrix}$$

$$C = \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix} \begin{bmatrix} 19 \\ 0 \end{bmatrix} \bmod 26 = \begin{bmatrix} 38 \\ 57 \end{bmatrix} \bmod 26 = \begin{bmatrix} 12 \\ 5 \end{bmatrix} = \begin{bmatrix} M \\ F \end{bmatrix}$$

$$C = \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix} \begin{bmatrix} 2 \\ 10 \end{bmatrix} \bmod 26 = \begin{bmatrix} 34 \\ 66 \end{bmatrix} \bmod 26 = \begin{bmatrix} 8 \\ 14 \end{bmatrix} = \begin{bmatrix} I \\ O \end{bmatrix}$$

Ciphertext = FKMFIO

Decryption:



Hill Cipher

Decryption FKMFIO $\Rightarrow$

$$\begin{pmatrix} F \\ K \end{pmatrix} \begin{pmatrix} M \\ F \end{pmatrix} \begin{pmatrix} I \\ O \end{pmatrix} \Rightarrow \begin{pmatrix} 5 \\ 10 \end{pmatrix} \begin{pmatrix} 12 \\ 5 \end{pmatrix} \begin{pmatrix} 8 \\ 14 \end{pmatrix}$$

$P = K^{-1} C \bmod 26$

$K^{-1} = D^{-1} \operatorname{adj}(K)$

$D = 3$

$DD^{-1} = 1 \bmod 26$

$\frac{3(k)+1}{3}$

$3D^{-1} = 1 \bmod 26 = 3D^{-1} \bmod 26 = 1$

$\underline{D^{-1} = 9}$

$$\operatorname{adj}(K) = \begin{bmatrix} 6 & -3 \\ -3 & 2 \end{bmatrix} = \begin{bmatrix} 6 & 23 \\ 23 & 2 \end{bmatrix}$$

$$K^{-1} = 9 \begin{bmatrix} 6 & 23 \\ 22 & 2 \end{bmatrix} \bmod 26 = \begin{bmatrix} 54 & 207 \\ 207 & 18 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix}$$

$$P = \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix} \begin{bmatrix} 5 \\ 10 \end{bmatrix} \bmod 26 = \begin{bmatrix} 260 \\ 305 \end{bmatrix} \bmod 26 = \begin{bmatrix} 0 \\ 19 \end{bmatrix} = \begin{bmatrix} a \\ t \end{bmatrix}$$

$$P = \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix} \begin{bmatrix} 12 \\ 5 \end{bmatrix} \bmod 26 = \begin{bmatrix} 149 \\ 390 \end{bmatrix} \bmod 26 = \begin{bmatrix} 19 \\ 0 \end{bmatrix} = \begin{bmatrix} t \\ a \end{bmatrix}$$

$$P = \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix} \begin{bmatrix} 8 \\ 14 \end{bmatrix} \bmod 26 = \begin{bmatrix} 366 \\ 452 \end{bmatrix} \bmod 26 = \begin{bmatrix} 2 \\ 10 \end{bmatrix} = \begin{bmatrix} c \\ k \end{bmatrix}$$

$P = \underline{\text{attack}}$

3.3 Vigenère Cipher

3.3.1 Computational Complexity

Vigenère cipher is a repeating keyword polyalphabetic substitution cipher.

- Encryption is the process of shifting each character with respect to the key (O(n)).
- Decryption is the process of reversing shifting (O(n)).
- Total complexity: O(n).

3.3.2 Mathematical Formulation

Encryption is performed using:

$$C_i = (P_i + K_i) \, mod \; 26$$

Where:

- C_i the encrypted character,
- P_i is the plaintext character,
- K_i is the key character.

Decryption is:

$$P_i = (C_i - K_i) \, mod \; 26$$

3.3.3 Cryptanalysis

Frequency Analysis: With known key length, frequency patterns can be utilized to deduce shifts.

Modern Attacks:

- Automated Kasiski Examination: Computer algorithms approximate-check for repeating sequences quite fast.
- Index of Coincidence: Utilizes mathematical rationality to ascertain the length of a key.
- Parallel Processing Attack: Modern-day computers attempt to analyze multiple key lengths in parallel.

- Dictionary-Based Attack: Words and phrases in common use may be inputted to attack parts of the keys.

Example of Cryptanalysis:

By Kasiski approach:

- Identify repeated patterns of ciphertext.
- Calculate greatest common divisor of distances to deduce key length.
- Perform frequency analysis for each letter shift.

3.3.4 Time and Space Complexity

Encryption/Decryption Time Complexity: O(n)
Space Complexity: O(n) for storing repeated key.

3.3.5 Security Strengths and Weaknesses

Strengths:

- Polyalphabetic substitution
- Variable key length
- Relatively simple implementation
- Security benefits over monoalphabetic ciphers

Weaknesses:

- The pattern of a repeated key
- Brings vulnerability to Kasiski examination
- Statistical analysis is easy
- Management with respect to keys

3.3.6 Modern Variants

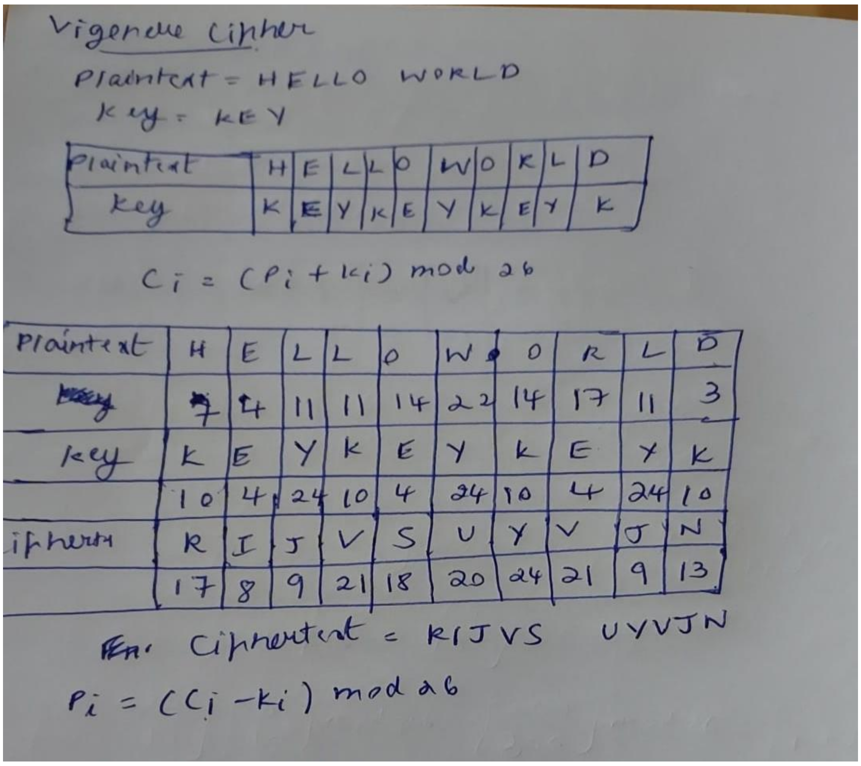
Several modifications improve the basic Vigenère cipher:

- Running Key Variant
- Autokey Cipher
- Progressive key modification

- Multiple Alphabet Substitution

3.3.7 Solved Example

Encryption:



Vigenere cipher

Plaintext = HELLO WORLD

Key = KEY

Plaintext	H	E	L	L	O	W	O	R	L	D
key	K	E	Y	K	E	Y	K	E	Y	K

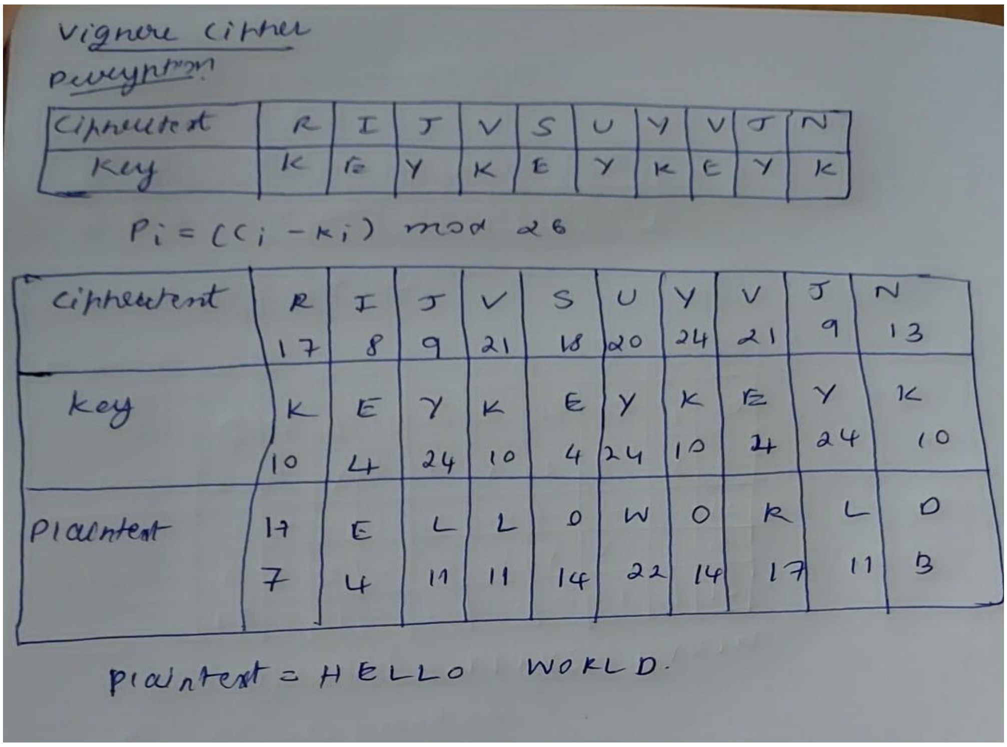
$C_i = (P_i + k_i) \bmod 26$

Plaintext	H	E	L	L	O	W	O	R	L	D
~~key~~	7	4	11	11	14	22	14	17	11	3
key	K	E	Y	K	E	Y	K	E	Y	K
	10	4	24	10	4	24	10	4	24	10
iphertext	R	I	J	V	S	U	Y	V	J	N
	17	8	9	21	18	20	24	21	9	13

~~En.~~ Ciphertext = RIJVS UYVJN

$P_i = (C_i - k_i) \bmod 26$

Decryption:



Vignere cipher
Decryption

Ciphertext	R	I	J	V	S	U	Y	V	J	N
Key	K	E	Y	K	E	Y	K	E	Y	K

$P_i = (C_i - k_i) \bmod 26$

Ciphertext	R 17	I 8	J 9	V 21	S 18	U 20	Y 24	V 21	J 9	N 13
key	K 10	E 4	Y 24	K 10	E 4	Y 24	K 10	E 4	Y 24	K 10
Plaintext	H 7	E 4	L 11	L 11	O 14	W 22	O 14	R 17	L 11	D 3

plaintext = HELLO WORLD.

4. Comparative Analysis

4.1 Security Comparison

A systematic comparison of three classical ciphers reveals:

Playfair:

- Key Space: 25! possible arrangements.
- Primary Strength: Digraph substitution.
- Main Vulnerability: Known plaintext attack.

Hill:

- Key Space: Depends upon matrix size.
- Primary Strength: Mathematical complexity.
- Main Vulnerability: Linear algebra-based attacks.

Vigenère:

- Key Space: 26^k where k is key length.
- Primary Strength: Polyalphabetic substitution.
- Main Vulnerability: Kasiski examination.

4.2 Performance Metrics

Computational performance comparison:

Cipher	**Time Complexity**	**Space Complexity**	**Implementation Difficulty**
Playfair	O(n)	O(1)	Medium
Hill	O(n^3)	O(n^2)	High
Vigenère	O(n)	O(n)	Low

4.3 Implementation Considerations

Common challenges with all implementation:

- Character set handling.
- Key generation and validation.
- Error handling and input sanity.
- Performance optimization.
- Memory management.

5. Modern Applications and Relevance

5.1 Educational Value

Instructional on the basic concepts of cryptography:

- The history of encryption techniques.
- Cultivating skills pertaining to cryptanalysis.
- The importance of key management.

5.2 Building Blocks for Modern Cryptography

- Basic principles of substitution and transposition.
- Mathematical foundation.
- Security analysis methods.
- Techniques for performance optimization.

5.3 Legacy System Considerations

- The study of historical encrypted documents.
- Analysis of older security systems.
- Compatibility with legacy applications.
- Research and documentation of history.

5.4 Industrial Applications

Although classical ciphers fall short against modern security demands, their principles are still evident in:

- Scholarship and educational software meant for cryptography training
- Legacy systems on-the-spots analysis and documentation
- Historical simulation studies revolving around cipher devices
- Basic training on security awareness.

5.5 Applications in Research

Classical ciphers still imply more to cryptographic research with regards to:

- Innovating various methods of cryptanalysis.
- Gaining insight into the basic principles of security.
- Probing into its mathematical fundamentals.
- Testing of contemporary theories of cryptography.

6. Hybrid Cipher Design

For security enhancement, we recommend a hybrid cipher using:

- AES substitution cipher (128-bit strength) for strong confusion.
- Transposition (shuffling) for diffusion.

6.1 Reasoning for Security Enhancement

- Conventional ciphers lack sufficient key space; AES strengthens substitution.
- Transposition adds more entropy, rendering frequency analysis irrelevant.
- The combination balances each weakness, producing a secure encryption algorithm.

6.2 Advanced Security Features

The proposed hybrid system incorporates:

- Dynamic key generation
- Multiple encryption rounds
- Feedbacks
- Error detection and correction.

6.3 Performance Optimization

Optimization strategies include:

- Efficient parallel processing
- Memory utilization efficiency
- Reducing computational overhead
- Scalable implemented.

System Optimization Techniques:

A hybrid design optimizes for performance by balancing:

- Better data structures in order to use memory well.
- With optimized algorithms.
- Also with scalability ratios found for varying message sizes.
- Platform-specific optimizations for different environments where it should be used.

6.4 Security Analysis

- Entropy Analysis: Increased randomness in ciphertext improves security.
- Resistance to Frequency Analysis: The substitution step destroys character distribution, and transposition resists pattern detection.
- Key Space Considerations: AES with a 128-bit key far outshines conventional techniques.

6.5 Time and Space Complexity

Encryption/Decryption Time Complexity: O(n) for transposition, O(n) for AES (constant time block cipher).
Space Complexity: O(n) for storing shuffled text.

7. Implementation & GitHub Repository

The implementation of all ciphers, including the hybrid approach, can be accessed at:
https://github.com/Saanvi-U/Information-Network-and-Security-Lab/tree/master

8. Future Research Directions

8.1 Implications of Quantum Computing

- Effects of classical cryptography
- Adaptation of old methods
- Unique vulnerability assessments
- Modification to include quantum-resistance.

8.2 Integration with Modern Systems

- API development
- Applications in cloud computing
- Adaptation to mobiles
- Issues with IoT devices.

9. Conclusion

This comparison brings out the advantages and disadvantages of Playfair, Hill, and Vigenère ciphers. Traditional encryption methods, though of historical importance, are well known to have flaws. The combination of AES substitution and transposition methods significantly increases security withstanding higher resistance to cryptanalysis.

Traditional encryption knowledge is still relevant to modern cryptography since most modern encryption techniques are based on these basic principles. The addition of advanced techniques can render encryption more resistant to new cyber attacks.

Future studies can involve a comparison of hybrid techniques with modern cryptanalysis techniques to further establish resistance. Additional studies in post-quantum cryptography may also provide insight into securing data in the future quantum computing environment.

9.1 Recommendations:

For practical applications,

- Use classical ciphers purely for educational purposes.

- Implement modern encryption standards for security.
- Observe any advances in cryptography.
- Conduct security assessments and perform patch updates regularly.

9.2 Future Work

Potential areas for further research include:

- High-level hybrid implementations
- Effects of quantum computation
- Performance optimization mechanisms
- And unique methods of cryptanalysis.

10. References

- [1] M. Tarawneh, ‘Perspective Chapter: Cryptography – Recent Advances and Research Perspectives’, Biometrics and Cryptography. IntechOpen, Jun. 19, 2024. doi: 10.5772/intechopen.111847.
- [2] W. Stallings, *Cryptography and Network Security Principles and Practices*, 8th ed. New York, NY: Pearson Education, 2020.