



slington college
(इस्लिंग्टन कलेज)

Module Code & Module Title

CC5009NI Cyber Security in Computing

Assessment Weightage & Type

40% Individual Coursework 01

Year and Semester

2024 -25 Autumn Semester

Student Name: Rohan Prasad Adhikari

London Met ID: 23047505

College ID: NP01NT4A230177

Assignment Due Date: Monday, January 20, 2025

Assignment Submission Date: Monday, January 20, 2025





Word Count (Where required): 9260

I confirm that I understand my coursework needs to be submitted online via My Second teacher (MST) under the relevant module page before the deadline for my assignment to be accepted and marked. I am fully aware that late submissions will be treated as non-submission and a mark of zero will be awarded.




12% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Match Groups

-  **54 Not Cited or Quoted 10%**
Matches with neither in-text citation nor quotation marks
-  **16 Missing Quotations 2%**
Matches that are still very similar to source material
-  **0 Missing Citation 0%**
Matches that have quotation marks, but no in-text citation
-  **0 Cited and Quoted 0%**
Matches with in-text citation present, but no quotation marks

Top Sources

- 7%  Internet sources
- 1%  Publications
- 11%  Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

Abstract

In this report, it explores the basic and the key concepts of computer security, stressing on the paramount aspect of protecting information and other computer resources in the contemporary world that is characterized by information technology. As the utilization of technology, it has filled each person's and organization's life it has become clear that security is the foundation for the protection of data and the functionality of systems. The document covers the basics of security in computing where it defines its main goals, the so-called CIA Triad; that is confidentiality, integrity, and availability. It goes deeper other categories of computer security such as application, information, and network security which aims at addressing particular risks and issues that are faced in computer security in this age of computerized everything.

Cryptography, the subject of vital importance to cybersecurity, occupies a vast part of the report. The historical progression of cryptography is introduced from the simplest form of coded language starting from the Caesar Cipher to modern complex approaches to cryptography such as; symmetric and asymmetric. One contribution of this work is the creation of a new cryptographic algorithm called Spiral Algorithm. In terms of security, the current work introduces original numeric-based operations and logical operators for protecting the Spiral Algorithm, which is inspired by the Vigenère Cipher. This approach rectifies some of the major drawbacks encountered in the traditional ciphers while at the same time simplifying the implementation process. An ideal detail by detail exposition of the algorithm and the processes involved in the encryption and decryption of the algorithm is provided for easy understanding rounded by clear examples, tables and even flowcharts where necessary.

The report also stresses the significance of adequate protective mechanisms in minimizing the threat of cyber-related hazards and safeguarding the data from unauthorized access and manipulation. The possible creation of new algorithms, and ways to escalate the level of security this work offers insights on how to help people and companies guard their digitally accessible assets against the constantly emerging threats in the modern, increasingly technology-based world.

Table of Contents

List of Figures	I
List of Tables	II
1. Introduction	1
1.1. Aims	2
1.2. Objective	2
1.3. Security In computing	2
1.3.1. Objectives of Computer Security	3
1.3.2. Types of Computer Security	3
1.4. CIA Triad	5
1.4.1. Confidentiality, Integrity, and Availability	5
1.4.2. Components of CIA	5
1.4.6. Example of the CIA triad	7
1.4.7. Importance of CIA Triad	7
1.5. History	8
1.5.1. Ancient Beginnings of Cryptography	8
1.5.2. Classical Era of Cryptography	9
1.5.3. Modern Era of Cryptography	9
1.6. Cryptography	9
1.7. Types of Cryptography	10
1.7.1. Symmetric Key Cryptography	10
1.7.2. Asymmetric Key Cryptography	11
1.7.3. Hash Functions	11
2. Background	12
2.1. Vigenère Cipher	12
2.2. How It Works	12
2.3. Example of Vigenère Cipher	13

2.3.1.	Encryption of Vigenère Cipher	13
2.3.2.	Decryption of Vigenère Cipher	14
2.4.	Advantages and Disadvantages	14
2.4.1.	Advantages	14
2.4.2.	Disadvantages	15
3.	Development	16
3.1.	Spiral Algorithm	16
3.2.	Creation of Plaintext, Key and Cipher	16
3.2.1.	Creation of Plaintext and its value	16
3.2.2.	Formation of Key	17
3.2.3.	Formation of Cipher Text and Value	17
3.3.	Mathematical operator	18
3.4.	Logical operator	19
3.5.	Ciphering	19
3.6.	Encryption	19
3.7.	Decryption	22
3.8.	Algorithm	25
3.8.1.	Encryption	25
3.8.2.	Decryption	25
3.9.	Flowchart	26
3.9.1.	Encryption	26
3.9.2.	Decryption	27
4.	Testing	28
4.1.	Testing 1	28
4.2.	Testing 2	33
4.3.	Testing 3	40
4.4.	Testing 4	44

4.5. Testing 5.....	51
5. Analysis.....	61
5.1. Advantages:	61
5.2. Disadvantages:	61
5.3. Application Area	61
6. Conclusion	63
References.....	64

List of Figures

Figure 1 : Types of security (DataFlair Team, 2024).....	3
Figure 2 : CIA TRIAD (CyberOne, 2019).....	5
Figure 3: Cryptography (Weerasuriya, 20200)	10
Figure 4 : Symmetric Cryptography (yathursan, 2020).....	10
Figure 5 : Asymmetric Cryptography (Gupta, 2023)	11
Figure 6 : Hash Functions (tutorialspoint, 2024).....	11
Figure 7 : Vigenère Cipher table (GeeksforGeeks, 2016)	13
Figure 8 : Encryption Flowchart.....	26
Figure 9 : Decryption Flowchart	27

List of Tables

Table 1 : Plaintext table	17
Table 2 : Key and Key value	17
Table 3 : Cipher table	18
Table 4 : Mathematical operator table	18
Table 5 : Logical operator table	19
Table 6 : CIPHERING	19
Table 7 : Encrypting	20
Table 8 : Decrypting	22
Table 9: Testing 1 Encryption	30
Table 10 : Testing 1 Decryption	33
Table 11 : Testing 2 Encryption	36
Table 12: Testing 2 Decryption	39
Table 13 : Testing 3 Encryption	42
Table 14 : Testing 3 Decryption	44
Table 15 : Testing 4 Encryption	47
Table 16 : Testing 4 Decryption	50
Table 17 : Testing 5 Encryption	55
Table 18 : Testing 5 Decryption	60

1. Introduction

In today's technologically connected environment, protecting our computers and saving data may be the most crucial thing. In personal uses such as banking, social communication and sharing, to core business functions, there is an extensive dependence in technology. But this dependence also makes us vulnerable to things such as hacking, unauthorized access and intrusion into our databases. This report provides an overview of the main aspects of computing security and looks at ways to safeguard the systems, data, and communication we use. Fundamental to the protection of computers, is the CIA Triad of Confidentiality, Integrity and Availability. The first three principles preserve privacy, currency, and give controlled availability to data that needs to be accessed in an organization. Other layers such as identity verification (system of verifying users' identity) and monitoring (system of tracking users' activities) supplement general security.

One of the most important components of cybersecurity is cryptography – the science of protecting messages from interception and understanding. This report goes down a brief history of cryptography that covers the Caesar cipher, symmetric encryption, and the KaZaA file-sharing system, and sophisticated new algorithms that can effectively meet new challenges.

Through addressing exposure to threats, mitigating threats, and preparing for threats that may occur this report and article major on how people and organizations can protect themselves from threats in today's digital world. For protecting individual information or business mission-critical activities, the objective of this guide is to unravel the sometimes-confusing realm of computer security and help you sort through what you need to do next.

1.1. Aims

- To have research about security in technology with covering all major's topic like CIA, cryptography and so on. And to develop a new cryptography algorithm and perform testing on it.

1.2. Objective

- To study about Security and its types and importance
- To study about the CIA TRIAD
- To research about the Cryptography
- To develop new Cryptographic algorithm
- To perform testing on newly developed algorithm
- To analyse the advantages and disadvantages of new algorithm

1.3. Security In computing

Security refers to the process of securing hardware, software, systems, and data from potential online threats, unauthorized access, theft, tampering, and destruction. Methods, instruments, and processes guarantee protection in terms of the confidentiality, availability, and integrity of data and systems. Computing prevents possible harm by either external or internal threats while guaranteeing that the systems function consistently and only as intended. (Shari Lawrence Pfleeger, 2024)

Security for computers is essential in this modern digital era. Almost everything we do, including social networking and online banking, depends on computers. But this dependence also leaves us open to cyberattacks. Hackers have the ability to steal our private data, compromise with necessary services, and even harm vital infrastructure. Computer security must be our first priority if we want to safeguard ourselves. We can lower the danger of cyberattacks by using strong passwords, updating software, and exercising precaution when using the internet. To protect their operations and sensitive data, businesses and organizations also need to invest in strong security measures. (Fasano, 2022)

1.3.1. Objectives of Computer Security

The main objective of it is to maintain CIA Triad.

- **Confidentiality:** Ensuring that only authorized individuals have access to sensitive information.
- **Integrity:** Information accuracy, completeness, and unaltered Ness is maintained by integrity in computing security. This involves protecting information from unwanted additions or deletions. We can preserve digital information's reliability and trustworthiness by putting strong security measures in place.
- **Availability:** Making certain that resources and data are available to authorized users when they're needed.
- **Authentication:** Authentication makes guarantee that only people with permission may access data and systems. Various techniques, such as security tokens, biometrics (facial recognition, fingerprint), and passwords, are utilized for this.
- **Accountability:** It is the process of making people answerable for how they behave online. Systems for logging and monitoring user activities are used to achieve this. Organizations are able to prevent threatening actions, enforce regulations, and investigate problems by identifying users and logging behaviours. (GeeksforGeeks, 2022)

1.3.2. Types of Computer Security

These are some of the primary types of computer security methods and techniques that people and companies uses to protect their hardware, software, and private information.



Figure 1 : Types of security (DataFlair Team, 2024)

- **Application Security**

Application security is the term used to describe the introduction of security elements within the first stage of the development process. It is highly effective in defending your computer system from online dangers like illegal access and data breaches. Additionally, it could help your computer system in defending against denial-of-service attempts and SQL attacks.

Some of the main application tools, such as firewalls, antivirus software, and software encryption, are used to install application security features. (Sharma, 2024)

- **Information Security**

Information security is an element of cyber security that focuses on the methods and strategies used to protect computers. Information security as a process was created to safeguard computer systems' confidentiality, availability, and integrity against data theft, illegal access, damage, and destruction. (Sharma, 2024)

- **Endpoint Security**

Using endpoint security is one method for doing that with a mobile workforce. It creates micro-segments around data, wherever it may be, is advised by the zero-trust security concept. By using data and network security controls, complex threat prevention tools like anti-phishing and anti-ransomware, and forensics technologies like endpoint detection and response (EDR) solutions, businesses may protect end-user devices like desktops and laptops. (Point, 2022)

- **Critical infrastructure security**

The networks, apps, systems, and digital assets that critical infrastructure firms (such as those in the public sector, energy, communications, dams, and transportation) depend on are protected using specialized security procedures and cybersecurity solutions. Cyberattacks that target older systems, such as SCADA (supervisory control and data acquisition) systems, have increased the vulnerability of critical infrastructure. (Sailpoint, 2024)

- **Network Security**

Network security, as the name means, is an additional form of computer security that guards against allowed access to your computer networks and breaches into your computer system. In that it protects your computer networks' confidentiality, availability, and integrity, it is comparable to information security. Network security is built to function as efficiently as possible with a variety of settings. It includes hardware and software security. (Hasons, 2024)

1.4. CIA Triad

1.4.1. Confidentiality, Integrity, and Availability.

The CIA triad is an important concept in the information security industry and is used in ISO 27001, a global standard for managing information security. The GDPR also mentions the CIA triad in Article 32, which requires organisations to use appropriate measures to protect the confidentiality, integrity, availability, and resilience of their information processing systems and services.

An essential cybersecurity model that serves as a basis for creating security guidelines intended for protecting data is the CIA triad. The three letters that make up the CIA triad are confidentiality, integrity and availability. One popular model that serves as the foundation for the creation of security systems is the CIA Triad. They are used to identify weaknesses and develop solutions. (Irwin, 2022)

1.4.2. Components of CIA



Figure 2 : CIA TRIAD (CyberOne, 2019)

1.4.3. Confidentiality

Confidentiality is a core principle of information security, ensuring that sensitive data is only accessible to authorized individuals. Passwords, multi-factor authentication (MFA), role-based access control (RBAC), and data encryption during storage and transmission are some of the methods used to manage access. However, insider threats and other forms of assaults including phishing, malware, and system vulnerability exploitation could compromise confidentiality. Maintaining secrecy is essential for preserving consumer confidence, securing company assets, according to privacy laws (such as GDPR or HIPAA), and preserving competitive advantage. Legal consequences, financial loss, and harm to one's reputation may result from breaches. (Knowledgehut, 2022)

1.4.4. Integrity

Integrity ensures that data is correct, genuine, and trustworthy and is not subject to manipulation or unauthorized alterations. It can be hacked purposefully by hackers who get around security measures, change configurations, or manipulate with logs, or unintentionally by people making careless or improper code mistakes. Integrity violations without obvious responsibility might also result from inadequate security practices. Organizations can employ techniques like hashing, encryption, digital certificates, and digital signatures to protect data integrity. One crucial technique for confirming integrity is non-repudiation, which prevents acts by the sender or recipient from being rejected. For example, digital signatures in emails serve as proof of authenticity and reception. (Fortinet, 2023)

1.4.5. Availability

The availability of data is essential in a world where real-time information access is necessary for organizations, services, and technology to function smoothly. Organizations risk process interruptions, financial loss, and a drop in consumer trust if they do not have dependable access to data. Reliable networks, disaster recovery plans, and redundant systems are all necessary components of a strong infrastructure that ensures data availability. Additionally, it is more important than ever to have continuous access to reliable data due to growing automation and networked devices. To preserve sensitive information's

integrity and confidentiality, businesses must strike a balance between security and availability, making sure that although data is available, it is not subject to manipulation or illegal access. (Fortinet, 2023)

1.4.6. Example of the CIA triad

Consider using an e-commerce website to verify your orders and do anything else. The following are the ways in which the e-commerce website applies the three CIA circle principles:

- **Confidentiality:** When you log in, you're asked for a password. If it's been a while since your last log-in, you may be asked to input a code that's been sent to you or some other form of two-factor authentication.
- **Integrity:** Data integrity is provided by making sure your purchases are reflected in your account and allowing you to contact a representative if there's a discrepancy.
- **Availability:** You can log into your account whenever you want, and you may even be able to contact customer support at any time of the day or night. (SecurityScorecard, 2024)

1.4.7. Importance of CIA Triad

- **Secure Data:** By implementing strong security measures like encryption, access controls, data validation, and regular backups, organizations can safeguard their valuable assets and mitigate risks.
- **Identify vulnerabilities:** Weak passwords, out-of-date software, unpatched systems, unsafe network setups, malware infections, social engineering, phishing attempts, insider threats, physical security breaches, and insufficient staff training. For protection of private information, preserve system integrity, and maintain ongoing availability, addressing the vulnerabilities.
- **Risk Management:** Implementing the CIA principles allows organizations to mitigate risks associated with data breaches and cyberattacks. For instance, strong confidentiality controls can prevent unauthorized access, while integrity measures ensure data remains accurate and trustworthy. This comprehensive risk management is essential for safeguarding sensitive information.

- **Incident Response and Recovery:** The CIA triad aids in developing effective incident response plans by clarifying what needs protection during a security incident. Analysing breaches through the lens of the triad allows organizations to identify weaknesses and improve their defences against future incidents. (Leeson, 2024)

1.5. History

From simple substitution ciphers like the **Caesar Cipher** to complex systems like the **Vigenère Cipher**, which introduced encryption keys, to electro-mechanical devices like the **Hebern rotor** and the **Enigma machine**, which were crucial in World War II, cryptography has been used for thousands of years to protect communications. After World War II, cryptography which had previously been mostly military in nature became more significant in the business world. IBM's Lucifer cipher helped the **DES** standard be adopted in 1973. Later, because of weaknesses, **AES** took the role of **DES**. These days, quantum computing poses a threat to encryption, which is why programs like NIST's post-quantum cryptography program are working to create algorithms that are resistant to quantum errors. (Sidhpurwala, 2023)

1.5.1. Ancient Beginnings of Cryptography

- **Egyptian Hieroglyphs:** Back to 1900 BC, they are among the oldest identified uses of cryptography. Non-standard symbols were employed by Egyptian scribes to hide the meaning of specific words or phrases. (Sidhpurwala, 2023)
- **Spartan Scytale:** The scytale is a straightforward transposition cipher used by the Spartans. A piece of paper wrapped around a wooden stick had a message. When it was opened, the message was a puzzled string of letters. (Schneider, 2024)
- **Caesar Cipher:** Julius Caesar used a substitution cipher in which the plaintext's letters were moved down the alphabet by a predetermined number. (Jarry, 2019)

1.5.2. Classical Era of Cryptography

- **Arabic Contributions:** Al-Kindi and Al-Khalil, two Arab mathematicians, made important contributions to cryptanalysis by creating methods such as frequency analysis that decipher monoalphabetic substitution ciphers.
- **Vigenère Cipher:** Blaise de Vigenère created the polyalphabetic Vigenère cipher in the 16th century, and because of its complexity, it was thought to be unreadable for generations. (Schneider, 2024)

1.5.3. Modern Era of Cryptography

- **Enigma Machine:** The German military employed an advanced electromechanical cryptography device known as the Enigma machine during World War II. An important turning point in the history of cryptography was reached when Allied codebreakers, namely Alan Turing and his group at Bletchley Park, cracked it. (Schneider, 2024)
- **DES (Data Encryption Standard):** DES (Data Encryption system), a popular symmetric-key encryption system that was created in the 1970s.
- **AES (Advanced Encryption Standard):** The current symmetric-key encryption standard, AES (Advanced Encryption Standard), provides great security and efficiency levels. (NordLayer, 2021)
- **Public-Key Cryptography:** Using a pair of keys a public key for encryption and a private key for decryption public key cryptography, which was developed in the 1970s, transformed secure communication. (Schneider, 2024)

1.6. Cryptography

The word comes from the Greek word "Krypto's," meaning 'secret' or 'hidden.' The literal translation for cryptography is "secret writing." It comes from the study of cryptology, the art of breaking codes or ancient hieroglyphics and solving them.

The study and use of methods designed to protect data from unwanted access and enable secure communication is known as cryptography. Codes, protocols, and algorithms are used to transform readable data (plaintext) into unreadable

format (ciphertext) and vice versa. Only authorized parties will be able to access the original data thanks to this change. (Chin, 2024)

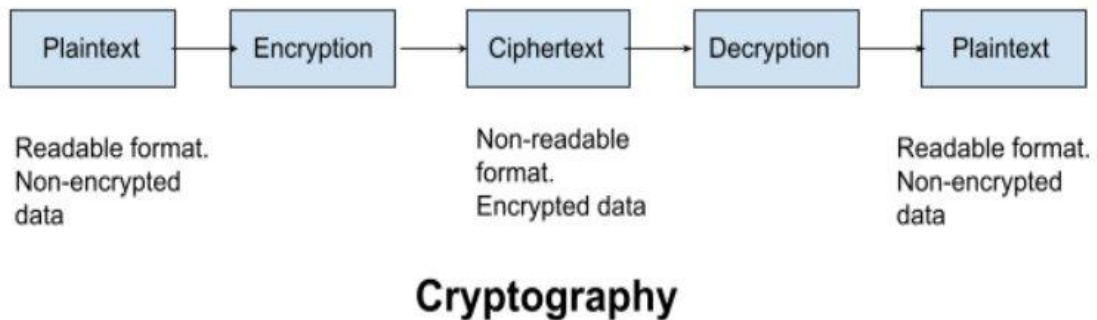


Figure 3: Cryptography (Weerasuriya, 20200)

1.7. Types of Cryptography

1.7.1. Symmetric Key Cryptography

It is an encryption technique in which a single common key is used by both the sender and the recipient to encrypt and decrypt communications. The issue with symmetric key cryptography is that it requires a safe key exchange between the sender and the recipient, despite its speed and simplicity. Advanced Encryption technologies (AES) and Data Encryption Systems (DES) are the two most widely used symmetric key encryption technologies.

Private keys can be distributed via a secure communication channel that has already been created, such as a protected line or private courier, or, more realistically, a secure key exchange technique like the Diffie-Hellman key agreement. (GeeksforGeeks, 2019)

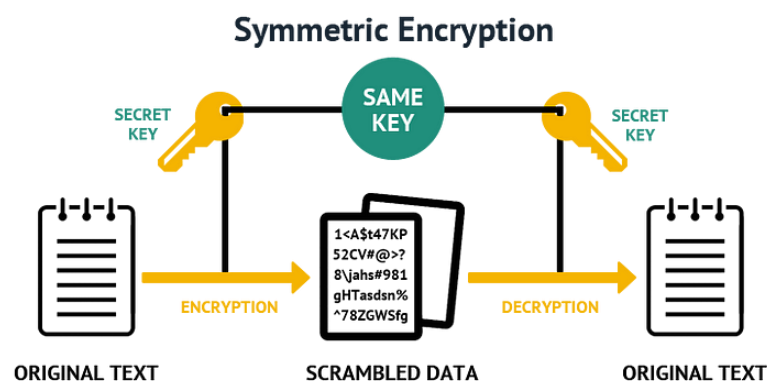


Figure 4 : Symmetric Cryptography (yathursan, 2020)

1.7.2. Asymmetric Key Cryptography

It is also known as Public-key cryptography. It uses two keys one for encryption and other for decryption. This type of encryption is different from symmetric key cryptography and is more secure. Each user of this system uses a pair of keys (private key and public key) to encrypt and decode data. Every user maintains the confidentiality of their private key, but the public key circulates throughout the network, allowing anybody to use it to communicate with any other user. Any one of those keys can be used to encrypt the message, and the other key can be used to decode it. (Singh, 2019)

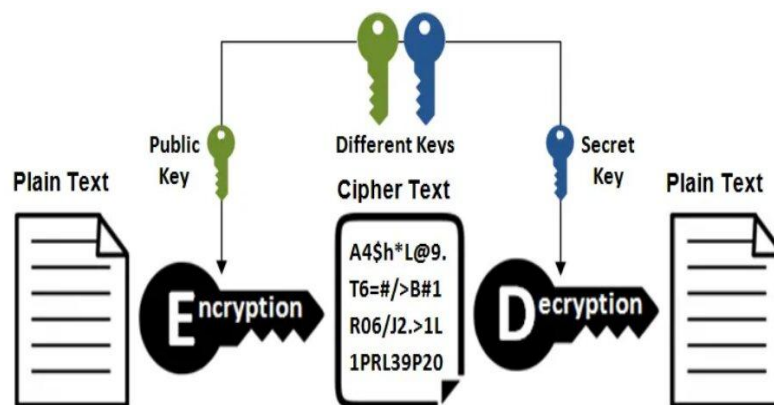


Figure 5 : Asymmetric Cryptography (Gupta, 2023)

1.7.3. Hash Functions

There is no usage of any key in this algorithm. A hash value with a fixed length is calculated as per the plain text which makes it impossible for the contents of plain text to be recovered. Many operating systems use hash functions to encrypt passwords. (tutorialspoint, 2024)

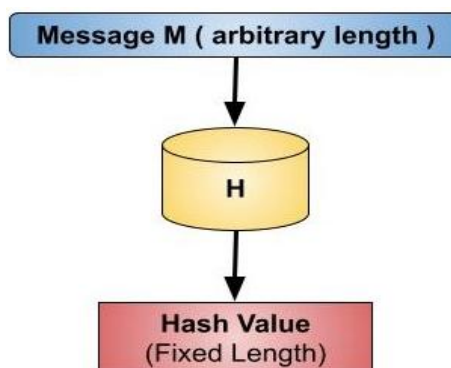


Figure 6 : Hash Functions (tutorialspoint, 2024)

2. Background

2.1. Vigenère Cipher

The Vigenère cipher is a method of encrypting alphabetic text. It employs many replacement alphabets, making it a kind of polyalphabetic substitution cipher. Because of this, it is far more difficult to decipher than straightforward substitution ciphers.

The Vigenère cipher, while often attributed to Blaise de Vigenère, was actually first described by Giovan Battista Bellaso in 1553. However, due to Vigenère's popularization of the cipher in his 1586 book "Traicté des Chiffres," it became associated with his name. The Vigenère encryption made frequency analysis significantly more challenging by employing a repeating key. Because of this, it was a powerful encryption technique at the time and was known as "indecipherable." But as cryptanalysis techniques improved, strategies to crack the Vigenère encryption were created, such as the index of coincidence and Kasiski inspection.

The Vigenère encryption is no longer regarded as secure, despite its historical significance and once-unbreakable reputation. It is a useful illustration of how encryption methods have changed throughout time and the continuous battle among codemakers and codebreakers. (Kester, 2012)

2.2. How It Works

To encrypt a message using the Vigenère cipher, the following steps are followed:

- i. **Choose a Keyword:** A keyword is selected, which will dictate the encryption shifts.
- ii. **Repeat the Keyword:** The keyword is repeated until it matches the length of the plaintext message.
- iii. **Encryption Process:**
 - Each letter in the plaintext is shifted according to the corresponding letter in the keyword.
 - The shift value for each letter is determined by its position in the alphabet (A=0, B=1, ..., Z=25).
 - The resulting letter from this shift forms part of the ciphertext.

- iv. Decryption Process: Decryption involves reversing the encryption steps by shifting back according to the keyword.

2.3. Example of Vigenère Cipher

2.3.1. Encryption of Vigenère Cipher

The key's first letter, A, is linked with the plaintext's first letter, G. Use the Vigenère square's row G and column A, namely G. Likewise, for the second letter of the plaintext, the letter in row E and column Y is C, which is also the second letter of the key. A similar method is used to encrypt the remaining plaintext. (GeeksforGeeks, 2016)

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

Figure 7 : Vigenère Cipher table (GeeksforGeeks, 2016)

Input: Plaintext: GEEKSFORGEEKS

Keyword: AYUSH

Output: Ciphertext: GCYCFMPLYEIM

For generating key, the given keyword is repeated in a circular manner until it matches the length of the plain text.

The keyword "AYUSH" generates the key "AYUSHAYUSHAYU" The plain text is then encrypted using the process explained above.

(GeeksforGeeks, 2016)

2.3.2. Decryption of Vigenère Cipher

Decryption is done by locating the ciphertext letter in the row that corresponds to the key in the table, then using the label of the column as the plaintext. In row A (from AYUSH), for instance, the first plaintext letter, column G, has the ciphertext G. The second plaintext letter is E, which we find in column E after moving to row Y (from AYUSH) and locating the ciphertext C.

(GeeksforGeeks, 2016)

An easier **implementation** could be to visualize Vigenère algebraically by converting [A-Z] into numbers [0–25].

Encryption:

The plaintext(P) and key(K) are added modulo 26.

$$E_i = (P_i + K_i) \bmod 26$$

Decryption:

$$D_i = (E_i - K_i) \bmod 26$$

Note: D_i denotes the offset of the i -th character of the plaintext. Like offset of **A** is 0 and of **B** is 1 and so on.

2.4. Advantages and Disadvantages

2.4.1. Advantages

- **Increased Security:** The use of multiple cipher alphabets makes it more secure than monoalphabetic ciphers. (Tutorialspoint, 2024)
- **Resistance to Frequency Analysis:** It disrupts frequency analysis by masking letter frequencies in plaintext, making it difficult for attackers to decipher messages based solely on letter frequency patterns. (Tutorialspoint, 2024)
- **Flexibility with Key Management:** Different keywords can be used for different messages, allowing for enhanced security through variability. (Tutorialspoint, 2024)
- **Moderate Complexity:** It is relatively easy to implement and understand compared to more complex modern encryption techniques. (Learnearn., 2023)
- **Wide Key Space:** The potential number of keys grows exponentially with key length, making brute-force attacks impractical against long keys. (Learnearn., 2023)

2.4.2. Disadvantages

- **Vulnerability to Cryptanalysis:** Despite its strengths, it can be broken using techniques such as Kasiski examination and Friedman test if the key length is known or guessed. (Learnearn., 2023)
- **Key Repetition Weakness:** The repeating nature of the keyword can create patterns that are exploitable by cryptanalysts. (Tutorialspoint, 2024)
- **Known-Plaintext Attacks:** If an attacker knows parts of both plaintext and ciphertext, they can derive information about the keyword used. (Tutorialspoint, 2024)
- **No Authentication or Integrity:** It provides confidentiality but lacks mechanisms for ensuring message integrity or authenticity, making it susceptible to tampering. (Learnearn., 2023)
- **Key Management Issues:** Long and complex keys are harder to remember and manage, which can lead to security weaknesses if keys are reused or poorly chosen. (Learnearn., 2023)

3. Development

3.1. Spiral Algorithm

The new algorithm is named the **Spiral Algorithm** and is inspired by the Vigenère Cipher, which was invented by Leon Battista Alberti in 1467. The Vigenère Cipher encodes alphabetic text using a polyalphabetic substitution method, where a key and cipher text are used to encrypt and decrypt the plaintext. In the Spiral Algorithm, numeric values are assigned to each alphabet letter, and mathematical operators are used for encrypting and decrypting instead of the traditional approach. This makes the process a bit easier compared to the Vigenère Cipher, as the use of numbers simplifies the operations.

3.2. Creation of Plaintext, Key and Cipher

First, a numeric table was created for all the alphabet letters, assigning each letter a numeric value. Then, a key was made using the word **SPIRAL**, with its numeric values placed randomly. After that, a Cipher Letters and Cipher Values table was produced. In this table, all the alphabet letters were arranged in the ascending order of the **QWERTY** keyboard pattern. The values for the keyword were placed accordingly, and the cipher letters were given random values that were not based on any specific pattern.

3.2.1. Creation of Plaintext and its value

The original table used in the algorithm had alphabet letters arranged for both rows and columns in alphanumeric order. This was changed into a numeric table. In the updated version, all uppercase alphabets from A-Z were assigned numeric values from 0-25, and the value 26 was assigned for spaces. In this algorithm, there are no case sensitivity issues. Both capital and small letters are treated equally, meaning they hold the same value. This applies to plaintext. The table for plaintext is shown below.

Plain Text	Plaintext Value	Plain Text	Plaintext Value	Plain Text	Plaintext Value	Plain Text	Plaintext Value	Plain Value	Plaintext Value
A	0	G	6	M	12	S	18	Y	24
B	1	H	7	N	13	T	19	Z	25
C	2	I	8	O	14	U	20	Space	26

D	3	J	9	P	12	V	21		
E	4	K	10	Q	16	W	22		
F	5	L	11	R	17	X	23		

Table 1 : Plaintext table

Example: Plaintext: APPLE

Plaintext	Plaintext value
A	0
P	15
P	15
L	11
E	4

3.2.2. Formation of Key

To display the rules and numeric values of the plaintext, a custom key word was also created along with its corresponding key values. The word SPIRAL was chosen as the key, and the value assigned to each letter in the key is constant and fixed. The respective values are provided below.

Key Word	Key value
S	2
P	4
I	6
R	5
A	3
L	1

Table 2 : Key and Key value

3.2.3. Formation of Cipher Text and Value

Finally, a table was designed for the cipher text and its corresponding values. The cipher values were assigned to the cipher text, following the key placement protocol based on the QWERTY order. The cipher values were chosen but they are fixed and constant. The table for these values is provided below.

Cipher Text	Cipher Value	Cipher Text	Cipher Value	Cipher Text	Cipher Value	Cipher Text	Cipher Value
Q	0	O	8	J	16	N	24
W	1	P	9	K	17	M	25
E	2	A	10	L	18	SPACE	26
R	3	S	11	Z	19	!	27
T	4	D	12	X	20	@	28
Y	5	F	13	C	21	\$	29
U	6	G	14	V	22	#	30
I	7	H	15	B	23	%	31
						&	32

Table 3 : Cipher table

3.3. Mathematical operator

After creating the Plaintext, Key, and Cipher Text along with their values, a mathematical operation was performed, which was straightforward. The values of the plaintext and the key were placed in the table, and their sum was calculated. This process hides the importance of the key within the operation.

The key word was repeated to match the length of the plaintext, and if the plaintext was shorter, only the required key values were used. Finally, the sum of the plaintext values was obtained, referred to as the shift value, along with the numeric value of the key.

Plaintext	Plaintext value	Key	Key value	Shift value
A	0	S	2	2
P	15	P	4	19
P	15	I	6	21
L	11	R	5	16
E	4	A	3	7

Table 4 : Mathematical operator table

3.4. Logical operator

Finally, the process reached the mathematical operator stage. At this point, the **shift value**, originally in decimal form, was converted into binary for encryption and decryption. After the conversion, a **NOT operation** was applied to the binary form of the shift value.

Plain Text	Value	BINARY	NOT Value	Cipher value
A	2	00010	11101	29
P	19	10011	01100	12
P	21	10101	01010	10
L	16	10000	01111	15
E	7	00111	11000	24

Table 5 : Logical operator table

3.5. Ciphering

In the final stage of encryption, the logical result of the decimal value obtained was used, and the corresponding alphabetical character from the table was assigned to it.

PLAINTEXT = APPLE

CIPHER TEXT = \$MKPY

CIPHER VALUE	CIPHER TEXT
29	\$
12	M
10	K
15	P
24	Y

Table 6 : Ciphering

3.6. Encryption

Plaintext: HARISH

Plaintext	Plaintext Value	Key	Key Value	Shift Value	BINARY	NOT	Cipher VALUE	CIPHER
H	7	S	2	9	01001	10110	22	V
A	0	P	4	4	00100	11011	27	!

R	17	I	6	23	10111	01000	8	O
I	8	R	5	13	01101	10010	18	L
S	18	A	3	21	10101	01010	10	A
H	7	L	1	8	01000	10111	23	B

Table 7 : Encrypting

- entered the plaintext as HARISH
- input the value of HARISH from plaintext table

Plaintext	Plaintext Value
H	7
A	0
R	17
I	8
S	18
H	7

- entered key with its key value from the key table

Key	Key Value
S	2
P	4
I	6
R	5
A	3
L	1

- after that summed the value of plaintext and key known as shift value

Plaintext Value	Key Value	Shift Value
7	2	9
0	4	4
17	6	23
8	5	13
18	3	21

7	1	8
---	---	---

- converted the shift value into the binary

Shift value	Binary
9	01001
4	00100
23	10111
13	01101
21	10101
8	01000

- applied NOT logical operator to the binary value

Binary	Not
01001	10110
00100	11011
10111	01000
01101	10010
10101	01010
01000	10111

- convert the NOT value in decimal again known as cipher value

Not	Cipher value
10110	22
11011	27
1000	8
10010	18
1010	10
10111	23

- input the cipher value and entered the correct letters of cipher value

Cipher value	Cipher
--------------	--------

22	V
27	!
8	O
18	L
10	A
23	B

- and at last, plaintext converted as V!OLAB

3.7. Decryption

Cipher text: V!OLAB

Cipher	Cipher Value	Binary	Not	Shift Value	Key	Key value	Plaintext VALUE	Plaintext
V	22	10110	01001	9	S	2	7	H
!	27	11011	00100	4	P	4	0	A
O	8	01000	10111	23	I	6	17	R
L	18	10010	01101	13	R	5	8	I
A	10	01010	10101	21	A	3	18	S
B	23	10111	01000	8	L	1	7	H

Table 8 : Decrypting

- entered the cipher text in table: V!OLAB
- input the correct values of letter from the cipher table

Cipher	Cipher Value
V	22
!	27
O	8
L	18
A	10
B	23

- convert it into binary

Cipher Value	Binary
22	10110
27	11011
8	01000
18	10010
10	01010
23	10111

- applied NOT logical operator

Binary	Not
10110	01001
11011	00100
01000	10111
10010	01101
01010	10101
10111	01000

- convert the NOT value in decimal; shift value

Not	Shift Value
01001	9
00100	4
10111	23
01101	13
10101	21
01000	8

- input the key and the key value

Key	Key value
S	2

P	4
I	6
R	5
A	3
L	1

- subtracted the key with shift value which is plaintext value

Shift value	Key	Key value	Plaintext value
9	S	2	7
4	P	4	0
23	I	6	17
13	R	5	8
21	A	3	18
8	L	1	7

- arrange the letters with plaintext value

Plaintext value	Plaintext
7	H
0	A
17	R
8	I
18	S
7	H

- and at last, we got the plaintext: HARISH

3.8. Algorithm

3.8.1. Encryption

Step 1: input plain text in the table

Step 2: input the value of plain text

Step 3: insert key with plaintext

Step 4: input the value of key

Step 5: sum the value of key and plain text

Step 6: convert the sum value into the binary

Step 7: apply NOT logical operator

Step 8: convert the NOT value in decimal

Step 9: input the decimal value in table named as cipher value

Step 10: input and arrange the correct letters of cipher value

3.8.2. Decryption

Step 1: input the cipher text in table

Step 2: input the correct cipher values of letter

Step 3: convert it into binary

Step 4: apply NOT logical operator

Step 5: convert the NOT value in decimal

Step 6: input the decimal value; shift value

Step 7: input the key

Step 8: input the key value

Step 9: subtract the key with shift value

Step 10: subtracted value is plaintext value

Step 11: arrange the letters with plaintext value; plaintext

3.9. Flowchart

3.9.1. Encryption

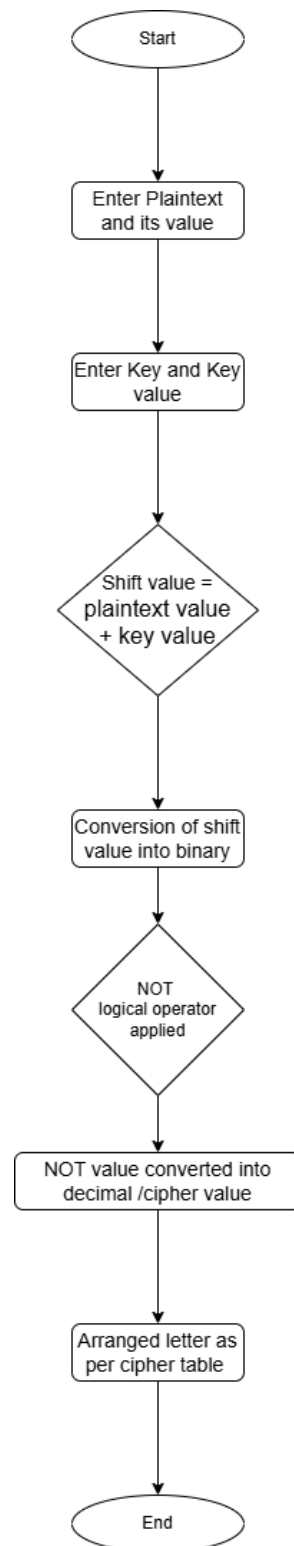


Figure 8 : Encryption Flowchart

3.9.2. Decryption

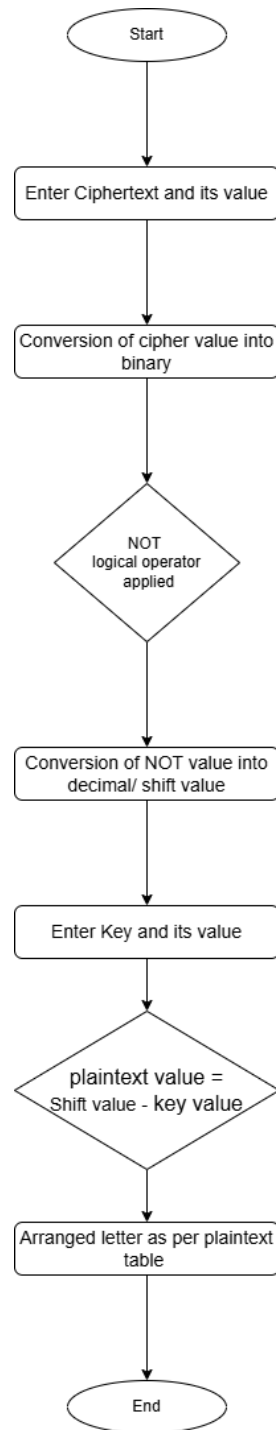


Figure 9 : Decryption Flowchart

4. Testing

The testing section of the document explains how the Spiral Algorithm works for encryption and decryption. It shows step-by-step examples that make it easy to understand how plaintext (regular text) is changed into ciphertext (coded text) and then back to plaintext. The process begins with taking the plaintext and matching it with its numeric values from a predefined table. Then, a key is used, and its numeric values are added to the plaintext values. This sum, called the "shift value," is converted into binary numbers. After that, a logical NOT operation is applied to these binary numbers, flipping them. The flipped binary is turned back into decimal numbers, which are used to find the final coded characters that form the ciphertext.

To decode the ciphertext, the process is reversed. First, the ciphertext values are converted into binary, and the NOT operation is undone. The binary is then changed back into decimal numbers. Using the same key values, the original plaintext numbers are calculated by subtracting the key values from the shifted values. These numbers are then matched with their corresponding characters to reveal the original text.

The document includes five examples of how this encryption and decryption process works. For example, the plaintext "A DOG" is encrypted into "\$BVDV" by following all the steps. Similarly, the ciphertext "\$BVDV" is decrypted back into "A DOG" using the reverse steps. Other examples, such as "AN ATTACK" and "SUDDENLY," show how the process can be repeated for different types of text.

4.1. Testing 1

Encryption:

Plaintext: A DOG

Steps:

- entered the plaintext as: **A DOG**
- input the value of A DOG from plaintext table

Plaintext	Plaintext Value
A	0
Space	26

D	3
O	14
G	6

- entered key with its key value from the key table (as much needed for plaintext FROM KEY SPRIAL)

Key	Key Value
S	2
P	4
I	6
R	5
A	3

- after that summed the value of plaintext and key known as shift value

Plaintext	Plaintext Value	Key	Key Value	Shift Value
A	0	S	2	2
space	26	P	4	30
D	3	I	6	9
O	14	R	5	19
G	6	A	3	9

- converted the shift value into the binary

Shift Value	Binary
2	00010
30	11110
9	01001
19	10011
9	01001

- applied NOT logical operator to the binary value

Binary	Not
00010	11101

11110	00001
01001	10110
10011	01100
01001	10110

- convert the NOT value in decimal again known as cipher value

Not	Cipher value
11101	29
00001	1
10110	22
01100	12
10110	22

- input the cipher value in table with the correct letters of cipher value

Cipher Value	Cipher Text
29	\$
1	B
22	V
12	D
22	V

- and at last, plaintext converted as: **\$BVDV**

Encryption								
Plaintext	Plaintext value	Key	Key Value	Shift Value	Binary	Not	Cipher Value	Cipher
A	0	S	2	2	00010	11101	29	\$
Space	26	P	4	30	11110	00001	1	B
D	3	I	6	9	01001	10110	22	V
O	14	R	5	19	10011	01100	12	D
G	6	A	3	9	01001	10110	22	V

Table 9: Testing 1 Encryption

Plaintext: A DOG

Cipher text: \$BVDV

Decryption:

Cipher text: \$BVDV

Steps:

- entered the cipher text in table: **\$BVDV**
- input the correct values of letter from the cipher table

Cipher text	Cipher value
\$	29
B	1
V	22
D	12
V	22

- convert it into binary

Cipher Value	Binary
29	11101
1	00001
22	10110
12	01100
22	10110

- applied NOT logical operator

Binary	Not
11101	00010
00001	11110
10110	01001
01100	10011
10110	01001

- convert the NOT value in decimal named as Shift value

Not	Shift Value
00010	2
11110	30
01001	9
10011	19
01001	9

- input the key and the key value

Key	Key value
S	2
P	4
I	6
R	5
A	3

- subtracted the key with shift value which will be the plaintext value

Key	Key value	Plaintext value
S	2	0
P	4	26
I	6	3
R	5	14
A	3	6

- arrange the letters with plaintext value

Plaintext value	Plaintext
0	A
26	space
3	D
14	O
6	G

- and at last, we got the plaintext: A DOG

DECRYPTION								
Cipher Text	Cipher Value	Binary	Not	Shift Value	Key	Key value	Plaintext VALUE	Plaintext
\$	29	11101	00010	2	S	2	0	A
B	1	00001	11110	30	P	4	26	space
V	22	10110	01001	9	I	6	3	D
D	12	01100	10011	19	R	5	14	O
V	22	10110	01001	9	A	3	6	G

Table 10 : Testing 1 Decryption

Cipher text: \$BVDV

Plaintext: A DOG

4.2. Testing 2

Encryption:

Plaintext: AN ATTACK

Steps:

- entered the plaintext as: AN ATTACK
- input the value of AN ATTACK from plaintext table

Plaintext	Plaintext Number
A	0
N	13
Space	26
A	0
T	19
T	19
A	0
C	2
K	10

- entered key with its key value from the key table

Key	Key Number
S	2
P	4
I	6
R	5
A	3
L	1
S	2
P	4
I	6

- after that summed the value of plaintext and key known as shift value

Plain text	Key	Plaintext No.	Key no.	Shift Value
A	S	0	2	2
N	P	13	4	17
Space	I	26	6	32
A	R	0	5	5
T	A	19	3	22
T	L	19	1	20
A	S	0	2	2
C	P	2	4	6
K	I	10	6	16

- converted the shift value into the binary

Shift value	Binary
2	00010
17	10001
32	100000
5	00101
22	10110
20	10100

2	00010
6	00110
16	10000

- applied NOT logical operator to the binary value

Binary	Not
00010	11101
10001	01110
100000	011111
00101	11010
10110	01001
10100	01011
00010	11101
00110	11001
10000	01111

- convert the NOT value in decimal again known as cipher value

Not	Chiper value
11101	29
01110	14
011111	31
11010	26
01001	9
01011	11
11101	29
11001	25
01111	15

- input the cipher value in table and placed the correct letters of cipher value

Cipher Value	Cipher Text
29	\$
14	G
31	%
26	SPACE
9	V
11	S
29	\$
25	M
15	H

- and at last, plaintext converted as: \$G% VS\$MH

Encryption								
Plain text	Key	Pt. No.	Key no.	Shift value	Binary	Not	Chiper value	Cipher text
A	S	0	2	2	00010	11101	29	\$
N	P	13	4	17	10001	01110	14	G
Space	I	26	6	32	100000	011111	31	%
A	R	0	5	5	00101	11010	26	Space
T	A	19	3	22	10110	01001	9	V
T	L	19	1	20	10100	01011	11	S
A	S	0	2	2	00010	11101	29	\$
C	P	2	4	6	00110	11001	25	M
K	I	10	6	16	10000	01111	15	H

Table 11 : Testing 2 Encryption

Plaintext: AN ATTACK

Cipher text: \$G% VS\$MH

Decryption:

Cipher text: \$G% VS\$MH

Steps:

- entered the cipher text in table: \$G% VS\$MH
- input the correct values of letter from the cipher table

Cipher	Cipher value
\$	29
G	14
%	31
Space	26
V	9
S	11
\$	29
M	25
H	15

- convert it into binary

Cipher value	Binary
29	11101
14	01110
31	11111
26	11010
9	01001
11	01011
29	11101
25	11001
15	01111

- applied NOT logical operator

Binary	Not
11101	00010
01110	10001
11111	10000
11010	00101
01001	10110

01011	10100
11101	00010
11001	00110
01111	10000

- convert the NOT value in decimal; shift value

Not	Shift value
00010	2
10001	17
100000	32
00101	5
10110	22
10100	20
00010	2
00110	6
10000	16

- input the key and the key value

Key	Key value
S	2
P	4
I	6
R	5
A	3
L	1
S	2
P	4
I	6

- subtracted the key with shift value named as plaintext value

Shift value	Key value	Plaintext value
2	2	0

17	4	13
32	6	26
5	5	0
22	3	19
20	1	19
2	2	0
6	4	2
16	6	10

- arrange the letters with plaintext value

Plaintext Value	Plain Text
0	A
13	N
26	SPACE
0	A
19	T
19	T
0	A
2	C
10	K

- and at last, we got the plaintext: AN ATTACK

Decryption								
Cipher	Cipher value	Binary	Not	Shift value	Key	Key value	Pt Value	Plain text
\$	29	11101	00010	2	S	2	0	A
G	14	01110	10001	17	P	4	13	N
%	31	11111	100000	32	I	6	26	Space
Space	26	11010	00101	5	R	5	0	A
V	9	01001	10110	22	A	3	19	T
S	11	01011	10100	20	L	1	19	T
\$	29	11101	00010	2	S	2	0	A
M	25	11001	00110	6	P	4	2	C
H	15	01111	10000	16	I	6	10	K

Table 12: Testing 2 Decryption

Cipher text: \$G% VS\$MH

Plaintext: AN ATTACK

4.3. Testing 3

Encryption:

Plaintext: BARKS

Steps:

- entered the plaintext as: BARKS
- input the value of BARKS from plaintext table

Plain text	Plaintext number
B	1
A	0
R	17
K	10
S	18

- entered key with its key value from the key table

Key	Pt. No.	Key no.
S	1	2
P	0	4
I	17	6
R	10	5
A	18	3

- after that I summed the value of plaintext and key known as shift value

Pt. No.	Key no.	Shift value
1	2	3
0	4	4
17	6	23
10	5	15
18	3	21

- converted the shift value into the binary

Shift value	Binary
3	00011
4	00100
23	10111
15	01111
21	10101

- applied NOT logical operator to the binary value

Binary	Not
00011	11100
00100	11011
10111	01000
01111	10000
10101	01010

- convert the NOT value in decimal again known as cipher value

Not	Chiper value
11100	28
11011	27
01000	8
10000	16
01010	10

- input the cipher value in table and the correct letters of cipher value

Chiper value	Cipher text
28	@
27	!
8	O
16	J
10	A

- and at last, plaintext converted as: @!OJA

Encryption								
Plain text	Key	Pt. No.	Key no.	Shift value	Binary	Not	Chiper value	Cipher text
B	S	1	2	3	00011	11100	28	@
A	P	0	4	4	00100	11011	27	!
R	I	17	6	23	10111	01000	8	O
K	R	10	5	15	01111	10000	16	J
S	A	18	3	21	10101	01010	10	A

Table 13 : Testing 3 Encryption

Plaintext: BARKS

Cipher text: @!OJA

Decryption:

Cipher text: @!OJA

Steps:

- entered the cipher text in table: @!OJA
- input the correct values of letter from the cipher table

Cipher	Cipher value
@	28
!	27
O	8
J	16
A	10

- convert the cipher value into binary

Cipher value	Binary
28	11100
27	11011
8	01000
16	10000
10	01010

- applied NOT logical operator

Binary	Not
11100	00011
11011	00100
01000	10111
10000	01111
01010	10101

- convert the NOT value in decimal; shift value

Not	Shift value
00011	3
00100	4
10111	23
01111	15
10101	21

- input the key and the key value

Key	Key value
S	2
P	4
I	6
R	5
A	3

- subtracted the key with shift value named as plaintext value

Shift value	Key value	Pt value
3	2	1
4	4	0
23	6	17
15	5	10
21	3	18

- arrange the letters with plaintext value

Pt value	Plain text
1	B
0	A
17	R
10	K
18	S

- and at last, we got the plaintext: BARKS

Decryption								
Cipher	Cipher value	Binary	Not	Shift value	Key	Key value	Pt value	Plain text
@	28	11100	00011	3	S	2	1	B
!	27	11011	00100	4	P	4	0	A
O	8	01000	10111	23	I	6	17	R
J	16	10000	01111	15	R	5	10	K
A	10	01010	10101	21	A	3	18	S

Table 14 : Testing 3 Decryption

Cipher text: @!OJA

Plaintext: BARKS

4.4. Testing 4

Encryption:

Plaintext: SUDDENLY

Steps:

- entered the plaintext as: SUDDENLY
- input the value of SUDDENLY from plaintext table

Plain text	Pt. No.
S	18
U	15
D	3
D	3
E	4

N	13
L	11
Y	24

- entered key with its key value from the key table

Key	Key no.
S	2
P	4
I	6
R	5
A	3
L	1
S	2
P	4

- after that I summed the value of plaintext and key known as shift value

Plain text	Key	Pt. No.	Key no.	Shift value
S	S	18	2	20
U	P	15	4	19
D	I	3	6	9
D	R	3	5	8
E	A	4	3	7
N	L	13	1	14
L	S	11	2	13
Y	P	24	4	28

- converted the shift value into the binary

Shift value	Binary
20	10100
19	10011
9	01001

8	01000
7	00111
14	01110
13	01101
28	11100

- applied NOT logical operator to the binary value

Binary	Not
10100	01011
10011	01100
01001	10110
01000	10111
00111	11000
01110	10001
01101	10010
11100	00011

- convert the NOT value in decimal again known as cipher value

Not	Chiper value
01011	11
01100	12
10110	22
10111	23
11000	24
10001	17
10010	18
00011	3

- input the cipher value and entered the correct letters of cipher value

Chiper value	Cipher text
11	S

12	D
22	V
23	B
24	N
17	K
18	L
3	R

- and at last, plaintext converted as: SDVBNKLR

Encryption								
Plain text	Key	Pt. No.	Key no.	Shift value	Binary	Not	Chiper value	Cipher text
S	S	18	2	20	10100	01011	11	S
U	P	15	4	19	10011	01100	12	D
D	I	3	6	9	01001	10110	22	V
D	R	3	5	8	01000	10111	23	B
E	A	4	3	7	00111	11000	24	N
N	L	13	1	14	01110	10001	17	K
L	S	11	2	13	01101	10010	18	L
Y	P	24	4	28	11100	00011	3	R

Table 15 : Testing 4 Encryption

Plaintext: SUDDENLY

Cipher text: SDVBNKLR

Decryption:

Cipher text: SDVBNKLR

Steps:

- entered the cipher text in table: SDVBNKLR

- input the correct values of letter from the cipher table

Cipher	Cipher value
S	11
D	12
V	22
B	23
N	24
K	17
L	18
R	3

- convert it into binary

Cipher value	Binary
11	01011
12	01100
22	10110
23	10111
24	11000
17	10001
18	10010
3	00011

- applied NOT logical operator

Binary	Not
01011	10100
01100	10011
10110	01001
10111	01000
11000	00111
10001	01110

10010	01101
00011	11100

- convert the NOT value in decimal; shift value

Not	Shift value
10100	20
10011	19
01001	9
01000	8
00111	7
01110	14
01101	13
11100	28

- input the key and the key value

Key	Key value
S	2
P	4
I	6
R	5
A	3
L	1
S	2
P	4

- subtracted the key with shift value which is plaintext value

Shift value	Key value	Pt value
20	2	18
19	4	15
9	6	3
8	5	3

7	3	4
14	1	13
13	2	11
28	4	24

- arrange the letters with plaintext value

Pt value	Plain text
18	S
15	U
3	D
3	D
4	E
13	N
11	L
24	Y

- and at last, we got the plaintext: SUDDENLY

Decryption								
Cipher	Cipher value	Binary	Not	Shift value	Key	Key value	Pt value	Plain text
S	11	01011	10100	20	S	2	18	S
D	12	01100	10011	19	P	4	15	U
V	22	10110	01001	9	I	6	3	D
B	23	10111	01000	8	R	5	3	D
N	24	11000	00111	7	A	3	4	E
K	17	10001	01110	14	L	1	13	N
L	18	10010	01101	13	S	2	11	L
R	3	00011	11100	28	P	4	24	Y

Table 16 : Testing 4 Decryption

Cipher text: SDVBNKLR

Plaintext: SUDDENLY

4.5. Testing 5

Encryption:

Plaintext: HARI PLAY BALL

Steps:

- entered the plaintext as: HARI PLAY BALL
- input the value of HARI PLAY BALL from plaintext table

Plain text	Pt. No.
H	7
A	0
R	17
I	8
Space	26
P	15
L	11
A	0
Y	24
Space	26
B	1
A	0
L	11
L	11

- entered key with its key value from the key table

Key	Key no.
S	2
P	4
I	6
R	5
A	3
L	1
S	2

P	4
I	6
R	5
A	3
L	1
S	2
P	4

- after that summed the value of plaintext and key known as shift value

Plain text	Key	Pt. No.	Key no.	Shift value
H	S	7	2	9
A	P	0	4	4
R	I	17	6	23
I	R	8	5	13
Space	A	26	3	29
P	L	15	1	16
L	S	11	2	13
A	P	0	4	4
Y	I	24	6	30
Space	R	26	5	31
B	A	1	3	4
A	L	0	1	1
L	S	11	2	13
L	P	11	4	15

- converted the shift value into the binary

Shift value	Binary
9	01001
4	00100
23	10111
13	01101
29	11101

16	10000
13	01101
4	00100
30	11110
31	11111
4	00100
1	00001
13	01101
15	01111

- applied NOT logical operator to the binary value

Binary	Not
01001	10110
00100	11011
10111	01000
01101	10010
11101	00010
10000	01111
01101	10010
00100	11011
11110	00001
11111	00000

- convert the NOT value in decimal again known as cipher value

NOT	CHIPER VALUE
10110	22
11011	27
01000	8
10010	18
00010	2
01111	15
10010	18

11011	27
00001	1
00000	0
11011	27
11110	30
10010	18
10000	16

- entered the cipher value and correct letters of cipher value

Chiper value	Cipher text
22	V
27	!
8	O
18	L
2	E
15	H
18	L
27	!
1	B
0	A
27	!
30	#
18	L
16	J

- and at last, plaintext converted as: V!OLEHL!BA!#LJ

Encryption								
Plain text	Key	Pt. No.	Key no.	Shift value	Binary	Not	Chiper value	Cipher text
H	S	7	2	9	01001	10110	22	V
A	P	0	4	4	00100	11011	27	!
R	I	17	6	23	10111	01000	8	O
I	R	8	5	13	01101	10010	18	L
Space	A	26	3	29	11101	00010	2	E
P	L	15	1	16	10000	01111	15	H
L	S	11	2	13	01101	10010	18	L
A	P	0	4	4	00100	11011	27	!
Y	I	24	6	30	11110	00001	1	B
Spcae	R	26	5	31	11111	00000	0	A
B	A	1	3	4	00100	11011	27	!
A	L	0	1	1	00001	11110	30	#
L	S	11	2	13	01101	10010	18	L
L	P	11	4	15	01111	10000	16	J

Table 17 : Testing 5 Encryption

Plaintext: HARI PLAY BALL

Cipher text: V!OLEHL!BA!#LJ

Decryption:

Cipher text: V!OLEHL!BA!#LJ

Steps:

- entered the cipher text in table: V!OLEHL!BA!#LJ
- input the correct values of letter from the cipher table

Cipher	Cipher value
V	22
!	27
O	8
L	18
E	2

H	15
L	18
!	27
B	1
A	0
!	27
#	30
L	18
J	16

- convert it into binary

Cipher value	Binary
22	10110
27	11011
8	01000
18	10010
2	00010
15	01111
18	10010
27	11011
1	00001
0	00000
27	11011
30	11110
18	10010
16	10000

- applied NOT logical operator

Binary	Not
10110	10001
11011	00100
01000	10111
10010	01101

00010	11101
01111	10000
10010	01101
11011	00100
00001	11110
00000	11111
11011	00100
11110	00001
10010	01101
10000	01111

- convert the NOT value in decimal; shift value

Not	Shift value
10001	9
00100	4
10111	23
01101	13
11101	29
10000	16
01101	13
00100	4
11110	30
11111	31
00100	4
00001	1
01101	13
01111	15

- input the key and the key value

Key	Key value
S	2
P	4

I	6
R	5
A	3
L	1
S	2
P	4
I	6
R	5
A	3
L	1
S	2
P	4

- subtracted the key with shift value which is plaintext value

Shift value	Key value	Pt value
9	2	7
4	4	0
23	6	17
13	5	8
29	3	26
16	1	15
13	2	11
4	4	0
30	6	24
31	5	26
4	3	1
1	1	0
13	2	11
15	4	11

- arrange the letters with plaintext value

Pt value	Plain text
7	H
0	A
17	R
8	I
26	Space
15	P
11	L
0	A
24	Y
26	Space
1	B
0	A
11	L
11	L

- and at last, we got the plaintext: HARI PLAY BALL

Decryption								
Cipher	Cipher value	Binary	Not	Shift value	Key	Key value	Pt value	Plain text
V	22	10110	10001	9	S	2	7	H
!	27	11011	00100	4	P	4	0	A
O	8	01000	10111	23	I	6	17	R
L	18	10010	01101	13	R	5	8	I
E	2	00010	11101	29	A	3	26	Space
H	15	01111	10000	16	L	1	15	P
L	18	10010	01101	13	S	2	11	L
!	27	11011	00100	4	P	4	0	A
B	1	00001	11110	30	I	6	24	Y
A	0	00000	11111	31	R	5	26	Space
!	27	11011	00100	4	A	3	1	B

#	30	11110	00001	1	L	1	0	A
L	18	10010	01101	13	S	2	11	L
J	16	10000	01111	15	P	4	11	L

Table 18 : Testing 5 Decryption

Cipher text: V!OLEHL!BA!#LJ

Plaintext: HARI PLAY BALL

5. Analysis

5.1. Advantages:

- I. It employs a number of substitution alphabets, and therefore is less vulnerable to frequency analysis than simple substitution ciphers.
- II. The cipher is very comprehensible and can easily be applied from the given text once one is familiar with a certain table.
- III. This cipher has a different table for plain text and cipher text which provide an additional layer as security features.
- IV. It can be very helpful in teaching cryptography concepts since it relatively easier to implement a concept from the algorithm.
- V. With the assistance of mathematical and logical approaches, the system has become complicated and safe.

5.2. Disadvantages:

- I. If it is short keyword or keyword has lot of repetition then it can be vulnerable, a measure of statistic used to find the length of the keyword.
- II. It can be broken with ease provided one employs complex methods such as index of coincidence and statistic.
- III. This cipher cannot encrypt the numbers and specials characters which is the one of the biggest drawbacks of this cipher.
- IV. It may not be very efficient, even for big data problem, because of some of the methods used in the process.
- V. As we have seen, even with the modern computing power brute force attacks can be employed to break the cipher especially where short keywords are used.

5.3. Application Area

- For protecting files or documents which contain private information on individuals' personal computers or hand-held devices against threat of hacking.
- It can be used for encrypting the messages for a chat in conveyancing the real time communication applications.
- In Data Obfuscation for Protecting sensitive information during software development or API communication it can be used to transform the plain

text data into a more difficult to read information on personal computers or mobile devices to prevent unauthorized access.

- It can be used to encrypt chat messages in real-time communication applications
- Demonstrating cryptographic concepts in universities and research institutions, as your algorithm combines classic and modern approaches.
- It can be used in Data Obfuscation for Protecting sensitive information during software development or API communication by obfuscating plain text data.

6. Conclusion

In conclusion, computer security is very important in today's world because everything we do is connected to technology. Whether it is using social media, banking online, or running a business, we rely on computers to manage our tasks. But this also exposes us to dangers like hacking and data theft. To stay safe, we need strong security systems that protect our information and ensure our devices work properly. The CIA Triad Confidentiality, Integrity, and Availability is the main principle of computer security. It helps keep data private, accurate, and accessible to those who are authorized to use it.

Cryptography is another vital part of computer security. It has evolved from simple methods like Caesar Cipher to advanced systems like public-key cryptography. This report introduced the Spiral Algorithm, a new method inspired by the Vigenère Cipher. The Spiral Algorithm uses numbers and logical operations to make encryption more secure. Although it has some weaknesses, like being vulnerable to attacks with short keywords, it is a good example of how new ideas can improve the safety of our information.

The report also shows how different types of computer security, like application security, network security, and endpoint security, work together to protect systems. These layers of protection are necessary to defend against threats and ensure that systems can function without interruptions. Algorithms like the Spiral Algorithm can be used in areas such as secure messaging, data obfuscation, and teaching students about cryptography.

Finally, as technology keeps advancing, we must continue to develop better security measures to face new challenges. Research and innovation in computer security will help individuals and organizations stay safe in this fast-changing world. By understanding and applying security principles, we can ensure a safer digital future for everyone.

References

Chin, K., 2024. *What is Cryptography? And How You Can Secure Your Data | UpGuard*. [Online]

Available at: <https://www.upguard.com/blog/cryptography>
[Accessed 7 December 2024].

CyberOne, 2019. *What is the CIA triad?*. [Online]

Available at: <https://cyberone.security/what-is-the-cia-triad/>
[Accessed 8 December 2024].

DataFlair Team, 2024. *Computer Security Tutorial*. [Online]

Available at: <https://data-flair.training/blogs/computer-security/>
[Accessed 8 December 2024].

Fasano, E., 2022. *5 Ways to Reduce the Risk of Cyber Attacks*. [Online]

Available at: <https://www.align.com/blog/5-ways-to-reduce-the-risk-of-cyber-attacks>
[Accessed 6 December 2024].

Fortinet, 2023. *What is the CIA Triad and Why is it important?*. [Online]

Available at: <https://www.fortinet.com/resources/cyberglossary/cia-triad#:~:text=2.-,Integrity,authentic%2C%20accurate%2C%20and%20reliable>

[Accessed 6 December 2024].

GeeksforGeeks, 2016. *Vigenere Cipher*. [Online]

Available at: <https://www.geeksforgeeks.org/vigenere-cipher/>
[Accessed 8 December 2024].

GeeksforGeeks, 2019. *Cryptography and its Types*. [Online]

Available at: <https://www.geeksforgeeks.org/cryptography-and-its-types/>
[Accessed 7 December 2024].

GeeksforGeeks, 2022. *Computer Security and its Challenges*. [Online]

Available at: <https://www.geeksforgeeks.org/computer-security-and-its-challenges/>
[Accessed 6 December 2024].

Gupta, N., 2023. *Symmetric vs. Asymmetric Encryption - What are differences?*

[Online]

Available at: <https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption->

what-are-differences

[Accessed 8 December 2024].

Hasons, 2024. *Types of Computer Security*. [Online]
Available at: https://hasonss.com/blogs/types-of-computer-security/?srsltid=AfmBOoqrgY1Zx_end9L5sXQUyo-T3w32hPbrp86fi5cmNaZTU5yDsVi

[Accessed 6 December 2024].

Irwin, L., 2022. *What Is the CIA Triad and Why Is It Important?*. [Online]
Available at: <https://www.itgovernance.co.uk/blog/what-is-the-cia-triad-and-why-is-it-important>

[Accessed 6 December 2024].

Jarry, J., 2019. *From Julius Caesar to the blockchain: a brief history of cryptography*. [Online]

Available at: <https://variances.eu/?p=3942#:~:text=The%20art%20of%20substitution,posted%20in%20the%20war%20front>

[Accessed 7 December 2024].

Kester, Q.-A., 2012. *A cryptosystem based on Vigenère cipher with varying key*. [Online]

Available at: https://www.researchgate.net/publication/235618077_A_cryptosystem_based_on_Vigenere_cipher_with_varying_key

[Accessed 8 December 2024].

Knowledgehut, 2022. *What is CIA Triad? Examples, Components, Importance & Goals*. [Online]

Available at: <https://www.knowledgehut.com/blog/security/cia-in-cyber-security#what-is-cia-triad%C2%A0in-cyber-security?>

[Accessed 6 December 2024].

Learnearn., 2023. *Vigenere Cipher*. [Online]

Available at: <https://learnlearn.uk/edexcel-igcse-computer-science/vigenere-cipher/>

[Accessed 8 December 2024].

Leeson, S., 2024. *The Importance of the CIA Triad to Cybersecurity*. [Online]
Available at: <https://yourshortlist.com/the-importance-of-the-cia-triad-to-cybersecurity/>
[Accessed 6 December 2024].

MacDonald, R., 2023. *What Is Symmetric Encryption, How Does It Work & Why Use It?*. [Online]
Available at: <https://www.1kosmos.com/blockchain/symmetric-encryption/>
[Accessed 7 December 2024].

NordLayer, 2021. *Public-Key Cryptography*. [Online]
Available at: <https://nordlayer.com/blog/aes-encryption/>
[Accessed 7 December 2024].

Pedamkar, P., 2023. *Symmetric Algorithms*. [Online]
Available at: <https://www.educba.com/symmetric-algorithms/>
[Accessed 7 December 2024].

Point, C., 2022. *What is Cybersecurity*. [Online]
Available at: <https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cybersecurity/>
[Accessed 6 December 2024].

Roy, S., 2023. *What are the Challenges faced in Symmetric Cryptography?*. [Online]
Available at: <https://www.encryptionconsulting.com/what-are-the-challenges-faced-in-symmetric-cryptography/>
[Accessed 7 December 2024].

Sailpoint, 2024. *Types of cybersecurity*. [Online]
Available at: <https://www.sailpoint.com/identity-library/five-types-of-cybersecurity>
[Accessed 6 December 2024].

Schneider, J., 2024. *Cryptography history*. [Online]
Available at: <https://www.ibm.com/think/topics/cryptography-history>
[Accessed 7 December 2024].

SecurityScorecard, 2024. *What is the CIA Triad? Definition, Importance, & Examples*. [Online]

Available at: <https://securityscorecard.com/blog/what-is-the-cia-triad/>
[Accessed 6 December 2024].

Shari Lawrence Pfleeger, C. P. P. J. M., 2024. What is Security Computing ?. *Security in Computing*, FIFTH EDITION(2015), p. 103.

Sharma, V., 2024. *What is Computer Security? Types, Importance, Threats*. [Online]
Available at: <https://www.knowledgehut.com/blog/security/computer-security>
[Accessed 6 December 2024].

Sidhpurwala, H., 2023. *A Brief History of Cryptography*. [Online]
Available at: <https://www.redhat.com/en/blog/brief-history-cryptography>
[Accessed 7 December 2024].

Singh, A., 2019. *What are Different Types of Cryptography?*. [Online]
Available at: <https://www.shiksha.com/online-courses/articles/types-of-cryptography/>
[Accessed 7 December 2024].

TechTarget Contributor, 2023. *stream cipher*. [Online]
Available at: <https://www.techtarget.com/searchsecurity/definition/stream-cipher>
[Accessed 7 December 2024].

tutorialspoint, 2024. *Cryptography - Hash functions*. [Online]
Available at: https://www.tutorialspoint.com/cryptography/cryptography_hash_functions.htm
[Accessed 9 December 2024].

Tutorialspoint, 2024. *Cryptography - Vigenere Cipher*. [Online]
Available at: https://www.tutorialspoint.com/cryptography/cryptography_vigenere_cipher.htm
[Accessed 8 December 2024].

Weerasuriya, D., 2020. *What is Cryptography?*. [Online]
Available at: <https://www.bartleby.com/subject/engineering/computer-science/concepts/cryptography>
[Accessed 8 December 2024].

yathursan, V., 2020. *Secret-Key (Symmetric) algorithms in cryptography*. [Online]
Available at: <https://vadivelyathursan.medium.com/secret-key-symmetric-algorithms->

in-cryptography-10d3ef428cf8

[Accessed 08 December 2024].