LONDON METROPOLITAN UNIVERSITY

Islington college
(इस्लिङ्टन कलेज)

Module Code & Module Title

CC5004NI Security in Computing

Assessment Weightage & Type

30% Individual Coursework

Year and Semester

2021 -22 Autumn

Student Name: Sarthak Bikram Rana

London Met ID: 20049228

College ID: NP01NT4S210129

Assignment Due Date: 10th January 2022

Assignment Submission Date: 10th January 2022

Word Count (Where Required): 11852

I confirm that I understand my coursework needs to be submitted online via Google Classroom 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.

Acknowledgement

This is the first coursework in the Security in the Computing module, in which we were given the task to create our new cryptographic algorithm by modifying one. I choose Caesar cipher as the base cryptographic algorithm for my module and for the modification I had to undertake research on the issue for my coursework by looking at a variety of related articles, journals, reports and websites.

Finally, I'd like to express my gratitude to our respected module leader Mr. Akchayat Bikram Dhoj Joshi for introducing me to the topic of cryptography and helping me by guiding me for the modification of the algorithm and reviewing my coursework at various points.

Abstract

The main focus of this coursework is the development of a new cryptographic algorithm, and extensive research is conducted on the topic through various reports, journals, articles, and websites. The terms Information Security, CIA triad, cryptography, its history and types, detail elaboration on the base algorithm of this coursework, Caesar cipher, and finally the development of a new cryptographic algorithm, including its algorithm and flowchart, test cases, and strengths and weaknesses, are all covered in the background, development, and evaluation section.

Table of Contents

1. Introduction 1
   1.1 CIA Triad 2
      1.1.1 Confidentiality: 3
      1.1.2 Integrity: 3
      1.1.3 Availability: 3
   1.2 Introduction to Cryptography 4
   1.3 History of Cryptography 5
      1.3.1 The Ancient Roots of Cryptography 6
      1.3.2 Cryptography in the Middle Ages 10
      1.3.3 Cryptography during World War I 11
      1.3.4 Cryptography during World War II 13
   1.4 Types of Cryptography 15
      1.4.1 Symmetric Key Encryption 16
      1.4.2 Asymmetric Key Encryption 17
2. Background 18
   2.1 Caesar Cipher 18
      2.1.1 Example of Caesar Cipher 19
      2.1.2 Advantages of Caesar Cipher 21
      2.1.3 Disadvantages of Caesar Cipher 21
3. Development 22
   3.1 New Cryptographic Algorithm 22
   3.2 Modification 29
   3.3 Algorithm 30
      3.3.1 New Encryption Algorithm 30
      3.3.2 New Decryption Algorithm 31
   3.4 Flowchart 32
      3.4.1 New Encryption Flowchart 32
      3.4.2 New Decryption Flowchart 33
4. Testing 34
   4.1 Test 1 34
   4.2 Test 2 40
   4.3 Test 3 44
   4.4 Test 4 48

4.5 Test 5 53
5. Evaluation 57
5.1 Strength and Weakness 57
6. Conclusion 58
References 59
Appendices 61

List of Figures

Figure 1: Figure of C.I.A Triad (Comtact, 2019). 2
Figure 2: Process of cryptography (Priyanka Bhatia, 2014). 4
Figure 3: Picture of Hieroglyphic cryptography (KASADOO, 2021). 6
Figure 4: Picture of Scytale cryptography (Emory Oxford College, 2019)..... 7
Figure 5: Picture of substitution cipher used by Julius Caesar (McDonald, 2009)..... 8
Figure 6: Picture of Jefferson wheel cipher (McDonald, 2009). 9
Figure 7: Picture of Zimmermann Telegram (Britannica, 2021)..... 12
Figure 8: Picture of Enigma encryption machine (Wikipedia, 2012). 13
Figure 9: Picture of Purple encryption machine (Wikimedia Commons, 2020). 14
Figure 10: Symmetric key encryption (SSL2BUY, 2021). 16
Figure 11: Asymmetric key encryption (SSL2BUY, 2021). 17
Figure 12: Substitution table for Caesar cipher. 19
Figure 13: Vigenere Table..... 23
Figure 14: Example for encryption step of Vigenere Cipher. 24
Figure 15: Example for decryption step of Vigenere Cipher. 25
Figure 16: New modified Substitution table for Caesar cipher. 26
Figure 17: New modified character table for Vigenere cipher. 27
Figure 18: Encryption flowchart. 32
Figure 19: Decryption Flowchart. 33
Figure 20: Encryption using vigenere cipher for test 1. 36
Figure 21: Decryption using vigenere cipher for test 1. 37

List of Tables

Table 1: Example of encryption step for Vigenere Cipher. 24
Table 2: Example of decryption step for Vigenere Cipher. 25
Table 3: Encryption using odd and even rule for test 1. 35
Table 4: Encryption using vigenere cipher for test 1. 35
Table 5: Decryption using vigenere cipher for test 1. 37
Table 6: Decryption using odd and even rule for test 1. 38
Table 7: Encryption using odd and even rule for test 2. 41
Table 8: Encryption using vigenere cipher for test 2. 41
Table 9: Decryption using vigenere cipher for test 2. 42
Table 10: Decryption using odd and even rule for test 2. 42
Table 11: Encryption using odd and even rule for test 3. 45
Table 12: Encryption using vigenere cipher for test 3. 45
Table 13: Decryption using vigenere cipher for test 3. 46
Table 14: Decryption using odd and even rule for test 3. 47
Table 15: Encryption using odd and even rule for test 4. 49
Table 16: Encryption using vigenere cipher for test 4. 49
Table 17: Decryption using vigenere cipher for test 4. 50
Table 18: Decryption using odd and even rule for test 4. 51
Table 19: Encryption using odd and even rule for test 5. 54
Table 20: Encryption using vigenere cipher for test 4. 54
Table 21: Decryption using vigenere cipher for test 4. 55
Table 22: Decryption using odd and even rule for test 4. 55

1. Introduction

Security is a condition or state of being safe from harm, as well as a process of detecting and fixing loopholes. When it comes to today's world, which has become increasingly globalized, technology has played a significant role. Using any type of technology gives others easy access to our personal information on the device we are using.

Information security refers to the state of safeguarding security methods and policies against the unauthorized use of data. We must protect our precious data/assets by employing security measures when using technology. Physical security, operational security, network security, and data/information security are all examples of security measures. Maintaining CIA, firewalls, anti-virus systems, and other security measures can all help to protect information systems from external and internal threats, with all data backed up and encrypted (Fruhlinger, 2020).

1.1 CIA Triad

The C.I.A. triangle is a three-sided figure in which each end represents a component of Confidentiality, Integrity, and Availability. C.I.A.'s main purpose is to provide security features that assist in avoiding compliance concerns, ensuring business continuity, and preventing any hazards or damage to the company.

It is commonly used because it assists in establishing a system security standard by determining whether the system's confidentiality, integrity, and accessibility meet the system's needs and rules.

Figure 1: Figure of C.I.A Triad (Comtact, 2019).

1.1.1 Confidentiality:

This term is associated with data security and encryption and it is one of the security standards in which only authorized individuals have access to the data in this scenario. When data is kept confidential, it means it hasn't been accessed by anyone who shouldn't have. To protect against social engineering and a number of other dangers, a secure password must be used. Two-factor authentication can also be utilized to increase the device's reliability.

1.1.2 Integrity:

One of the ends of the C.I.A. triangle is data integrity, which refers to the assurance that data has not been tampered with or damaged during or after submission. The document's integrity may be compromised at two points throughout the transmission process. To ensure data security, it must be protected from interference, delete, and other natural disasters such as flood, fire, earthquake, and other natural disasters.

1.1.3 Availability:

The availability of information is one of the ends of the C.I.A. triangle, which means that authorized person will have access to it when it is needed. More contact through output must be given to avoid availability issues, which also avoids bottlenecks. RAID, redundancy, and other devices can all be used in the same way.

1.2 Introduction to Cryptography

Cryptography is a method of safeguarding information and communications by encoding it in a way that only the people who need to know about it can understand and process it. It is concerned with the establishment and review of protocols that prevent malicious third parties from gaining access to information shared between two companies (GeeksforGeeks, 2020).

Plaintext is turned into encrypted text and vice versa in cryptography and the procedures used to safeguard data are derived from mathematical principles and a set of rule-based calculations known as algorithms. Modern cryptography's fundamental concepts include data confidentiality, data integrity, authentication, and non-repudiation (GeeksforGeeks, 2020).

These cryptographic algorithms are used to generate cryptographic keys, verify data privacy, perform digital signing, project confidential transactions such as credit card and debit card transactions and surf the web. Cryptography plays a huge role on maintaining the basic component of an organization by maintaining the C.I.A. triad.

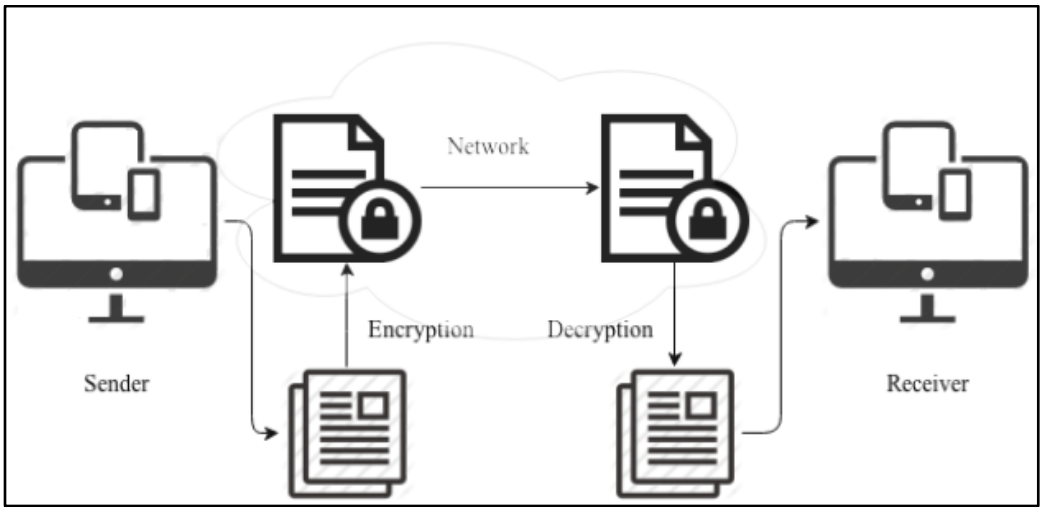

Figure 2: Process of cryptography (Priyanka Bhatia, 2014).

1.3 History of Cryptography

The process of creating codes and ciphers for secure communication is known as cryptography. It's one of the key components that allows modern cryptocurrencies and blockchains to exist. Today's cryptographic approaches are the result of an incredibly long development process. Cryptography has been used to safeguard information transmission since the beginning of time (Binance Academy, 2019).

Since thousands of years ago, the term cryptography and its application have existed. From 1900 BC, the first known evidence of cryptography was discovered in Egypt. Since then, the concept and methods of cryptography has evolved into modern cryptography. There are several stages in the development of cryptography, such as (Binance Academy, 2019).

1.3.1 The Ancient Roots of Cryptography

Primitive cryptographic techniques are known to have existed in ancient times, and cryptography appears to have been utilized in some form by most early civilizations. Different civilizations have created and used various sorts of cryptographic systems in the past (Binance Academy, 2019).

1.3.1.1 Egypt

The first known evidence of cryptography was discovered in the tomb of an Egyptian ruler named Khnumhotep II, who lived around 3900 years ago in the Egyptian town of Menet Khufu. He carved a number of odd symbols into the hieroglyphics to conceal the understanding of the writings. The hieroglyphics is an example of substitution cipher (McDonald, 2009).

As Egypt's civilization developed, hieroglyphic substitution became more popular since it was very simple to decipher for those who could recognize the symbols that reflected their culture and the formal aspect of their writing (McDonald, 2009).

Figure 3: Picture of Hieroglyphic cryptography (KASADOO, 2021).

1.3.1.2 Greece

When it comes to Greece, the Spartans invented a cylindrical device with a thin stripe and a parchment wound called Scytale, approximately in 500 B.C. for secret message communication. Letters were written lengthwise on the parchment and it would become unreadable if the parchment was ruined. When it comes to receive a message a similar cylinder was required. The Scytale is an example of transposition cipher (McDonald, 2009).

Figure 4: Picture of Scytale cryptography (Emory Oxford College, 2019).

1.3.1.3 Rome

When it comes to Rome, the commander of the Roman army group Julius Caesar developed his own cryptography method, which is now known as the Caesar cipher, to communicate with his troops 2000 years ago. To protect their troops communication from enemies, he simply replaced the letters with alternative letters that the enemies couldn't comprehend, giving them a significant advantage (McDonald, 2009).

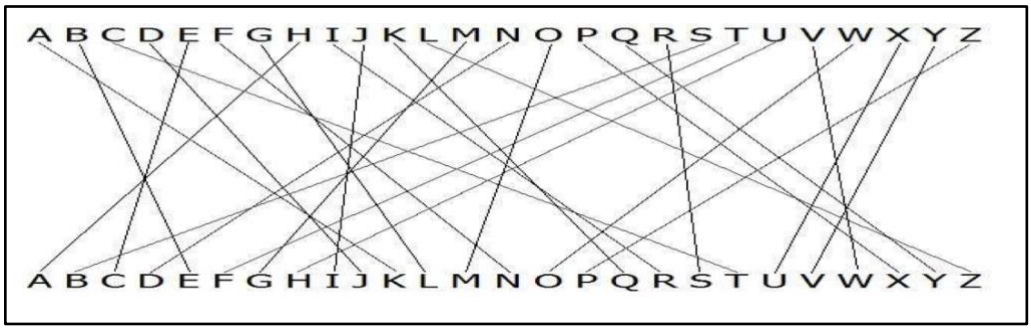

Figure 5: Picture of substitution cipher used by Julius Caesar (McDonald, 2009).

1.3.1.4 Jefferson wheel cipher

In the late 1700s, Thomas Jefferson developed a cryptographic algorithm that was similar to Vigenere Cipher but significantly more secure. His invention consists of 26 wheels, each of which was numbered in a specific order and had the letters scattered about randomly (McDonald, 2009).

The wheels were lined up in a precise sequence and rotated to jumble up the text to encrypt the message, but when decrypting the message, the wheels should be positioned in the correct order and turned in the correct order (McDonald, 2009).

Figure 6: Picture of Jefferson wheel cipher (McDonald, 2009).

1.3.2 Cryptography in the Middle Ages

Caesar cipher became one of the most important encryption algorithms during the Middle Ages. Around 800 AD, an Arab mathematician named Al-Kindi discovered a technique called frequency analysis that made substitution ciphers vulnerable to decryption. Leone Alberti invented the polyalphabetic cipher in 1465 as a counter-measure to Al-frequency Kindi's analysis approach (Binance Academy, 2019).

A message is encoded using two different alphabets in a polyalphabetic cipher. The first is the alphabet in which the original message is written and the second is the alphabet in which the message appears after it has been encoded. The frequency analysis technique was useless unless the reader knew the alphabet in which the message was initially written, hence polyalphabetic cipher, when combined with regular substitution ciphers significantly strengthened the security of encoded information (Binance Academy, 2019).

1.3.3 Cryptography during World War I

During World War One, Germans and Americans utilized two main cryptography techniques to communicate with their allies. The fundamental goal of those cryptographic safeguards was to keep their communication safe from others countries access (Binance Academy, 2019).

1.3.3.1 Choctaw Codetalkers

During World War I, the United States has the major problem of the lack of secure communication. The phone calls made to each other by the allies of United States was intercepted by the Germans and steal their data. To encounter that the army commander captain Lewis made a plan to talk in code languages (McDonald, 2009).

He discovered eight guys in the unit who spoke an American Indian language and utilized them to communicate with one another across radio and phone lines, making the Germans unable to decipher the message because they couldn't tell which language they were speaking in. The United States gained the advantage within 24 hours of adopting the Choctaw language, which was actually an American Indian language as encryption (McDonald, 2009).

1.3.3.2 Zimmermann Telegram

During World War I, British cryptographers came across a German-encoded communication known as the Zimmerman Telegram in early 1917. These cryptographers were able to decipher the telegram and by changing the message they convince the United States to join the war (McDonald, 2009).

The Zimmerman Telegram was a secret message sent by German Foreign Secretary Arthur Zimmerman to German Ambassador Heinrich von Eckardt in Mexico. According to the message, if Mexico joined the German cause, it could reclaim its territories of New Mexico, Texas, and Arizona. The telegram was sent during the height of World War I. Until that point, the United States had attempted to remain neutral (McDonald, 2009).

The British and other allies had urged the US to come to their aid, and public opinion in the US was gradually shifting toward war. The British delivered the decrypted telegraph to the United States on February 24, 1917, and the United States declared war on Germany on April 6, 1917 (McDonald, 2009).

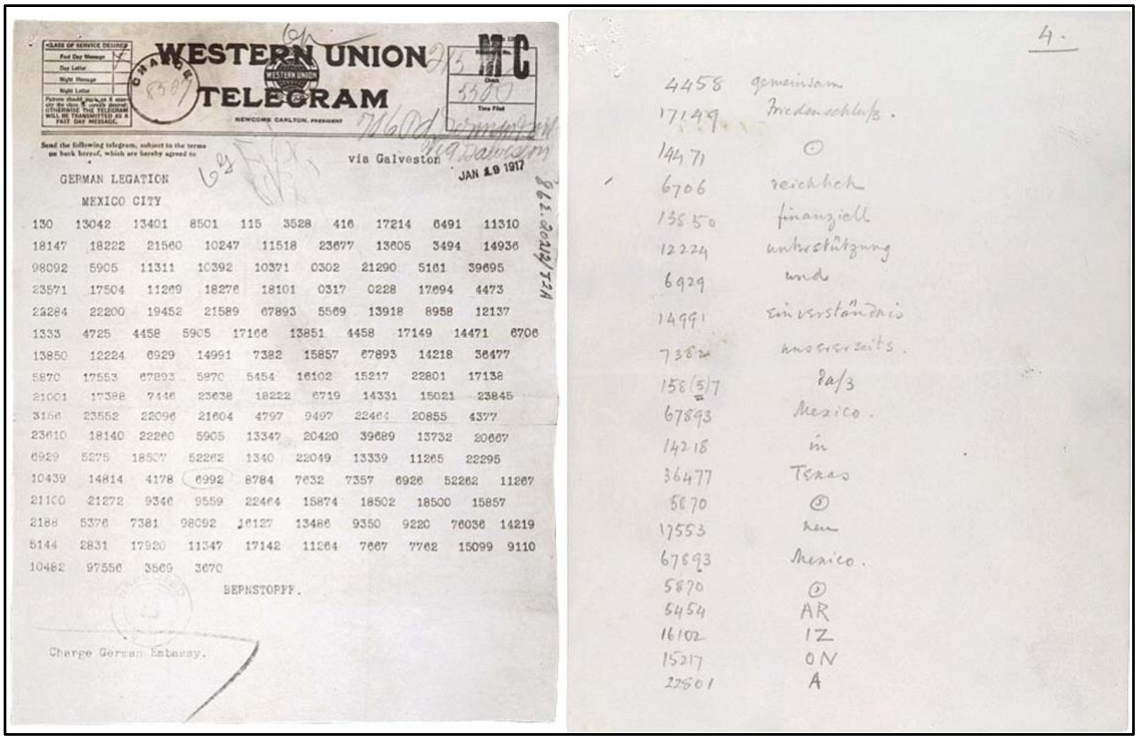

Figure 7: Picture of Zimmermann Telegram (Britannica, 2021).

1.3.4 Cryptography during World War II

The Germans and Japanese introduced the world to two new cryptographic techniques during World War II: the enigma encryption machine and the purple machine (Binance Academy, 2019).

1.3.4.1 Enigma Encryption Machine

Arthur Scherbius designed Enigma, an electromechanical machine that was used to encrypt and decrypt secret messages at the close of World War I. It contained many rotors and gears, allowing for up to 10^{114} different configurations. Because of the multiple permutations, it was also virtually unbreakable using brute force methods because of the numerous configurations (McDonald, 2009).

Because of Enigma's statistical security, Nazi Germany became overconfident in their capacity to encrypt secret messages and the system became popular. This was also the reason behind t he Enigma's downfall. The Enigma had multiple built-in flaws that Allied cryptographers exploited, in addition to numerous German operator errors. Its main flaw was that its substitution technique prevented any letter from being reassigned to itself. This allowed Allied cryptographers to decrypt a large quantity of Nazi German ciphered messages (McDonald, 2009).

Figure 8: Picture of Enigma encryption machine (Wikipedia, 2012).

1.3.4.2 Purple

While the Allies worked on cracking the German Enigma code, the Japanese created Purple encryption machine. It was constructed with stepping switches which are often used to route telephone signals. No one was able to decrypt the message because the Japanese kept their encryption methods secret (McDonald, 2009).

Late, famous cryptographer William Friedman and his colleagues developed a duplicate of purple simply based on the encrypted data obtained. They had never seen a Purple machine and had no idea how it functioned, but the team eventually figured out Purple's encryption mechanism and were able to decrypt it using a different machine. During World War II, this development helped the US to gain access to Japanese diplomatic secrets (McDonald, 2009).

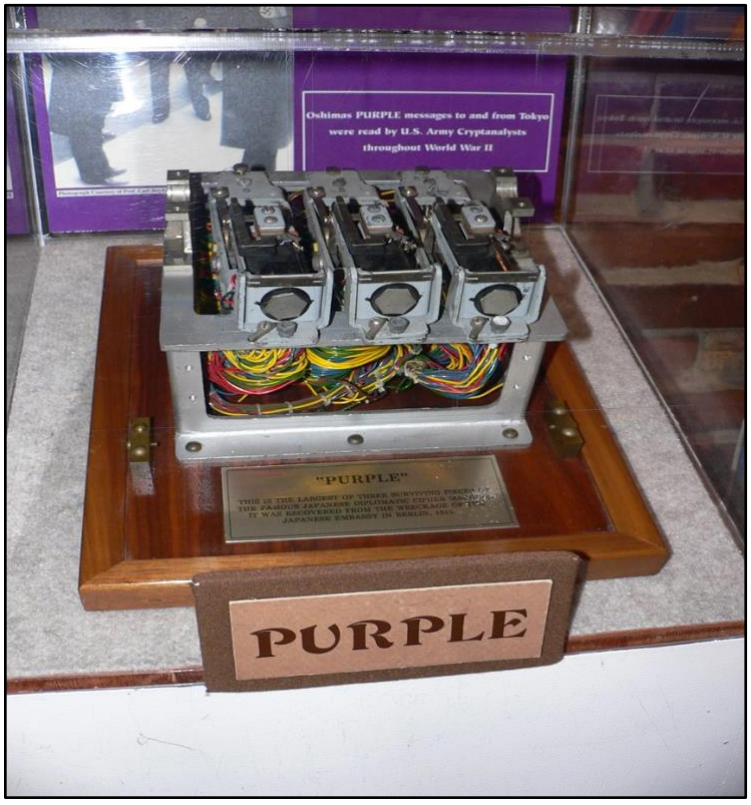

Figure 9: Picture of Purple encryption machine (Wikimedia Commons, 2020).

1.4 Types of Cryptography

As time passed in the digital or modern era, algorithms have been developed which are based on mathematical concepts and can be used to encrypt any data commonly known as cryptography. Cryptography is divided into three categories, which are as follows:

- Symmetric Key Encryption
- Asymmetric Key Encryption

1.4.1 Symmetric Key Encryption

Symmetric key encryption is a type of cryptography in which both the sender and the receiver use the same key for encryption and decryption. Symmetric key systems are faster and easier to use, but because the sender and receiver use the same key for encryption and decryption. Hence, sharing the key is difficult in terms of confidentiality (Priyanka Bhatia, 2014).

The examples of Symmetric key encryption are AES, DES, RC4, Block Cipher, IDEA, Blowfish. Among them advanced encryption standard (AES) and data encryption standard (DES) are the common symmetric encryption algorithms (Priyanka Bhatia, 2014).

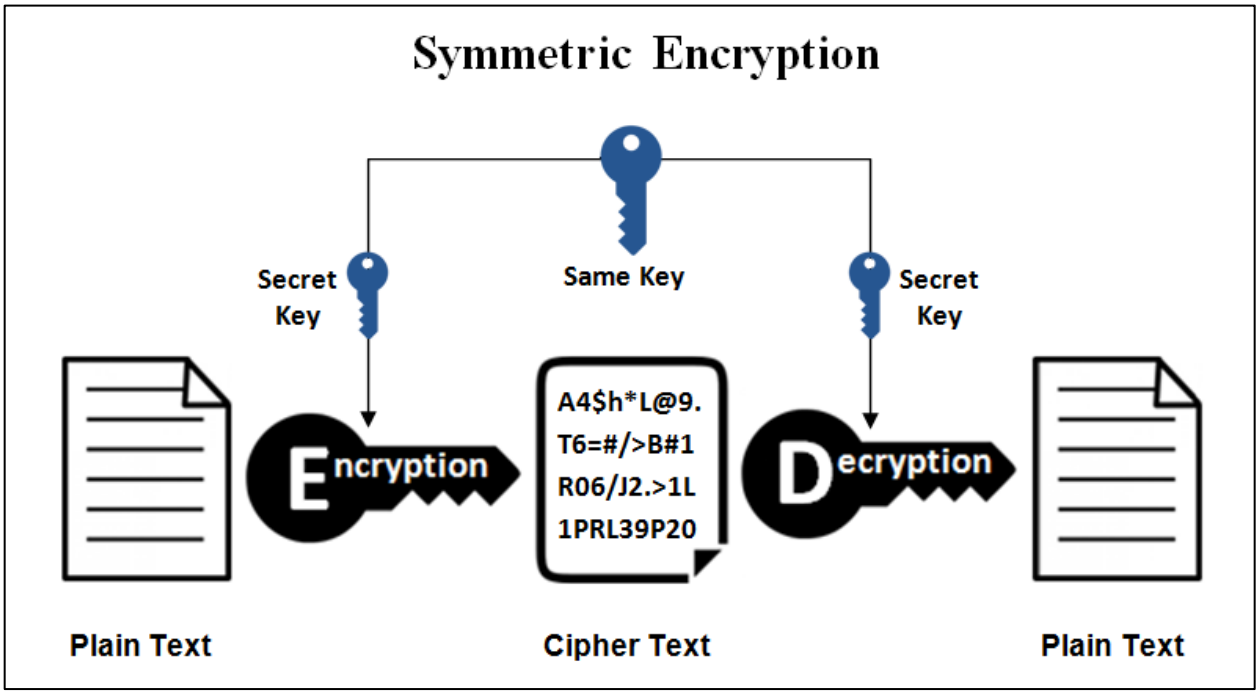

Figure 10: Symmetric key encryption (SSL2BUY, 2021).

1.4.2 Asymmetric Key Encryption

Asymmetric key encryption is a type of cryptography that uses two separate keys for encryption and decryption, one public key and one private key. Every user's private key is kept private, but the public key is spread over the network, allowing anyone to send messages to any other user (Priyanka Bhatia, 2014).

Asymmetric key encryption, also known as public key encryption is safer than symmetric key encryption. The most popular and commonly used asymmetric algorithms are RSA and ECC. RSA, ECC, and DSA are examples of asymmetric key encryption (Priyanka Bhatia, 2014).

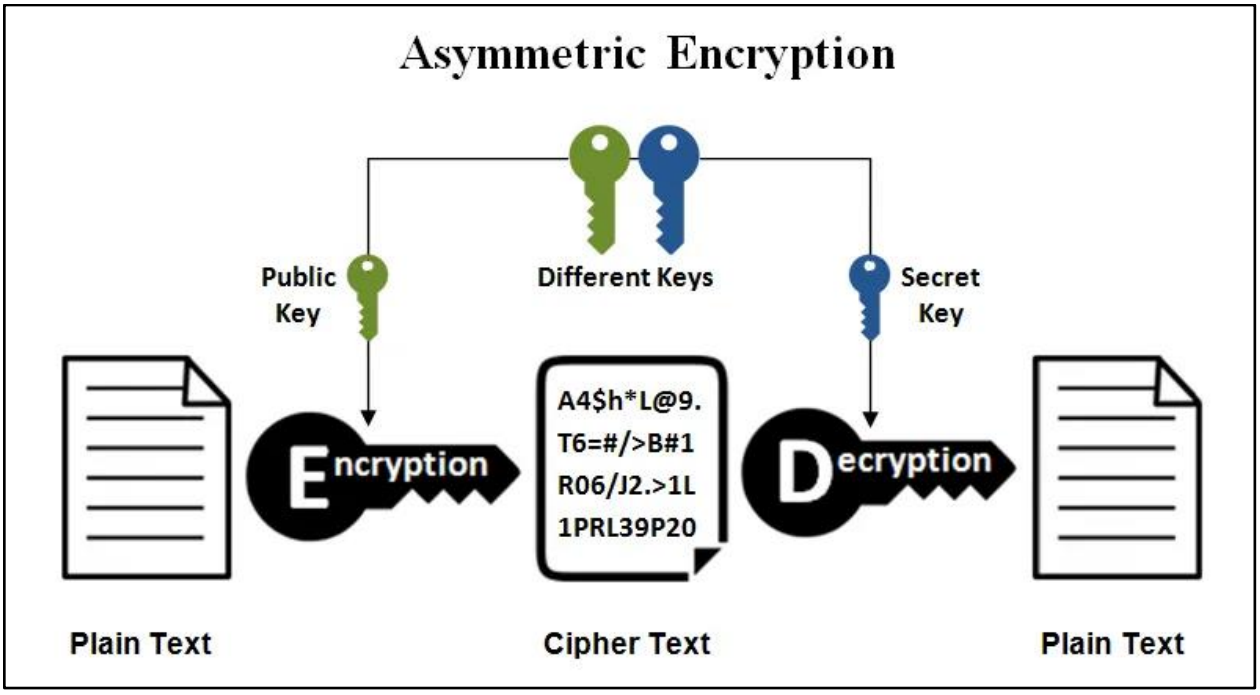

Figure 11: Asymmetric key encryption (SSL2BUY, 2021).

2. Background

2.1 Caesar Cipher

The Caesar cipher is one of the earliest known and simplest form of ciphers based on a basic symmetric substitution method which replaces alphabets with characters which are three block down the line. The default value of the key in Caesar cipher is three. For example the letter ‘A’ becomes ‘D’ and the letter ‘B’ becomes ‘E’.

The algorithm of the Caesar cipher is expressed as: C = (P + 3) mod 26, where ‘C’ is the substitute for the cipher text letter, ‘P’ is the substitute for the plain text letter and ‘3’ is the default key.

In Caesar cipher, encryption and decryption process is expressed as:

- **Encryption:** C = (P + K) mod 26, where K takes the value in range 1-25
- **Decryption:** P = (C – K) mod 26

2.1.1 Example of Caesar Cipher

Below is the example of Caesar cipher encryption and decryption process,

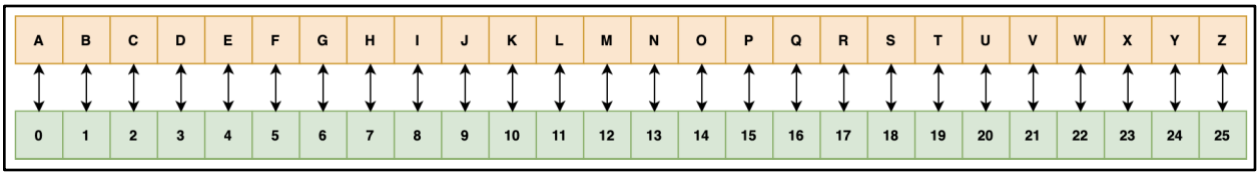

Figure 12: Substitution table for Caesar cipher.

Let suppose A = 0, B = 1 ……. Z = 25 as same from the above table and using them to replace the value of each alphabet which performing encryption and decryption.

Now,

Taking Plaintext as “COURSEWORK” and Key as default i.e. “3”.

For encryption:

We have the formula for encryption as C = (P + K) mod 26, where ‘C’ stands for ciphered text and ‘P’ stands for plain text.

- C = (P + K) mod 26 = (2 + 3) mod 26 = 5 = F
- O = (P + K) mod 26 = (14 + 3) mod 26 = 17 = R
- U = (P + K) mod 26 = (20 + 3) mod 26 = 23 = X
- R = (P + K) mod 26 = (17 + 3) mod 26 = 20 = U
- S = (P + K) mod 26 = (18 + 3) mod 26 = 21 = V
- E = (P + K) mod 26 = (4 + 3) mod 26 = 7 = H
- W = (P + K) mod 26 = (22 + 3) mod 26 = 25 = Z
- O = (P + K) mod 26 = (14 + 3) mod 26 = 17 = R
- R = (P + K) mod 26 = (17 + 3) mod 26 = 20 = U
- K = (P + K) mod 26 = (10 + 3) mod 26 = 13 = N

Therefore, the ciphertext of the plaintext of the word “COURSEWORK” is “FRXUVHZRUN”.

For decryption:

We have the formula for decryption as P = (C – K) mod 26, where ‘P’ stands for plain text and ‘C’ stands for ciphered text.

- F = (C – K) mod 26 = (5 - 3) mod 26 = 2 = C
- R = (C – K) mod 26 = (17 - 3) mod 26 = 14 = O
- X = (C – K) mod 26 = (23 - 3) mod 26 = 20 = U
- U = (C – K) mod 26 = (20 - 3) mod 26 = 17 = R
- V = (C – K) mod 26 = (21 - 3) mod 26 = 18 = S
- H = (C – K) mod 26 = (7 - 3) mod 26 = 4 = E
- Z = (C – K) mod 26 = (25 - 3) mod 26 = 22 = W
- R = (C – K) mod 26 = (17 - 3) mod 26 = 14 = O
- U = (C – K) mod 26 = (20 - 3) mod 26 = 17 = R
- N = (C – K) mod 26 = (13 - 3) mod 26 = 10 = K

Therefore, the plain text of the ciphertext of the word “FRXUVHZRUN” is “COURSEWORK”.

2.1.2 Advantages of Caesar Cipher

The advantages of Caesar Cipher are mentioned below:

- It is one of the simplest methods to use in cryptography and is very simple to understand.
- It only utilizes a single short key throughout the encryption and decryption process.
- If the system cannot use any complicated coding techniques, this is one of the best methods to use.
- It requires the least amount of computing resources.
- Caesar Cipher is a type of transposition cipher in which the letters written in plain text cannot be changed by others.

2.1.3 Disadvantages of Caesar Cipher

The disadvantages of Caesar Cipher are mentioned below:

- The Caesar cipher is simple to understand, but it is vulnerable because anyone can easily decrypt it.
- Transposition ciphers are more affected and blunder than simpler ciphers.
- Transposition ciphers can be used for short messages only.
- It can only provide minimum security to the information.
- Because of the frequency of the letters, the Caesar cipher provides a significant hint to decrypt the message.

3. Development

3.1 New Cryptographic Algorithm

The concept for this new cryptographic algorithm was inspired by the research papers "Developing a Modified Hybird Caesar Cipher and Vigenere Cipher for Secure Data Communication" by O.E. Omolara, A.I. Oludare, and S.E. Abdulahi, and "Modified Caesar Cipher for Better Security Enhancement" by Kashish Goyal and Supriya Kinger, as well as the content provided by our module leader Mr. Akchayat Bikram Dhoj Joshi.

This new cryptographic algorithm uses a three-step encryption method that includes running the basic Caesar cipher once, then changing the ciphered text using the new odd even rule and finally conducting the polyalphabetic encryption process known as Vigenere Cipher for added security. Finally, the Vigenere cipher is employed once in the decryption procedure, followed by the odd even rule to extract the ciphered text, and finally the Caesar cipher.

Vigenere Cipher

The Vigenere Cipher is a polyalphabetic cryptographic system that uses a caesarean code sequence depending on the letters of the keyword to encode alphabetic text. The Vigenere Cipher uses a character table for encryption and decryption, with the keywords letters represented in the leftmost column and the plaintext letters represented in the top line (Moch. Hari Purwidiantoro, 2018).

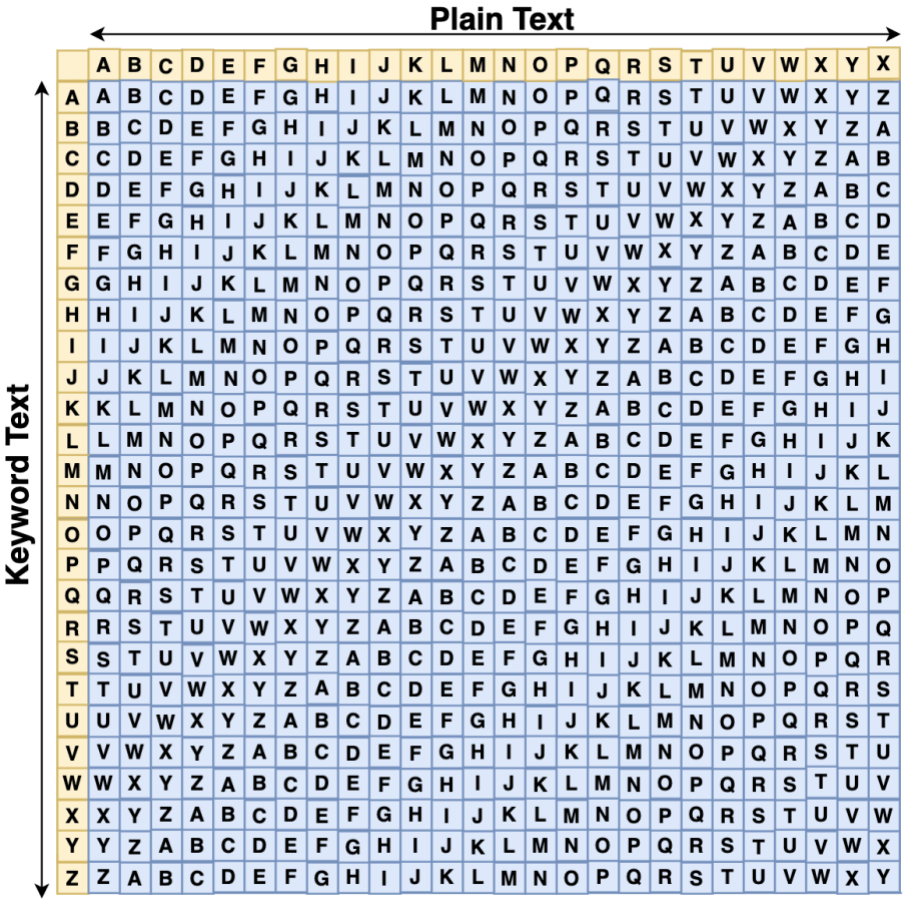

Figure 13: Vigenere Table

If the length of the keywords is shorter than the length of the plaintext then the key word is repeatedly used. For example, lets take the plaintext as “NO WAY HOME” and the keyword as “PETER”. The encryption and decryption process goes as,

For encryption:

Table 1: Example of encryption step for Vigenere Cipher.

Plaintext	N	O	W	A	Y	H	O	M	E
Keyword	P	E	T	E	R	P	E	T	E
Ciphertext	C	S	P	E	P	W	S	F	I

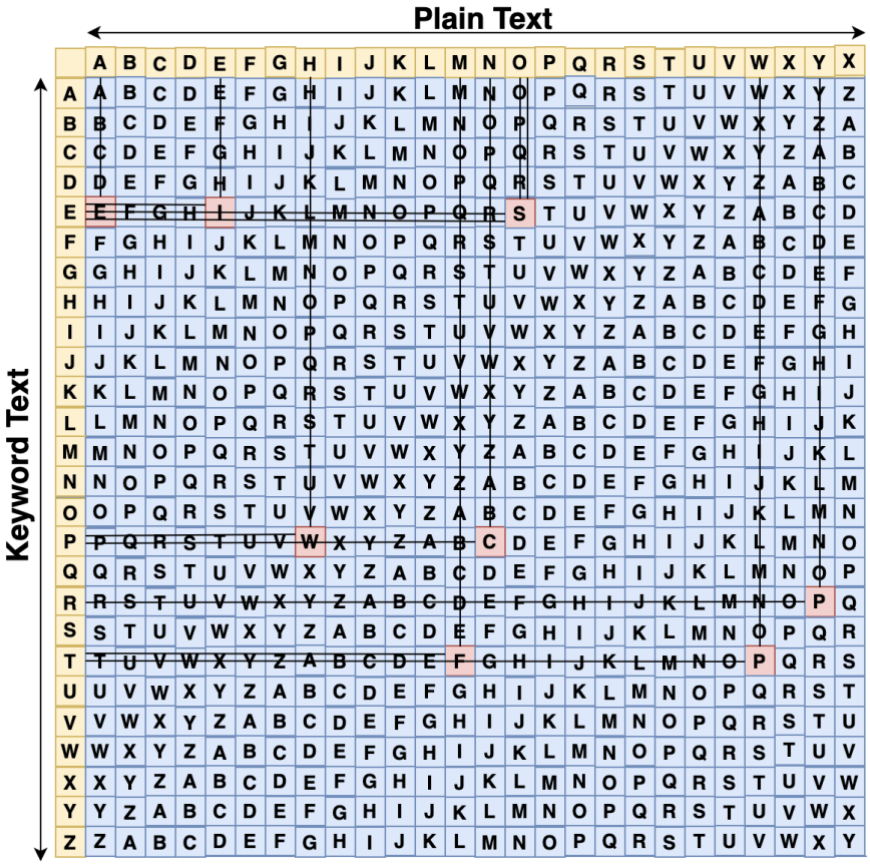

Figure 14: Example for encryption step of Vigenere Cipher.

For decryption:

Table 2: Example of decryption step for Vigenere Cipher.

Ciphertext	C	S	P	E	P	W	S	F	I
Keyword	P	E	T	E	R	P	E	T	E
Plaintext	N	O	W	A	Y	H	O	M	E

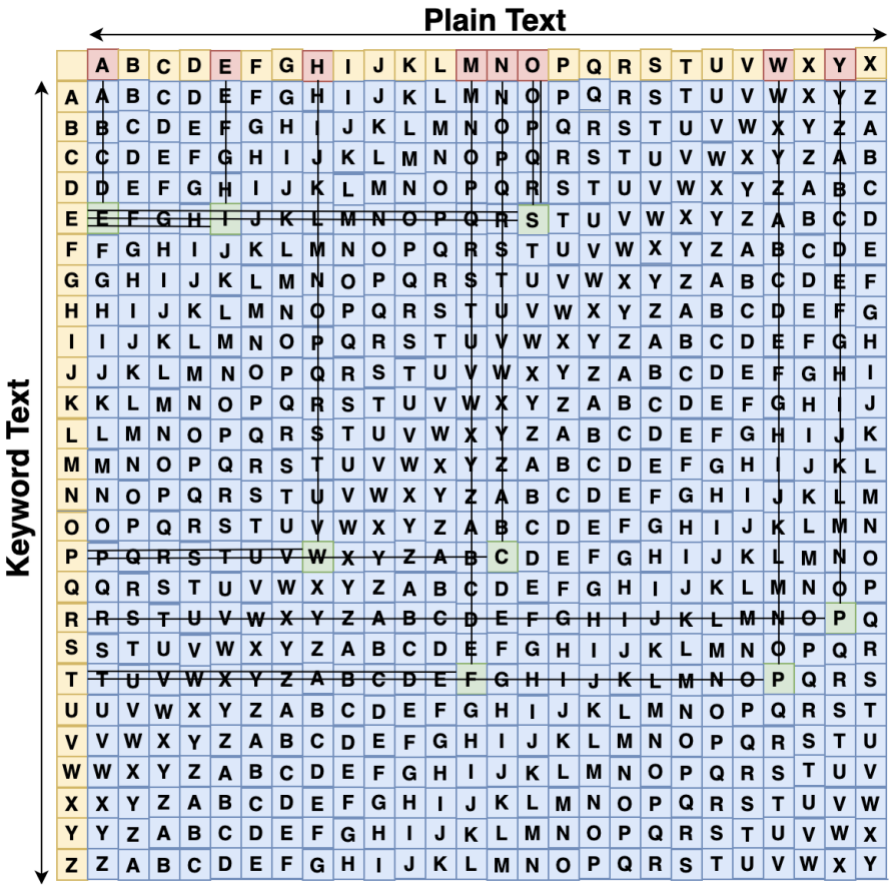

Figure 15: Example for decryption step of Vigenere Cipher.

For the modification of the Caesar cipher basic Caesar cipher is performed with extracting the character from the new substitution table. Then the encrypted text is modified using odd and even rule and finally vigenere cipher with 48x48 table is used to get the final ciphered text. The encryption and decryption formula for the Caesar cipher are,

En = (P + K) mod 47

Dn = (C - K) mod 47

Where En is the encryption, Dn is the decryption, P is the the plaintext, C is the cipheredtext whose value is extracted from the new modified substitution table for Caesar cipher and K is the key for Caesar cipher.

The modified Caesar cipher substitution table and the modified 48x48 Vigenere cipher is added below.

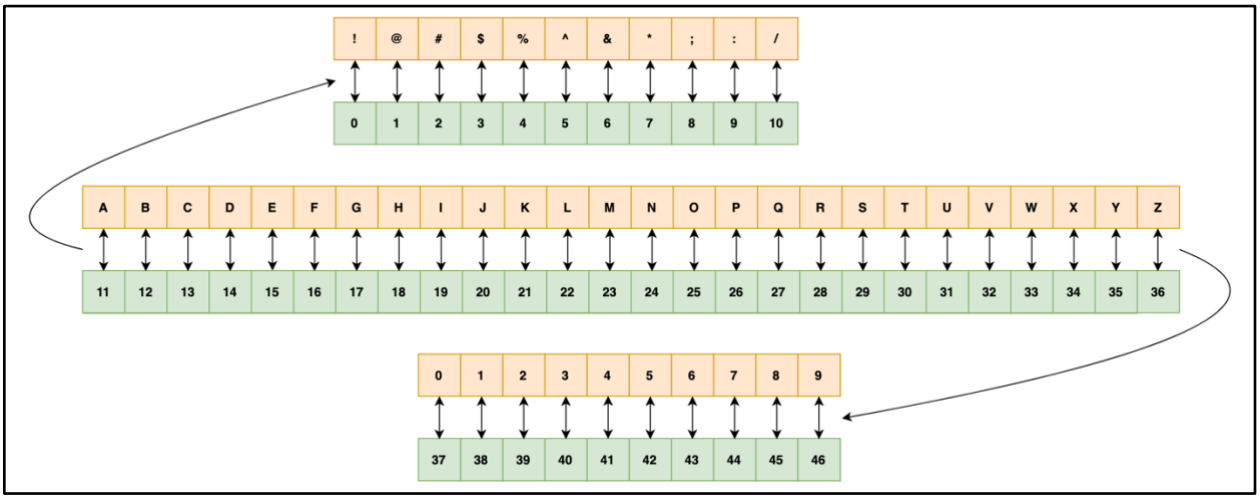

Figure 16: New modified Substitution table for Caesar cipher.

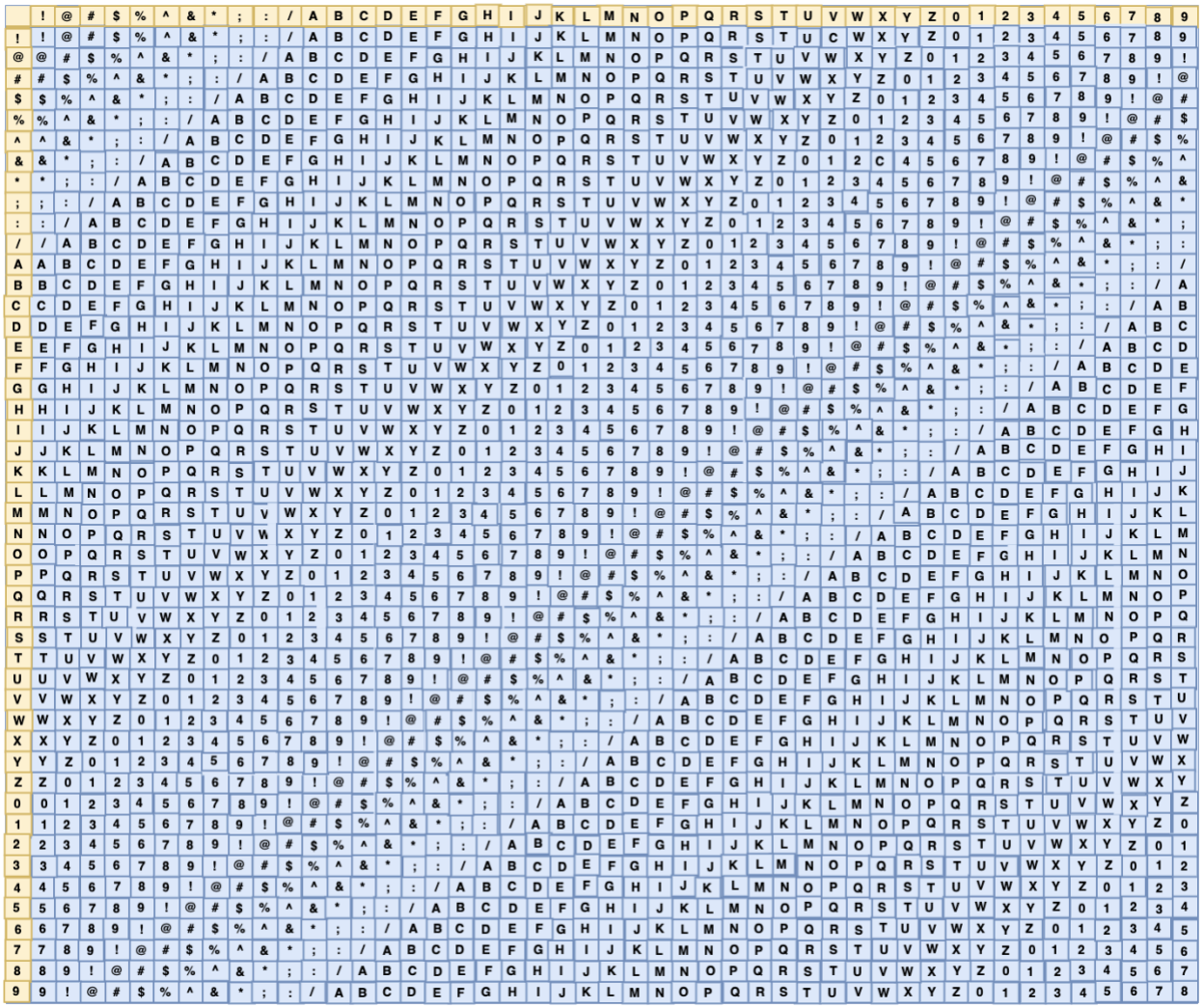

Figure 17: New modified character table for Vigenere cipher.

Encryption:

The standard Caesar cipher is used in the encryption process of the new cryptographic method, with the formula En = (P + K) mod 47, where the key is set to '77' in particular and divided by '47', which is the entire number of characters in the process. The output number is then substituted with its actual value from the Caesar cipher's new modified substitution table.

The next step goes by the new set of rules or algorithm implied in this cryptographic technique where if the output number is even or 0, three is added and again the actual value is extracted from the newly modified substitution table and if the output number is odd, three is subtracted and the actual value is extracted from the modified substitution table again.

Finally, for the third step of the encryption process the newly modified 48x48 Vigenere table is used to encrypt where, the keyword is used as the output which has come from the normal Caesar cipher encryption process and the plaintext for the process is taken as the output which comes from the odd even rule. These steps result in being the final ciphertext of the new cryptographic algorithm.

Decryption:

To decrypt the newly modified cryptographic algorithm, the traditional Vigenere cipher decryption method is used first, followed by the newly modified 48x48 Vigenere table. The ciphertext is the final output of the encryption process and the keyword is the same as that used in the encryption process for the Vigenere cipher.

The value of the decrypted characters from the Vigenere cipher is extracted from the newly modified substitution table and if the output number is even or 0, three is added and the actual value is extracted and if the output number is odd, three is subtracted and the actual value is extracted, which would be used as the value of 'C' in the basic Caesar cipher decryption process.

Finally, the Caesar cipher is used in the third step of the decryption process, with the formula Dn = (C – K) mod 47, where the key is set to '77' in specific and divided by '47,' which is the total number of characters in the process. The output number is then swapped with its true value from the Caesar cipher's new modified substitution table, providing the new cryptographic algorithm's final plaintext.

3.2 Modification

The name of this new modified cryptographic algorithm is “Caenere Algorithm based upon odd and even rule”. In the new algorithm the modification of odd and even rule and implementation of Vigenere cipher was necessary because of the frequency of the letters, the Caesar cipher provides a significant hint to decrypt the message. The basic Caesar cipher is very simple to understand and anyone can easily decrypt by shifting the alphabets to three steps the block.

The new encryption algorithm, on the other hand, has a key of '77' and adds integers from 0 to 9 as well as a few characters to the alphabets, bringing the total number of characters to '47.' The odd and even rule is then applied to the Caesar cipher for the production of the ciphertext, which is the second phase of the new method.

For more security aspect after the odd and even process the concept of polyalphabetic cipher process, the classic Vigenere cipher is also implemented with the newly modified 48x48 Vigenere table.

3.3 Algorithm

3.3.1 New Encryption Algorithm

Step 1: Start

Step 2: Take any plaintext

Step 3: Encrypt the plaintext using Caesar cipher

Step 4: Use formula En = (P + K) mod 47

Step 5: Take value of P from new modified substitution table and K as ‘77’

Step 6: Substitute the value from the new modified substitution table

Step 7: Encrypt using odd and even rule

Step 8: If the value is even or 0

Step 9: Add three into it

Step 9: Else the value is odd

Step 10: Subtract three into it

Step 11: Extract the value form the substitution table

Step 11: Encrypt using Vigenere cipher

Step 12: Use the plaintext as the output from odd and even rule and keyword as output from Caesar cipher

Step 11: Stop

3.3.2 New Decryption Algorithm

Step 1: Start
Step 2: Take the ciphertext from the encryption process
Step 3: Decrypt using Vigenere cipher
Step 4: Use the ciphertext from the above and keyword as which was used in encryption process.
Step 5: Decrypt using odd and even rule
Step 6: If the value is even or 0
Step 7: Add three into it
Step 8: Else the value is odd
Step 9: Subtract three into it
Step 10: Extract the value form the substitution table
Step 11: Decrypt using Caesar cipher
Step 12: Use formula Dn = (C – K) mod 47
Step 13: Take value of C from new modified substitution table and K as ‘77’
Step 14: Substitute the value from the new modified substitution table
Step 15: Stop

3.4 Flowchart

A flow chart is a type of diagram that illustrates a process by using various symbols that contain information about steps or a sequence of events. Each of these symbols is connected with arrows to show the process's flow direction (Techopedia, 2011).

3.4.1 New Encryption Flowchart

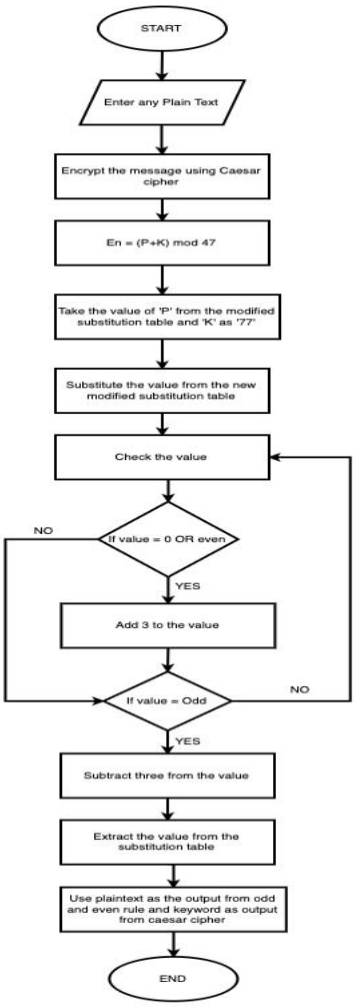

Figure 18: Encryption flowchart.

3.4.2 New Decryption Flowchart

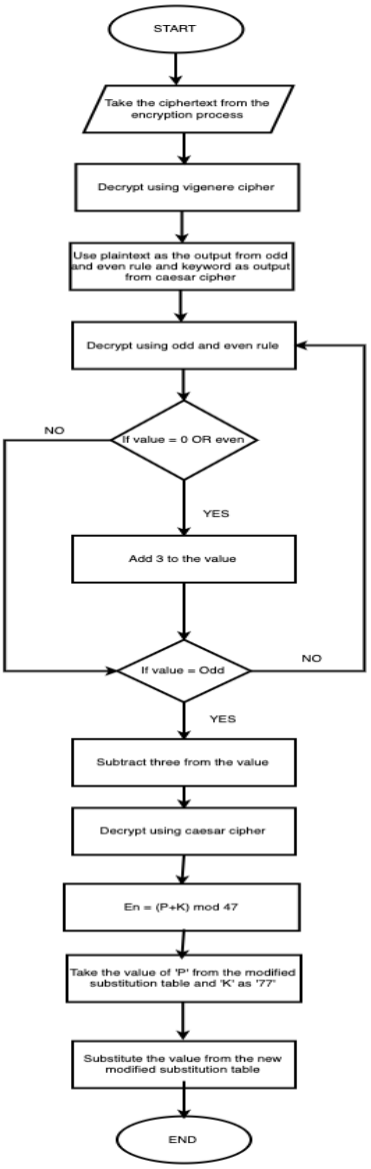

Figure 19: Decryption Flowchart.

4. Testing

4.1 Test 1

For encryption:

Performing Caesar cipher at first with taking the plaintext as “COURSEWORK”, key as ‘77’. We have the modified formula for encryption as En = (P + K) mod 47, where ‘En’ stands for encryption and ‘P’ stands for the value of plain text and substituting their value from the newly modified Substitution table for Caesar cipher.

- C = En = (P + K) mod 47 = (13 +77) mod 47 = 90 mod 47 = 43 = (6)
- O = En = (P + K) mod 47 = (25 + 77) mod 47 = 102 mod 47 = 8 = (;)
- U = En = (P + K) mod 47 = (31 + 77) mod 47 = 108 mod 47 = 14 = (D)
- R = En = (P + K) mod 47 = (28 + 77) mod 47 = 105 mod 47 = 11 = (A)
- S = En = (P + K) mod 47 = (29 + 77) mod 47 = 106 mod 47 = 12 = (B)
- E = En = (P + K) mod 47 = (15 + 77) mod 47 = 92 mod 47 = 45 = (8)
- W = En = (P + K) mod 47 = (33 + 77) mod 47 = 110 mod 47 = 16 = (F)
- O = En = (P + K) mod 47 = (25 + 77) mod 47 = 102 mod 47 = 8 = (;)
- R = En = (P + K) mod 47 = (28 + 77) mod 47 = 105 mod 47 = 11 = (A)
- K = En = (P + K) mod 47 = (21 + 77) mod 47 = 98 mod 47 = 4 = (%)

The ciphertext of the plaintext of the word “COURSEWORK” is 6;DAB8F;A% after performing Caesar cipher.

Now,

Performing the odd and even rule where if the output number is even or 0, three is added and if the output number is odd, three is subtracted and the actual value is extracted from the modified substitution table. Here, the plaintext for the process is the ciphertext from the above Caesar cipher process.

Table 3: Encryption using odd and even rule for test 1.

Plaintext	Value	Odd / Even	Final Value	Ciphertext
6	43	Odd	43 – 3 = 40	3
;	8	Even	8 + 3 = 11	A
D	14	Even	14 + 3 = 17	G
A	11	Odd	11 – 3 = 8	;
B	12	Even	12 + 3 = 15	E
8	45	Odd	45 – 3 = 42	5
F	16	Even	16 + 3 = 19	I
;	8	Even	8 + 3 = 11	A
A	11	Odd	11 – 3 = 8	;
%	4	Even	4 + 3 = 7	*

The ciphertext for the plaintext 6;DAB8F;A% is 3AG;E5IA;*

Then,

Performing the vigenere cipher with taking the plaintext as 3AG;E5IA;* which is the ciphertext after performing Caesar cipher and keyword as 6;DAB8F;A% for the third step of the encryption process.

Table 4: Encryption using vigenere cipher for test 1.

Plaintext	3	A	G	;	E	5	I	A	;	*
Keyword	6	;	D	A	B	8	F	;	A	%
Ciphertext	Z	I	U	I	Q	3	Y	I	I	A

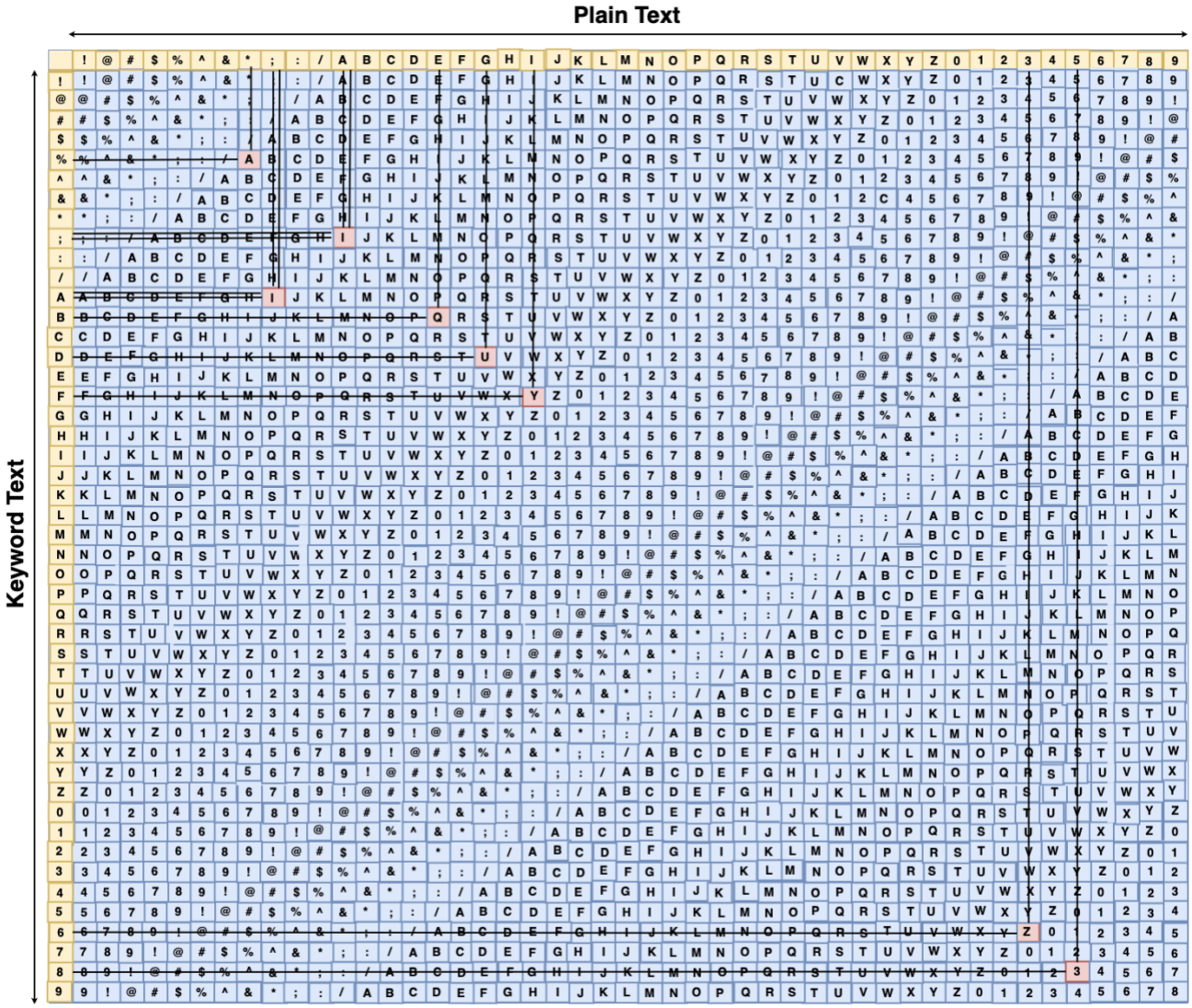

Figure 20: Encryption using vigenere cipher for test 1.

ZIUIQ3YIIA is the final encryption for the plaintext COURSEWORK after performing encryption process of the new cryptographic algorithm.

For decryption:

Performing the vigenere cipher at first with taking the ciphertext as ZIUIQ3YIIA which is the final encryption output after performing the encryption process using new cryptographic algorithm and taking keyword as 6;DAB8F;A% for the first step of the decryption process.

Table 5: Decryption using vigenere cipher for test 1.

Ciphertext	Z	I	U	I	Q	3	Y	I	I	A
Keyword	6	;	D	A	B	8	F	;	A	%
Plaintext	3	A	G	;	E	5	I	A	;	*

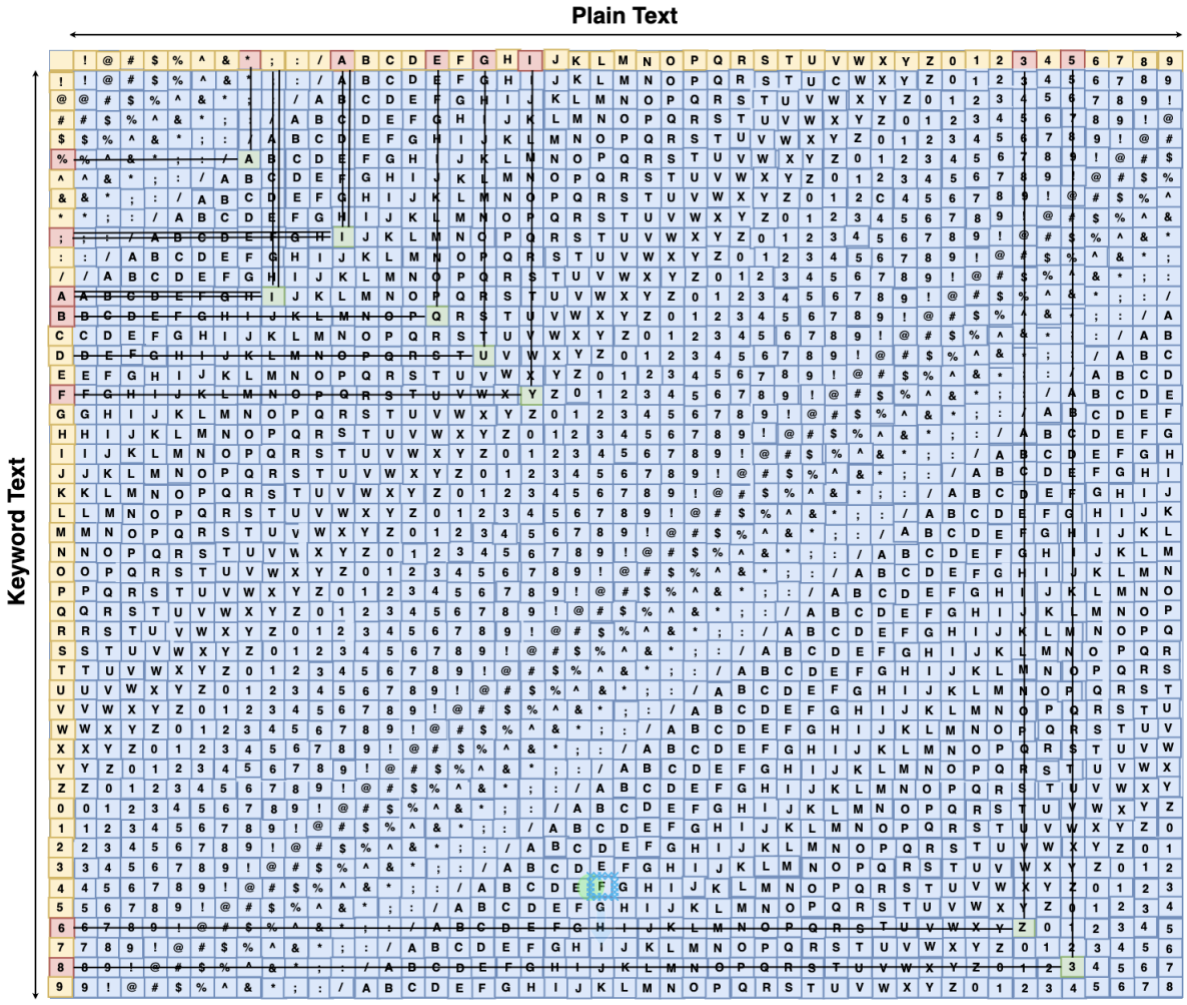

Figure 21: Decryption using vigenere cipher for test 1.

By performing the vigenere cipher with ciphertext ZIUIQ3YIIA and keyword 6;DAB8F;A% we get the plaintext 3AG;E5IA;*

Now,

Performing the odd and even rule where if the output number is even or 0, three is added and if the output number is odd, three is subtracted and the actual value is extracted from the modified substitution table. Here, the ciphertext for the process is the plaintext from the above Vigenere cipher process.

Table 6: Decryption using odd and even rule for test 1.

Ciphertext	Value	Odd / Even	Final Value	Plaintext
3	40	Even	40 + 3 = 43	6
A	11	Odd	11 - 3 = 8	;
G	17	Odd	17 - 3 = 14	D
;	8	Even	8 + 3 = 11	A
E	15	Odd	15 - 3 = 12	B
5	42	Even	42 + 3 = 45	8
I	19	Odd	19 - 3 = 16	F
A	11	Odd	11 - 3 = 8	;
;	8	Even	8 + 3 = 11	A
*	7	Odd	7 - 3 = 4	%

The plaintext for the ciphertext 3AG;E5IA;* is 6;DAB8F;A%

Then,

Performing Caesar cipher taking the ciphertext as 6;DAB8F;A% and key as ‘77’. We have the modified formula for decryption as Dn = (C - K) mod 47, where ‘Dn’ stands for decryption and ‘C’ stands for the value of cipher text and substituting their value from the newly modified Substitution table for Caesar cipher.

- 6 = Dn = (C - K) mod 47 = (43 - 77) mod 47 = -34 mod 47 = 13 = (C)
- ; = Dn = (C - K) mod 47 = (8 - 77) mod 47 = -69 mod 47 = 25 = (O)
- D = Dn = (C - K) mod 47 = (14 - 77) mod 47 = -63 mod 47 = 31 = (U)
- A = Dn = (C - K) mod 47 = (11 - 77) mod 47 = -66 mod 47 = 28 = (R)
- B = Dn = (C - K) mod 47 = (12 - 77) mod 47 = -65 mod 47 = 29 = (S)
- 8 = Dn = (C - K) mod 47 = (45 - 77) mod 47 = -32 mod 47 = 15 = (E)
- F = Dn = (C - K) mod 47 = (16 - 77) mod 47 = -61 mod 47 = 33 = (W)
- ; = Dn = (C - K) mod 47 = (8 - 77) mod 47 = -69 mod 47 = 25 = (O)
- A = Dn = (C - K) mod 47 = (11 - 77) mod 47 = -66 mod 47 = 28 = (R)
- % = Dn = (C - K) mod 47 = (4 - 77) mod 47 = -73 mod 47 = 21 = (K)

The final plain text of the ciphertext 6;DAB8F;A% is “COURSEWORK” after performing Caesar cipher.

4.2 Test 2

For encryption:

Performing Caesar cipher at first with taking the plaintext as “CARNAGE”, key as ‘77’. We have the modified formula for encryption as En = (P + K) mod 47, where ‘En’ stands for encryption and ‘P’ stands for the value of plain text and substituting their value from the newly modified Substitution table for Caesar cipher.

- C = En = (P + K) mod 47 = (13 +77) mod 47 = 90 mod 47 = 43 = (6)
- A = En = (P + K) mod 47 = (11 + 77) mod 47 = 88 mod 47 = 41 = (4)
- R = En = (P + K) mod 47 = (28 + 77) mod 47 = 105 mod 47 = 11 = (A)
- N = En = (P + K) mod 47 = (24 + 77) mod 47 = 101 mod 47 = 7 = (*)
- A = En = (P + K) mod 47 = (11 + 77) mod 47 = 88 mod 47 = 41 = (4)
- G = En = (P + K) mod 47 = (17 + 77) mod 47 = 94 mod 47 = 0 = (!)
- E = En = (P + K) mod 47 = (15 + 77) mod 47 = 92 mod 47 = 45 = (8)

The ciphertext of the plaintext of the word “CARNAGE” is 64A*4!8 after performing Caesar cipher.

Now,

Performing the odd and even rule where if the output number is even or 0, three is added and if the output number is odd, three is subtracted and the actual value is extracted from the modified substitution table. Here, the plaintext for the process is the ciphertext from the above Caesar cipher process.

Table 7: Encryption using odd and even rule for test 2.

Plaintext	Value	Odd / Even	Final Value	Ciphertext
6	43	Odd	43 – 3 = 40	3
4	41	Odd	41 – 3 = 38	1
A	11	Odd	11 – 3 = 8	;
*	7	Odd	7 – 3 = 4	%
4	41	Odd	41 – 3 = 38	1
!	0	Even	0 + 3 = 3	$
8	45	Odd	45 – 3 = 42	5

The ciphertext for the plaintext 64A*4!8 is 31;%1$5

Then,

Performing the vigenere cipher with taking the plaintext as 31;%1$5 which is the ciphertext after performing Caesar cipher and keyword as 64A*4!8 for the third step of the encryption process. The encryption process of the vigenere cipher is carried out as done in the Task 1.

Table 8: Encryption using vigenere cipher for test 2.

Plaintext	3	1	;	%	1	$	5
Keyword	6	4	A	*	4	!	8
Ciphertext	Z	V	I	A	V	$	3

ZVIAV$3 is the final encryption for the plaintext CARNAGE after performing encryption process of the new cryptographic algorithm.

For decryption:

Performing the vigenere cipher at first with taking the ciphertext as ZVIAV$3 which is the final encryption output after performing the encryption process using new cryptographic algorithm and taking keyword as 64A*4!8 for the first step of the decryption process. The decryption process of the vigenere cipher is carried out as done in the Task 1.

Table 9: Decryption using vigenere cipher for test 2.

Ciphertext	Z	V	I	A	V	$	3
Keyword	6	4	A	*	4	!	8
Plaintext	3	1	;	%	1	$	5

By performing the vigenere cipher with ciphertext ZVIAV$3 and keyword 64A*4!8 we get the plaintext 31;%1$5

Now,

Performing the odd and even rule where if the output number is even or 0, three is added and if the output number is odd, three is subtracted and the actual value is extracted from the modified substitution table. Here, the ciphertext for the process is the plaintext from the above Vigenere cipher process.

Table 10: Decryption using odd and even rule for test 2.

Ciphertext	**Value**	**Odd / Even**	**Final Value**	**Plaintext**
3	40	Even	40 + 3 = 43	6
1	38	Even	38 + 3 = 41	4
;	8	Even	8 + 3 = 11	A
%	4	Even	4 + 3 = 7	*
1	38	Even	38 + 3 = 41	4
$	3	Odd	3 - 3 = 0	!
5	42	Even	42 + 3 = 45	8

The plaintext for the ciphertext 31;%1$5 is 64A*4!8

Then,

Performing Caesar cipher taking the ciphertext as 64A*4!8 and key as ‘77’. We have the modified formula for decryption as Dn = (C - K) mod 47, where ‘Dn’ stands for decryption and ‘C’ stands for the value of cipher text and substituting their value from the newly modified Substitution table for Caesar cipher.

- 6 = Dn = (C - K) mod 47 = (43 - 77) mod 47 = -34 mod 47 = 13 = (C)
- 4 = Dn = (C - K) mod 47 = (41 - 77) mod 47 = -36 mod 47 = 11 = (A)
- A = Dn = (C - K) mod 47 = (11 - 77) mod 47 = -66 mod 47 = 28 = (R)
- * = Dn = (C - K) mod 47 = (7 - 77) mod 47 = -70 mod 47 = 24 = (N)
- 4 = Dn = (C - K) mod 47 = (41 - 77) mod 47 = -36 mod 47 = 11 = (A)
- ! = Dn = (C - K) mod 47 = (0 - 77) mod 47 = -77 mod 47 = 17 = (G)
- 8 = Dn = (C - K) mod 47 = (45 - 77) mod 47 = -32 mod 47 = 15 = (E)

The final plain text of the ciphertext 64A*4!8 is “CARNAGE” after performing Caesar cipher.

4.3 Test 3

For encryption:

Performing Caesar cipher at first with taking the plaintext as “18JAN2001”, key as ‘77’. We have the modified formula for encryption as En = (P + K) mod 47, where ‘En’ stands for encryption and ‘P’ stands for the value of plain text and substituting their value from the newly modified Substitution table for Caesar cipher.

- 1 = En = (P + K) mod 47 = (38 +77) mod 47 = 115 mod 47 = 21 = (K)
- 8 = En = (P + K) mod 47 = (45 + 77) mod 47 = 122 mod 47 = 28 = (R)
- J = En = (P + K) mod 47 = (20 + 77) mod 47 = 97 mod 47 = 3 = ($)
- A = En = (P + K) mod 47 = (11 + 77) mod 47 = 88 mod 47 = 41 = (4)
- N = En = (P + K) mod 47 = (24 + 77) mod 47 = 101 mod 47 = 7 = (*)
- 2 = En = (P + K) mod 47 = (39 + 77) mod 47 = 116 mod 47 = 22 = (L)
- 0 = En = (P + K) mod 47 = (37 + 77) mod 47 = 114 mod 47 = 20 = (J)
- 0 = En = (P + K) mod 47 = (37 + 77) mod 47 = 114 mod 47 = 20 = (J)
- 1 = En = (P + K) mod 47 = (38 + 77) mod 47 = 115 mod 47 = 21 = (K)

The ciphertext of the plaintext of the word “18JAN2001” is KR$4*LJJK after performing Caesar cipher.

Now,

Performing the odd and even rule where if the output number is even or 0, three is added and if the output number is odd, three is subtracted and the actual value is extracted from the modified substitution table. Here, the plaintext for the process is the ciphertext from the above Caesar cipher process.

Table 11: Encryption using odd and even rule for test 3.

Plaintext	Value	Odd / Even	Final Value	Ciphertext
K	21	Odd	21 – 3 = 18	H
R	28	Even	28 + 3 = 31	U
$	3	Odd	3 – 3 = 0	!
4	41	Odd	41 – 3 = 38	1
*	7	Odd	7 – 3 = 4	%
L	22	Even	22 + 3 = 25	O
J	20	Even	20 + 3 = 23	M
J	20	Even	20 + 3 = 23	M
K	21	Odd	21 – 3 = 18	H

The ciphertext for the plaintext KR$4*LJJK is HU!1%OMMH

Then,

Performing the vigenere cipher with taking the plaintext as HU!1%OMMH which is the ciphertext after performing Caesar cipher and keyword as KR$4*LJJK for the third step of the encryption process. The encryption process of the vigenere cipher is carried out as done in the Task 1.

Table 12: Encryption using vigenere cipher for test 3.

Plaintext	H	U	!	1	%	O	M	M	H
Keyword	K	R	$	4	*	L	J	J	K
Ciphertext	2	B	S	V	A	!	6	6	2

2BSVA!662 is the final encryption for the plaintext CARNAGE after performing encryption process of the new cryptographic algorithm.

For decryption:

Performing the vigenere cipher at first with taking the ciphertext as 2BSVA!662 which is the final encryption output after performing the encryption process using new cryptographic algorithm and taking keyword as KR$4*LJJK for the first step of the decryption process. The decryption process of the vigenere cipher is carried out as done in the Task 1.

Table 13: Decryption using vigenere cipher for test 3.

Ciphertext	2	B	S	V	A	!	6	6	2
Keyword	K	R	$	4	*	L	J	J	K
Plaintext	H	U	!	1	%	O	M	M	H

By performing the vigenere cipher with ciphertext 2BSVA!662 and keyword KR$4*LJJK we get the plaintext HU!1%OMMH

Now,

Performing the odd and even rule where if the output number is even or 0, three is added and if the output number is odd, three is subtracted and the actual value is extracted from the modified substitution table. Here, the ciphertext for the process is the plaintext from the above Vigenere cipher process.

Table 14: Decryption using odd and even rule for test 3.

Ciphertext	Value	Odd / Even	Final Value	Plaintext
H	18	Even	18 + 3 = 21	K
U	31	Odd	31 - 3 = 28	R
!	0	Even	0 + 3 = 3	$
1	38	Even	38 + 3 = 41	4
%	4	Even	4 + 3 = 7	*
O	25	Odd	25 - 3 = 22	L
M	23	Odd	23 - 3 = 20	J
M	23	Odd	23 – 3 = 20	J
H	18	Even	18 + 3 = 21	K

The plaintext for the ciphertext HU!1%OMMH is KR$4*LJJK

Then,

Performing Caesar cipher taking the ciphertext as KR$4*LJJK and key as ‘77’. We have the modified formula for decryption as Dn = (C - K) mod 47, where ‘Dn’ stands for decryption and ‘C’ stands for the value of cipher text and substituting their value from the newly modified Substitution table for Caesar cipher.

- K = Dn = (C - K) mod 47 = (21 - 77) mod 47 = -56 mod 47 = 38 = (1)
- R = Dn = (C - K) mod 47 = (28 - 77) mod 47 = -49 mod 47 = 45 = (8)
- $ = Dn = (C - K) mod 47 = (3 - 77) mod 47 = -74 mod 47 = 20 = (J)
- 4 = Dn = (C - K) mod 47 = (41 - 77) mod 47 = -36 mod 47 = 11 = (A)
- * = Dn = (C - K) mod 47 = (7 - 77) mod 47 = -70 mod 47 = 24 = (N)
- L = Dn = (C - K) mod 47 = (22 - 77) mod 47 = -55 mod 47 = 39 = (2)
- J = Dn = (C - K) mod 47 = (20 - 77) mod 47 = -57 mod 47 = 37 = (0)
- J = Dn = (C - K) mod 47 = (20 - 77) mod 47 = -57 mod 47 = 37 = (0)
- K = Dn = (C - K) mod 47 = (21 - 77) mod 47 = -56 mod 47 = 38 = (1)

The final plain text of the ciphertext KR$4*LJJK is “18JAN2001” after performing Caesar cipher.

4.4 Test 4

For encryption:

Performing Caesar cipher at first with taking the plaintext as “NP01NT4S210129”, key as ‘77’. We have the modified formula for encryption as En = (P + K) mod 47, where ‘En’ stands for encryption and ‘P’ stands for the value of plain text and substituting their value from the newly modified Substitution table for Caesar cipher.

- N = En = (P + K) mod 47 = (24 + 77) mod 47 = 101 mod 47 = 7 = (*)
- P = En = (P + K) mod 47 = (26 + 77) mod 47 = 103 mod 47 = 9 = (:)
- 0 = En = (P + K) mod 47 = (37 + 77) mod 47 = 114 mod 47 = 20 = (J)
- 1 = En = (P + K) mod 47 = (38 + 77) mod 47 = 115 mod 47 = 21 = (K)
- N = En = (P + K) mod 47 = (24 + 77) mod 47 = 101 mod 47 = 7 = (*)
- T = En = (P + K) mod 47 = (30 + 77) mod 47 = 107 mod 47 = 13 = (C)
- 4 = En = (P + K) mod 47 = (41 + 77) mod 47 = 118 mod 47 = 24 = (N)
- S = En = (P + K) mod 47 = (29 + 77) mod 47 = 106 mod 47 = 12 = (B)
- 2 = En = (P + K) mod 47 = (39 + 77) mod 47 = 116 mod 47 = 22 = (L)
- 1 = En = (P + K) mod 47 = (38 + 77) mod 47 = 115 mod 47 = 21 = (K)
- 0 = En = (P + K) mod 47 = (37 + 77) mod 47 = 114 mod 47 = 20 = (J)
- 1 = En = (P + K) mod 47 = (38 + 77) mod 47 = 115 mod 47 = 21 = (K)
- 2 = En = (P + K) mod 47 = (39 + 77) mod 47 = 116 mod 47 = 22 = (L)
- 9 = En = (P + K) mod 47 = (46 + 77) mod 47 = 123 mod 47 = 29 = (S)

The ciphertext of the plaintext of the word “NP01NT4S210129” is *:JK*CNBLKJKLS after performing Caesar cipher.

Now,

Performing the odd and even rule where if the output number is even or 0, three is added and if the output number is odd, three is subtracted and the actual value is extracted from the modified substitution table. Here, the plaintext for the process is the ciphertext from the above Caesar cipher process.

Table 15: Encryption using odd and even rule for test 4.

Plaintext	Value	Odd / Even	Final Value	Ciphertext
*	7	Odd	7 – 3 = 4	%
:	9	Odd	9 – 3 = 6	&
J	20	Even	20 + 3 = 23	M
K	21	Odd	21 – 3 = 18	H
*	7	Odd	7 – 3 = 4	%
C	13	Odd	13 – 3 = 10	/
N	24	Even	24 + 3 = 27	Q
B	12	Even	12 + 3 = 15	E
L	22	Even	22 + 3 = 25	O
K	21	Odd	21 – 3 = 18	H
J	20	Even	20 + 3 = 23	M
K	21	Odd	21 – 3 = 18	H
L	22	Even	22 + 3 = 25	O
S	29	Odd	29 – 3 = 26	P

The ciphertext for the plaintext *:JK*CNBLKJKLS is %&MH%/QEOHMHOP

Then,

Performing the vigenere cipher with taking the plaintext as %&MH%/QEOHMHOP which is the ciphertext after performing Caesar cipher and keyword as *:JK*CNBLKJKLS for the third step of the encryption process. The encryption process of the vigenere cipher is carried out as done in the Task 1.

Table 16: Encryption using vigenere cipher for test 4.

Plaintext	%	&	M	H	%	/	Q	E	O	H	M	H	O	P
Keyword	*	:	J	K	*	C	N	B	L	K	J	K	L	S
Ciphertext	A	E	6	2	A	M	%	Q	!	2	6	2	!	;

AE62AM%Q!262!; is the final encryption for the plaintext NP01NT4S210129 after performing encryption process of the new cryptographic algorithm.

For decryption:

Performing the vigenere cipher at first with taking the ciphertext as AE62AM%Q!262!; which is the final encryption output after performing the encryption process using new cryptographic algorithm and taking keyword as *:JK*CNBLKJKLS for the first step of the decryption process. The decryption process of the vigenere cipher is carried out as done in the Task 1.

Table 17: Decryption using vigenere cipher for test 4.

Ciphertext	A	E	6	2	A	M	%	Q	!	2	6	2	!	;
Keyword	*	:	J	K	*	C	N	B	L	K	J	K	L	S
Plaintext	%	&	M	H	%	/	Q	E	O	H	M	H	O	P

By performing the vigenere cipher with ciphertext AE62AM%Q!262!; and keyword *:JK*CNBLKJKLS we get the plaintext %&MH%/QEOHMHOP

Now,

Performing the odd and even rule where if the output number is even or 0, three is added and if the output number is odd, three is subtracted and the actual value is extracted from the modified substitution table. Here, the ciphertext for the process is the plaintext from the above Vigenere cipher process.

Table 18: Decryption using odd and even rule for test 4.

Ciphertext	Value	Odd / Even	Final Value	Plaintext
%	4	Even	4 + 3 = 7	*
&	6	Even	6 + 3 = 9	:
M	23	Odd	23 - 3 = 20	J
H	18	Even	18 + 3 = 21	K
%	4	Even	4 + 3 = 7	*
/	10	Even	10 + 3 = 13	C
Q	27	Odd	27 - 3 = 24	N
E	15	Odd	15 - 3 = 12	B
O	25	Odd	25 - 3 = 22	L
H	18	Even	18 + 3 = 21	K
M	13	Odd	13 – 3 = 20	J
H	18	Even	18 + 3 = 21	K
O	25	Odd	25 – 3 = 22	L
P	26	Even	26 + 3 = 29	S

The plaintext for the ciphertext %&MH%/QEOHMHOP is *:JK*CNBLKJKLS

Then,

Performing Caesar cipher taking the ciphertext as *:JK*CNBLKJKLS and key as ‘77’. We have the modified formula for decryption as Dn = (C - K) mod 47, where ‘Dn’ stands for decryption and ‘C’ stands for the value of cipher text and substituting their value from the newly modified Substitution table for Caesar cipher.

- * = Dn = (C - K) mod 47 = (7 - 77) mod 47 = -70 mod 47 = 24 = (N)
- : = Dn = (C - K) mod 47 = (9 - 77) mod 47 = -68 mod 47 = 26 = (P)
- J = Dn = (C - K) mod 47 = (20 - 77) mod 47 = -57 mod 47 = 37 = (0)
- K = Dn = (C - K) mod 47 = (21 - 77) mod 47 = -56 mod 47 = 38 = (1)
- * = Dn = (C - K) mod 47 = (7 - 77) mod 47 = -70 mod 47 = 24 = (N)
- C = Dn = (C - K) mod 47 = (13 - 77) mod 47 = -64 mod 47 = 30 = (T)

- N = Dn = (C - K) mod 47 = (24 - 77) mod 47 = -53 mod 47 = 41 = (4)
- B = Dn = (C - K) mod 47 = (12 - 77) mod 47 = -65 mod 47 = 29 = (S)
- L = Dn = (C - K) mod 47 = (22 - 77) mod 47 = -55 mod 47 = 39 = (2)
- K = Dn = (C - K) mod 47 = (21 - 77) mod 47 = -56 mod 47 = 38 = (1)
- J = Dn = (C - K) mod 47 = (20 - 77) mod 47 = -57 mod 47 = 37 = (0)
- K = Dn = (C - K) mod 47 = (21 - 77) mod 47 = -56 mod 47 = 38 = (1)
- L = Dn = (C - K) mod 47 = (22 - 77) mod 47 = -55 mod 47 = 39 = (2)
- S = Dn = (C - K) mod 47 = (29 - 77) mod 47 = -48 mod 47 = 46 = (9)

The final plain text of the ciphertext *:JK*CNBLKJKLS is “NP01NT4S210129” after performing Caesar cipher.

4.5 Test 5

For encryption:

Performing Caesar cipher at first with taking the plaintext as “9851069507”, key as ‘77’. We have the modified formula for encryption as En = (P + K) mod 47, where ‘En’ stands for encryption and ‘P’ stands for the value of plain text and substituting their value from the newly modified Substitution table for Caesar cipher.

- 9 = En = (P + K) mod 47 = (46 + 77) mod 47 = 123 mod 47 = 29 = (S)
- 8 = En = (P + K) mod 47 = (45 + 77) mod 47 = 122 mod 47 = 28 = (R)
- 5 = En = (P + K) mod 47 = (42 + 77) mod 47 = 119 mod 47 = 25 = (O)
- 1 = En = (P + K) mod 47 = (38 + 77) mod 47 = 115 mod 47 = 21 = (K)
- 0 = En = (P + K) mod 47 = (37 + 77) mod 47 = 114 mod 47 = 20 = (J)
- 6 = En = (P + K) mod 47 = (43 + 77) mod 47 = 120 mod 47 = 26 = (P)
- 9 = En = (P + K) mod 47 = (46 + 77) mod 47 = 123 mod 47 = 29 = (A)
- 5 = En = (P + K) mod 47 = (42 + 77) mod 47 = 119 mod 47 = 25 = (O)
- 0 = En = (P + K) mod 47 = (37 + 77) mod 47 = 114 mod 47 = 20 = (J)
- 7 = En = (P + K) mod 47 = (44 + 77) mod 47 = 121 mod 47 = 27 = (Q)

The ciphertext of the plaintext of the word “9851069507” is SR0KJPAOJQ after performing Caesar cipher.

Now,

Performing the odd and even rule where if the output number is even or 0, three is added and if the output number is odd, three is subtracted and the actual value is extracted from the modified substitution table. Here, the plaintext for the process is the ciphertext from the above Caesar cipher process.

Table 19: Encryption using odd and even rule for test 5.

Plaintext	Value	Odd / Even	Final Value	Ciphertext
S	29	Odd	29 – 3 = 26	P
R	28	Even	28 + 3 = 31	U
O	25	Odd	25 + 3 = 28	R
K	21	Odd	21 – 3 = 18	H
J	20	Even	20 + 3 = 23	M
P	26	Even	26 + 3 = 29	S
A	29	Odd	29 - 3 = 26	P
O	25	Odd	25 - 3 = 22	L
J	20	Even	20 + 3 = 23	M
Q	27	Odd	27 – 3 = 24	N

The ciphertext for the plaintext SROKJPAOJQ is PURHMSPLMN

Then,

Performing the vigenere cipher with taking the plaintext as PURHMSPLMN which is the ciphertext after performing Caesar cipher and keyword as SROKJPAOJQ for the third step of the encryption process. The encryption process of the vigenere cipher is carried out as done in the Task 1.

Table 20: Encryption using vigenere cipher for test 4.

Plaintext	P	U	R	H	M	S	P	L	M	N
Keyword	S	R	O	K	J	P	A	O	J	Q
Ciphertext	;	B	&	2	6	;	0	!	6	%

;B&26;0!6% is the final encryption for the plaintext 9851069507 after performing encryption process of the new cryptographic algorithm.

For decryption:

Performing the vigenere cipher at first with taking the ciphertext as ;B&26;0!6% which is the final encryption output after performing the encryption process using new cryptographic algorithm and taking keyword as SROKJPAOJQ for the first step of the decryption process. The decryption process of the vigenere cipher is carried out as done in the Task 1.

Table 21: Decryption using vigenere cipher for test 4.

Ciphertext	;	B	&	2	6	;	0	!	6	%
Keyword	S	R	O	K	J	P	A	O	J	Q
Plaintext	P	U	R	H	M	S	P	L	M	N

By performing the vigenere cipher with ciphertext ;B&26;0!6% and keyword SROKJPAOJQ we get the plaintext PURHMSPLMN

Now,

Performing the odd and even rule where if the output number is even or 0, three is added and if the output number is odd, three is subtracted and the actual value is extracted from the modified substitution table. Here, the ciphertext for the process is the plaintext from the above Vigenere cipher process.

Table 22: Decryption using odd and even rule for test 4.

Ciphertext	**Value**	**Odd / Even**	**Final Value**	**Plaintext**
P	26	Even	26 + 3 = 29	S
U	31	Odd	31 - 3 = 28	R
R	28	Even	28 + 3 = 25	O
H	18	Even	18 + 3 = 21	K
M	23	Odd	23 - 3 = 20	J
S	29	Odd	29 - 3 = 26	P
P	26	Even	26 + 3 = 29	A

L	22	Even	22 + 3 = 25	O
M	23	Odd	23 - 3 = 20	J
N	24	Even	24 + 3 = 27	Q

The plaintext for the ciphertext PURHMSPLMN is SROKJPAOJQ

Then,

Performing Caesar cipher taking the ciphertext as SROKJPAOJQ and key as ‘77’. We have the modified formula for decryption as Dn = (C - K) mod 47, where ‘Dn’ stands for decryption and ‘C’ stands for the value of cipher text and substituting their value from the newly modified Substitution table for Caesar cipher.

- S = Dn = (C - K) mod 47 = (29 - 77) mod 47 = -48 mod 47 = 46 = (9)
- R = Dn = (C - K) mod 47 = (28 - 77) mod 47 = -49 mod 47 = 45 = (8)
- O = Dn = (C - K) mod 47 = (25 - 77) mod 47 = -52 mod 47 = 42 = (5)
- K = Dn = (C - K) mod 47 = (21 - 77) mod 47 = -56 mod 47 = 38 = (1)
- J = Dn = (C - K) mod 47 = (20 - 77) mod 47 = -57 mod 47 = 37 = (0)
- P = Dn = (C - K) mod 47 = (26 - 77) mod 47 = -51 mod 47 = 43 = (6)
- A = Dn = (C - K) mod 47 = (29 - 77) mod 47 = -48 mod 47 = 46 = (9)
- O = Dn = (C - K) mod 47 = (25 - 77) mod 47 = -52 mod 47 = 42 = (5)
- J = Dn = (C - K) mod 47 = (20 - 77) mod 47 = -57 mod 47 = 37 = (0)
- Q = Dn = (C - K) mod 47 = (27 - 77) mod 47 = -50 mod 47 = 44 = (7)

The final plain text of the ciphertext *:JK*CNBLKJKLS is “NP01NT4S210129” after performing Caesar cipher.

5. Evaluation

5.1 Strength and Weakness

The strength and weakness of this new cryptographic algorithm are explained below:

Strength

- The new algorithm utilizes three distinct steps for encryption and decryption, resulting in a high level of data security.
- It is impossible to break the ciphertext if one of the algorithm steps is missed.
- In order to obtain the key and plaintext for the vigenere cipher, the attacker must first perform the Caesar cipher as well as the odd and even rule, which they are unaware of.
- The addition of numbers and characters in addition to alphabets in the substitution table generates complex ciphertext that is difficult to understand to any individual.
- The algorithm is easy to understand and teach if explained properly.

Weakness

- The algorithm is quite lengthy so any individual need to perform each step carefully in order to encrypt and decrypt the message.
- The algorithm is unable to use lowercase alphabets and certain characters.
- The algorithm cannot separate space between the plaintext while performing encryption and decryption.
- If the attacker does not know the key while performing the Vigenere cipher, he or she can use the trial method and a small amount of computer resources to extract the key.

This new cryptographic algorithm can be used in a variety of applications, including keeping transaction records in banks, storing valuable passwords and messages of an individual for the protection of the message from being encrypted by an unknown user and even making it more difficult to encrypt as the three steo encryption method is used. This cryptosystem can be used by any organization to keep data and information secure. It is also applicable in information transmission, online transactions of any organization and e-commerce transactions.

6. Conclusion

Finally, the coursework provided us with the opportunity to learn more about cryptography and how it plays a significant role in the aspect of information security, including its types, history, and many other details. We studied and researched various Mobile Algorithms for this task. We discussed Cryptography, Caesar Cipher, Algorithm, and Flowchart in this report. The completion of this task improved our research and information-finding abilities.

References

Moch. Hari Purwidiantoro, D. F. K. S. W., 2018. *Super Encryption Concepts using Vigenere Cipher Modification to Produce Color Imaginary as Ciphertext,* Indonesia: International Conference on Recent Innovations.

Techopedia, 2011. *What is Flowchart? - Definition from Techopedia.* [Online]
Available at: https://www.techopedia.com/definition/5512/flowchart
[Accessed 12 December 2021].

Fruhlinger, J., 2020. *What is information security? Definition, principles, and jobs | CSO Online.* [Online]
Available at: https://www.csoonline.com/article/3513899/what-is-information-security-definition-principles-and-jobs.html
[Accessed 10 December 2021].

Comtact, 2019. *What is the CIA triad? - Comtact.* [Online]
Available at: https://comtact.co.uk/what-is-the-cia-triad/
[Accessed 10 December 2021].

GeeksforGeeks, 2020. *Cryptography and its Types - GeeksforGeeks.* [Online]
Available at: https://www.geeksforgeeks.org/cryptography-and-its-types/
[Accessed 10 December 2021].

Priyanka Bhatia, R. S., 2014. *Framework for Wireless Network Security using Wuantum Cryptography,* Dubai: BITS Pilani Dubai.

SSL2BUY, 2021. *Symmetric vs. Asymmetric Encryption - What are differences?.* [Online]
Available at: https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences
[Accessed 12 December 2021].

Binance Academy, 2019. *History of Cryptography | Binance Academy.* [Online]
Available at: https://academy.binance.com/en/articles/history-of-cryptography
[Accessed 10 December 2021].

KASADOO, 2021. *Hieroglyphics - KASADOO.* [Online]
Available at: https://kasadoo.com/egypt/cairo/mythology/hieroglyphics
[Accessed 11 December 2021].

Emory Oxford College, 2019. *Transposition Ciphers.* [Online]
Available at: http://mathcenter.oxford.emory.edu/site/math125/transpositionCiphers/
[Accessed 15 December 2021].
McDonald, N. G., 2009. *Past, Present and future methods of cryptography and data encryption,* Utah: University of Utah.

Britannica, 2021. *Zimmermann Telegram | Facts, Text, & Outcome | Britannica.* [Online]
Available at: https://www.britannica.com/event/Zimmermann-Telegram
[Accessed 16 December 2021].

Wikipedia, 2012. *Enigma machine - Wikipedia.* [Online]
Available at:
https://en.wikipedia.org/wiki/Enigma_machine#/media/File:Enigma_(crittografia)_-_Museo_scienza_e_tecnologia_Milano.jpg
[Accessed 16 December 2021].

Wikimedia Commons, 2020. *File:Purple code machine 1.jpg - Wikimedia Commons.* [Online]
Available at: https://commons.wikimedia.org/wiki/File:Purple_code_machine_1.jpg
[Accessed 17 December 2021].

Bibliography

Kashish Goyal, S. K., 2013. Modified Caesar Cipher for Better Security Enhancement. *International Journal of Computer Applications ,* 73(3), pp. 26-30.
Sidik, A. P., 2021. Improve the Security of the Vigenere Cypher Algorithm by Modifying the Encoding Table and Key. *International Journal of Basic and Applied Science,* 10(2), pp. 52-60.

Damico, T. M., 2009. A Brief History of Cryptography. *Inquiries Journal,* 1(11), p. 1.

Appendices

The base for this coursework to develop the new cryptographic algorithm named “Caenere Algorithm based upon odd and even rule” was referenced from the reference paper which can be obtained from the link below.

https://core.ac.uk/download/pdf/234644813.pdf