ABSTRACT:

The current study discusses several cryptography systems and explains how to utilize them. In today's era of online data, data protection is becoming a top responsibility. Data cryptography aids in the protection of data against attacks. Even though the attacker has the data, if they are unable to decrypt it, the information is meaningless to them. We may study well about evolution of encryption techniques and their application throughout human history. We may design our own data encryption by learning several types of cryptography systems. We can put the algorithm through a variety of tests. It lets us comprehend the algorithm's benefits and its flaws. We may make improvements by minimizing flaws. We can improve the security of our encryption technology by addressing the flaws.

Table of Contents

List of Figure:

List of Tables:

1. INTRODUCTION

From humanity's dark ages, information security has been a major concern. Countless historical facts had happened because of a low importance assigned on information security. Such occurrences have occurred across human history. Information is important in many facets of human existence. Similar data has since been moved from traditional to digital methods in the current day. And, with the rise of the Web, such digital files have become much more vulnerable. That since turn of the century, several cyberattacks have been carried out to retrieve such data. As a result, the security system for safeguarding our data has been given requirements. The security precautions must adhere to the CIA trinity.

Information security is more than just protecting data from unwanted access. The act of protecting the network, exploitation, exposure, interruption, alteration, examination, storage, or erasure is known as information security. There are two pieces of data: physical and electronic. Information may be anything from your personal information to your social networking profile, cellular telephone data, fingerprints, and so on. As a result, Infosec encompasses a wide range of academic topics, including cryptography, portable computing, digital investigations, and internet, among others (geeksforgeeks, 2021).

During WWI, the Multi-tier Classification System was created with the sensitive nature of data in mind. The official establishment of a Classification System began with the outbreak of The War. Alan Turing decoded the Enigma Code, that is being used by the Germans for encode military information (geeksforgeeks, 2021).

Confidentiality, Integrity, and Availability (CIA) are the three main goals of information security initiatives.

1.1 CIA TRAIDS:

The CIA TRAIDS, unlike most other core notions in data security, does not appear to get a specific defender or originator; instead, it has evolved quite a bit as just an element of knowledge between information security professionals. In a blog post, Ben Miller, a VP at security company Dragos, goes all the way back initial notices of a three factors of the triad; he believes the concept of confidentiality in computer scientific research was finalized in a 1976 US Air Force study, and indeed the general idea of dignity was set out in such a 1987 paper that acknowledged that marketing computer technology had unique requirements all over financial statements that needed a concentrate on information accuracy. The Morris worm, was among the first popular kinds of malware, took a substantial chunk of the newborn website down in 1988, sparking concerns about availability (Fruhlinger, 2020).

It is indeed unclear whenever the three conceptions started to just be considered as if they're a three-legged tripod. However, it appears to are now well developed as a core notion by 1998, as Donn Parker advocated expanding that to a sixelement structure dubbed the Parkerian Hexad in his booklet Fighting Computer Crime (Fruhlinger, 2020).

For even more over twenty years, the CIA triad has provided as a means for security analysts to understand over their project requires. Several have expanded just on notion and implemented their personal perceptions because it is something of cybersecurity legend but does not "conform" to anybody (Fruhlinger, 2020).

The CIA Triad is such a well and long-standing framework of developing security protocols that are being used to identify the issues and provide essential remedies in the field of cybersecurity (forcepoint, 2021).

CIA TRAID BREAK DOWN

- **Confidentiality**

Users must secure their delicate, personal data from unlawful access in today's day and age.

It is necessary to effectively to start enforcing levels of access for data in needed to shield confidentiality. In certain circumstances, this entails sorting data into different categories according on who topic to and how important material is - that is, the degree of harm that would be caused if the confidentiality were to be compromised.

Access controls, container and encryption algorithms, and Unix permission are among the most prevalent ways to address secrecy (forcepoint, 2021).

- **Integrity**

The "I" in CIA Triad stands for data integrity. This is an important aspect of the CIA Triad because it protects data against unauthorized deletion or alteration, and it assures that if an accepting information takes action that shouldn't be done, the destruction can also be undone (forcepoint, 2021).

- **Availability**

This is the third part of the CIA Triad, and it pertains to your data's real availability. Validity scales, entrances, and platforms must all function effectively to safeguard data and guarantee that it is able to be obtained (Fruhlinger, 2020).

Rising systems are cloud computing infrastructure with designs tailored to increase availability. This could target equipment failure, repairs, or severe storms to enhance availability, or it could control many networks access to reroute through different networking disruptions, depending on the exact HA system architecture (forcepoint, 2021).

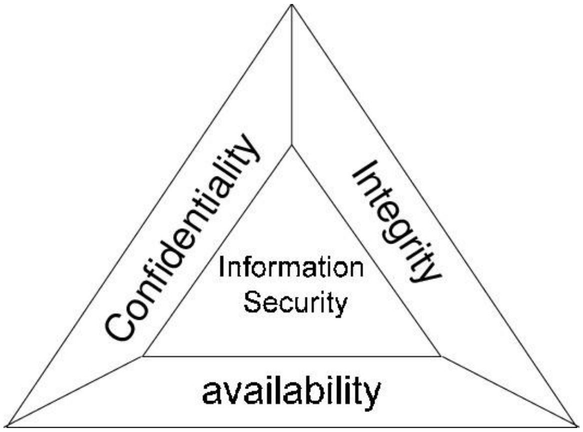

Figure 1 CIA Traids (Osei-Bryson, 2021)

1.2 AIMS AND OBJECTIVES:

The purpose of this paper is to help us comprehend the importance of cryptography as well as its structure. We study about the origins of cryptography, asymmetric -key encryption, and many current data encryptions. We may design a new program and check its strengths and weaknesses by identifying the different algorithms.

Its main objectives are:

- Understand the differences between symmetric and asymmetric encryption.
- Conduct research on several algorithms to develop a new algorithm.
- Describe how the newly constructed algorithm works.
- Run a series of tests on the newly generated algorithm.

2. INTRODUCTION TO CRYPTOGRAPHY

Cryptography is the analysis and use of strategies for strong encryption while third party candidates, known as adversaries, are present. It is important for the development and analysis of procedures that prohibit harmful third users from accessing communicate accordingly among 2 parties, therefore adhering to many elements of information security.

A circumstance in which a transmission or information formed between two individuals cannot be intercepted by an attacker is referred to as strong encryption. In cryptography, an attacker is a malevolent organization that seeks to obtain valuable data by compromising data protection standards (geeksforgeeks, cryptography introduction, 2020).

Modern cryptography's key concepts include data confidentiality, data integrity, authentication, and non-repudiation.

- ✞ Confidentiality relates to a set of guiding principles which are normally followed within confidentiality laws to guarantee that data is only shared with specific persons or even in specific areas.
- ✞ Data integrity relates to the procedure of preserving and ensuring that information is available and reliable throughout its lifetime.
- ✞ Authentication is the procedure of verifying that the information becoming asserted by client is theirs.
- ✞ Non-repudiation describes the capacity to ensure that the client or party contractual obligation or communications never dispute the legitimacy of their signatures on a paper or the transmission of a signal (geeksforgeeks, cryptography introduction, 2020).

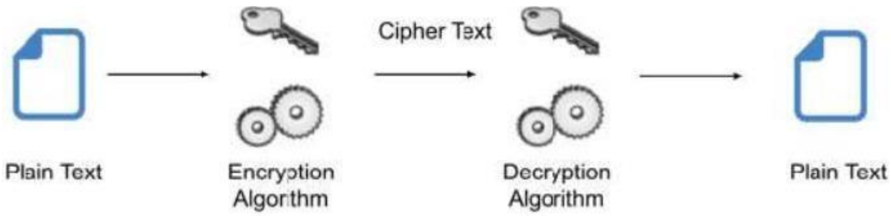

Figure 2 Basic Cryptography (Alassafi, 2022)

2.1 Types of cryptography

2.1.1 Symmetric key encryption

Symmetric encryption is the method of encryption in which digital data is encrypted and decrypted just using single variable (a secret key). The secret should be exchanged between the organizations interacting using encryption algorithm so that it will be utilized inside the decoding process. This encryption method varies from asymmetric encryption, which encrypts and decrypts communications using two different keys, one accessible including one confidential.

Data is changed to a comprehensible form by anybody who might not have the security code to decode it by utilizing symmetric encryption methods. As once information has been sent to the receiver who makes a significant contribution, the algorithms repeat its operations, returning the information to its previous and comprehensible state. The private key used both by transmitter and the recipient might be a particular passphrase or a randomized sequence containing random letters created using a secured random word generator (RNG). The shared key must be generated using a RNG that's also verified thus according to standards, such as FIPS 140-2, for financial services encrypting (cryptomathic, 2022).

The following are some examples of symmetric key encryption:

- AES (Advanced Encryption Standard)
- DES (Data Encryption Standard)
- IDEA (International Data Encryption Algorithm)
- Blowfish (Drop-in replacement for DES or IDEA)
- RC4 (Rivest Cipher 4)
- RC5 (Rivest Cipher 5)
- RC6 (Rivest Cipher 6) (cryptomathic, 2022).

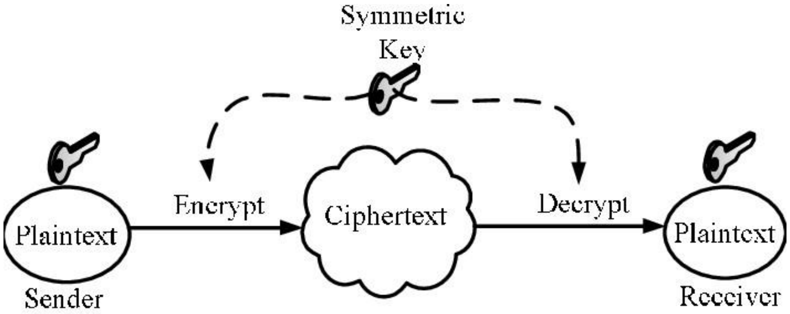

Figure 3 Symmetric key encryption (Javed, 2022)

2.1.2 Asymmetric key encryption

Encryption is the process of transforming information into a cryptographic structure with the use of a secret. Data that has been encoded can indeed be securely transmitted with everyone. If somehow the algorithm/key used is powerful and well applied, breaking the cipher style will indeed be challenging. Applying the key for encryption the information, the recipient decrypts it to its initial form (Sathyanarayanan, 2022).

In symmetric encryption, the encrypting information and password are transmitted to the recipient for consuming after decoding, using the process described previously. The accessibility of various individuals and the trustworthy exchange of a password are also challenges in just this approach (Sathyanarayanan, 2022).

With a shared key: a public key and a private key, asymmetric encryption effectively overcomes those issues. Whereas the information is protected utilizing recipient's key pair at the user's endpoint, the material is decoded by the recipient utilizing his secret key. Even though public password is released publicly, the owner retains the secret key, which is required to decode any information (Sathyanarayanan, 2022).

Some examples of asymmetric key encryption are:

- Diffie_Hellman key exchange Protocol
- DSS (Digital Signature Standard)
- ElGamal
- Elliptic-curve cryptography
- Paillier cryptosytem

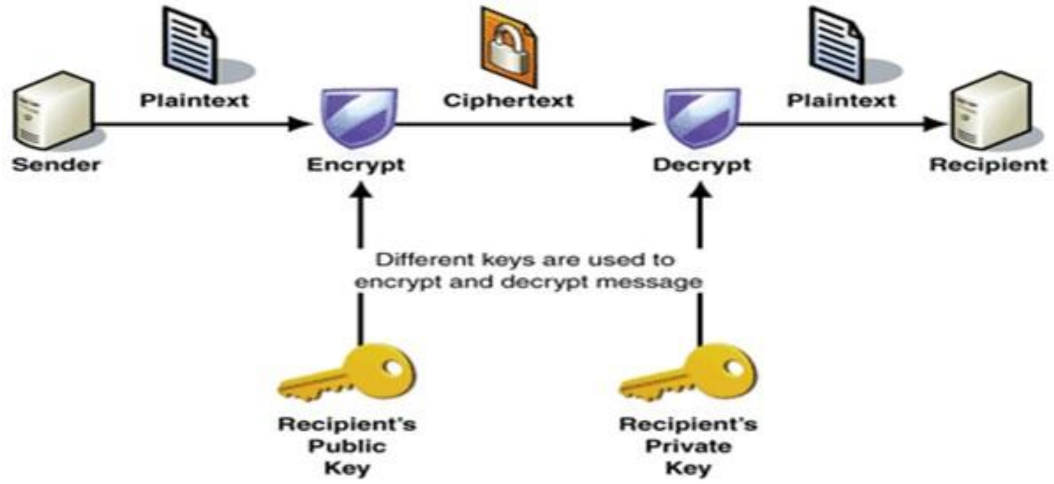

Figure 4 Asymmetric key encryption (Gaba, 2022)

2.2 History Of Cryptography

YEAR	EVENT

1900 BCE	Monumental Hieroglyphs of Old kingdom of Egypt found in walls of pyramid.
1500 BCE	Mesopotamian Hieroglyphs found in tablets made using pottery glaze.
800	Al-Kindi, "The Philosopher of the Arabs" was able to translate many Greek writings into Arabic, also known as first code breaking.
1467	Leon Battista Alberti, “Father of Western Cryptography” was the inventor of the Cipher Wheel for fast and simple encryption and decryption.
1586	Anthony Babington planned a coup by writing letters and encrypting using a chipper to bring England back to Catholicism.
1853	During the Crimean war, Charles Babbage created a machine to break Vigenere's Auto key Cipher used by enemies at that time.
1917	Gilbert Vernam invented the teleprinter cipher also known as Vernam Cipher which was world’s first unbreakable chipper. It used key on paper tape to encrypt phrases.
1923	German scientist Arthur Scherbius created a cipher machine, Enigma rotor machine during world war II.
1940	Edgar Allen Poe decrypted many encrypted messages from Germany to aid Britain during world war.
1942	During world war II, Japanese navy cryptography was encrypted by Americans to turn tide against them.
1943	Max Newman and Tommy Flowers created world’s first digital electronic computer which was used for Britain’s cryptanalysis during world war II.

1953	Soviet spy Reino Häyhänen used VIC cipher to relay message to undercover Russian spy which was later discovered by FBI.
1975	Data Encryption Standard (DES) was published by National Institute of Standards and Technology (NIST).
1976	Diffie-Hellman key exchange known as exponential key exchange created a cipher that would be mathematically overwhelming for code breaker.
1991	Phil Zimmermann created PGP (Pretty Good Privacy), a cryptography system that can authenticate message with digital signature.
2001	Advanced Encryption Standards (AES) was created by using encryption algorithm by two Belgian Cryptographers Joan Daemen and Vincent Rijmen which increased the block size of key lengths.

Table 1 History of cryptography (cbaron12, 2007)

3. SUBSTITUION CIPHER

Encryption is the process of concealing material. If ordinary text is encoded, it'll become ciphertext, which is inaccessible. A substitution cipher replaces any simple text sign from such a fixed input cast of characters with another sign out of the same set based on a key. With a shift of one, for example, A would be substituted by B, B by C, and so on.

The encryption may be expressed using mathematical operations by converting the letters to integers using the A = 0, B = 1,..., Z = 25 approach. The mathematical formula for encrypting a letter with a shift n is (geeksforgeeks, substitution cipher, 2021).

$E_n(x) = (x+n) \bmod 26$

$D_n(x) = (x-n) \bmod 26$

As an example to encrypt ATTACK using key 5 we get:

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

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
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

Table 2 Substitution cipher

ATTACK encrypts plain text into FYYFHP using the table above.

For decryption, the characters in plain text have been relocated 5 times to the right of their initial location. The letters have been shifted 5 times to the left to decipher the encrypted text.

The cipher string FYYFHP decrypts to ATTACK using the table above.

3.1 ADVANTAGES AND DISADVANTAGES:

It has the following advantages:

- It is simple.
- It takes less time.
- The key is simple to remember.
- Prevents data from being intercepted.
- Text can be modified by using different key ciphers.

It has the following drawbacks:

- It is simple to decrypt if the key is known.
- It can still be deciphered using the hit-and-try approach.
- Letter frequency stays unchanged.
- No symbols or letter cases are utilized.

4. TRANSPOSITION CIPHER

The arrangement of alphabets in plaintext is changed to generate a cipher text in a cryptographic procedure known as a Transposition cipher. The alphabets of plain text are not included in this procedure (tutorialspoint.com, 2022).

Columnar transposition cipher is a basic example of a transposition cipher, in which each letter in plain text is printed horizontally with a predetermined alphabet width. The encryption then typed vertically, resulting in a completely new cipher text.

Let's take the basic text hello world and use the columnar transposition approach as shown below.

h	e	l	l
o	w	o	r
l	d		

Table 3 Transposition cipher

The plain text letters are arranged horizontally, whereas the cipher text is formatted vertically, as follows: holewdlo lr. The recipient must now decide the encryption text to plain text using the same table (tutorialspoint.com, 2022).

4.1 ADVANTAGES AND DISADVANTAGES:

It has the following advantages:

- It is simple to comprehend.
- It takes less time.
- Encryption of long sentences and phrases is possible.
- Text may be varied by using different key ciphers.

Its drawbacks are as follows:

- If the key is known, decryption is simple.
- Letter frequency remains constant.
- If the key is unknown, it can be decrypted using the hit-and-miss approach.
- No symbols or letter cases are utilized.

5. Development of new cipher

According to the paper, a novel encryption algorithm was developed based on substitution and transposition ciphers. Subtransposition cipher is the name of the newly developed encryption. The same key is used for plain text substitution and transposition encryption in this cipher. The substitution cipher uses the number of letters in the key, whereas the transposition cipher uses the letters themselves.

ASCII (American Standard Code for Information Interchange) characters ranging from 32 to 126 are employed to make this encryption more secure than its underlying source. All of the numbers, alphabets, and symbols that are utilized to construct information are employed in this way. If the letters pass the ASCII value of 126 during the substitution phase of the sub-transposition cipher, they return to 32, and if the ASCII value is below 32 during decryption of the text, the loop returns to 126. The number of characters in the phrase determines the replacement key.

After that, a table is produced in the same way as in transposition cipher, with plain text in the rows and encrypted text extracted from the column. The ASCII value of the key word character determines column position. If two characters appear in a row, the later is given the higher place. Then there are blank spaces between the letters of the encrypted text, which ends with a complete stop.

5.1 Working steps for encryption:

- Step 1: Choose simple text and a key phrase.
- Step 2: Substituting the number of characters from the key word.
- Step 3: Create a table for ASCII value replacement.
- Step 4: Adding a key number to the ASCII value converts plain text characters to encryption text.
- Step 5: Using letters from the key word, create a table for transposition. ✞ Step 6: Filling rows in the table with characters following substitution.
- Step 7: Uneven characters might cause an irregular table, with the number of columns in the last row not matching the other rows.
- Step 7: Assigning column position with ACII value in ascending order.
- Step 8: From the smallest to the largest ASCII value column, write encrypted text.
- Step 9: Going to assign random spaces to the cipher text, ranging from 2 to 6 letters and terminating with a full stop, to the cipher text.
- Step 10: If the ASCII value 32 (blank space) is used, a second blank space is appended after it.
- Step 11: Get the cipher text.

5.2 Working steps for encryption

- Step 1: Decide on the cipher text and the key word.
- Step 2: Counting how many characters are in the key word.
- Step 3: Remove any blank spaces and terminate the encrypted text with a full stop.
- Step 4: If two vacant spots are next to each other, just one gets eliminated.
- Step 5: In encrypted text, the total number of characters is tallied.
- Step 6: The cipher text number is divided by the key word number.
- Step 7: Create a table with the quotient indicating the number of rows and the remainder indicating the number of columns in the final row from the left side below the quotient-created row. (It's possible that the table is uneven.)
- Step 8: The column is given a position based on the ASCII value of the key word letters.
- Step 9: Fill the appropriate column of the table with cipher text characters.
- Step 10: From the rows, characters are retrieved.
- Step 11: Subtracting the ASCII value from the resulting text, key word number replacement is conducted.
- Step 12: Obtain plain text.

The table for the transposition phase may change depending on the key word, while the table for the replacement phase remains the same. Character placement varies per key word, but we get the same table for characters with ASCII values ranging from 32 to 126, as shown below:

ASCII value	Character	ASCII value	Character	ASCII value	Character
32		64	@	96	`
33	!	65	A	97	a
34	“	66	B	98	b
35	#	67	C	99	c
36	$	68	D	100	d

37	%	69	E	101	e
38	&	70	F	102	f
39	‘	71	G	103	g
40	(	72	H	104	h
41	)	73	I	105	i
42	*	74	J	106	j
43	+	75	K	107	k
44	,	76	L	108	l
45	-	77	M	109	m
46	.	78	N	110	n
47	/	79	O	111	o
48	0	80	P	112	p
49	1	81	Q	113	q
50	2	82	R	114	r
51	3	83	S	115	s
52	4	84	T	116	t
53	5	85	U	117	u
54	6	86	V	118	v
55	7	87	W	119	w
56	8	88	X	120	x
57	9	89	Y	121	y
58	:	90	Z	122	z

59	;	91	[	123	{
60	<	92	\	124	|
61	=	93	]	125	}
62	>	94	^	126	~
63	?	95	_		

Table 4 ASCII Value for Characters used in Substitution Phase

The new cipher is demonstrated in the testing below, where test 1 provides an in-depth description of the above working stages.

6. TESTING:

'Table 4 is utilized as a reference throughout the replacement phase of testing.'

6.1 Test 1:

Plain Text: Simon says, “Come here @ 4p.m”

Key Word: T!meZone

Plain text number (N) = 30

Key word number (n) = 8 Substitution

phase.

ASCII value of all characters.

= 83 105 109 111 110 32 115 97 121 115 44 32 34 67 111 109 101 32 104 101 114 101 32 64 32 52 112 46 109 34

Adding n to ASCII value of all characters.

= 91 113 117 119 118 40 123 105 (129 = 34) 123 52 40 42 75 119 107 109 40 112 109 122 109 40 72 40 60 120 54 107 42

Because 126 is the top limit and counting begins at 32, 129 is altered to 34.

Using table 4;

Resulting text = [quwv({i”{4(*Kwkm(pmzm(H(<x6k*

Transposition phase;

Now, a table is built using the characters from the key word, and column position is set. Characters from the generated text are utilized to fill the table's rows.

2	1	6	4	3	8	7	5
T	!	m	e	Z	o	n	e
[	q	u	w	v	(	{	i
“	{	4	(	*	K	w	k
m	(	p	m	z	m	(	H
(	<	x	6	k	*		

Table 5 Transposition table for Test 1

Characters are selected from the table from the column with the lowest position to the column with the highest position.

Resulting Text = !q{(<T[“m(Zv*zkew(m6eikHmu4pxn{w(o(Km*

After that, random spaces ranging from 2 to 6 characters are added to the text, finishing with a full stop (.). There are no multiple blank spaces in the final text since there is no blank space. If there was a () character, a blank space is placed to the right of it.

Final encrypted text = !q {(<T [“m(Zv *zke w(m6ei kHm u4pxn {w(o(Km*.

All blank spaces and the full stop at the conclusion of the encrypted text are eliminated for decryption. The number of key words (n) and plain text (N) is counted.

Cipher text = !q {(<T [“m(Zv *zke w(m6ei kHm u4pxn {w(o(Km*. Cipher

text after removing blank spaces and full stop;

!q{(<T[“m(Zv*zkew(m6eikHmu4pxn{w(o(Km*

Calculating rows and column of table;

N / n = 30 / 8

The quotient is 3 and the remainder is 6. As a result, our table has three full rows and six additional columns in the fourth row. The table's column is assigned using the characters from the key word position. The cipher text characters are then utilized to fill each column of the table from top to bottom. As a result, we get the same table as table 5.

From top to bottom, characters are taken from the table's rows.

The following is the result: [quwv(i"4(*Kwkm(pmzm(H(x6k*)]

Substitution Phase

Plain text is obtained by subtracting n from each character's ASCII value. If the ASCII value returned is not within the range of 32-126, the loop is repeated to maintain the result inside the range.

By using table 4;

Plain text = Simon says, “Come here @ 4p.m”

6.2 Test 2:

Plain Text: Please! HeLp me today!!

Key Word: WOrkLoad

Plain Text Number (N) = 23

Key word Number (n) = 8 Substitution phase, n is added to

ASCII value of each character of plain text.

Using table 4;

Before addition

80 108 101 97 115 101 33 32 72 101 76 112 32 109 101 32 116 111 100 97 121 33 33

After addition of n,

88 116 109 105 123 109 41 40 80 109 84 120 40 107 109 40 124 118 108 105 (129 = 34) 41 41

Resulting text = Xtmi{m)(PmTx(km(|vli”))

Transposition phase;

Table is created using key word.

3	2	8	6	1	7	4	5
W	O	r	k	L	o	a	d
X	t	m	i	{	m	)	(

P	m	T	x	(	k	m	(
|	v	l	i	“	)	)	

Table 6 Transposition table for Test 2

Resulting text = L{(“OtmvWXP|a)m)d((kixiomk)rmTl

Cipher text = L{(“Otm vWXP |a)m) d((k ixi omk) rmTl.

For decryption;

Cipher text after removing blank space and full stop;

L{(“OtmvWXP|a)m)d((kixiomk)rmTl

N/n = 23/ 8

Quotient = 2 and remainder 7

A fraction and remaining table is generated, in which letters from the cipher text fill the column in accordance with the column's location owing to the key word. Following that, we get the same table as table 6.

The letters are then selected from the rows.

Before the swap, the following is the resultant text: Xtmi{m)(PmTx(km(|vli”))

After multiplying by 8, the following is the resultant text: "Come here at 4 p.m.," Simon adds.

6.3 Test 3:

Plain Text: Can’t UnderstanD symbols =(

Key Word: (*+})

Plain text number (N) = 27

Key word number (n) = 5

ASCII value of plain text before substitution;

67 97 110 39 116 32 85 110 100 101 114 115 116 97 110 68 32 115 121 109 98 111 108 115 32 61 40

ASCII value of plain text after substitution by n;

72 102 115 44 121 37 90 115 105 106 119 120 121 102 115 73 37 120 126 114 103 116 113 120 37 66 45

Resulting text: Hfs,y%ZsijwxyfsI%x~rgtqx%B- Creating table
for transposition using key word;

1	3	4	5	2
(	*	+	}	)
H	f	s	,	y
%	Z	s	i	j
w	x	y	f	s
I	%	x	~	r
g	t	q	x	%
B	-			

Table 7 Transposition Table for Test 3

Resulting text: H%wIgByjsr%fZx%t-ssyxq,if~x

Cipher text: H% wIgB yjsr% fzx %t-ss yxq, if~x.

Decryption;

Cipher text after removing blank space and full stop;

H%wIgByjsr%fZx%t-ssyxq,if~x

N/n = 27/5

Quotient = 5 and remainder 2

A fraction and remaining table are generated, in which letters from the cipher text fill the column in accordance with the column's location owing to the key word. Following that, we get the same table as table 7.

Then, letters are taken from the rows;

Resulting text before substitution: Hfs,y%ZsijwxyfsI%x~rgtqx%B-

Resulting text after substitution by 5: Can't UnderstanD symbols =(

6.4 Test 4:

Plain Text: GoOd Morning. Please; come down for Breakfast. Right Now!

Key Word: #Lol ;)

Plain text number (N) = 57

Key word number (n) = 7

ASCII value of plain text before substitution;

71 111 79 100 32 77 111 114 110 105 110 103 46 32 80 108 101 97 115 101 59 32 99 111 109 101 32 100 111 119 110 32 102 111 114 32 66 114 101 97 107 102 97 115 116 46 32 82 105 103 104 116 32 78 111 119 33

ASCII value of plain text after substitution by n;

78 118 86 107 39 84 118 121 117 112 117 110 53 39 87 115 108 104 122 108 66 39 106 119 116 108 39 107 118 126 117 39 109 119 121 39 73 121 108 104 114 109 104 122 123 53 39 89 112 110 111 123 39 85 118 126 40

Resulting text: NvVk'Tvyupun5'WslhzlB'jwtl'kv~u'mwy'Iylhrmhz{5'Ypno{'Uv~(Creating table for transposition using key word;

2	5	7	6	1	4	3
#	L	o	l		;	)
N	v	V	k	‘	T	v
y	u	p	u	n	5	‘
W	s	l	h	z	l	B
‘	j	w	t	l	‘	k
v	~	u	‘	m	w	y
‘	l	y	l	h	r	m
h	z	{	5	‘	Y	p
n	o	{	‘	U	v	~
(						

Table 8 Transposition table for Text 4

Resulting text: ‘nzlmh’UNyW’v’hn(v’Bkymp~T5l’wrYvvusj~lzokuht’l5’Vplwuy{{

Cipher text: ‘nz lm h’UNy W’v’ hn(v’B kym p~T 5l’w rYvv usj~ lz okuht ’l5’V pl wuy{{.

Decryption;

Cipher text after removing blank space and full stop;

‘nzlmh’UNyW’v’hn(v’Bkymp~T5l’wrYvvusj~lzokuht’l5’Vplwuy{{

N/n = 57/7

Quotient = 8 and remainder 1

A fraction and remaining table is generated, in which letters from the cipher text fill the column in accordance with the column's location owing to the key word. Following that, we get the same table as table 8. Then, letters are taken from the rows;

Resulting text before substitution:

NvVk'Tvyupun5'WslhzlB'jwtl'kv~u'mwy'Iylhrmhz{5'Ypno{'Uv~(

Resulting text after substitution by 5: GoOd Morning. Please; come down for Breakfast. Right Now!

6.5 Test 5:

Plain Text: What is 587 * 468? I’m confused :|

Key Word: (<.>|<.>)

Plain Text number (N) = 34

Key word number (n) = 9

ASCII value of plain text before substitution;

87 104 97 116 32 105 115 32 53 56 55 32 42 32 52 54 56 63 32 73 39 109 32 99 111 110 102 117 115 101 100 32 58 124

ASCII value of plain text after substitution by n;

96 113 106 125 41 114 124 41 62 65 64 41 51 41 61 63 65 72 41 82 48 118 41 108 120 119 111 126 124 110 109 41 67 (133=38)

Resulting text: `qj})r|)>A@)3)=?AH)R0v)lxwo~|nm)C&

Creating table for transposition using key word;

1	5	3	7	9	6	4	8	2
(	<	.	>	|	<	.	>	)
`	q	j	}	)	r	|	)	>
A	@	)	3	)	=	?	A	H
)	R	0	v	)	I	x	w	o
~	|	n	m	)	C	&		

Table 9 Transposition Table for Test 5

Resulting text: `A)~q@R|j)0n}3vm))))r=IC|?x&)Aw>Ho

Cipher text: `A)~q@ R|j)0 n}3 vm))))r =IC| ?x&)A w>Ho.

Decryption;

Cipher text after removing blank space and full stop;

`A)~q@R|j)0n}3vm))))r=IC|?x&)Aw>Ho

N/n = 34/9

Quotient = 3 and remainder 7

A fraction and remaining table is generated, in which letters from the cipher text fill the column in accordance with the column's location owing to the key word. Following that, we get the same table as table 9.

Then, letters are taken from the rows;

Resulting text before substitution: `qj})r|)>A@)3)=?AH)R0v)lxwo~|nm)C&

Resulting text after substitution by 5: What is 587 * 468? I’m confused :|

7. EVALUTION OF NEW CHIPER:

Sub-transposition cipher, a newly designed encryption, outperforms substitution cipher and transposition cipher. However, it has its own set of benefits:

7.1 Advantages:

- It outperforms its predecessor in terms of strength, security, and ease of use.
- A program might be written to follow this cipher.
- Encryption is possible for long sentences.
- Various key words can be utilized.
- Changes in plain text and encrypted text frequency.
- There are also numbers and symbols.

7.2 Disadvantages:

- Encryption by manually takes longer.
- The chances of mistake are higher.
- If a key word is revealed, the encryption text may be decoded quickly.
- Processing big phrases or paragraphs may use a lot of CPU.
- This is still not the greatest encryption technique available.

This new chipper can be utilized in small businesses where significant amounts of data are not sent. It is possible to encrypt a basic message and a little image by utilizing the RGB of each pixel. However, it can put a lot of strain on the CPU, which may make encryption by hand impossible. Because it is a basic encryption, it is straightforward to develop a program using this technique.

It still has flaws, but those flaws can be addressed. This cipher may be made more secure by employing the RSA technique in between the substitution and transposition phases, where the public key can be a prime number less than the key word number and the private key can be a prime number bigger than the key word. As a result, even if the key word is released, the encryption cannot be easily decoded thanks to the RSA technique.

8. CONCLUSION:

We can see the importance of data encryption from this study. Security is essential in the digital era, when large amounts of data are stored digitally and exchanged via a network. Encryption also serves as an additional layer of data security. We recognize the importance of cryptanalysis throughout human history, and its effect may still be seen now. It's crucial to understand cipher and learn about encryption and decoding. We learn from this research that the greatest cipher isn't the one that's unbreakable, but one that can process quickly for both encryption and decryption and is difficult to crack.

References

Alassafi, M. O. (2022). *Basic-Cryptography-Process_fig2_309321387*. Retrieved from reserchgate.net: https://www.researchgate.net/figure/Basic-CryptographyProcess_fig2_309321387 cbaron12. (2007). *The history of cryptography*. Retrieved from timetoast.com: https://www.timetoast.com/timelines/the-history-of-cryptography

cryptomathic. (2022). *Symmetric Key Encryption - why, where and how it's used in banking*. Retrieved from cryptomathic.com: https://www.cryptomathic.com/newsevents/blog/symmetric-key-encryption-why-where-and-how-its-used-in-banking

forcepoint. (2021). *cia traids*. Retrieved from forcepoint.com: https://www.forcepoint.com/cyber-edu/cia-triad

Fruhlinger, J. (2020, 02 10). *The CIA triad: Definition, components and examples*. Retrieved from csoonline.com: https://www.csoonline.com/article/3519908/thecia-triad-definition-components-and-examples.html

Gaba, G. S. (2022). *Asymmetric-key-cryptography_fig17_305323730*. Retrieved from researchgate.net: https://www.researchgate.net/figure/Asymmetric-keycryptography_fig17_305323730

geeksforgeeks. (2020). *cryptography introduction*. Retrieved from geeksforgeeks.com: https://www.geeksforgeeks.org/cryptography-introduction/

geeksforgeeks. (2021). *substitution cipher*. Retrieved from geeksforgeeks.org: https://www.geeksforgeeks.org/substitution-cipher/

geeksforgeeks. (2021). *what is information security*. Retrieved from geeksforgeeks.org: https://www.geeksforgeeks.org/what-is-information-security/

Javed, M. Y. (2022). *symmetric key encryption*. Retrieved from https://www.researchgate.net/figure/Symmetric-Key-Encryption_fig2_4365726

Osei-Bryson, K.-M. (2021). *reserchgate.net*. Retrieved from Information-SecurityProperties-CIA-Triad_figure: https://www.researchgate.net/figure/InformationSecurity-Properties-CIA-Triad_fig1_220121692

Sathyanarayanan, A. (2022). *asymmetric encryption*. Retrieved from educba.com: https://www.educba.com/asymmetric-encryption/

tutorialspoint.com. (2022). *tutorialspoint.com*. Retrieved from cryptography_with_python/cryptography_with_python_transposition_cipher.htm: https://www.tutorialspoint.com/cryptography_with_python/cryptography_with_python_transposition_cipher.htm