LONDON METROPOLITAN UNIVERSITY

Islington college
(इस्लिङ्टन कलेज)

Module Code & Module Title

CC5004NI Security in Computing

Assessment Weightage & Type

30% Individual Coursework

Year and Semester

2023 -24 Autumn

Student Name: Mohammad Nurullah

London Met ID: 22067059

College ID: NP01NT4A220019

Assignment Due Date: Monday, 15th January 2023

Assignment Submission Date: Monday, 15th January 2023

Word Count (Where Required):

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

I would like to express my sincere gratitude to my teacher, **Mr. Avinav Neupane**, for his insightful advice, steadfast support, and helpful criticism during the course of this coursework. His knowledge and support were crucial when assessing how this project was finished.

I would like to express my gratitude to the professors and staff of London Metropolitan University's Departments of **Security in Computing** for creating an inviting atmosphere for learning and offering essential tools that deepened my understanding of the subject.

I would especially like to thank my friends and learners for their working together, knowledge sharing, and kindness. Your combined efforts made a substantial contribution to this project's success.

I owe my family a lot of gratitude for their unwavering support, understanding, and confidence in me. Their unfailing assistance has served as a source of encouragement and inspiration.

Finally, I would like to express my gratitude for the advice and insight that my seniors provided. Their experiences provided insightful viewpoints that helped shape the planning and implementation of this project.

This project would not have been possible without the support and contributions of these individuals, and for that, I am truly thankful.

ABSTRACT

The goal of cryptography is to transform messages into secret codes that only the intended recipient can understand. It is a vital technology for securing distributed systems. As the internet usage increases rapidly, it becomes more important than ever to safeguard user's data and infrastructures. However, many existing cryptography algorithms neglect some crucial aspects. One of them is how to connect each character in the plaintext with the one before it. This paper introduces a new cryptography algorithm that takes into account this connection during encryption and decryption. The algorithm can deal with various scenarios in cryptography applications. The simulations demonstrate the algorithm's effectiveness.

Table of Contents

Table of Figures

1. INTRODUCTION

Sending confidential information across the internet or other networks carries some risk. Your information could be attempted to be stolen, altered, stopped, or seen by someone without your consent. It is therefore necessary to provide your information as a code that only those who you desire can decipher. We call this encryption. The opposite action is required to convert the code back into regular information. Decryption is the term for this. Protecting your confidential data from intrusions is the primary objective of information security (KAHN, 1972).

Electronic protection is becoming more and more crucial as digital communications proliferate. Many algorithms are designed to offer customers of communications technologies safety (Sadowsky, 2003). Everyone with a hobby in protection continues attempting to broaden new techniques and algorithms to provide the most stage of safety. Additionally, users' information of facts safety troubles desires to be multiplied. Cryptography is the maximum broadly used technique of facts protection (Sharma, 2021). The science of remodelling information into a selected format such that only the intended recipient and no different unauthorized events can get entry to its miles called cryptography.

The technology of sending a message to make it stable and impenetrable to attacks is known as cryptography. A cipher is a technology that uses encryption to transform a simple text communication into an unintelligible text (cipher text), and then decoding allows the original, unquestionable text content to be retrieved. The process of encrypting a communication involves using complicated mathematical elements and an algorithm to render it unintelligible without the decryption key. On the sender website, the message should be encrypted, and on the recipient website, it should be decrypted (Forouzan, 2008).

Cryptography has an extended and captivating history. The earliest form of cryptography was involved with changing messages into unreadable businesses of figures to defend the message’s content (Forouzan, 2008). Recently, cryptography has grown to

encompass a few levels of message integrity checking, identification authentication, virtual signatures, among different matters (Y. Priyanka, 2008) (Gligor, 2002). Cryptography may be seen in many programs consisting of ATM playing cards, pc passwords, and digital trade.

Despite the numerous efforts documented in the literature on cryptography, the field remains challenging due to technological advancements that facilitate hackers and attackers in achieving their goals of data theft and hacking. Symmetric and asymmetric cryptography are the two main categories of cryptography (Michel Abdalla, 2001) (Shaligram Prajapat, 2013), (Kouch, 2015). The fundamental flaw with symmetric cryptography, which is the central issue of this work, is the use of the same secret key for both encryption and decryption. This work presents a novel symmetric cryptography technique that increases the level of security by varying the encryption and decryption of text characters based on their location.

The relaxation of this document is made as follows. The background history of cryptography is compiled in Section 2. Section 3 introduces the essential work. The details of the suggested algorithm are provided in Section 4. In the fifth segment, a few tests of encryption and decryption are provided. Section 6 concludes with a summary of the conclusions.

2. BACKGROUND HISTORY OF CRYPTOGRAPHY

A. Ancient Spartan cryptography

In the 6th century around Circa 600 BC, Greek created a simple clever method for encryption (Okamoto, 1999). They were the use of a stick with a particular diameter referred to as "scytale" with the aid of wrapping it with a protracted thin piece of paper and writing the message on the thin paper in a horizontal line. After that they were sending the paper to the supposed receiver who uses the same “scytale” to examine the message

https://www.thalesgroup.com/en/markets/digital-identity-and-security/magazine/brief-history-encryption (A BRIEF HISTORY OF ENCRYPTION (AND CRYPTOGRAPHY), 2023).

Al Kindi is the first who wrote approximately it in the ninth century whilst messages were despatched by means of homing pigeon. He discovered a famous approach of encryption –by means of reading and analysing Holy Qur'an- that depends on repetition precept. For example, in English language, the letter "e" is extra repeated by thirteen% than different letters this means that that any symbol encrypts "e" may be repeated greater via thirteen% than different encryption symbols (Shiddiky, 2005).

B. Roman encryption and cyphers

Circa 60 BC Julius Caesar invents a cypher that shifts characters with the aid of 3 locations inside the alphabet: A becomes D, B turns into E, etc. A simple and powerful encoding approach at that time.

Surprisingly, inside the **2000s,** Bernardo Provenzano, the Sicilian Mafia boss, nevertheless used a variant of the Caesar cipher to speak through Pizzini, coded messages written on tiny portions of paper (A BRIEF HISTORY OF ENCRYPTION (AND CRYPTOGRAPHY), 2023).

1553: Giovan Battista Bellaso envisions the first cypher to apply a proper encryption key - an agreed-upon key-word the recipient must know to decode the message.

1854: Charles Wheatstone invents the Playfair Cipher, which encrypts pairs of letters rather than unmarried ones and is, consequently, more difficult to crack.

C. Hebern rotor machine

1917: An American, Edward Hebern, invented the electro-mechanical device in which the secret is embedded in a rotating disc. It's the first instance of a rotor device. It encodes a substitution table this is modified on every occasion a new character is typed.

1918: German engineer Arthur Scherbius invented the Enigma device (pictured) for business use. It uses numerous in preference to the one rotor used by Hebern's tool. Recognizing its genius, the German navy began to use it to ship coded transmissions (A BRIEF HISTORY OF ENCRYPTION (AND CRYPTOGRAPHY), 2023).

D. WW2 cryptography

1932: Polish cryptographer Marian Rejewski observed how Enigma worked. In 1939, Poland shared this statistic with French and British intelligence, allowing cryptographers like Alan Turing to figure out how to crack the key, which was modified day by day (A BRIEF HISTORY OF ENCRYPTION (AND CRYPTOGRAPHY), 2023).

It proved essential to the Allied victory in World War II.

Another huge yet often overlooked contribution came from Hedy Lamarr, renowned actress and inventor.

During the battle, Lamarr co-invented the era of the evolving spectrum with frequency hopping, which was supposed to save you from jamming allied torpedoes to begin with. Although it is now not immediately used in cryptography during conflict, its invention laid the foundation for future stable wireless communication that includes Wi-Fi and Bluetooth, representing a great leap in era and encryption strategies (A BRIEF HISTORY OF ENCRYPTION (AND CRYPTOGRAPHY), 2023).

1945: : Claude E. Shannon of Bell Labs posted an editorial called "A Mathematical Theory of Cryptography." It's the place to begin of cutting-edge cryptography.

For centuries, governments have managed mystery codes: applied to international relations, hired in wars, and used in espionage.

But with contemporary technologies, using codes by means of individuals has exploded.

E. Modern cryptography (computer-based encryption)

In the early Nineteen Seventies: IBM fashioned a 'crypto institution,' which designed a block cypher to protect its clients' statistics. In **1973**, the United States followed it as a countrywide general - the Data Encryption Standard, or DES. It remained in use till it cracked in **1997** (A BRIEF HISTORY OF ENCRYPTION (AND CRYPTOGRAPHY), 2023)**.**

In the **1970s**, educational papers on encryption were labelled. Cryptographic gadgets were concern to export controls and rated as munitions, specifically inside the US. Encryption become regarded as a rely of country wide security.

In **1976,** Whitfield Diffie and Martin Hellman published a studies paper on what could be described because the Diffie-Hellman key trade.

The code key became now not pre-organized for the first time, but a pair of keys (one public, one private however mathematically connected) become dynamically created for each correspondent.

2000: the Advanced Encryption Standard replaces DES, or AES (asymmetric key - the person and sender need to realize the identical secret key), found via a opposition open to the public. Today, AES is royalty-unfastened international and authorised for use in classified US government records. **(Public Key Infrastructure)** is a generic term used to define solutions for creating and managing public-key encryption. It is activated by browsers for the Internet and public and private organizations to secure communications (A BRIEF HISTORY OF ENCRYPTION (AND CRYPTOGRAPHY), 2023).

2005: Elliptic-curve cryptography (ECC) is a complicated public-key cryptography scheme that lets in shorter encryption keys. Elliptic curve cryptosystems are greater tough to break than RSA and Diffie-Hellman.

what is the meaning of encryption, and how is it different from cryptography?

Cipher: A cipher encodes or scrambles statistics to make them unreadable without the correct interpretation key or algorithm. It's like a secret code, protecting sensitive facts that turn incomprehensible. Ciphers can take unique forms, such as replacing letters with symbols or rearranging the order of words. Only those with the decryption key can decipher the code and understand the unique message, just as a secret code between friends keeps messages safe from others.

Cryptography vs encryption: Cryptography is the science of hiding messages using a secret code. Encryption is a way of encrypting and decrypting facts. The first is a set of analytical techniques for maintaining message secrecy between events (such as symmetric and asymmetric keys), and the second is prepared for the method itself. Cryptanalysis is the science of deciphering statistics and revealing the message in plain text.

Encrypting and decrypting messages during transmission is called cryptography. Messages are encrypted on the sender's side and decrypted on the receiver's side [13]. Securing statistics at some stage of transmission is the primary intent of cryptography. There are 3 main classes of cryptography – symmetric, non-uniform and hybrid cryptography that use each kind [10]. In symmetric cryptography, a single key is used to encrypt (lock) the plaintext or decrypt (unload) the ciphertext. Whereas in uneven cryptography, which is also called public key cryptography, two separate keys are used for encryption and decryption. No single key will fulfill all functions.

- **Symmetric Key Cryptography**

  A cryptographic symmetric key can be classified according to the taxonomy shown in Fig. 1. Since this type is the primary recognition of this document, more information is given than the opposite types. In practice, symmetric key cryptography is extra commonly used than other types of cryptography for many reasons. These reasons include its low computational complexity, low reminiscence consumption and resources. In addition, symmetric cryptography is unbiased towards undeniable text and therefore the algorithm can go through several iterations in multiple rounds without problems (Consulting for information

security, 2018). According to Fig. 1, some details about the three forms of symmetric cryptography are given at this stage.

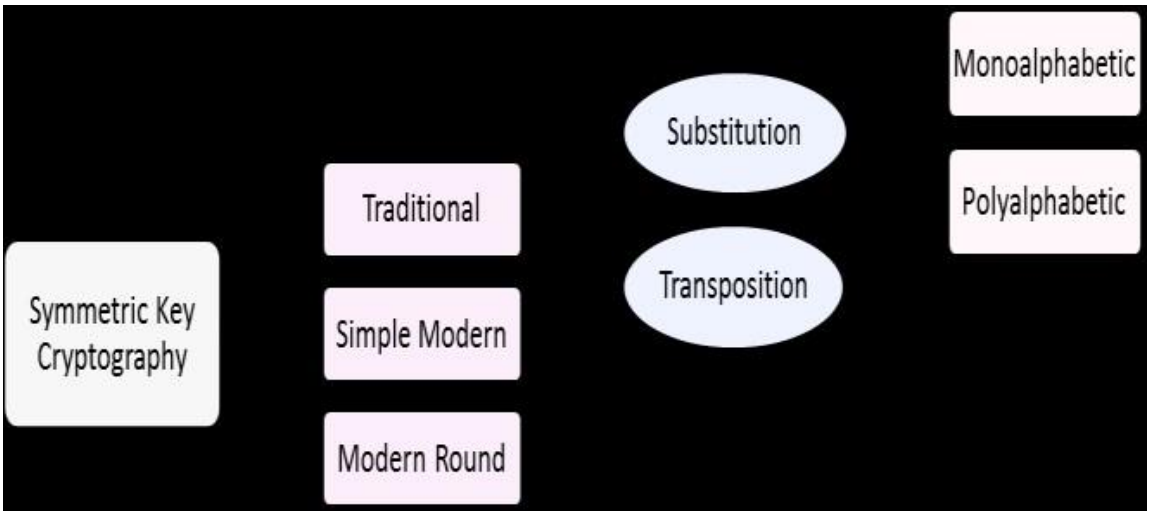

Figure 1 Symmetric key cryptography classification

❖ **Traditional Cipher**

Traditional ciphers are human-centric ciphers that can only be used to encrypt and decrypt text messages. These strategies are considered and used since cryptography has become known (Hans, 2015). There are two distinct types of conventional ciphers; substitution ciphers and transposition ciphers. Substitution ciphers are perhaps the ultimate non-unusual form of ciphers (Stallings, 2006). They work by changing each letter of the plaintext to another. A substitution cipher can use both a fixed substitution form (monoalphabetic ciphers) and a variable alternative structure (polyalphabetic ciphers) (Knight, 2009). On the other hand, transposition ciphers divide the plaintext into blocks of a specific length, that is the size of the important thing, after which they record the symbols in each block depending on the order of the given mapping key.

❖ **Simple Modern Cipher**

The first type of symmetric cryptography is called easy current cipher. This form of cipher is a bit-oriented cipher that can be used to encrypt and decrypt a message with some content material (Stallings, 2006). Examples of simple ciphers are rotary cipher, XOR cipher, S-container and P-box. Details of these ciphers can be found in (Stallings, 2006). Simple contemporary ciphers gave rise to a new method called product ciphers. Product ciphers are complex ciphers that combine substitution, permutation, and some other components. This concept was added by Shannon (Hans, 2015). Shannon's theory is based on two main ideas; confusion and diffusion. In the confusion, the connection between the plaintext and the key is hidden. While in dissemination, the relationship between plaintext and ciphertext is hidden. These two principles can be completed by creating a product cipher with several iterations. Each iteration works using a combination of several components such as S-boxes (substitution box cipher), Poxes (transposition box cipher) and other ingredients. The product cipher is referred to as spherical. Information about this kind of cipher can be found in (Consulting for information security, 2018).

❖ **Modern Round Ciphers**

They also are called round ciphers due to the fact they involve more than one rounds. Each spherical is a complex cipher of multi easy ciphers. Examples are Data Encryption Standard (DES), and Advanced Encryption Standard (AES) (Bellovin, 2000).

❖ **Asymmetric Key Cryptography**

The asymmetric key cryptography verified in Fig. 2 uses two exclusive keys to encrypt and decrypt a message. The first secret is called the public key, which is shared between the sender and receiver. The public key is for the encryption procedure. A second key known as the private key is used for the decryption

technique (Al-Hassani, 2002). Examples of asymmetric keys are Diffie-Hellman Exchange (Bellovin, 2000) and RSA . Due to their low performance compared to the widely used symmetric schemes, uneven encryption schemes are used in practice mainly for the transmission of symmetric keys.

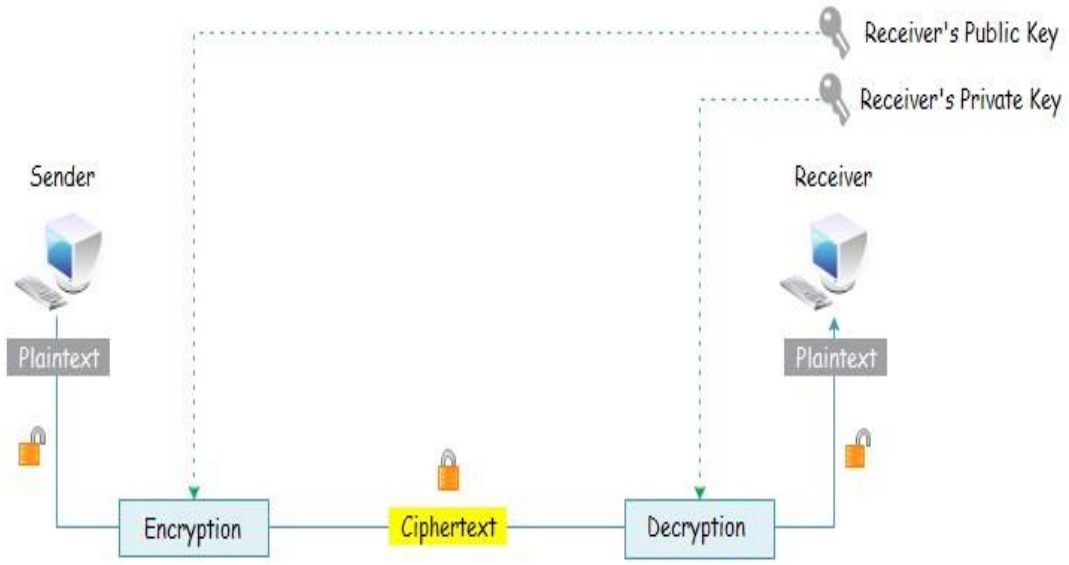

Figure 2 Asymmetric Key Cryptography

- **Hybrid Cryptography**

Hybrid cryptography gadget combines a symmetric and an uneven key machine and for this reason combining the benefits of two structures: the protection of the asymmetric key and the speed of the symmetric key. The real message is encrypted the usage of symmetric key this is called session key. The session secrets encrypted the use of asymmetric key algorithm. Message and session key are routinely combined right into a single bundle. The receiver makes use of his private key to decrypt the consultation key after which uses the session key to decrypt the message .

3. ESSENTIAL WORK

As the modern-day paper is a category of symmetric cryptography, a literature survey on this symmetric key cryptography is introduced on this section.

Caesar Shift Cipher is a easy symmetric set of rules which encrypts every letter inside the plaintext through moving the alphabet to the left by using some of locations given as a key. Also, one of the common ciphers is Atbash Cipher in which each letter has a set replacement given with the aid of a given desk. An instance of mathematical symmetric ciphers is the Affine cipher wherein the letters are encrypted based on a mathematical equation. All of those algorithms are categorized as Monoalphabetic substitution symmetric ciphers.

Another category of substitution ciphers, as demonstrated in Fig. 1, are polyalphabetic substitution symmetric ciphers. The Vigenère cipher is the most unusual cipher in this class. It works by encrypting the plaintext using a random selection of keywords. Repeats the keyword normally until it reaches plain text. Another example of this class is the Autokey Shift cipher. It works like a Vigenère cipher. He is exceptional among them in creating a key current. An autokey cipher creates a keystream by repeating a random keyword followed by plaintext content until it accepts the plaintext all the way to the end. It then continues as the Vigenère cipher.

For transposition symmetric ciphers, an example is the Rail Fence cipher. It is also referred to as a zigzag cipher. Open text writes in zigzags across the page. The key to this cipher is the number of lines. It then reads the letters line by line to find the ciphertext.

Four popular simple modern ciphers appear in the literature. The first is a rotational cipher in which the plaintext is circled across a key charge to the left or right [13]. It uses the identical key value inside the reverse path for decryption. Second; an XOR cipher that requires two inputs: a plaintext and an important thing of the same length. Simply, it applies an XOR operation between the input bits and the key bits. Third; the S-container cipher (Substitution container cipher), which has the same concept of substitution as traditional ciphers. The difference is that the S-box is at the bit level. It is commonly

performed as a search. The input motion needs to be split into blocks of n-bit size. Fourth, the cipher is a P-field Cipher, which has the same concept of transposition as conventional ciphers. The difference is that the P-box is on the bit stage.

The last class of Symmetric Key Cryptography Ciphers is the Modern Round Ciphers Which is also called Round Ciphers because they involve a couple of rounds. Each round is a complex cipher of multi simple ciphers. DES Cipher (Data Encryption Standard) is one of the most not unusual ciphers on this category [28]. It divides the plaintext into blocks of 64bit then the encryption is done using a sixty-four-bit key.

4. PROPOSED ALGORITHM

The primary aim of this paper is to develop a new cryptographic algorithm. The new proposed algorithm is categorised as polyalphabetic substitution symmetric ciphers. This work is encouraged with the aid of the lack of algorithms handling linking the encryption and decryption of characters with their preceding characters inside the message. Linking the encryption of characters with their previous characters make the technique more mystery than other symmetric algorithms. The presented algorithm may be used to encrypt letters, numbers and emblems depending on their ASCII codes. The ASCII code is selected due to the fact it's miles a well-known code of alphanumeric that deals with maximum of the programming languages. The range of the algorithm rule is between the decimal values (32 – 126) in the ASCII table as shown in table 1.

The plaintext is encrypted character by character according to the following equation:

$$Ci = (Pi – Pi\text{-}1) + 32 \qquad (1)$$

Where: Ci is the encryption of the current character

Pi is current character to be encrypted

Pi-1 is previous character in the plaintext

TABLE 1.

ASCII TABLE

Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char
0	0	[NULL]	32	20	[SPACE]	64	40	@	96	60	`
1	1	[START OF HEADING]	33	21	!	65	41	A	97	61	a
2	2	[START OF TEXT]	34	22	"	66	42	B	98	62	b
3	3	[END OF TEXT]	35	23	#	67	43	C	99	63	c
4	4	[END OF TRANSMISSION]	36	24	$	68	44	D	100	64	d
5	5	[ENQUIRY]	37	25	%	69	45	E	101	65	e
6	6	[ACKNOWLEDGE]	38	26	&	70	46	F	102	66	f
7	7	[BELL]	39	27	'	71	47	G	103	67	g
8	8	[BACKSPACE]	40	28	(	72	48	H	104	68	h
9	9	[HORIZONTAL TAB]	41	29	)	73	49	I	105	69	i
10	A	[LINE FEED]	42	2A	*	74	4A	J	106	6A	j
11	B	[VERTICAL TAB]	43	2B	+	75	4B	K	107	6B	k
12	C	[FORM FEED]	44	2C	,	76	4C	L	108	6C	l
13	D	[CARRIAGE RETURN]	45	2D	-	77	4D	M	109	6D	m
14	E	[SHIFT OUT]	46	2E	.	78	4E	N	110	6E	n
15	F	[SHIFT IN]	47	2F	/	79	4F	O	111	6F	o
16	10	[DATA LINK ESCAPE]	48	30	0	80	50	P	112	70	p
17	11	[DEVICE CONTROL 1]	49	31	1	81	51	Q	113	71	q
18	12	[DEVICE CONTROL 2]	50	32	2	82	52	R	114	72	r
19	13	[DEVICE CONTROL 3]	51	33	3	83	53	S	115	73	s
20	14	[DEVICE CONTROL 4]	52	34	4	84	54	T	116	74	t
21	15	[NEGATIVE ACKNOWLEDGE]	53	35	5	85	55	U	117	75	u
22	16	[SYNCHRONOUS IDLE]	54	36	6	86	56	V	118	76	v
23	17	[ENG OF TRANS. BLOCK]	55	37	7	87	57	W	119	77	w
24	18	[CANCEL]	56	38	8	88	58	X	120	78	x
25	19	[END OF MEDIUM]	57	39	9	89	59	Y	121	79	y
26	1A	[SUBSTITUTE]	58	3A	:	90	5A	Z	122	7A	z
27	1B	[ESCAPE]	59	3B	;	91	5B	[	123	7B	{
28	1C	[FILE SEPARATOR]	60	3C	<	92	5C	\	124	7C	|
29	1D	[GROUP SEPARATOR]	61	3D	=	93	5D	]	125	7D	}
30	1E	[RECORD SEPARATOR]	62	3E	>	94	5E	^	126	7E	~
31	1F	[UNIT SEPARATOR]	63	3F	?	95	5F	_	127	7F	[DEL]

Figure 3 ASCII Table

As shown in equation (1), the encryption is performed by using subtracting preceding man or woman from the modern character. In case of the primary individual, the algorithm subtracts 0 from the ASCII fee of individual. The subtraction procedure continually offers us small cost that could take us out of the variety (32 – 126) in ASCII table. Thus, the variety 32 is inserted in the equation to keep away from this problem.

In some cases, adding 32 doesn't clear up the out of variety problem (the range is either more than 126 or smaller than 32). As the worst case takes place while you subtract 32-126 which equals (-94) 32, the best cost to be introduced in this example is ninety-four. In these two unique instances the encryption equation may be both:

Ci =[(Pi – Pi-1) + 32]+ 94 (2)

when [(Pi – Pi-1) + 32] < 32 or

Ci =[(Pi – Pi-1) + 32]- 94 (3) when [(Pi – Pi-1) + 32] □ 126

EXAMPLE FOR ENCRYPTION:

Step 1: Suppose that the plaintext is: Happy

Step 2: Applying the encryption equation Ci = (Pi – Pi-1) + 32 to encrypt the plain text

Step 3: For each Ci , take a look at the value to look if it is inside the range or no longer. The message in this example includes an uppercase letter and 4 lowercase letters. After applying the proposed cipher, the ciphertext turns into a string of set of unique characters /,) and space similarly to the letters. As determined, the letter 'p' is duplicated inside the message and has been encrypted every time to one-of-a-kind person.

The ciphertext: h9/)

For decryption process, the ciphertext is decrypted character by character according to the following equation:

Pi = (Ci –32) + Pi-1 (4)

Where: Ci is current character to be decrypted

Pi is the decryption of the current character

Pi-1 is previous character in the plaintext

In the two special cases, the decryption equation will be either:

Pi =[(Ci –32) + Pi-1]+ 94 (5)

when [(Ci –32) + Pi-1] < 32 or

Pi =[(Ci –32) + Pi-1]- 94 (6) when [(Pi – Pi-1) + 32] □ 126

EXAMPLE FOR DECRYPTION:

The ciphertext: h9/)

Applying the decryption equation Pi = (Ci –32) + Pi-1 to get the original plaintext.

The plaintext is: Happy

5. TESTING

A. ENCRYPTION

TEST 1:

Step 1: Suppose that the plaintext is: sad :(

Step 2: Applying the encryption equation Pi = (Ci –32) + Pi-1 to encrypt the plain text

Step 3: For each Ci , check the value to see if it is range or not.

The message carries letters, set of unique characters : , (and space. As discovered, area is disappeared inside the ciphertext this means that it is encrypted to :. In this example, the algorithm applies all special cases of the out-of-range troubles (need to subtract 94 in encryption of letter s and upload 94 in encryption of letter a, area and ( ).

The ciphertext: 5l#::l

TEST 2:

Step 1: Suppose that the plaintext is: keep it secret !

Step 2: Applying the encryption equation Ci = (Pi – Pi-1) + 32 to encrypt the plain text.

Step 3: For each Ci , check the value to see if it is range or not.

The message in this situation includes letters, unique person ! And space. After making use of the proposed cipher, the ciphertext will become a string of set of unique characters in the range except letters.

As determined, the duplicated letters in the message had been encrypted each time to extraordinary man or woman. And spaces are disappeared inside the ciphertext which means every time encrypted to extraordinary man or woman.

The ciphertext: -x +.i+*sp|/q/*!}

TEST 3:

Step 1: Suppose that the plaintext is: Bank transfer of 5,000 S.R to the account IBAN: SA5305000068200910181000

Step 2: Applying the encryption equation Ci = (Pi – Pi-1) + 32 to encrypt the plain text.

Step 3: For each Ci , check the value to see if it is range or not.

The message in this case contains uppercase letters, lowercase letters, numbers, special man or woman , , . , : and area. After applying the proposed cipher, the ciphertext becomes a string of wide set of unique characters in the variety besides a few numbers and letters.

As discovered, the duplicated letters within the message had been encrypted every time to distinctive person. And areas are disappeared within the ciphertext because of this they're encrypted to different man or woman as nicely.

The ciphertext is: b?-{3t|m-%q}-,ou85u$ nSYDLty/tr{9a" ,&w&*Iw}-jdSlr|{%y &"x|)v}!'w}

TEST 4:

Step 1: Suppose the plain text is: Arab East College is one of the good colleges that offers Masters in: Business Administration, Executive MBA, Science in Accounting, Professional Accounting, Computer Science, Computer and Systems Management Techniques, Means and Technology Education and Special Education.

Step 2: Applying the encryption equation Ci = (Pi – Pi-1) + 32 to encrypt the plain text.

Step 3: For each Ci , take a look at the fee to peer if it's miles in range or no longer. The message in this example incorporates uppercase letters, lowercase letters and set of unique characters , , . And area. After making use of the proposed cipher, the ciphertext will become a string of extensive set of special characters inside the variety except some numbers and letters.

As found, the duplicated letters within the message were encrypted every time to unique character. And areas are disappeared inside the ciphertext because of this they're whenever encrypted to one-of-a-kind man or woman.

The ciphertext: “aQm!<E<2!*CL{ w"|9i*+o}u9ou8tr{9g(s:c,{ w"|.+trw3*ou}-!+mr2!o-,i%JdBS|t%u.+AC)z%y*!|m3s&}<rESk|2}sm9Ms}irS0&z)s"9i%0AB,&w&s%wCrPB{u}.t&}q+2AB,&w&s%wCrCL|#%}o,S0&z)s"ErCL|#%}o-,a-t:SFx!o(&+M4q&|(v)&*T1|%&y($n.7rM8z-%+at:T1|%&!{#v2%E?1l|3s&}0a-t:S=s|&v+2E?1l|3s&}>”

B. DECRYPTION

The second equation Pi = (Ci –32) + Pi-1 is used to decrypt the ciphertext to test the decryption part of the proposed cryptography algorithm.

TEST 1:

The ciphertext: “5l#::l”

Applying the decryption equation Pi = (Ci –32) + Pi-1 to get the original plaintext. The **plaintext:** sad :(

TEST 2:

The ciphertext: “-x +.i+*sp|/q/*!}”

Applying the decryption equation Pi = (Ci –32) + Pi-1 to get the original plaintext.

The plaintext: keep it secret !

TEST 3:

The ciphertext: “ b?-{3t|m-%q}-,ou85u$ nSYDLty/tr{9a" ,&w&*lw}jdSlr|{%y &"x|)v}!'w}”

Applying the decryption equation Pi = (Ci –32) + Pi-1 to get the original plaintext.

The plaintext: Bank transfer of 5,000 S.R to the account IBAN: SA5305000068200910181000

TEST 4:

The ciphertext: “aQm!<E<2!*CL{

w"|9i*+o}u9ou8tr{9g(s:c,{w"|.+trw3*ou}-
!+mr2!o,i%JdBS|t%u.+AC)z%y*!|m3s&}<rESk|2}sm9Ms}irS0&z)s"9i%0AB
,&w&s%wCrPB{u}. t&}q+2AB ,&w&s%wCrCL|#%}o-,S0&z)s"ErCL|#%}o-
,at:SFx!o(&+M4-q&|(v)&*T1|%&y($n.7rM8z-%+at:T1|%&!{#v2%E?1l|3s&}0a-t:
S=s|&v+2E?1l|3s&}>” Applying the decryption equation Pi = (Ci –32) + Pi-1 to get the original plaintext.

The plaintext: Arab East College is one of the good colleges that offers master in: Business Administration, Executive MBA, Science in Accounting, Professional Accounting, Computer Science, Computer and Systems Management Techniques, Means and Technology Education and Special Education.

For the purpose of better clarification and presentation of the proposed algorithm, a website is developed to be used as a tool for the implementation of the proposed algorithm as shown in Fig.3.

Figure 4 A website for the proposed algorithm

6. CONCLUSION

This paper introduces a brand-new symmetric cryptography algorithm for textual content message encoding, using ASCII codes and linking each individual to its predecessor at some stage in encryption and decryption. This method complements code complexity, established through simulations showcasing rapid and accurate text message encryption and decryption. This code can be useful for different things, such as hiding simple messages, doing research, and teaching teachers should use it as an example. Information security is always changing and improving, and so is cryptography. Many attacks and dangers to information security happen every day and are getting bigger and stronger. This makes people create new codes and much stronger codes to keep data safe from attackers.

7. REFERENCE

A BRIEF HISTORY OF ENCRYPTION (AND CRYPTOGRAPHY), 2023. *A BRIEF HISTORY OF ENCRYPTION (AND CRYPTOGRAPHY),* s.l.: https://www.thalesgroup.com/en/markets/digital-identity-and-security/magazine/brief-history-encryption.

Al-Hassani, S., 2002. *Encyclopedia of Law Enforcement ,* s.l.: https://www.nationalgeographic.com/pdf/1001-muslim-inventions-ed-guide.pdf.

Bellovin, D. W. B. S. S., 2000. *ES Key Agility Issues in High-Speed IPsec Implementations,* s.l.: https://www.cs.columbia.edu/~smb/papers/AES-KeyAgile.pdf.

Consulting for information security, 2018. *Cryptographic Mechanisms,* s.l.: https://www.on.de/informationssicherheits-management/?mtm_campaign=Google%20Ads%202022&mtm_kwd=ISMS%201&mtm_source=Google&mtm_medium=PPC&mtm_content=Website%20Informationssicherheits%20Management&mtm_cid=1004&mtm_placement=SEA&gclid=CjwKCAiAqY6tBhAtEiwAHe.

Forouzan, B. A., 2008. *Introduction to cryptography and network security,* s.l.: https://almuhammadi.com/sultan/books_2020/Forouzan.pdf.

Gligor, V. D., 2002. *On Message Integrity in Symmetric Encryption,* s.l.: https://www.cise.ufl.edu/~nemo/Security/public_html/reference/gligor02message.pdf.

Hans, R. B. a. R., 2015. *A Review and Comparative Analysis of Various Encryption,* s.l.: https://article.nadiapub.com/IJSIA/vol9_no4/27.pdf.

KAHN, D., 1972. *The Story of Secret Writing,* New York: The Macmillan Company, 866 Third Avenue.

Knight, S. R. a. K., 2009. *Attacking Letter Substitution Ciphers with Integer Programming,* s.l.:

https://www.researchgate.net/publication/220615776_Attacking_Letter_Substitution_Ciphers_with_Integer_Programming.

Kouch, Y. H. a. R. E., 2015. *A New Algorithm for Dynamic Encryption,* s.l.: https://ijias.issr-journals.org/abstract.php?article=IJIAS-14-298-04.

Michel Abdalla, L. R., 2001. *Lecture Notes in Computer Science,* s.l.: https://www.researchgate.net/publication/2442118_A_New_Forward-Secure_Digital_Signature_Scheme.

Okamoto, E. F. a. T., 1999. *Secure Integration of Asymmetric and,* s.l.: https://courses.grainger.illinois.edu/cs598dk/fa2019/Files/fujisaki_okamoto.pdf.

Sadowsky, G., 2003. *Information Technology Security Handbook,* Washington, DC: World Bank. http://hdl.handle.net/10986/15005.

Shaligram Prajapat, D. a. R., 2013. *Time Variant Approach Towards Symmetric Key,* s.l.: https://www.researchgate.net/publication/306531986_Time_Variant_Approach_Towards_Symmetric_Key_Shaligram_Prajapat_DRajput_and_RSThakur.

Sharma, S., 2021. *Cryptography: A brief overview,* s.l.: https://www.logetale.com/static/pdf/student_reviews/crypto.pdf.

Shiddiky, S., 2005. *Encyclopedia of Law Enforcement,* s.l.: https://www.academia.edu/6105924/Encyclopedia_of_Law_Enforcement.

Stallings, W., 2006. *CRYPTOGRAPHY AND NETWORK SECURITY,* s.l.: https://www.cs.vsb.cz/ochodkova/courses/kpb/cryptography-and-network-security_-principles-and-practice-7th-global-edition.pdf.

Y. Priyanka, S. S., 2008. *I.J.E.M.S, VOL.3,* s.l.: Vani. Digital Signature .