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: Riza Shrestha

London Met ID: 22067117

College ID: NP01NT4A220087

Assignment Due Date: Monday, January 15, 2024

Assignment Submission Date: Monday, January 15, 2024

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.

Table of Contents

Table of Figures

Abstract

The goal of this coursework is to give a thorough understanding of information security, with a focus on cryptography and the creation of the new cryptographic algorithm. The motivation of completing the coursework is a sincere interest to learn more about the fields of cryptography and information security. Securing sensitive data is more important than ever in our increasingly digital environment. The identification of the many flaws in traditional transposition ciphers led to a strong motivation to study, understand, and resolve the issues.

The first section of the course highlights the value of security, including the CIA Triad and the use of cryptography in secure communication. It covers the background of cryptography, delves into symmetric and asymmetric cryptography. The second introduces the background of the Columnar Transposition Cipher, introduces the historical method, emphasizing its role in complex ciphers. Explains the algorithm, encryption, and decryption with practical examples. Highlights advantages and disadvantages of columnar transposition ciphers.

The third introduces the Matrix Shift Transposition, an enhancement to traditional columnar transposition ciphers, addressing security concerns. Uses dynamic shifting, ASCII, XOR, and logical shifts for improved cryptographic strength. Multi-step encryption and decryption processes counter various attacks, represented by a flowchart. The fourth section provides five examples of plaintexts to ciphertexts and vice versa.

The coursework contributes to information security by introducing the Matrix Shift Transposition (MST) cipher, addressing vulnerabilities in traditional ciphers. MST's adaptability, practical applications in sectors like intellectual property and healthcare, and the hands-on learning experience enhance knowledge in information security. It also emphasizes resource management, legal considerations, and provides a foundation for addressing evolving cybersecurity challenges.

The knowledge gained from this coursework provides a fundamental understanding for putting into practice efficient security measures in an era of increasing digitalization. As a result, this project advances current efforts to safeguard sensitive data across numerous domains, making it a useful tool for those hoping to advance information security.

1. Introduction to Cryptographic System

1.1 Security

Security is basically about making sure things are safe and protected. It involves all the steps taken to keep people or places secure, ensuring that only authorized individuals can enter or exit (Collins English Dictionary, 2023). IT security is the process of protecting against cyberthreats and unauthorized access to a company's digital assets, such as computer networks and data. It includes the use of both technologies like endpoint, cloud, and network security as well as physical measures like locks and surveillance cameras. The goal of cybersecurity is to protect businesses from digital attacks like malware, ransomware, and phishing scams where IT security includes every part of an organization's technological infrastructure, including networks, endpoints (such as laptops and mobile devices), software, and hardware. Ransomware and other cyberattacks that encrypt a company's data, a large ransom must be paid to get the decryption key and restore access to the attacked systems (IBM, 2023).

1.2 CIA Triad

The "CIA triad" stands for Confidentiality, Integrity and Availability in information security. It guides businesses in developing strategies to protect data from threats and vulnerabilities, forming a strong foundation for overall system security (Fruhlinger, 2020).

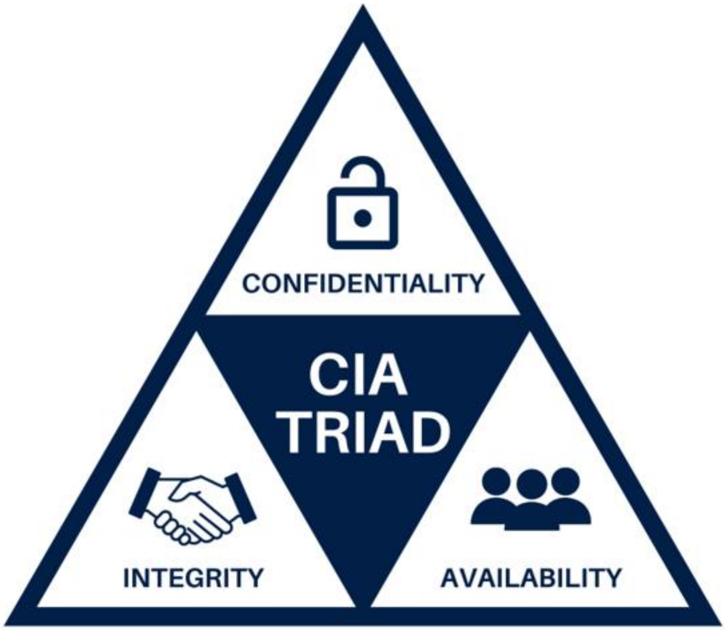


Figure 1: CIA Triad (SecurityMadeSimple, 2023)

1.2.1 Confidentiality

Confidentiality refers to keeping the information private so that only the authorized users can access or modify data. Data encryption is important since attackers can utilize the internet to obtain information. Without the required keys, an attacker will not be able to decrypt the data, even if they are able to access it. To limit access based on roles and enforce policies, secure restrictions are necessary (GeeksforGeeks, 2023). Breach of confidentiality can be unintentional or intentional, caused by direct attacks, the use of various techniques, or human error such as sharing passwords. Organizations should categorize data, implement access controls, encrypt data, use multi-factor authentication systems, and give staff members thorough training in order to protect confidentiality (Fortinet, 2023).

For example, confidentiality is used in healthcare. Sensitive information, such as diagnosis, treatment plans, and personal information, is found in patient medical records. In order to make sure that these documents are only accessible by authorized medical staff, healthcare providers implement strict confidentiality procedures. This protects patient privacy and develops trust between patients and healthcare professionals in the handling of sensitive health information.

1.2.2 Integrity

Integrity refers to making sure that data has not been modified, whether accessed by analysts or presented to the public. It assures reliability and prevents unintentional or unauthorized modifications. Data integrity can be threatened by intentional attacks and unintentional mistakes. Malicious behavior includes attempting to get around security, and coding errors can affect accuracy, particularly in cases where security policies are lacking. Protective techniques, including hashing, encryption, digital signatures, and digital certificates, are necessary for strengthening data integrity. By employing trusted certificate authorities for authentication, websites can improve their integrity. By using digital signatures in emails to assure non-repudiation, communication authority and data integrity are increased (Fortinet, 2023).

For example, of integrity in financial transactions. Digital signatures and encryption are commonly used to protect the integrity of an online financial transfer or payment that someone makes. By avoiding unwanted changes and maintaining the integrity of financial data, the use of digital signatures ensures that the transaction details are preserved from the sender to the recipient.

1.2.3 Availability

Availability refers to making sure that authorized users can access data whenever they need it without compromising confidentiality or integrity. It means networks and systems are regularly accessible. It is maintained by network administrators through hardware management, upgrades, failover planning, and obstacle prevention. DoS or DDoS assaults are examples of threats that can interfere with network availability. Therefore, taking proactive action is essential to lessening their impact on both customers and businesses that depend on the network. Data can be useless if it is not available to people within the organization and the clients they serve, even in cases when confidentiality and integrity are maintained. It is essential that applications, networks, and systems operate continuously and effectively. Organizations use redundant servers, networks, applications, frequent software and security updates reduce security risks and malfunctions to ensure availability (Fortinet, 2023).

For example, an e-commerce website that guarantees its platform is constantly reachable by clients. Authorized users constantly have access to their accounts, can explore products, and can make purchases. The website is committed to availability, which includes regular upgrades, the use of fail-over techniques, and redundant servers to minimize disruptions. Customers will have a great buying experience as a result, which will increase the online store's overall success and trust.

1.2.4 Importance of CIA Triad

The triad provides a comprehensive approach to information security by taking availability, integrity, and confidentiality into consideration in order to protect sensitive data.

- Every component of the triad offers a strong defense against a variety of attacks and covers every possible way that sensitive data can be compromised.
- Organizations are able to effectively prioritize their security measures by using all of the components. This balance keeps one element from taking priority over another, ensuring an overall and strong security posture.
- The triad offers an organized structure for evaluating and controlling risks. Organizations are able to recognize potential threats to availability, confidentiality, or integrity and take preventive measures to reduce these risks.
- The triad offers an organized structure for evaluating and controlling risks. Organizations are able to recognize potential threats to availability, confidentiality, or integrity and take preventive measures to reduce these risks.
- Businesses can choose wisely and strategically when it comes to investing in cybersecurity. In order to use resources more wisely, the trio raises important concerns regarding the effects of particular tools, services, or regulations on information security.

The triad provides an useful and flexible model for understanding and solving security issues in the actual world. Organizations can assess the effects of introducing safety measures such as multifactor authentication on availability, confidentiality, and integrity (Irwin, 2023).

1.3 Cryptography

In our increasingly digital world, making sure everything is secure more important than ever. This is where the study of secure communication methods, or cryptography, comes into action in cybersecurity. Cryptography is closely linked with encryption, the process of converting ordinary text (plaintext) into a coded form (ciphertext) and then decoding it back to plaintext at the destination (Kaspersky, 2023).

Cryptography is the practice of safeguarding information by turning a message into a secret code so that others can't understand it. In this process, an algorithm or mathematical operations is used to change the plain text into something that looks like gibberish or cipher text to anyone who doesn't know the code. In order for cryptographic systems to function properly, the encrypted data must be able to be decrypted by the intended recipient (Fruhlinger, 2022). It creates special codes, such as 128-bit or 256-bit encryption, Secure Sockets Layer (SSL), and Transport Layer Security (TLS). These codes are used to safeguard a variety of digital data and information, including emails, passwords, and information from online transactions like banking and shopping (Kaspersky, 2023).

1.3.1 Importance of Cryptography

Cryptography is a robust tool in the world of cybersecurity. It makes sure information remains private and secure from cyber-attacks by adding an additional layer of security to data and online activity. Its primary features are:

- Confidentiality: Cryptography ensures that the information exchanged is only visible to and understood by those who are allowed. It is similar to having a secret language that only the sender and the intended receiver understand.
- Data integrity: It makes sure that throughout transmission, the information has not been modified or messed with. Digital signatures and other cryptographic techniques function as investigative tools, identifying any unauthorized modifications.
- Authentication: Cryptography helps to confirm the identities involved in communication and where the information is coming from. It creates a secure digital exchange and confirms the identity of each party involved in the transaction.
- Non-repudiation: Cryptography acts as digital evidence of transmission, making it impossible for senders to deny their involvement. Email tracking and digital signatures act as proof tools, removing the possibility of message transmission denial (Kaspersky, 2023).

1.4 Terminology

1. Plaintext- Plaintext is human-readable text that has not been encrypted and can be read both before and after decryption. Cyberattacks often target unprotected plaintext files holding sensitive data, while cybersecurity technologies take use of weaknesses in plaintext credentials (Loshin, 2021).
2. Ciphertext- The encrypted form of plaintext that is generated by encryption methods is called ciphertext, and in order to convert it back into readable plaintext, it requires a key and a decryption cipher. Substitution, transposition, polygraphy, permutation, private-key (symmetric), and public-key (asymmetric) cryptography are some of the different cipher types (Rosencrance, 2020).
3. Key- In order to ensure secure communication, a cryptographic algorithm uses a set of bits called a cryptographic key to change plaintext into ciphertext or vice versa. There are two kinds of keys: symmetric, which functions similarly to having a single key that can be used to both lock and unlock data. The other is asymmetrical and requires two keys, one for locking and the other for unlocking. These keys are essential for numerous functions like encrypting and decrypting messages, certifying digital signatures (Rouse, 2017).
4. Encryption- Encryption refers to converting information (plaintext) into ciphertext, accessible only with an authorized decryption key. Information is protected from cyberattacks and its confidentiality, integrity and authenticity are maintained through this method. Various encryption types, like symmetric and asymmetric, uses keys such as AES, RSA, and DES which secure both stored and transmitted data (Fortinet, 2023).
5. Decryption- The process of converting encrypted data to its regular, understandable form is known as decryption. It is the method by which the system decrypts data that has been encrypted to restore its readable form. Keys or passwords can be used to execute this automatically or manually. The major goals are to protect privacy and stop unauthorized access to data that is sent over the internet, including user information and email communications (Rouse, 2023).

1.5 History of Cryptography

The word "cryptography" comes from the Greek word "kryptos," which means hidden. The beginning "crypt-" means "hidden," and the ending "-graphy" means "writing." It's like turning messages into secret codes. The Egyptians used hieroglyphics, which are unique symbols that are only known by a few people, around 2000 B.C. From 100 B.C. to 44 B.C., Julius Caesar used the first known modern secret code. In his messages, he substituted a letter three positions higher in the alphabet for each letter (Richards, 2021).

Cryptography mostly involved using substitution ciphers to secure government and military messages. When computers were developed, improvements in cryptography happened at the same time. In World War II, the Germans used the Enigma machine, and in Britain, Alan Turing's team created a similar machine to decode messages, which played a part in making modern computers. Even as cryptography became more complicated with computers, it was mainly used by spies and military leaders for many years (Fruhlinger, 2022).

1.6 Symmetric and Asymmetric cryptography

In the digital age, where information is a valuable asset and data security is important, cryptography protects private data and sensitive communications. In order to mitigate the risk of data theft, encryption must be implemented. Asymmetric and symmetric cryptography are two fundamental cryptographic techniques that are used.

1.6.1 Symmetric cryptography

Symmetric key encryption, also known as private key cryptography, uses a single key for both encryption and decryption. This technique is commonly used in industries like banking and data storage that ensures protection against fraudulent activity and protects stored data. The length and uniqueness of the key determine how strong symmetric key encryption is. Using this method, the sender and the intended recipients have the same secret key. Using an encryption algorithm (cipher), the sender uses this key to encrypt messages, converting plaintext into ciphertext. The messages are then decrypted by the intended receivers using the same key, converting the ciphertext to plaintext. This encryption method works effectively in situations where confidentiality is important (Phemex Academy, 2021).

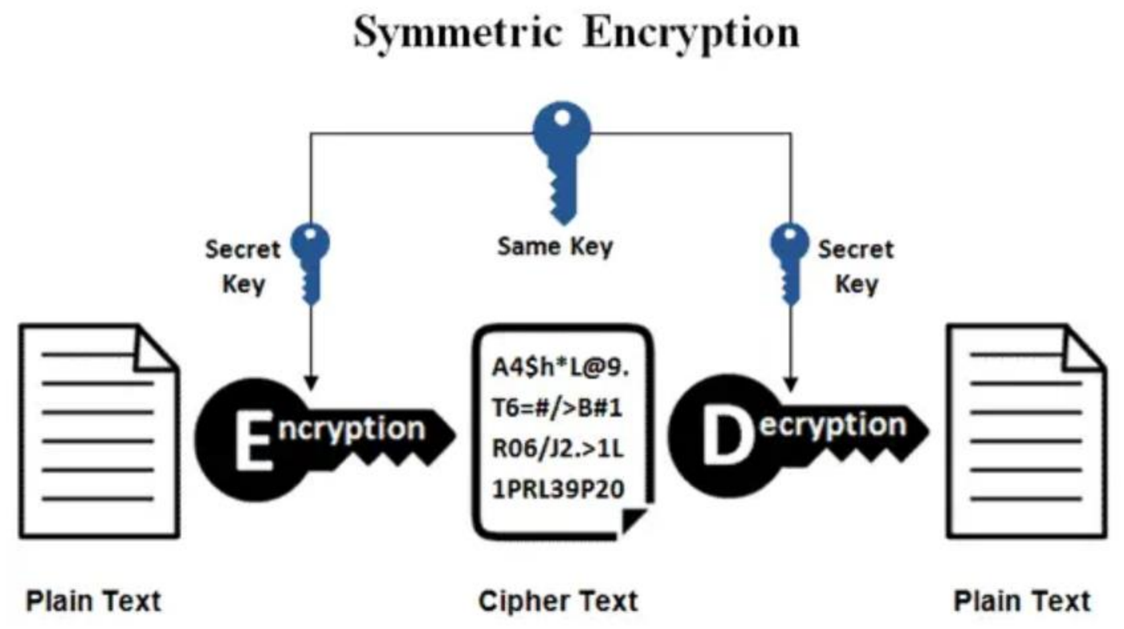


Figure 2: Symmetric Encryption (SSL2BUY, 2023)

Advantage of Symmetric Cryptography:

i. Ease of Implementation: Compared to asymmetric encryption, symmetric encryption is easier to implement.

ii. Faster Processing: Because it functions more quickly than asymmetric encryption, it is useful in situations where fast data processing is necessary.

iii. Managing Bigger Data Sets: It works properly for efficiently managing and transferring bigger data sets.

Disadvantage of Symmetric Cryptography

i. Key Loss Compromise: Any data encrypted with a lost encryption key is vulnerable to compromise and creates a security risk.

ii. Secure Key Sharing: It might be difficult and necessitates strong security measures to transfer the key safely with the intended recipient (ARNAUD, 2023).

1.6.2 Asymmetric cryptography

Asymmetric cryptography is also known as public-key cryptography, involves using two keys, a public key for data encryption and a private key for data decryption. The public key is openly accessible which encrypts messages that ensuring only the private key holder can decrypt. By minimizing the need for private key sharing, this technique improves data security and lowers the possibility of cyberattacks. Asymmetric cryptography is used by digital signatures and protocols like TLS and SSL to provide secure communications and authentication (Kate Brush, 2021).

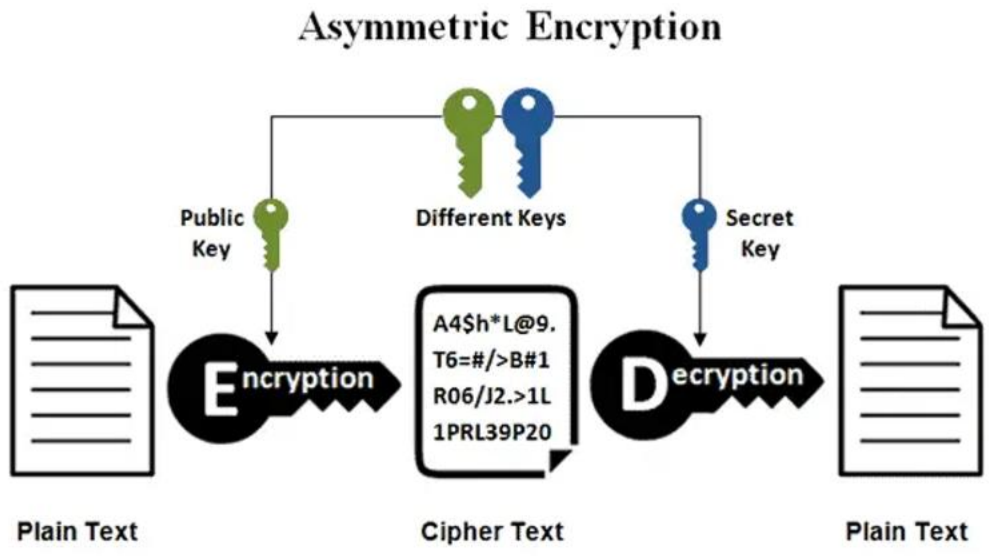


Figure 3: Asymmetric Cryptography (SSL2BUY, 2023).

Advantage of Asymmetric cryptography:

i. Enhanced Security: An additional layer of protection is added as data can only be decrypted with the owner's private key.
ii. Reduced Compromise Risk: The data is secure and protected from unwanted access even in the event that the public key gets lost or stolen.
iii. Extensive Security Features: Asymmetric encryption is a flexible security solution that offers authentication, non-repudiation, and confidentiality assurance.

Disadvantage of Asymmetric cryptography:

i. Slower Processing: The speed at which data is processed is affected by asymmetric encryption's potential to be slower than symmetric encryption.
ii. Increased Resource Usage: Asymmetric encryption implementation uses more computational resources, which reduces system efficiency.
iii. Irreversible Effects: Since there is no way to get the private key back, losing it could have serious consequences, including permanent data loss or security problem (ARNAUD, 2023).

2. Background of Columnar Transposition Cipher

The classical columnar transposition cipher was a popular encryption method back in the late 1800s and early 1900s. It was essential in the creation of increasingly complex ciphers, such as the double transposition encryption and ADFGVX. There's a new approach for dealing longer keys in this cipher, whereas traditional methods focused on shorter ones (George Lasry, 2016).The columnar transposition cipher refers to rearranging the letter order in the original text to encrypts messages. This belongs to the larger class of ciphers known as transposition ciphers, which focus on rearranging letters instead of substituting them (Agler, 2023). It uses a matrix during both encryption and decryption. The number of columns is decided by a secret keyword.

2.1 How does Columnar Transposition cipher work?

In the columnar transposition technique, the message is in rows of a certain length. The message is then read column by column, but the sequence of the columns is jumbled. A selected keyword indicates the rows' length and the columns' arrangement.   This method uses a two-dimensional setup, where the message is initially placed in rows and then rearranged by transposing the columns. The final result, known as the ciphered text, is obtained by reading the columns in the order specified by the keyword (StudyDriver.com, 2017).

2.2 Algorithm

For Encryption:

I. Select the Message: Choose the plaintext message to encrypt.
II. Choose a Keyword: Select a keyword that will determine the permutation of columns and row width. Also, specify the order of the keyword.
III. Create a Table: Form a table with rows and columns.
IV. Write the Keyword: In the first row of the table, write the keyword letters. In the second row, write the corresponding alphabetical order.
V. Enter the Message: Write the message in rows from left to right under the assigned numbers derived from the keyword. The length of the message determines the matrix size.
VI. Handle Empty Spaces: Leave empty spaces at the bottom or fill them with additional letters.
VII. Generate Ciphertext: Create the ciphertext by reading the columns from top to bottom in the order specified by the keyword.

For Decryption:

I. Know the Secret Keyword: Obtain the secret keyword used for encryption.
II. Determine Column Length: Divide the length of the message by the length of the keyword to determine the column length.
III. Create a Table: Form a table using the given keyword and the order of the alphabet.
IV. Arrange Ciphertext: Place the ciphertext into the table in column.
V. Rearrange According to Keyword: Rearrange the ciphertext within the table following the order of the alphabet defined by the keyword.
VI. Generate Plaintext: Retrieve the plaintext by reading from the top row and moving from left to right (GeeksforGeeks, 2023) (Crypto-IT, 2020).

2.2 Example of Columnar Transposition Cipher

Plain text- LIFE GOES ON

Keyword- BTS (31)

Step 1: A matrix is created using a keyword (BTS) and the order of alphabet(213), and the plain text is written in the corresponding box.

- ➔ The green color indicates the keyword BTS.
- ➔ The blue color indicates order of the keyword.

B	**T**	**S**
2	**3**	**1**
L	I	F
E	G	O
E	S	O
N		

Step 2: In the matrix, two empty boxes are identified, and the letter U and X are written to fill these spaces.

- ➔ The red color is use to indicate the letter added to fill empty spaces.

B	**T**	**S**
2	**3**	**1**
L	I	F
E	G	O
E	S	O
N	U	W

Step 3: Creating a ciphertext according to the order of alphabet, 123 where:

1 = FOOW

2 = LEEN

3 = IGSU

Cipher text: FOOW LEEN IGSU

Decryption

Step 1: Creating a table using the keyword. Dividing the length of the cipher text 12 by the length of the keyword 3 to determine the column length.

12/3 = 4

B	T	S
2	3	1

Step 2: Arranging the ciphertext in columns.

B	**T**	**S**
2	**3**	**1**
F	L	I
O	E	G
O	E	S
W	N	U

Step 3: Rearranging the cipher text according to the order of the alphabet.

Step 3.1

1 = FOOW

B	T	S
2	**3**	**1**
		F
		O
		O
		W

Step 3.2

2 = LEEN

B	T	S
2	**3**	**1**
L		F
E		O
E		O
N		W

Step 3.3

3 = IGSU

B	T	S
2	**3**	**1**
L	I	F
E	G	O
E	S	O
N	U	W

Step 4: The pain text is generated by reading from the top row and moving from left to right.

Plain text: LIFE GOES ON

2.3 Advantage of Columnar Transposition Cipher

- Columnar Transposition provides improved mixing of letters compared to some other ciphers, like the Rail Fence Cipher.
- The method is simple to comprehend and apply, so even users with limited experience with cryptography are able to use it.
- It is applicable multiple times. This increases the encryption's security and is referred to as double transposition.
- Columnar transposition becomes more secure when the key size is increased, strengthening its defense against cryptanalysis and brute force attacks.
- Without knowing the key, how long it is, and how many columnar transpositions were made, it is very difficult to decrypt the encrypted ciphertext.

2.3 Disadvantage of Columnar Transposition Cipher

- Columnar transposition is vulnerable to frequency analysis attacks because of a flaw in which the ciphertext's letter appearance frequency matches that of the plaintext.
- The strength and privacy of the key play a major role in Columnar Transposition security. A compromised key could make the encryption as a whole vulnerable.
- It is more vulnerable to known-plaintext attacks in situations when an attacker is aware of both the plaintext and the related ciphertext.
- Using it for the encryption and decryption of large volumes of data may become time-consuming, which could have an impact on overall performance.
- Mistakes that arise during the encryption process can make it more difficult to decipher the message correctly (StudyDriver.com, 2017) (Weng, 2023).

.

3. Development of Matrix Shift Transposition

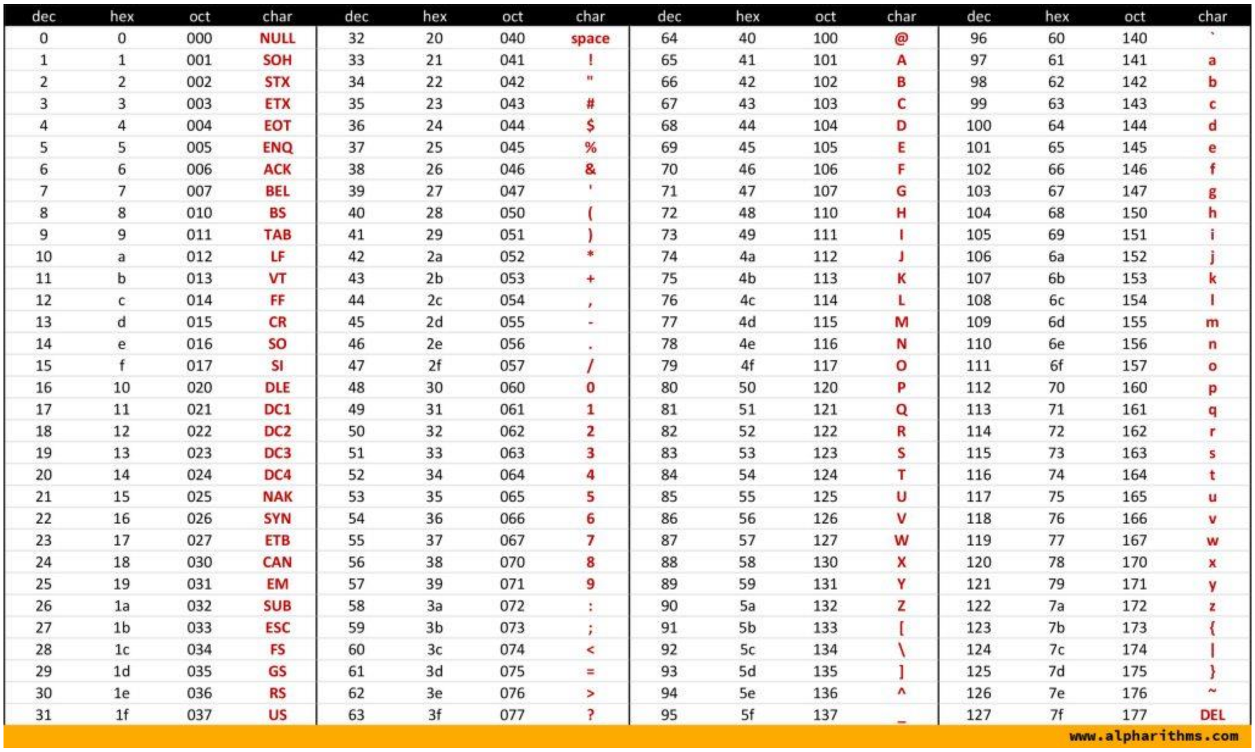
The modification of the traditional columnar transposition algorithm into Matrix Shift Transposition is needed to solve the basic vulnerabilities discovered in traditional transposition ciphers. While the new algorithm uses dynamic shifting to fix potential flaws and improve overall cryptographic strength, columnar transmission offers only a small level of protection. The shifting mechanism's constant change introduces an additional layer of complexity, which decreases predictability and strengthens the algorithm's defense against different cryptographic attacks.

3.1 Background

The new modify Matrix transposition cipher is done by using multiple steps to secure the encryption process. It uses the substitution technique, which was inspired by Kester's method, which involves rearranging characters and using Vigenère cipher elements (Kester, 2013). Every character in the plaintext, selected from a predetermined set of characters, is substituted with a different character from the same set, chosen in accordance with a particular key (GeeksforGeeks, 2023). Shifting operation are applied to each letter in the matrix, and a shift of three positions is performed in new modified cipher.

The American Standard Code for Information Interchange, or ASCII was developed in the 1960s, which makes it easy to send textual data in a way that that is readable by humans. By giving letters values, it guarantees accurate extraction from binary storage. There are 127 characters in ASCII, which are made up of letters, numbers, and symbols. It is case-sensitive nature and control characters enhance functionality (Jack, 2020).

The use of ASCII Table is one of the most important steps in creating this encryption method. It is a basic element of character encoding taught in schools that increased the process's flexibility and computing efficiency. It systematically translates every character was to its appropriate decimal representation, offering a globally acknowledged basis for cryptographic functions. The ASCII table was essential in the encryption process since it helped translate characters into their decimal equivalents, which was a necessary for the next step.

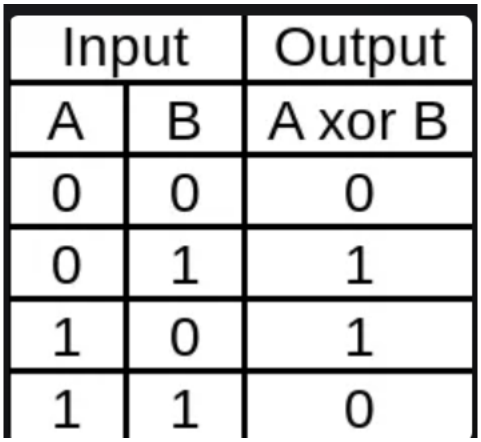


dec	hex	oct	char	dec	hex	oct	char	dec	hex	oct	char	dec	hex	oct	char
0	0	000	NULL	32	20	040	space	64	40	100	@	96	60	140	`
1	1	001	SOH	33	21	041	!	65	41	101	A	97	61	141	a
2	2	002	STX	34	22	042	"	66	42	102	B	98	62	142	b
3	3	003	ETX	35	23	043	#	67	43	103	C	99	63	143	c
4	4	004	EOT	36	24	044	$	68	44	104	D	100	64	144	d
5	5	005	ENQ	37	25	045	%	69	45	105	E	101	65	145	e
6	6	006	ACK	38	26	046	&	70	46	106	F	102	66	146	f
7	7	007	BEL	39	27	047	'	71	47	107	G	103	67	147	g
8	8	010	BS	40	28	050	(	72	48	110	H	104	68	150	h
9	9	011	TAB	41	29	051	)	73	49	111	I	105	69	151	i
10	a	012	LF	42	2a	052	*	74	4a	112	J	106	6a	152	j
11	b	013	VT	43	2b	053	+	75	4b	113	K	107	6b	153	k
12	c	014	FF	44	2c	054	,	76	4c	114	L	108	6c	154	l
13	d	015	CR	45	2d	055	-	77	4d	115	M	109	6d	155	m
14	e	016	SO	46	2e	056	.	78	4e	116	N	110	6e	156	n
15	f	017	SI	47	2f	057	/	79	4f	117	O	111	6f	157	o
16	10	020	DLE	48	30	060	0	80	50	120	P	112	70	160	p
17	11	021	DC1	49	31	061	1	81	51	121	Q	113	71	161	q
18	12	022	DC2	50	32	062	2	82	52	122	R	114	72	162	r
19	13	023	DC3	51	33	063	3	83	53	123	S	115	73	163	s
20	14	024	DC4	52	34	064	4	84	54	124	T	116	74	164	t
21	15	025	NAK	53	35	065	5	85	55	125	U	117	75	165	u
22	16	026	SYN	54	36	066	6	86	56	126	V	118	76	166	v
23	17	027	ETB	55	37	067	7	87	57	127	W	119	77	167	w
24	18	030	CAN	56	38	070	8	88	58	130	X	120	78	170	x
25	19	031	EM	57	39	071	9	89	59	131	Y	121	79	171	y
26	1a	032	SUB	58	3a	072	:	90	5a	132	Z	122	7a	172	z
27	1b	033	ESC	59	3b	073	;	91	5b	133	[	123	7b	173	{
28	1c	034	FS	60	3c	074	<	92	5c	134	\	124	7c	174	|
29	1d	035	GS	61	3d	075	=	93	5d	135	]	125	7d	175	}
30	1e	036	RS	62	3e	076	>	94	5e	136	^	126	7e	176	~
31	1f	037	US	63	3f	077	?	95	5f	137	_	127	7f	177	DEL

www.alpharithms.com

Figure 4: ASCII Table (West, 2022).

Exclusive or, or XOR, is a basic bitwise operation in cryptography that is frequently used in ciphers. It uses binary data and returns true when the inputs are opposites. XOR is commonly applied in practical applications for various encryption techniques, including AES-256 and DES, which particularly caught my attention to implement XOR into the new modified algorithm (Wagner, 2020). XOR operation is done with the key that is provided at the first along with the keyword to use it in the encryption steps which offers a simple yet effective way to manipulate binary data and introduce randomness.



Input		Output
A	B	A xor B
0	0	0
0	1	1
1	0	1
1	1	0

Figure 5: XOR operation (Wagner, 2020).

Logical shift left (LS-2) is a common operation in symmetric key algorithms, and it is often used to provide diffusion and non-linearity in the encryption process. I drew inspiration from well-known encryption S- DES for key generation steps. The LS-2 operation involves shifting the bits of a binary representation two positions to the left, has been recognized for its role in introducing confusion and strengthening the security posture of encryption schemes (GeeksforGeeks, 2021).

The Backward cipher text and Symbol Addition in this encryption method increase the algorithm's overall security and durability. Unlike traditional columnar transposition ciphers that depend on key numbers to generate ciphertext, the backward ciphertext adds a layer of complexity by disrupting the usual order of operations, making it more challenging for potential adversaries to decipher the message. Addition of symbols give the ciphertext a certain amount of unpredictability and irregularity that makes it harder for users used to typical columnar transposition techniques to decipher.

3.2 The New Encryption Algorithm and The New Decryption Algorithm

3.2.1 Encryption:

I. Matrix Formation: Write the plaintext in matrix form with the keyword as the row and the order of letters after it.

II. Shift by 3 Positions: Shift the letters in the matrix by 3 positions.

III. Convert to Decimal: Convert the shifted letters to decimal using the ASCII table.

IV. Convert Decimal to Binary: Convert the decimal values to binary.

V. Convert Key to Decimal: Convert the provided key to its decimal representation.

VI. XOR Operation: Perform XOR with the key and the binary numbers generated from the ASCII table.

VII. Left Shifts (LS-2): Apply LS-2 to the binary value obtained from the XOR operation.

VIII. Convert Binary to Decimal: Convert the binary result to its decimal equivalent.

IX. Convert Decimal to Letters: Translate the decimal values back into letters using the ASCII table.

X. Creating a Backward Ciphertext: Create the ciphertext by reading the columns from back to front and from bottom to top.

XI. Add Symbol (#): Add a symbol (#) after each encrypted letter.

3.2.2 Decryption:

I. Remove Symbol (#): Remove the symbol (#) after each encrypted letter.

II. Arrange Ciphertext: Arrange the ciphertext from back of the letter of keyword and from bottom to top.

III. Convert to Decimal: Convert the letters into decimal using the ASCII table.

IV. Convert Decimal to Binary: Convert decimal to its binary equivalent.

V. Left Shifts (LS-6): Apply LS-6 to the binary value.

VI. Convert Key to Decimal: Convert the provided key to its decimal representation

VII. XOR Operation: Perform XOR with the value from LS-6 and the provided key.

VIII. Convert Binary to Decimal: Convert the binary value obtained from the XOR operation to decimal.

IX. Convert Decimal to Letters: Convert the decimal values to letters using the ASCII table.

X. Substitute Letters Dynamically: Substitute each letter by shifting it back dynamically.

XI. Original Plaintext Recovery: The original plaintext is recovered.

3.3 Why the modification was necessary?

Certain attacks, such as Brute Force Attacks, Frequency Analysis, Known-Plaintext Attacks and Cryptanalysis Methods, are vulnerable against traditional transposition ciphers. Using of various mathematical and logical modification introduced by SMT adds another level of complexity and improves security overall by strengthening the security posture.

3.4 The new Methodology implied.

The new methodology implies a dynamic and multi-step approach to encryption and decryption. It introduces substituting letters, converting characters to binary, use of an ASCII table, shifting, XOR operations, left shifts LS-2 and LS-6, and dynamic replacement in the conversion of characters to binary. Together, these processes add non-linearity and diffusion, making the algorithm robust and secure.

3.5 The new Encryption algorithm.

The new encryption algorithm follows a multi-step process. It includes matrix formation, shifting, conversion to binary, bitwise XOR operations between the provided key and binary numbers, left shifts (LS-2), converting the binary output to its decimal equivalent, translating it back into letters, the creation of a backward ciphertext and adding symbol after each ciphertext letters. These steps collectively contribute to enhanced security and complexity in the encryption process.

3.6 The new Decryption algorithm

The decryption algorithm involves the reversal of encryption steps, including the removal of symbols, arrangement of ciphertext, conversion to binary, application of left shifts (LS-6), XOR operations, and the substitution of letters. This process ensures the recovery of the original plaintext.

3.7 Flow Chart

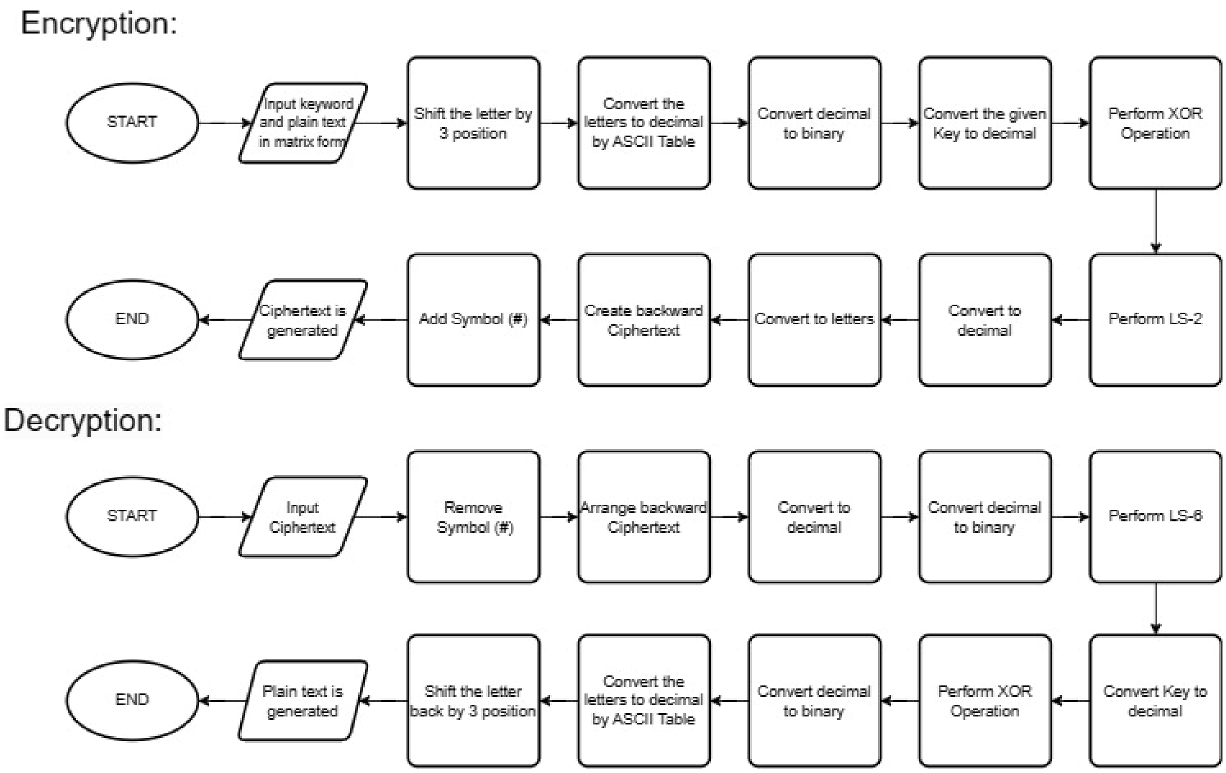

Encryption:
START
Input keyword and plain text in matrix form
Shift the letter by 3 position
Convert the letters to decimal by ASCII Table
Convert decimal to binary
Convert the given Key to decimal
Perform XOR Operation
Perform LS-2
Convert to decimal
Convert to letters
Create backward Ciphertext
Add Symbol (#)
Ciphertext is generated
END
Decryption:
START
Input Ciphertext
Remove Symbol (#)
Arrange backward Ciphertext
Convert to decimal
Convert decimal to binary
Perform LS-6
Convert Key to decimal
Perform XOR Operation
Convert decimal to binary
Convert the letters to decimal by ASCII Table
Shift the letter back by 3 position
Plain text is generated
END

Figure 6: Flowchart for encryption and Decryption process.

4. Testing

4.1 Case 1

Given Text: SECURITY IS IMPORTANT

Keyword: CODE

Key: 150

Step 1: The Matrix is formed according to the keyword “CODE,” and the plain text is written after “CODE.” The plain text is written from the first row. An extra empty space is filled by writing “A.”

- The blue color indicates the keyword.
- The red color indicates the empty space being filled.

C	**O**	**D**	**E**
S	E	C	U
R	I	T	Y
I	S	I	M
P	O	R	T
A	N	T	A

Step 2: Each letter is substituted by shifting 3 positions (example: S = V, E = H, C = F, U =X, R = U and so on).

C	O	D	E
V	H	F	X
U	L	W	B
L	V	L	P
S	R	U	W
D	Q	W	D

Step 3: The substituted letters are then converted to decimal using the ASCII Table.

C	O	D	E
86	72	70	88
85	76	87	66
76	86	76	80
83	82	85	87
68	81	87	68

Step 4: The decimal values are converted to binary.

C	O	D	E
01010110	01001000	01000110	01011000
01010101	01001100	01010111	01000010
01001100	01010110	01001100	01010000
01010011	01010010	01010101	01010111
01000100	01010001	01010111	01000100

Step 5: The key provided, 150, is converted to decimal.

K = 10010110

Step 6: XOR operation is performed with the key '10010110' and the binary numbers obtained from step 4.

C	O	D	E
11000000	11011110	11010000	11001110
11000011	11011010	11000001	11010100
11011010	11000000	11011010	11000110
11000101	11000100	11000010	11000001
11010010	11000111	11000001	11010010

Step 7: A left shifts by 2 (LS-2) position is performed with XOR result.

C	O	D	E
00000011	01111011	01000011	00111011
00001111	01101011	0000011	01010011
01101011	00000011	01101011	00011011
00010111	00010011	00001011	00000111
01001011	00011111	00000111	01001011

Step 8: The binary values obtained from LS-2 is converted to decimal.

C	O	D	E
3	123	67	59
15	107	7	83
107	3	107	27
23	19	11	7
75	31	7	75

Step 9: The decimal values are converted to letters using ASCII Table.

C	O	D	E
ETX	{	C	;
SI	k	BEL	S
k	ETX	k	ESC
ETB	DC3	VT	BEL
K	US	BEL	K

Step 10: The cipher text is written by reading the letters of columns from back to front and from bottom to top, adding # after every encrypted letter.

C	O	D	E
			;
			S
			ESC
			BEL
			K

Cipher text = K#BELI#ESC#S#;

C	O	D	E
		C	;
		BEL	S
		k	ESC
		VT	BEL
		BEL	K

Cipher text = K#BELI#ESC#S#; #BEL#VT#k#BEL#C

C	O	D	E
ETX	{	C	;
SI	k	BEL	S
k	ETX	k	ESC
ETB	DC3	VT	BEL
K	US	BEL	K

Therefore the Cipher text is K#BEL#ESC#S#; #BEL#VT#k#BEL#C #US#DC3#ETX#k#{ #K#ETB#k#SI#ETX

For Decryption

Step 1: Removing # after each letter letters in the ciphertext.

K BEL ESC S ; BEL VT k BEL C US DC3 ETX k { K ETB k SI ETX

Step 2: The matrix is made by first counting the letters, words and symbol from the cipher text and dividing the keyword.

20/4 = 5

5 columns are made, and 4 rows are made from the keyword CODE.

The cipher text is arranged by write the letters starting from the column E from bottom to top.

C	**O**	**D**	**E**
			;
			S
			ESC
			BEL
			K

C	O	D	E
ETX	{	C	;
SI	k	BEL	S
k	ETX	k	ESC
ETB	DC3	VT	BEL
K	US	BEL	K

Step 3: The letters are converted to decimal using the ASCII Table.

C	O	D	E
3	123	67	59
15	107	7	83
107	3	107	27
23	19	11	7
75	31	7	75

Step 4: The decimal values are converted to binary.

C	O	D	E
00000011	01111011	01000011	00111011
00001111	01101011	0000011	01010011
01101011	00000011	01101011	00011011
00010111	00010011	00001011	00000111
01001011	00011111	00000111	01001011

Step 5: A left by 6 (LS-6) is performed to the binary value.

C	O	D	E
11000000	11011110	11010000	11001110
11000011	11011010	11000001	11010100
11011010	11000000	11011010	11000110
11000101	11000100	11000010	11000001
11010010	11000111	11000001	11010010

Step 6: XOR operation is performed with the key 150 converted to '10010110' and the binary numbers obtained from step 5.

C	O	D	E
01010110	01001000	01000110	01011000
01010101	01001100	01010111	01000010
01001100	01010110	01001100	01010000
01010011	01010010	01010101	01010111
01000100	01010001	01010111	01000100

Step 7: The binary values are converted to decimal.

C	O	D	E
86	72	70	88
85	76	87	66
76	86	76	80
83	82	85	87
68	81	87	68

Step 8: The decimal values are converted to letters from ASCII Table.

C	O	D	E
V	H	F	X
U	L	W	B
L	V	L	P
S	R	U	W
D	Q	W	D

Step 9: The letters are substituted by shifting each letter back by 3 positions.

C	O	D	E
S	E	C	U
R	I	T	Y
I	S	I	M
P	O	R	T
A	N	T	A

Step 10: Plain text is obtained by reading the letters from rows to rows.

Therefore, Plain text = SECURITY IS IMPORTANT

4.2 Case 2

Given Text: SECURE INFORMATION

Keyword: GUARD

Key: 12

Step1: The Matrix is formed according to the keyword “GUARD,” and the plain text is written after it. The plain text is written from the first row. An extra empty space is filled by writing “X,Y,Z.”

G	U	A	R	D
S	E	C	U	R
E	I	N	F	O
R	M	A	T	I
O	N	X	Y	Z

Step 2: Each letter is substituted by shifting 3 positions (example: S = V, E = H, C = F, U =X, R = U and so on).

G	U	A	R	D
V	H	F	X	U
H	L	Q	I	R
U	P	D	Q	L
R	Q	A	B	C

Step 3: The substituted letters are then converted to decimal using the ASCII Table.

G	U	A	R	D
72	76	81	73	82
85	80	68	81	76
82	81	65	66	67

Step 4: The decimal values are converted to binary.

G	U	A	R	D
01010110	01001000	01000110	01011000	01010101
01001000	01001100	01010001	01001001	01010010
01010101	01010000	01000100	01010001	01001100
01010010	01010001	01000001	01000010	01000011

Step 5: The key provided, 12 is converted to decimal.

K = 00001100

Step 6: XOR operation is performed with the key '00001100' and the binary numbers obtained from step 4.

G	U	A	R	D
01011010	01000100	01001010	01010100	01011001
01000100	01000000	01011101	01000101	01011110
01011001	01011100	01001000	01011101	01000000
01011110	01011101	01001101	01001110	01001111

Step 7: A left shifts by 2 (LS-2) position is performed with XOR result.

G	U	A	R	D
01101001	00010001	00101001	01010001	01100101
00010001	00000001	01110101	00010101	01111001
01100101	01110001	00100001	01110101	00000001
01111001	01110101	00110101	00111001	00111101

Step 8: The binary values obtained from LS-2 is converted to decimal.

G	U	A	R	D
105	17	41	81	101
17	1	117	21	121
101	113	33	117	1
121	117	53	57	61

Step 9: The decimal values are converted to letters using ASCII Table.

G	U	A	R	D
i	DC1	)	Q	e
DC1	SOH	u	NAK	y
e	q	!	u	SOH
y	u	5	9	=

Step 10: The cipher text is written by reading the letters of columns from back to front and from bottom to top, adding # after every encrypted letter.

Cipher text is =#SOH#y#e #9#u#NAK#Q #5#!#u#) #u#q#SOH#DC1 #y#e#DC1#i

For Decryption

Step 1: Removing # after each letter letters in the ciphertext.

= SOH y e 9 u NAK Q 5 ! u) u q SOH DC1 y e DC1 i

Step 2: The matrix is made by first counting the letters, words and symbol from the cipher text and dividing the keyword.

20/5 = 4

4 columns are made, and 5 rows are made from the keyword GUARD.

The cipher text is arranged by write the letters starting from the column D from bottom to top.

G	U	A	R	D
i	DC1	)	Q	e
DC1	SOH	u	NAK	y
e	q	!	u	SOH
y	u	5	9	=

Step 3: The letters are converted to decimal using the ASCII Table.

G	U	A	R	D
105	17	41	81	101
17	1	117	21	121
101	113	33	117	1
121	117	53	57	61

Step 4: The decimal values are converted to binary.

G	U	A	R	D
01101001	00010001	00101001	01010001	01100101
00010001	00000001	01110101	00010101	01111001
01100101	01110001	00100001	01110101	00000001
01111001	01110101	00110101	00111001	00111101

Step 5: A left by 6 (LS-6) is performed to the binary value.

G	U	A	R	D
01011010	01000100	01001010	01010100	01011001
01000100	01000000	01011101	01000101	01011110
01011001	01011100	01001000	01011101	01000000
01011110	01011101	01001101	01001110	01001111

Step 6: XOR operation is performed with the key 12 converted to '00001100' and the binary numbers obtained from step 5.

G	U	A	R	D
01010110	01001000	01000110	01011000	01010101
01001000	01001100	01010001	01001001	01010010
01010101	01010000	01000100	01010001	01001100
01010010	01010001	01000001	01000010	01000011

Step 7: The binary values are converted to decimal.

G	U	A	R	D
86	72	70	88	85
72	76	81	73	82
85	80	68	81	76
82	81	65	66	67

Step 8: The decimal values are converted to letters from ASCII Table.

G	U	A	R	D
V	H	F	X	U
H	L	Q	I	R
U	P	D	Q	L
R	Q	A	B	C

Step 9: The letters are substituted by shifting each letter back by 3 positions.

G	U	A	R	D
S	E	C	U	R
E	I	N	F	O
R	M	A	T	I
O	N	X	Y	Z

Step 10: Plain text is obtained by reading the letters from rows to rows.

Plain text is SECURE INFORMATION

4.3 Case 3

Given Text: HELLO WORLD

Keyword: JAVA

Key: 20

Step 1: The Matrix is formed according to the keyword “JAVA,” and the plain text is written after the keyword. The plain text is written from the first row. An extra empty space is filled by writing “A,B.”

J	A	V	A
H	E	L	L
O	W	O	R
L	D	A	B

Step 2: Each letter is substituted by shifting 3 positions (example: H= K, E = H, L = O and so on).

J	A	V	A
K	H	O	O
R	Z	R	U
O	G	D	E

Step 3: The substituted letters are then converted to decimal using the ASCII Table.

J	A	V	A
75	72	79	79
82	90	82	85
79	71	68	69

Step 4: The decimal values are converted to binary.

J	A	V	A
01001011	01001000	01001111	01001111
01010010	01011010	01010010	01010101
01001111	01000111	01000100	01000101

Step 5: The key provided, 20 is converted to decimal.

K = 00010100

Step 6: XOR operation is performed with the key '00010100' and the binary numbers obtained from step 4.

J	A	V	A
01011111	01011100	01011011	01011011
01000110	01001110	01000110	01000001
01011011	01010011	01010000	01010001

Step 7: A left shifts by 2 (LS-2) position is performed with XOR result.

J	A	V	A
01111101	01110001	01101101	01101101
00011001	00111001	00011001	00000101
01101101	01001101	01000001	01000101

Step 8: The binary values obtained from LS-2 is converted to decimal.

J	A	V	A
125	113	109	109
25	57	25	5
109	77	65	69

Step 9: The decimal values are converted to letters using ASCII Table.

J	A	V	A
}	q	m	m
EM	9	EM	ENQ
m	M	A	E

Step 10: The cipher text is written by reading the letters of columns from back to front and from bottom to top, adding # after every encrypted letter.

Cipher text is E#ENQ#m #A#EM#m #M#9#q #m#EM#}

For Decryption

Step 1: Removing # after each letter letters in the ciphertext

E ENQ m A EM m M 9 q m EM }

Step 2: The matrix is made by first counting the letters, words and symbol from the cipher text and dividing the keyword.

12/4 = 3

3 columns are made, and 4 rows are made from the keyword JAVA.

The cipher text is arranged by write the letters starting from the column A from bottom to top.

J	**A**	**V**	**A**
}	q	m	m
EM	9	EM	ENQ
m	M	A	E

Step 3: The letters are converted to decimal using the ASCII Table.

J	**A**	**V**	**A**
125	113	109	109
25	57	25	5
109	77	65	69

Step 4: The decimal values are converted to binary.

J	**A**	**V**	**A**
01111101	01110001	01101101	01101101
00011001	00111001	00011001	00000101
01101101	01001101	01000001	01000101

Step 5: A left by 6 (LS-6) is performed to the binary value.

J	A	V	A
01011111	01011100	01011011	01011011
01000110	01001110	01000110	01000001
01011011	01010011	01010000	01010001

Step 6: XOR operation is performed with the key 20 converted to '00010100' and the binary numbers obtained from step 5.

J	A	V	A
01001011	01001000	01001111	01001111
01010010	01011010	01010010	01010101
01001111	01000111	01000100	01000101

Step 7: The binary values are converted to decimal.

J	**A**	**V**	**A**
75	72	79	79
82	90	82	85
79	71	68	69

Step 8: The decimal values are converted to letters from ASCII Table.

J	**A**	**V**	**A**
K	H	O	O
R	Z	R	U
O	G	D	E

Step 9: The letters are substituted by shifting each letter back by 3 positions.

J	**A**	**V**	**A**
H	E	L	L
O	W	O	R
L	D	A	B

Step 10: Plain text is obtained by reading the letters from rows to rows.

Plain text is HELLO WORLD

4.4 Case 4

Given Text: ALGORITHM

Keyword: KEY

Key: 20

Step 1: The Matrix is formed according to the keyword “KEY,” and the plain text is written after the keyword. The plain text is written from the first row.

K	E	Y
A	L	G
O	R	I
T	H	M

Step 2: Each letter is substituted by shifting 3 positions (example: A = D, L = O, G = J and so on).

K	E	Y
D	O	J
R	U	L
W	K	P

Step 3: The substituted letters are then converted to decimal using the ASCII Table.

K	E	Y
68	79	74
82	85	76
87	75	80

Step 4: The decimal values are converted to binary.

K	E	Y
01000100	01001111	01001010
01010010	01010101	01001100
01010111	01001011	01010000

Step 5: The key provided, 30 is converted to decimal.

K = 00010100

Step 6: XOR operation is performed with the key '00010100' and the binary numbers obtained from step 4.

K	E	Y
01011010	01010001	01010100
01001100	01001011	01010010
01001001	01010101	01001110

Step 7: A left shifts by 2 (LS-2) position is performed with XOR result.

K	E	Y
01101001	01000101	01010001
00110001	00101101	01001001
00100101	01010101	00111001

Step 8: The binary values obtained from LS-2 is converted to decimal.

K	E	Y
105	69	81
49	45	73
37	85	57

Step 9: The decimal values are converted to letters using ASCII Table.

K	E	Y
i	E	Q
1	-	I
%	U	9

Step 10: The cipher text is written by reading the letters of columns from back to front and from bottom to top, adding # after every encrypted letter.

Cipher text is 9#I#Q #U#-#E #%#1#i

For Decryption

Step 1: Removing # after each letter letters in the ciphertext.

9 I Q U - E % 1 i

Step 2: The matrix is made by first counting the letters, words and symbol from the cipher text and dividing the keyword.

9/3 = 3

3 columns are made, and 3 rows are made from the keyword KEY.

The cipher text is arranged by write the letters starting from the column Y from bottom to top.

K	E	Y
i	E	Q
1	-	I
%	U	9

Step 3: The letters are converted to decimal using the ASCII Table.

K	E	Y
105	69	81
49	45	73
37	85	57

Step 4: The decimal values are converted to binary.

K	E	Y
01101001	01000101	01010001
00110001	00101101	01001001
00100101	01010101	00111001

Step 5: A left by 6 (LS-6) is performed to the binary value.

K	E	Y
01011010	01010001	01010100
01001100	01001011	01010010
01001001	01010101	01001110

Step 6: XOR operation is performed with the key 30 converted to '00010100' and the binary numbers obtained from step 5.

K	E	Y
01000100	01001111	01001010
01010010	01010101	01001100
01010111	01001011	01010000

Step 7: The binary values are converted to decimal.

K	E	Y
68	79	74
82	85	76
87	75	80

Step 8: The decimal values are converted to letters from ASCII Table.

K	**E**	**Y**
D	O	J
R	U	L
W	K	P

Step 9: The letters are substituted by shifting each letter back by 3 positions.

K	**E**	**Y**
A	L	G
O	R	I
T	H	M

Step 10: Plain text is obtained by reading the letters from rows to rows.

Plain text is ALGORITHM

4.5 Case 5

Given Text: MOUNTAIN PEAK

Keyword: ASCEND

Key: 20

Step 1: The Matrix is formed according to the keyword “ASCEND,” and the plain text is written after the keyword. The plain text is written from the first row.

A	S	C	E	N	D
M	O	U	N	T	A
I	N	P	E	A	K

Step 2: Each letter is substituted by shifting 3 positions (example: M= P, O = R, U = X and so on).

A	S	C	E	N	D
P	R	X	Q	W	D
L	Q	S	H	D	N

Step 3: The substituted letters are then converted to decimal using the ASCII Table.

A	S	C	E	N	D
80	82	88	81	87	68
76	81	83	72	68	78

Step 4: The decimal values are converted to binary.

A	S	C	E	N	D
01010000	01010010	01011000	01010001	01010111	01000100
01001100	01010001	01010011	01001000	01000100	01001110

Step 5: The key provided, 135 is converted to decimal.

K = 10000111

Step 6: XOR operation is performed with the key '10000111' and the binary numbers obtained from step 4.

A	S	C	E	N	D
11010111	11010101	11011111	11010110	11010000	11000011
11001011	11010110	11010100	11001111	11000011	11001001

Step 7: A left shifts by 2 (LS-2) position is performed with XOR result.

A	S	C	E	N	D
01011111	01010111	01111111	01011011	01000011	00001111
00101111	01011011	01010011	00111111	00001111	00100111

Step 8: The binary values obtained from LS-2 is converted to decimal.

A	S	C	E	N	D
47	43	127	91	67	15
47	91	83	63	15	39

Step 9: The decimal values are converted to letters using ASCII Table.

A	S	C	E	N	D
_	+	DEL	[	(	SI
/	[	S	?	SI	’

Step 10: The cipher text is written by reading the letters of columns from back to front and from bottom to top, adding # after every encrypted letter.

Cipher text is ’#SI   #SI#(#?#[#S#DEL   #[#+   #/#_

For Decryption

Step 1: Removing # after each letter letters in the ciphertext.

- ’ SI   SI (? [S DEL   [+   / _

Step 2: The matrix is made by first counting the letters, words and symbol from the cipher text and dividing the keyword.

12/6 = 2

2 columns are made, and 6 rows are made from the keyword ASCEND.

The cipher text is arranged by write the letters starting from the column D from bottom to top

A	S	C	E	N	D
_	+	DEL	[	(	SI
/	[	S	?	SI	’

Step 3: The letters are converted to decimal using the ASCII Table.

A	S	C	E	N	D
47	43	127	91	67	15
47	91	83	63	15	39

Step 4: The decimal values are converted to binary.

A	S	C	E	N	D
01011111	01010111	01111111	01011011	01000011	00001111
00101111	01011011	01010011	00111111	00001111	00100111

Step 5: A left by 6 (LS-6) is performed to the binary value.

A	S	C	E	N	D
11010111	11010101	11011111	11010110	11010000	11000011
11001011	11010110	11010100	11001111	11000011	11001001

Step 6: XOR operation is performed with the key 135 converted to '10000111' and the binary numbers obtained from step 5.

A	S	C	E	N	D
01010000	01010010	01011000	01010001	01010111	01000100
01001100	01010001	01010011	01001000	01000100	01001110

Step 7: The binary values are converted to decimal.

A	S	C	E	N	D
80	82	88	81	87	68
76	81	83	72	68	78

Step 8: The decimal values are converted to letters from ASCII Table.

A	S	C	E	N	D
P	R	X	Q	W	D
L	Q	S	H	D	N

Step 9: The letters are substituted by shifting each letter back by 3 positions.

A	S	C	E	N	D
M	O	U	N	T	A
I	N	P	E	A	K

Step 10: Plain text is obtained by reading the letters from rows to rows.

Plain text: MOUNTIAN PEAK

5. Strength and Weakness of Matrix Shift Transposition

4.1 Strengths

I. To provide a stronger protection against popular cryptographic attacks, the algorithm combines numerous layers of encryption, such as XOR operations, logical shifts, and dynamic replacement.

II. Without knowledge of the exact technique, attackers would find it difficult to decipher the encrypted message due to the multi-step procedure involving multiple mathematical operations.

III. The algorithm's ability to modify key lengths makes it possible to adjust to various security scenarios and requirements.

IV. The algorithm demonstrates enhanced resistance to known-plaintext assaults, frequency analysis, and other cryptanalysis techniques by mitigating vulnerabilities seen in traditional transposition ciphers.

V. Due to its versatility, it can be used in a wide range of cryptographic applications, from data security across several domains to secure communication.

4.2 Weakness

I. Although complexity has its benefits, users who are not familiar with the algorithm may find it difficult to understand.

II. Key management can be complicated by using a fixed key, especially when frequent key changes are required for security purposes.

III. The multi-step processes could cause scalability issues, which would affect performance in scenarios with large demand.

IV. During the encryption and decryption procedures, cost may be introduced by the insertion of symbols and dynamic letter substitution.

V. In some cases, particularly those with limited resources or real-time processing requirements, the algorithm's complexity and resource requirements may make it less useful.

4.3 Application area

The newly developed cryptographic technique may find use in the following situations when data security is essential:

i. The algorithm can be used by sectors that depend on intellectual property, such software development or creative content creation, to safeguard confidential data and stop illegal access or piracy.

ii. The technique can be used to encrypt medical records, ensuring the privacy and accuracy of patient data. This is especially crucial for adhering to laws protecting patient information.

iii. The algorithm can find application in developing secure communication protocols for various domains, including military, government, and private sectors It can be used for protecting sensitive data while it is being transmitted because of its strong encryption and decryption mechanisms.

6. Conclusion

In conclusion, this coursework has provided a thorough examination of information security concepts, with a focus on cryptography and the CIA triad. The components of the CIA triad of confidentiality, integrity, and availability were explained in detail, highlighting their functions in protecting data. The importance of cryptography for information security was covered, along with important terms, historical background, and the differences between symmetric and asymmetric cryptography.

The workings and historical significance of the classical columnar transposition cipher is also mentioned in this coursework. Although there are benefits like better letter mixing and increased security, there are also drawbacks, such as frequency analysis susceptibility. The in-depth study of this traditional cipher prepared the way for the study of new cryptographic solutions and established the foundation for understanding its limitations.

The report further introduced the Matrix Shift Transposition (MST) cipher as a newly developed algorithm that addresses vulnerabilities in traditional ciphers. The new algorithm utilizes dynamic shifting, substitution techniques, ASCII, XOR, and logical shift operations for better cryptographic strength. The multi-step process that is described in the decryption and encryption methods increases complexity and strengthens security against many types of attacks.

Multi-layered encryption, attack resistance, adaptability, and versatility are among MST's strong points. On the other hand, acknowledged shortcomings include resource requirements, scalability concerns, complexity for users, and major management challenges. Applications for MST include secure communication protocols across a variety of industries, medical data encryption, and intellectual property protection. Because of its strong mechanisms, the algorithm can be used to protect sensitive data in a variety of situations.

The importance of information security has increased as a result of this practical experience creating a new cryptographic algorithm, which has also given me valuable knowledge about the complexities of algorithm design, implementation, and practical applications. I have acquired both theoretical knowledge and practical experience in the creation and evaluation of cryptographic algorithms because of this coursework. This learning journey has equipped me with a solid foundation in information security, which also gives me a framework to deal with the always-changing difficulties associated with digital security.

References

Fortinet, 2023. *What is the CIA Triad and Why is it important?.* [Online]
Available at: https://www.fortinet.com/resources/cyberglossary/cia-triad
[Accessed 26 December 2023].

GeeksforGeeks, 2021. *Simplified Data Encryption Standard Key Generation.* [Online]
Available at: https://www.geeksforgeeks.org/simplified-data-encryption-standard-key-generation/
[Accessed 4 January 2024].

IBM, 2023. *What is IT Security?.* [Online]
Available at: https://www.ibm.com/topics/it-security
[Accessed 26 December 2023].

Agler, D. W., 2023. *Columnar Transposition Cipher: An Introduction.* [Online]
Available at: https://davidagler.com/static/f/cryptography/columnar_cipher.pdf
[Accessed 29 December 2023].

ARNAUD, 2023. *Symmetric vs Asymmetric Encryption: What's the difference?.* [Online]
Available at: https://blog.mailfence.com/symmetric-vs-asymmetric-encryption/
[Accessed 29 December 2023].

Collins English Dictionary, 2023. *SECURITY definition and meaning.* [Online]
Available at: https://www.collinsdictionary.com/dictionary/english/security
[Accessed 26 December 2023].

Crypto-IT, 2020. *Columnar Transposition | Transposition Ciphers.* [Online]
Available at: https://www.crypto-it.net/eng/simple/columnar-transposition.html
[Accessed 30 December 2023].

Fortinet, 2023. *What is Encryption? Definition, Types & Benefits.* [Online]
Available at: What is Encryption? Definition, Types & Benefits | Fortinet.
[Accessed 29 December 2023].

Fruhlinger, J., 2020. *The CIA triad: Definition, components and examples.* [Online]
Available at: https://www.csoonline.com/article/568917/the-cia-triad-definition-components-and-examples.html
[Accessed 26 December 2023].

Fruhlinger, J., 2022. *What is cryptography? How algorithms keep information secret and safe.* [Online]
Available at: https://www.csoonline.com/article/569921/what-is-cryptography-how-algorithms-keep-information-secret-and-safe.html
[Accessed 28 December 2023].

GeeksforGeeks, 2023. *CIA Triad.* [Online]
Available at: https://www.geeksforgeeks.org/the-cia-triad-in-cryptography/
[Accessed 26 December 2023].

GeeksforGeeks, 2023. *Columnar Transposition Cipher.* [Online]
Available at: https://www.geeksforgeeks.org/columnar-transposition-cipher/
[Accessed 30 December 2023].

GeeksforGeeks, 2023. *Substitution Cipher.* [Online]
Available at: https://www.geeksforgeeks.org/substitution-cipher/
[Accessed 10 January 2024].

George Lasry, N. K. &. A. W., 2016. *Cryptanalysis of columnar transposition cipher with long keys: Cryptologia: Vol 40, No 4.* [Online]
Available at: https://www.tandfonline.com/doi/full/10.1080/01611194.2015.1087074
[Accessed 29 December 2023].

Irwin, L., 2023. *What Is the CIA Triad and Why Is It Important?.* [Online]
Available at: https://itgovernance.co.uk/blog/what-is-the-cia-triad-and-why-is-it-important
[Accessed 26 December 2023].

Jack, B., 2020. *What Is ASCII Text and How Is It Used?.* [Online]
Available at: https://www.makeuseof.com/what-is-ascii-text/
[Accessed 2 January 2024].

Kaspersky, 2023. *What is Cryptography?.* [Online]
Available at: https://www.kaspersky.com/resource-center/definitions/what-is-cryptography
[Accessed 28 December 2023].

Kate Brush, L. R. M. C., 2021. *What is Asymmetric Cryptography? Definition from SearchSecurity.* [Online]
Available at: https://www.techtarget.com/searchsecurity/definition/asymmetric-cryptography
[Accessed 29 December 2023].

Kester, Q.-A., 2013. *(PDF) A Hybrid Cryptosystem Based On Vigenere Cipher and Columnar Transposition Cipher.* [Online]
Available at:
https://www.researchgate.net/publication/253330353_A_Hybrid_Cryptosystem_Based_On_Vigenere_Cipher_and_Columnar_Transposition_Cipher
[Accessed 1 January 2024].

Loshin, P., 2021. *What is Plaintext? - Definition from SearchSecurity.* [Online]
Available at: https://www.techtarget.com/searchsecurity/definition/plaintext
[Accessed 29 December 2023].

Phemex Academy, 2021. *What Is Symmetric Key Encryption: Advantages and Vulnerabilities.* [Online]
Available at: What Is Symmetric Key Encryption: Advantages and Vulnerabilities -

Phemex Academy.
[Accessed 29 December 2023].

Richards, K., 2021. *What is Cryptography? Definition from SearchSecurity.* [Online]
Available at: https://www.techtarget.com/searchsecurity/definition/cryptography
[Accessed 28 December 2023].

Rosencrance, L., 2020. *What is Ciphertext?.* [Online]
Available at: https://www.techtarget.com/whatis/definition/ciphertext
[Accessed 29 December 2023].

Rouse, M., 2017. *What is a Cryptographic Key? - Definition from Techopedia.* [Online]
Available at: https://www.techopedia.com/definition/24749/cryptographic-key#:~:text=A%20cryptographic%20key%20is%20a%20string%20of%20bits,This%20key%20remains%20private%20and%20ensures%20secure%20communication.
[Accessed 29 December 2023].

Rouse, M., 2023. *What is Decryption? - Definition from Techopedia.* [Online]
Available at:
https://www.techopedia.com/definition/1773/decryption#:~:text=Decryption%20is%20the%20process%20of%20transforming%20data%20that,unreadable%20through%20encryption%20back%20to%20its%20unencrypted%20form.
[Accessed 29 December 2023].

SecurityMadeSimple, 2023. *What are the 3 principles of Information Security?.* [Online]
Available at: https://securitymadesimple.org/cybersecurity-blog/what-are-the-3-principles-of-information-security/
[Accessed 26 December 2023].

Sharma, A. K. A. K. M., 2016. *100-102,Tesma103,IJEAST.pdf.* [Online]
Available at: https://www.ijeast.com/papers/100-102,Tesma103,IJEAST.pdf
[Accessed 2 January 2024].

SSL2BUY, 2023. *Symmetric vs. Asymmetric Encryption - What are differences?.* [Online]
Available at: https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences
[Accessed 29 December 2023].

StudyDriver.com, 2017. *Columnar Transportation - Free Essay Example - 252 Words.* [Online]
Available at: https://studydriver.com/columnar-transportation/
[Accessed 29 December 2023].

Wagner, L., 2020. *Why Is Exclusive or (XOR) Important in Cryptography? | Boot.dev.* [Online]

Available at: https://blog.boot.dev/cryptography/why-xor-in-cryptography/
[Accessed 2 January 2024].

Weng, A., 2023. *Columnar Transposition by Andrew Weng.* [Online]
Available at: https://prezi.com/tzjqqlhkkvxf/columnar-transposition/
[Accessed 30 December 2023].

West, Z., 2022. *ASCII Table: Printable Reference & Guide - αlphαrithms.* [Online]
Available at: https://www.alpharithms.com/ascii-table-512119/
[Accessed 2 January 2024].

Appendices

The use of ASICC Table is inspired by this (Sharma, 2016).

The substitution technique, which was inspired by Kester's method, which involves rearranging characters and using Vigenère cipher elements (Kester, 2013).