Module Code & Module Title

CC5009NI Cyber Security in Computing

Assessment Weightage & Type

40% Individual Coursework 01

Year and Semester

2024 -25 Autumn Semester

Student Name: Prince Bista

London Met ID: 23056188

College ID: NP01NT4S240019

Assignment Due Date: 20 January 2025

Assignment Submission Date: 20 January 2025

Word Count: 5980

I confirm that I understand my coursework needs to be submitted online via My Second Teacher 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.

5% Overall Similarity

Filters

25 Exclusions →

Match Groups | Sources

32 matches found with Turnitin's database

Show Help

32	Not Cited or Quoted	5%
0	Missing Quotations	0%
0	Missing Citation	0%
0	Cited and Quoted	0%

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF FIGURES

ABSTRACT

This documentation takes on the evolution and application of cryptographic techniques, starting with a brief presentation of information security principles like the CIA triad, one of which is the most important, and explores in-depth the main cryptographic concepts as symmetric and asymmetric encryption is. Then, the author illustrates the Caesar cipher as a foundational algorithm, mentioning its positives, negatives as well as its important history. On the other hand, a new algorithm, "PriCipher," proved to be more secure by the introduction of the Caesar cipher, Rail Fence cipher, transposition cipher, and XOR operations. The development of the modified version of the algorithm, encryption, decryption processes, and testing make the equipment work in such a way as to cover the loopholes of the traditional methods. Thus, this exploration of the security protocols is important in cryptography since the academic and associated practical initial knowledge must be combined with the use of reasonable methods for addressing security threats.

1. Introduction

In today's digital world, the effectiveness of security in information systems cannot be overemphasized despite the level of technology developments. The purpose of information security is to protection sensitive data from unauthorized access, utilization, disclosure, destruction, disruption, or modification (Doumenjou, 2022). In the current cyber landscape, organizations should implement the best security measures to protect their data and maintain the operational capabilities. Developing insufficient security protocols may lead to large amounts of money loss, legal problems, and reputation damage.

1.1 Aim and Objectives

The main aim of this report is to choose a cryptographic algorithm and hence modify it with different modification that maybe logical or mathematical. The specific objectives include:

- To provide various types of security solutions and the significance of them as an information system defense.
- To summarize the CIA triad and how the provision of reliable information security is tied to it.
- To break down the intricate points involved with security issues and cryptography.
- To trace the historic events in cryptography and evaluate their relevance to contemporary security protocols.
- To compare symmetric and asymmetric encryption algorithms and elucidate their differences and aspects. (Kime, 2023)

1.2 Types of Security

Physical Security: This deals with the defense of physical assets, such as hardware, facilities, and staff, from physical activities that may either harm it or allow for unauthorized access. For instance, surveillance cameras, access control systems, and environmental controls. (SentinelOne, 2024)

Application Security: This is simply measures followed to bring to light the security issue in app development by identifying, resolving and stopping bugs and vulnerabilities. The methods referred to are the use of secure coding practices, application firewalls, and regular software updates. (GeeksforGeeks, 2019)

Information Security: This refers to the process designed to help in keeping the information from being accessed or disclosed to an unauthorized person. They may use some strategy on data encryption, user authentication, and data loss prevention to ensure information security. (GeeksforGeeks, 2019)

Network Security: The main goal of Network Security is to protect the security, private life, and availability of user's information and data. This includes being cautious about the implementation of safety technology such as firewalls, intrusion detection systems, and method secure networking protocols to lock the doors. (GeeksforGeeks, 2019)

1.3 CIA Triad

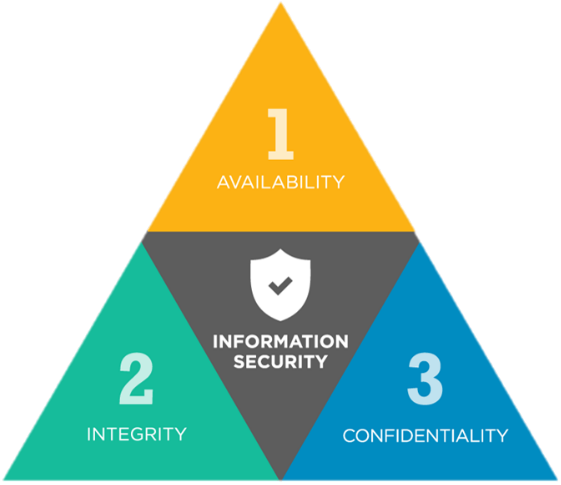


Figure 1: CIA Triad (Irwin, 2023)

The CIA Triad stands for Confidentiality, Integrity, and Availability, which are the three core principles of information security:

Confidentiality is the process that only an authorized person can access the sensitive information. Such as in encrypting the data and using access control is the practice of making the system safe. (Irwin, 2023)

Integrity is the maintaining of the latest data and the consistency of the data. So, that means no changes of data randomly or without permission. Functions like Hashing and checksums are regularly used to ensure data integrity. (Irwin, 2023)

Availability is a guarantee that the useful information will be present at the required time and place to authorized users. This would involve the implementation of redundant systems, regular backups, and the development of disaster recovery plans to ensure uninterrupted access. (GeeksforGeeks, 2019)

1.4 Key Terminology

Encryption: The change of plain text into an unrecognizable form with the help of ciphertext to hide unauthorized usage.

Example: A famous instance of encryption is the Advanced Encryption Standard (AES) that is universally applied for safeguarding sensitive data. For example, when a customer sends their credit card information over the internet, AES encrypts this data so that it stays safe and will be sent securely (Daniel, 2023).

Cipher: An algorithm meant for either encryption or decryption.

Example: The Caesar cipher is a simple substitution cipher for which each letter of the plain text is moved in either the up or down direction by a fixed number of positions along the alphabet. Such as shifting by which the 3 letters are "HELLO" and "KHOOR" encrypted (SentinelOne, 2024).

Key: A string of information that defines the result of a cryptography procedure.

Example: In RSA encryption, the key is a combination of two sections: public (used for encryption) and private (used for decryption). You can publicly email the public key and keep the private key secret the likes of an engagement ring (Arcserve, 2023).

Hash Function: Function that decodes the entered information into a fixed-volume bundle of bytes

Example: The SHA-256 hash function computes a 256-bit hash value as the result of transforming a given input. The use case for blockchain is to check if a document or contract has been tampered with. For example, if you hash the phrase "Hello World," it will generate a unique hash value which represents that specific input. (Sheldon, 2024)

Malware: Malicious software created for the purpose of assaulting or picking flaws in any programmable device or group of networks.

Example: Ransomware, like WannaCry, selects and encrypt files on a victim's computer to appease cybercriminals and obtain the decryption key. Under these circumstances, a malicious software of this kind will not only harm the individual but may also affect a business or a group by making their files inaccessible and thus avoiding or restricting their operation (Kime, 2023)

1.5 History of Cryptography

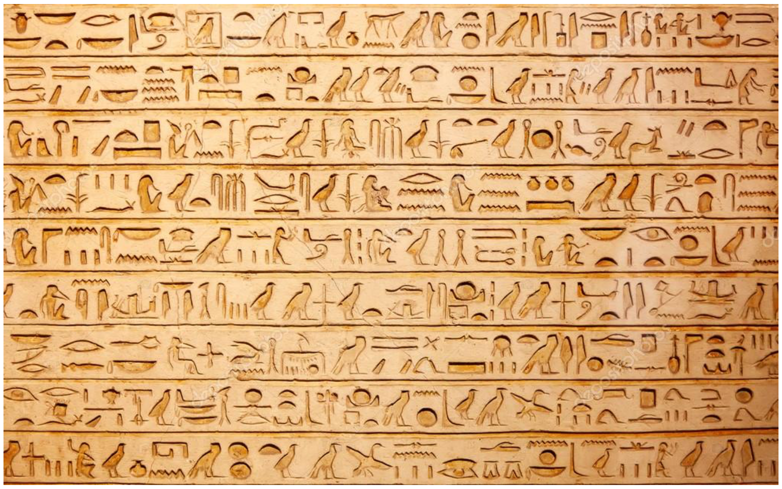


Figure 2: Hieroglyphic Inscription (Doumenjou, 2022)

Cryptography first appeared in ancient times, and the ancient Egyptians were the first to use cryptography around 1900 BCE. back in Egypt, where non-standard hieroglyphs were employed for secret communication. The Greeks and Romans further developed cryptographic techniques; most notably, the Caesar cipher developed around 100 BCE, which implemented a single substitution technique. Stemming from the Middle Ages was a period during which pivotal advances were made by key figures such as Leon Battista Alberti, who created the invention of the polyalphabetic cipher in the 15th century. Consequently, the Vigenère cipher in the 16th century was a revolutionary development for the cryptography field. During the World Wars, the use of cryptography technology by the military grew considerably, most notably with the Enigma machine - a German encryption machine during World War II that was broken by Allied cryptanalysts, most notably, Alan Turing (Thales Group, 2023).

From the 20th century, cryptography enters its current era with the onset of the electronic computer. In the 1970s IBM was the one that launched the Data Encryption Standard (DES), the federal government of the United States adopted it as the standard. At this time, there was also the beginning of public key cryptography which was introduced through the Diffie-Hellman key exchange model, RSA encryption algorithm which both facilitated secure communication by allowing two parties to exchange information without the fear of sharing their private keys. DES was finally replaced by the Advanced Encryption Standard (AES) in 2001 owing to the concern of its security problem as the computer calculating power made incredible progress. The evolving cryptography field is still there nowadays with the quantum computer coming and limited encryption methods being created to protect the digital information against more and more difficult threats (Sidhpurwala, 2023).

1.6 Symmetric Encryption

Symmetric encryption is the encryption of a data message using one cipher as the basis for both the encryption and decryption processes. Efficiently used for large chunks of data enabled uploading but requiring the safe managing of the key (P., 2021).

Stream Ciphers: Data is encoded as one bit or one byte in these systems. For instance, RC4.

Block Ciphers: These are the ones that encrypt data of one size so that it cannot be changed (e.g., 64-bit or 128-bit). DES is a block cipher that is commonly known.

I. Data Encryption Standard (DES)

The DES algorithm functions with a 56-bit key for the encryption process of 64-bit data. This is achieved via the execution of multiple permutation and substitution activities. Over the course of several decades, this method was widely adopted even though the greater number of hacker showed the world its weakness.

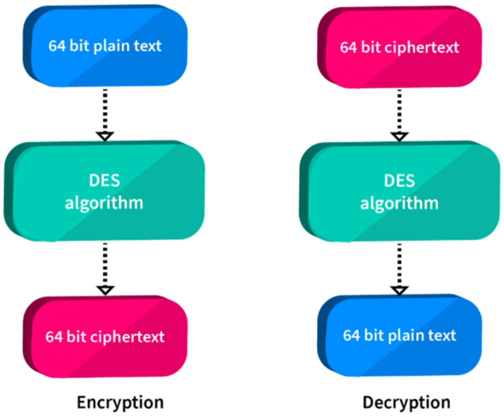


Figure 3: DES Algorithm (Koneti, 2021)

II. Advanced Encryption Standard (AES)

The DES encryption technique was a standard one for over two decades when its enhancing security features were taken over by the block cipher called AES. The AES algorithm can come with three key sizes (128, 192, or 256 bits) and operates using 128-bit blocks. AES is known to be secure against all feasible attacks, hence it is found being used in many software tools that are running on different servers.

1.7 Asymmetric Encryption

In asymmetric Encryption, both receiver and sender have two keys (public key and private key) that are connected and differently operated. The private key is used for decryption the data supplied by the public key. The private key is made exclusive as indicated by its names, so only the verifier who has the allowed person can decrypt the message.

2. Introduction to Caesar Cipher

Caesar Cipher is chosen for this coursework because of its simplicity, historical significance, and its significance as a foundation in cryptography. Being one of the oldest used cryptographic tools, it challenges cryptography on the ground that the learners should know the very basics of cryptography, such as substitution and transposition methods to solve it successfully.Its simplicity makes it possible for the lesser learned students to understand the major concepts without even going to the math level that is required for it, thus forming the perfect base for exploring more advanced algorithms. Click for more details.

2.1 Background

Caesar Cipher is termed after Julius Caesar from ancient rome who use to communicate to his soliders using this method. This cipher operates according to the principle of shifting letters in the alphabet by a fixed number, called the shift value or key. It is positioned against a symmetric cipher since it uses the same key for both encryption and decryption. The method implies replacing every letter of the plaintext with another letter, which is a certain number of places down the alphabet. For instance, with the shift of 3. 'A' now changes to 'D', 'B' now becomes 'E', and so on, wrapping around to 'A' from 'Z' when there is a need to.

2.2 Encryption and Decryption

Encryption algorithm for caesar cipher is :

C = (P+3) MOD 26

Decryption algorithm for Caesar Cipher is :

C = (P-3) MOD 26

where,

P= Plain Text

C= Cipher Text

For Encryption,

C= (P+K) MOD 26

where, K value range from 1-25

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

Table 1: Encryption letters with shift of 3.

The letters from a to z are represented in the illustration above encrypted using the Caesar Shift Cipher technique with a shift of 3. The secret key needed to convert the encrypted text into plain text must be known by the recipient when they get the cipher text.

Example:

Plain text- PRINCEBISTA

Cipher text- SULQFHELVWD

For Decryption,

P= (C - K) MOD 26

Where, K value ranges from 1-25

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

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

Table 2: Decryption letters taking shift of 3.

The letters from a to z are represented in the illustration above decrypted using the Caesar Shift Cipher technique with a shift of 3. The secret key needed to convert the decrypted text into plain text must be known by the recipient when they get the cipher text.

Example:

Cipher text- SULQFHELVWD

Plain text- PRINCEBISTA

2.3 Advantages and Disadvantages of Caesar Cipher

Advantages

- Simplicity and Ease of Implementation
- Low Computational Requirements
- Historical Significance in Cryptography Education
- Basic Form of Encryption for Understanding More Complex Algorithms

Disadvantages

- Vulnerability to Frequency Analysis Attacks
- Limited Keyspace Due to a Small Fixed Shift Range
- Lack of Security for Modern Applications
- Inability to Protect Against Brute-Force Attacks Due to Predictability

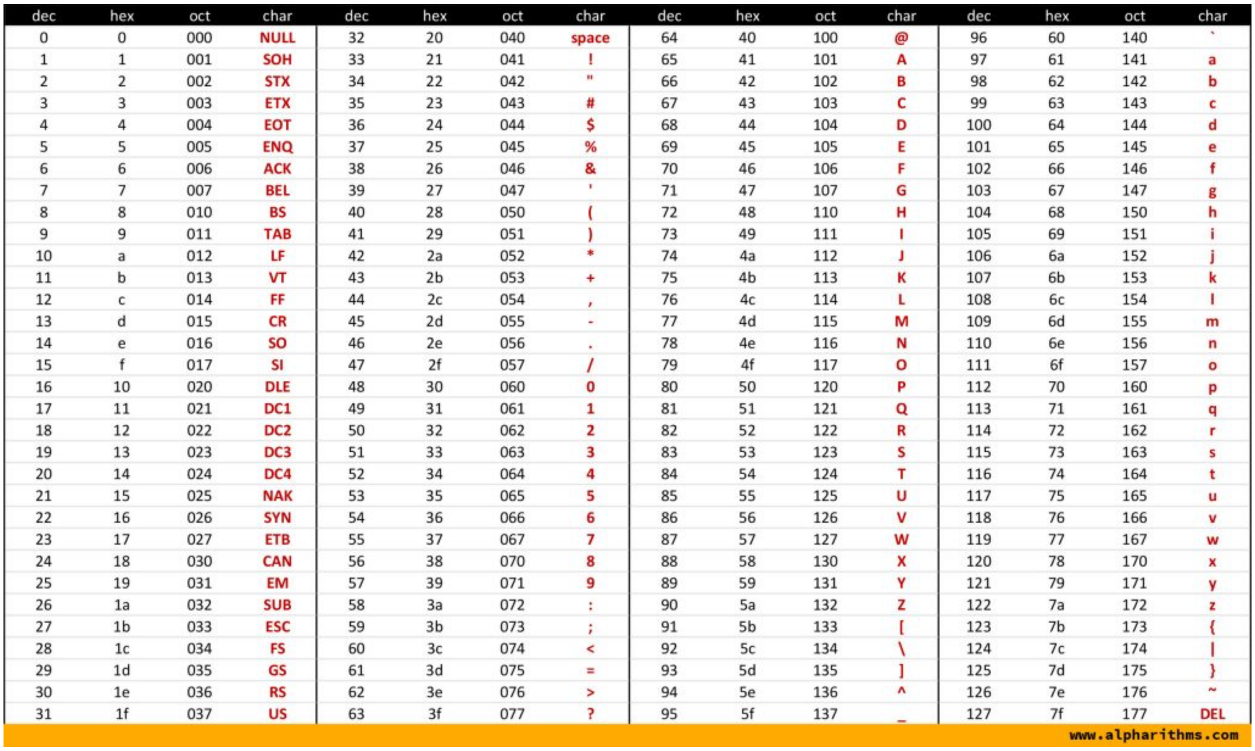
3. Development

The security of the Caesar cipher can be improved by adding several changes that eliminate the fundamental weakness of the system. Our way includes the use of different cryptographic ways to build up stronger encryption.

3.1 Background Information

XOR bitwise operation

The cryptographic technique converts each character in the ciphertext to its ASCII value and uses the key to perform a bitwise XOR operation. The resulting value is changed into a character. For instance, the character is 'A' (ASCII 65), then: 65⨁107=42. The result (42) is transformed back into a character ('*'). Below is the chart for ASCII value:



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, 2020)

Transposition ciphers

- **Rail Fence Cipher:** Rail Fence cipher is a transposition cipher where plaintext is written down as a series of diagonals and then read off as a sequence of rows.

- **Row Transposition Cipher:**This cipher uses are more complex scheme by writing the Plaintext in a rectangle, row by row and read off the message column by column.

3.2 Creation of New Algorithms

The newly created cryptographic algorithm makes use of the Caeser cipher, Rail Fence Cipher and XOR operation. As this is the modified and more secure Cryptographic algorithm than standard caeser cipher, we named it as **PriCipher** where Pri is the initials of the founders name and Cipher as it is a algorithm for cipher**.**

Encryption Algorithm

Step 1: Use Caeser cipher shift by 2. Each letter in the plaintext is shifted by 2 positions in the alphabet. For instance, 'A' becomes 'C'.

Step 2: Rail Fence Cipher: Characters are written diagonally in a zigzag pattern across a specific number of rails and read row-by-row.

Step 3: Transposition Cipher (Key 42153): The ciphertext is reordered according to the numerical key. For instance, a 5-character block is rearranged based on the key's order.

Step 4: Using XOR using key 107.

For example:

Plain text = ABORTTHEMISSION

Step 1: Use caeser cipher shift by 2.

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

Table 3: Encryption letters with shift of 3.

C = (P+2) MOD 26

Where, C= cipher text index and P = Plain text index

Cipher text = **CDQTVVJGOKUUKQP**

Step 2: Rail Fence Cipher.

Write diagonally zigzag and read row-by-row.

C	Q	V	J	O	U	K	P
D	T	V	G	K	U	Q	

Table 4: Rail Fence Table

Cipher Text = **CQVJOUKPDTVGKUQ**

Step 3: Row Transposition Cipher.

Key: **42153**

Key	**4**	**2**	**1**	**5**	**3**
Plain Text	C	Q	V	J	O
	U	K	P	D	T
	V	G	K	U	Q

Table 5: Row transposition table

Cipher Text = **VPKQKGOTQCUVJDU**

Step 4: Using XOR operation.

Cipher Character: V, P, K, Q, K, G, O, T, Q, C, U, V, J, D, U

Cipher Character Decimal: 86, 80, 75, 81, 75, 71, 79, 84, 81, 67, 85, 86, 74, 68, 85

Plain Binary: 01010110, 01010000, 01001011, 01010001, 01001011, 01000111, 01001111, 01010100, 01010001, 01000011, 01010101, 01010110, 01001010, 01000100, 01010101

Key Binary: 01101011 (Applicable for all)

XOR Binary Result: 00111101, 00111011, 00100000, 00111010, 00100000, 00101100, 00100100, 00111111, 00111010, 00101000, 00111110, 00111101, 00100001, 00101111, 00111110

XOR Binary Result in Decimal: 61, 59, 32, 58, 32, 44, 36, 63, 58, 40, 62, 61, 33, 47, 62

Final Encrypted Text Using ASCII Table: **=; : ,$?:(>=!/>**

Decryption Algorithm

Step 1: Reverse XOR operation (Key 107)

Step 2: Reverse Transposition Cipher (Key 42153)

Step 3: Reverse Rail Fence Cipher

Step 4: Reverse Caesar Cipher (Shift by 2)

For example:

Use Reverse XOR operation.

Cipher text: =; : ,$?:(>=!/>

Encrypted Decimal (ASCII): 61, 59, 32, 58, 32, 44, 36, 63, 58, 40, 62, 61, 33, 47, 62

Encrypted Binary (From Decimal): 00111101, 00111011, 00100000, 00111010, 00100000, 00101100, 00100100, 00111111, 00111010, 00101000, 00111110, 00111101, 00100001, 00101111, 00111110

Key Binary (Applicable for all): 01101011

XOR Binary Result: 01010110, 01010000, 01001011, 01010001, 01001011, 01000111, 01001111, 01010100, 01010001, 01000011, 01010101, 01010110, 01001010, 01000100, 01010101

Decrypted Text: VPKQKGOTQCUVJDU

Use Reverse Transposition Cipher.

Cipher text : VPKQKGOTQCUVJDU

Arranging in table with key 42153

Key	**4**	**2**	**1**	**5**	**3**
Plain Text	C	Q	V	J	O
	U	K	P	D	T
	V	G	K	U	Q

Table 6: Row transposition table

Reading column by column : **CQVJOUKPDTVGKUQ**

Use reverse Rail Fence Cipher.

Write row by row and read zigzag diagonally.

C	Q	V	J	O	U	K	P
D	T	V	G	K	U	Q	

Table 7: Rail Fence Table

Encrypted Text: **CDQTVVJGOKUUKQP**

Use reverse caeser cipher shift by 2.

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

Table 8: Ceaser Cipher shift by 2 table

Use Formula,

P = (C-2) MOD 26

Plain Text = **ABORTTHEMISSION**

3.3 Overview of the Modified Cryptographic Algorithm

The cryptographic algorithm recently established aims to combine the Caeser cipher, Row Fence cipher, and Row Transposition cipher and XOR bitwise operation into a single method. The changes are designed to eliminate known vulnerabilities which the traditional Caesar cipher inherits and are risk in security.

Necessity for the modification:

The original Caesar cipher, as its name suggests, is a type of simple substitution cipher that moves letters in the alphabet and encodes by a fixed number. Moreover, the fact that it was an important historical document is considerably overshadowed by the reality that it is now an unsecure protocol associated with the risks of frequency analysis and brute-force attacks. The challenges that need to be dealt with in the process of modification are:

Security Flaw: This makes a person’s use of the Caesar cipher a potential headache for them as it can be easily broken through the trial-error method and other related problems.

Increasing The Degree of Complicatedness: As of today, encryption standards have become more intricate, and hence, new algorithms capable of resisting more vigorous attacks have to combine various techniques to increase formation and security.

3.4 FLOWCHART

Below is the flowchart for the encryption and decryption method for the new cryptographic algorithm “PriCipher”.

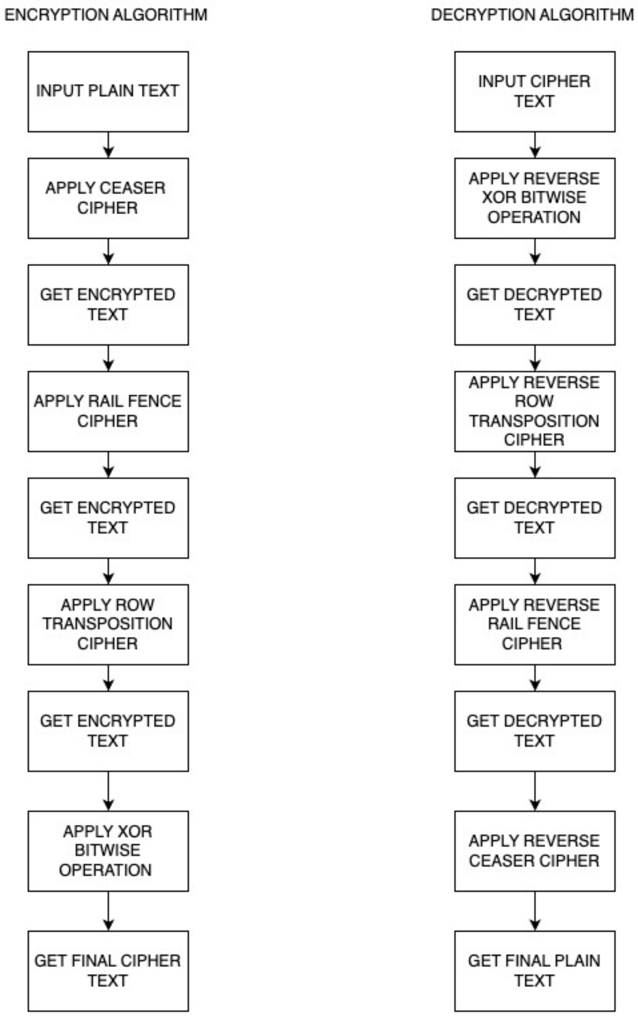


Figure 5: FLOWCHART OF ENCRYPTION AND DECRYPTION PROCESS

4. Testing

Here, we are going to present the algorithm that I created which uses a multi-layered encryption process to improve data security. With Caeser cipher, the total code shifts 2 positions for all the letters in the text, then goes to a Rail Fence cipher, where the characters are arranged in a zigzag pattern across several rows and are read row by row. Next, a transposition cipher is applied to the plaintext to create a cipher text which is then reordered according to the numerical key (42153), contributing to the complexity. The last step is the XOR operation with a key value of 107 being used to code the output, which results in a final encrypted message being thoroughly mixed up and hard to be decoded by unauthorized persons. The combination of these methods shows the effectiveness of layered encryption in protecting confidential documents.

TEST 1

Encryption

Plain text = PRINCEISHERO

Step 1: Use caeser cipher shift by 2.

C = (P+2) MOD 26

Where, C= cipher text index and P = Plain text index

Cipher text = RTKPEGKUJGTQ

Step 2: Rail Fence Cipher.

Write diagonally zigzag and read row-by-row.

R	K	E	K	J	T
T	P	G	U	G	Q

Table 9: Rail fence table for test 1

Cipher Text = RKEKJTTPGUGQ

Step 3: Row Transposition Cipher.

Key: 42153

Key	4	2	1	5	3
Plain Text	R	K	E	K	J
	T	T	P	G	U
	G	Q			

Table 10: Row transposition table for test 1

Cipher Text = RTGKTQEPKGJU

Step 4: Using XOR operation.

Cipher Character: R, T, G, K, T, Q, E, P, K, G, J, U

Cipher Character Decimal: 82, 84, 71, 75, 84, 81, 69, 80, 75, 71, 74, 85

Plain Binary: 01010010, 01010100, 01000111, 01001011, 01010100, 01010001, 01000101, 01010000, 01001011, 01000111, 01001010, 01010101

Key Binary: 01101011 (Applicable for all)

XOR Binary Result: 00111001, 00111111, 00101100, 00100000, 00111111, 00111010, 00101110, 00111011, 00100000, 00101100, 00100001, 00111110

XOR Binary Result in Decimal: 57, 63, 44, 32, 63, 58, 46, 59, 32, 44, 33, 62

Final Encrypted Text Using ASCII Table: 9?, ?:.; ,!>

Decryption

Cipher text: 9?, ?:.; ,!>

Step 1: Using Reverse XOR operation

Encrypted Decimal (ASCII Values): 57, 63, 44, 32, 63, 58, 46, 59, 32, 44, 33, 62

Encrypted Binary (From Decimal): 00111001, 00111111, 00101100, 00100000, 00111111, 00111010, 00101110, 00111011, 00100000, 00101100, 00100001, 00111110

Key Binary (Applicable for all): 01101011

XOR Binary Result: 01010010, 01010100, 01000111, 01001011, 01010100, 01010001, 01000101, 01010000, 01001011, 01000111, 01001010, 01010101

Decrypted Text: RTGKTQEPKGJU

Step 2: Use Reverse Transposition Cipher.

Cipher text : RTGKTQEPKGJU

Arranging in table with key 42153

Key	4	2	1	5	3
Plain Text	R	K	E	K	J
	T	T	P	G	U
	G	Q			

Table 11: Row transposition table for test 1

Reading column by column : RKEKJTTPGUGQ

Step 3: Use reverse Rail Fence Cipher.

Write row by row and read zigzag diagonally.

R	K	E	K	J	T
T	P	G	U	G	Q

Table 12: Rail Fence table for test 1

Encrypted Text: **RTKPEGKUJGTQ**

Step 4: Use reverse caeser cipher shift by 2.

Use Formula,

P = (C-2) MOD 26

Plain Text = **PRINCEISHERO**

TEST NO	1
OBJECTIVE	To test the encryption and decryption of text "PRINCEISHERO" using newly discovered Pricipher.
ACTION	• For encryption: The plain text was applied Caeser cipher shift by 2 following with rail fence and row transposition cipher with key 42153 and finally applied XOR bitwise operation. • For decryption: The encrypted text was applied reverse XOR bitwise operation following with row transposition with key 42153 and rail fence cipher and then finally applied caeser cipher shift by 2.
CONCLUSION	Test was encrypted and decrypted successfully.

Table 13: TEST TABLE 1

TEST 2

Encryption

Plain text = STOP_SHOOTING

Step 1: Use caeser cipher shift by 2.

C = (P+2) MOD 26

Where, C= cipher text index and P = Plain text index

Cipher text = UVQR_UJQQVKPI

Step 2: Rail Fence Cipher.

Write diagonally zigzag and read row-by-row.

U	Q		J	Q	K	I
V	R	U	Q	V	P	

Table 14: Rail fence table for test 2

Cipher Text = UQ_JQKIVRUQVP

Step 3: Row Transposition Cipher.

Key: 42153

Key	4	2	1	5	3
Plain Text	U	Q	_	J	Q
	K	I	V	R	U
	Q	V	P		

Table 15: Row transpositon table for test 2

Cipher Text = _VPQIVQUUKQJR

Step 4: Using XOR operation.

Cipher Character: _, V, P, Q, I, V, Q, U, U, K, Q, J, R

Cipher Character Decimal: 95, 86, 80, 81, 73, 86, 81, 85, 85, 75, 81, 74, 82

Plain Binary: 01011111, 01010110, 01010000, 01010001, 01001001, 01010110, 01010001, 01010101, 01010101, 01001011, 01010001, 01001010, 01010010

Key Binary: 01101011 (Applicable for all)

XOR Binary Result: 00110100, 00111101, 00111011, 00111010, 00100010, 00111101, 00111010, 00111110, 00111110, 00100000, 00111010, 00100001, 00111001

XOR Binary Result in Decimal: 52, 61, 59, 58, 34, 61, 58, 62, 62, 32, 58, 33, 57

Final Encrypted Text Using ASCII Table: 4=;:"=:>> :!9

Decryption

Cipher text: 4=;:"=:>> :!9

Step 1: Using Reverse XOR operation

Cipher Character: 4, =, ;, :, ", =, :, >, >, ** **, :, !, 9

Cipher Character Decimal: 52, 61, 59, 58, 34, 61, 58, 62, 62, 32, 58, 33, 57

Encrypted Binary (From Decimal): 00110100, 00111101, 00111011, 00111010, 00100010, 00111101, 00111010, 00111110, 00111110, 00100000, 00111010, 00100001, 00111001

Key Binary: 01101011 (Applicable for all)

XOR Binary Result: 01011111, 01010110, 01010000, 01010001, 01001001, 01010110, 01010001, 01010101, 01010101, 01001011, 01010001, 01001010, 01010010

XOR Binary Result in Decimal: 95, 86, 80, 81, 73, 86, 81, 85, 85, 75, 81, 74, 82

Decrypted Text: _VPQIVQUUKQJR

Step 2: Use Reverse Transposition Cipher.

Arranging in table with key 42153

Key	4	2	1	5	3
Plain Text	U	Q	_	J	Q
	K	I	V	R	U
	Q	V	P		

Table 16: Row transposition table for test 2

Reading column by column : UQ_JQKIVRUQVP

Step 3: Use reverse Rail Fence Cipher.

Write row by row and read zigzag diagonally.

R	K	E	K	J	T
T	P	G	U	G	Q

Table 17: Rail fence table for test 2

Encrypted Text: UVQR_UJQQVKPI

Step 4: Use reverse caeser cipher shift by 2.

Use Formula,

P = (C-2) MOD 26

Plain Text = STOP_SHOOTING

TEST NO	2
OBJECTIVE	To test the encryption and decryption of text "STOP_SHOOTING" using newly discovered Pricipher.
ACTION	• For encryption: The plain text was applied Caeser cipher shift by 2 following with rail fence and row transposition cipher with key 42153 and finally applied XOR bitwise operation. • For decryption: The encrypted text was applied reverse XOR bitwise operation following with row transposition with key 42153 and rail fence cipher and then finally applied caeser cipher shift by 2.
CONCLUSION	Test was encrypted and decrypted successfully.

Table 18: TEST TABLE 2

TEST 3

Encryption

Plain text = @FACEBOOK.COM

Step 1: Use caeser cipher shift by 2.

C = (P+2) MOD 26

Where, C= cipher text index and P = Plain text index

Cipher text = @HCEGDQQM.EQO

Step 2: Rail Fence Cipher.

Write diagonally zigzag and read row-by-row.

@	C	G	Q	M	E	O
H	E	D	Q	.	Q	

Table 19: Rail fence table for test 3

Cipher Text = @CGQMEOHEDQ.Q

Step 3: Row Transposition Cipher.

Key: 42153

Key	4	2	1	5	3
Plain Text	@	C	G	Q	M
	E	O	H	E	D
	Q	.	Q		

Table 20: Row transposition table for test 3

Cipher Text = GHQCO.MD@EQQE

Step 4: Using XOR operation.

Cipher Character: G, H, Q, C, O, ., M, D, @, E, Q, Q, E

Cipher Character Decimal: 71, 72, 81, 67, 79, 46, 77, 68, 64, 69, 81, 81, 69

Plain Binary: 01000111, 01001000, 01010001, 01000011, 01001111, 00101110, 01001101, 01000100, 01000000, 01000101, 01010001, 01010001, 01000101

Key Binary: 01101011 (Applicable for all)

XOR Binary Result: 00101100, 00100011, 00111010, 00101000, 00100100, 01000101, 00100110, 00101111, 00101011, 00101110, 00111010, 00111010, 00101110

XOR Binary Result in Decimal: 44, 35, 58, 40, 36, 69, 38, 47, 43, 46, 58, 58, 46

Final Encrypted Text Using ASCII Table: ,#:($E&/+.::.

Decryption

Cipher text: ,#:($E&/+.::.

Step 1: Using Reverse XOR operation

Cipher Text: ,, #, :, (, $, E, &, /, +, ., :, :, .

Encrypted Decimal (ASCII Values): 44, 35, 58, 40, 36, 69, 38, 47, 43, 46, 58, 58, 46

Encrypted Binary (From Decimal): 00101100, 00100011, 00111010, 00101000, 00100100, 01000101, 00100110, 00101111, 00101011, 00101110, 00111010, 00111010, 00101110

Key Binary (Applicable for all): 01101011

XOR Binary Result: 01000111, 01001000, 01010001, 01000011, 01001111, 00101110, 01001101, 01000100, 01000000, 01000101, 01010001, 01010001, 01000101

XOR Binary Result in Decimal: 71, 72, 81, 67, 79, 46, 77, 68, 64, 69, 81, 81, 69

Decrypted Text: GHQCO.MD@EQQE

Step 2: Use Reverse Transposition Cipher.

Arranging in table with key 42153

Key	4	2	1	5	3
Plain Text	@	C	G	Q	M
	E	O	H	E	D
	Q	.	Q		

Table 21: Row transposition table for test 3

Reading column by column : @CGQMEOHEDQ.Q

Step 3: Use reverse Rail Fence Cipher.

Write row by row and read zigzag diagonally.

@	C	G	Q	M	E	O
H	E	D	Q	.	Q	

Table 22: Rail fence table for test 3

Encrypted Text: @HCEGDQQM.EQO

Step 4: Use reverse caeser cipher shift by 2.

Use Formula,

P = (C-2) MOD 26

Plain Text = @FACEBOOK.COM

TEST NO	3
OBJECTIVE	To test the encryption and decryption of text "@FACEBOOK.COM" using newly discovered Pricipher.
ACTION	• For encryption: The plain text was applied Caeser cipher shift by 2 following with rail fence and row transposition cipher with key 42153 and finally applied XOR bitwise operation. • For decryption: The encrypted text was applied reverse XOR bitwise operation following with row

	transposition with key 42153 and rail fence cipher and then finally applied caeser cipher shift by 2.
CONCLUSION	Test was encrypted and decrypted successfully.

Table 23: TEST TABLE 3

TEST 4

Encryption

Plain text = HELLO@WORLD

Step 1: Use caeser cipher shift by 2.

C = (P+2) MOD 26

Where, C= cipher text index and P = Plain text index

Cipher text = JGNNQ@YQTNF

Step 2: Rail Fence Cipher.

Write diagonally zigzag and read row-by-row.

J	N	Q	Y	T	F	
G	N	@	Q	N		

Table 24: Rail fence table for test 4

Cipher Text = JNQYTFGN@QN

Step 3: Row Transposition Cipher.

Key: 42153

Key	4	2	1	5	3
Plain Text	J	N	Q	Y	T
	F	G	N	@	Q
	N				

Table 25: Row transposition table for test 4

Cipher Text = QNNGTQJFNY@

Step 4: Using XOR operation.

Cipher Character: Q, N, N, G, T, Q, J, F, N, Y, @

Cipher Character Decimal: 81, 78, 78, 71, 84, 81, 74, 70, 78, 89, 64

Plain Binary: 01010001, 01001110, 01001110, 01000111, 01010100, 01010001, 01001010, 01000110, 01001110, 01011001, 01000000

Key Binary: 01101011 (Applicable for all)

XOR Binary Result: 00111010, 00100101, 00100101, 00101100, 00111111, 00111010, 00100001, 00101101, 00100101, 00110010, 00101011

XOR Binary Result in Decimal: 58, 37, 37, 44, 63, 58, 33, 45, 37, 50, 43

Final Encrypted Text Using ASCII Table: **:%%,?:!-%2+**

Decryption

Cipher Text: :, %, %, ,, ?, :, !, -, %, 2, +

Encrypted Decimal (ASCII Values): 58, 37, 37, 44, 63, 58, 33, 45, 37, 50, 43

Encrypted Binary (From Decimal): 00111010, 00100101, 00100101, 00101100, 00111111, 00111010, 00100001, 00101101, 00100101, 00110010, 00101011

Key Binary (Applicable for all): 01101011

XOR Binary Result: 01010001, 01001110, 01001110, 01000111, 01010100, 01010001, 01001010, 01000110, 01001110, 01011001, 01000000

XOR Binary Result in Decimal: 81, 78, 78, 71, 84, 81, 74, 70, 78, 89, 64

Decrypted Text: **QNNGTQJFNY@**

Step 2: Use Reverse Transposition Cipher.

Arranging in table with key 42153

Key	4	2	1	5	3
Plain Text	J	N	Q	Y	T
	F	G	N	@	Q
	N				

Table 26: Row transposition table for test 4

Reading column by column : JNQYTFGN@QN

Step 3: Use reverse Rail Fence Cipher.

Write row by row and read zigzag diagonally.

J	N	Q	Y	T	F	
G	N	@	Q	N		

Table 27: Rail fence table for test 4

Encrypted Text: JGNNQ@YQTNF

Step 4: Use reverse caeser cipher shift by 2.

Use Formula,

P = (C-2) MOD 26

Plain Text = HELLO@WORLD

TEST NO	4
OBJECTIVE	To test the encryption and decryption of text "HELLO@WORLD" using newly discovered Pricipher.
ACTION	• For encryption: The plain text was applied Caeser cipher shift by 2 following with rail fence and row transposition cipher with key 42153 and finally applied XOR bitwise operation. • For decryption: The encrypted text was applied reverse XOR bitwise operation following with row

	transposition with key 42153 and rail fence cipher and then finally applied caeser cipher shift by 2.
CONCLUSION	Test was encrypted and decrypted successfully.

Table 28: TEST TABLE 4

TEST 5

Encryption

Plain text = ENEMIES_AHEAD

Step 1: Use caeser cipher shift by 2.

C = (P+2) MOD 26

Where, C= cipher text index and P = Plain text index

Cipher text = GPGOKGU_CJGCF

Step 2: Rail Fence Cipher.

Write diagonally zigzag and read row-by-row.

G	G	K	U	C	G	F
P	O	G	_	J	C	

Table 29: Rail fence table for test 5

Cipher Text = GGKUCGFPOG_JC

Step 3: Row Transposition Cipher.

Key: 42153

Key	4	2	1	5	3
Plain Text	G	G	K	U	C
	G	F	P	O	G
	_	J	C		

Table 30: Row transposition table for test 5

Cipher Text = KPCGFJCGGG_UO

Step 4: Using XOR operation.

Cipher Character: K, P, C, G, F, J, C, G, G, G, _, U, O

Cipher Character Decimal: 75, 80, 67, 71, 70, 74, 67, 71, 71, 71, 95, 85, 79

Plain Binary: 01001011, 01010000, 01000011, 01000111, 01000110, 01001010, 01000011, 01000111, 01000111, 01000111, 01011111, 01010101, 01001111

Key Binary: 01101011 (Applicable for all)

XOR Binary Result: 00100000, 00111011, 00101000, 00101100, 00101101, 00100001, 00101000, 00101100, 00101100, 00101100, 00110100, 00111110, 00100100

XOR Binary Result in Decimal: 32, 59, 40, 44, 45, 33, 40, 44, 44, 44, 52, 62, 36

Final Encrypted Text Using ASCII Table: ** ;(,-!(,,4>$**

Decryption

Cipher Text: :, ;, (, ,, -, !, (, ,, ,, 4, >, $

Encrypted Decimal (ASCII Values): 58, 59, 40, 44, 45, 33, 40, 44, 44, 52, 62, 36

Encrypted Binary (From Decimal): 00111010, 00111011, 00101000, 00101100, 00101101, 00100001, 00101000, 00101100, 00101100, 00110100, 00111110, 00100100

Key Binary (Applicable for all): 01101011

XOR Binary Result: 01001011, 01010000, 01000011, 01000111, 01000110, 01001010, 01000011, 01000111, 01000111, 01011111, 01010101, 01001111

XOR Binary Result in Decimal: 75, 80, 67, 71, 70, 74, 67, 71, 71, 95, 85, 79

Decrypted Text: **KPCGFJCGGG_UO**

Step 2: Use Reverse Transposition Cipher.

Arranging in table with key 42153

Key	4	2	1	5	3
Plain Text	G	G	K	U	C
	G	F	P	O	G
	_	J	C		

Table 31: Row transposition table for test 5

Reading column by column : GGKUCGFPOG_JC

Step 3: Use reverse Rail Fence Cipher.

Write row by row and read zigzag diagonally.

G	G	K	U	C	G	F
P	O	G	_	J	C	

Table 32: Rail fence table for test 5

Encrypted Text: GPGOKGU_CJGCF

Step 4: Use reverse caeser cipher shift by 2.

P = (C-2) MOD 26

Plain Text = ENEMIES_AHEAD

TEST NO	5
OBJECTIVE	To test the encryption and decryption of text “ENEMIES_AHEAD” using newly discovered Pricipher.
ACTION	• For encryption: The plain text was applied Caeser cipher shift by 2 following with rail fence and row transposition cipher with key 42153 and finally applied XOR bitwise operation. • For decryption: The encrypted text was applied reverse XOR bitwise operation following with row transposition with key 42153 and rail fence cipher and then finally applied caeser cipher shift by 2.
CONCLUSION	Test was encrypted and decrypted successfully.

Table 33: TEST TABLE 5

5. CONCLUSION

The given document is presented with cryptographic techniques that are both historical and modern, namely the methods of securing sensitive information. Initially, a simple Caesar cipher is presented and proves to be an excellent gateway to cryptography. However, its weaknesses indirectly show the importance of the constant development of encryption algorithms to address new threats. "PriCipher," which is an altered algorithm, was grown from a classical and a fresher cryptographic technique by combining various cryptographic techniques thus resulting in both complexity and security.

The PriCipher algorithm strengthens a system against common cryptographic attacks, where Caesar cipher, Rail Fence cipher, transposition cipher, and XOR operations are used in the PriCipher. The detailed mechanism is a general case which demonstrates the idea of the fact that the old ways of doing things might be old, but it is individual works like combining past concepts with the latest ones which produce a very stable digital ecosystem that resists stronger cyber-attacks. Not only does this project reinforce the cryptographic principles in cybersecurity but it also provides an example where creativity could be used as a problem-solving approach for a real security challenge. According to the trials and conclusions, the modified algorithm has been demonstrated as being a versatile tool for ensuring the integrity and confidentiality of data.

6. BIBLIOGRAPHY

Daniel, B. (2023, 9 25). *Symmetric vs. Asymmetric Encryption: What's the Difference?* Retrieved from Trenton Systems | Customer-Driven & USA-Made Computing Solutions: https://www.trentonsystems.com/en-au/blog/symmetric-vs-asymmetric-encryption

SentinelOne. (2024, 08 27). *What is Ciphertext? Types and Best Practices*. Retrieved from SentinelOne: https://www.sentinelone.com/cybersecurity-101/cybersecurity/what-is-ciphertext/

Arcserve. (2023, 9 19). *5 Common Encryption Algorithms and the Unbreakables of the Future | Arcserve*. Retrieved from Arcserve: https://www.arcserve.com/blog/5-common-encryption-algorithms-and-unbreakables-future

Sheldon, R. (2024, 2 7). *What is Encryption and How Does it Work? | Definition from TechTarget*. Retrieved from Search Security: https://www.techtarget.com/searchsecurity/definition/encryption

Kime, C. (2023, 12 7). *What Is Encryption? Definition, How it Works, & Examples*. Retrieved from eSecurity Planet: https://www.esecurityplanet.com/networks/encryption/

GeeksforGeeks. (2019, 5 27). *Need Of Information Security - GeeksforGeeks*. Retrieved from GeeksforGeeks: https://www.geeksforgeeks.org/need-of-information-security/

Thales Group. (2023, 02 01). *History of encryption (cryptography timeline)*. Retrieved from Thales Group: https://www.thalesgroup.com/en/markets/digital-identity-and-security/magazine/brief-history-encryption

Sidhpurwala, H. (2023, 01 12). *A Brief History of Cryptography*. Retrieved from Red Hat - We make open source technologies for the enterprise: https://www.redhat.com/en/blog/brief-history-cryptography

P., N. (2021, 06 15). *Encryption choices: rsa vs. aes explained*. Retrieved from Prey: reliable device tracking and security tool: https://preyproject.com/blog/types-of-encryption-symmetric-or-asymmetric-rsa-or-aes#:~:text=AES%20is%20one%20of%20the,length%20vulnerable%20to%20brute%20force.

Irwin, L. (2023, 2 14). *What Is the CIA Triad and Why Is It Important?* Retrieved from IT Governance UK Blog: https://www.itgovernance.co.uk/blog/what-is-the-cia-triad-and-why-is-it-important

Doumenjou, J.-B. (2022, 11 1). *The Art of Cryptography in Ancient and Medieval History*. Retrieved from Run APIs Easily. Anywhere. | Traefik Labs: https://traefik.io/blog/the-art-of-cryptography-in-ancient-and-medieval-history/

Koneti, V. (2021, 11 25). *Data Encryption Standard (DES) Algorithm - Scaler Topics*. Retrieved from Scaler Topics: https://www.scaler.com/topics/des-algorithm/

West, Z. (2020, 12 3). *ASCII Table: Printable Reference & Guide - αlphαrithms*. Retrieved from αlphαrithms: https://www.alpharithms.com/ascii-table-512119/

7. APPENDIX

Caeser Cipher

The Caesar cipher, one of the earliest known encryption techniques, was historically used by Julius Caesar for military communications by shifting letters in the alphabet by a fixed number, commonly three. As a substitution cipher, it laid the groundwork for more advanced encryption methods and demonstrated the importance of secrecy in early communication.

Its simplicity makes it a valuable educational tool, helping learners grasp basic cryptographic principles and engage in algorithmic analysis. However, the cipher has significant vulnerabilities, such as only 25 possible keys and susceptibility to brute-force and frequency analysis attacks, rendering it insecure for modern applications.

Despite these limitations, the Caesar cipher remains relevant in educational contexts, introductory cryptography courses, and cultural references like puzzles and games. It serves as a historical reference and a gateway to understanding the evolution of cryptographic techniques.