Module Code & Module Title

CC5004NI Security in Computing

Assessment Weightage & Type

30% Individual Coursework

Year and Semester

2022 -23 Autumn

Student Name: Arjay Bikram Khand

London Met ID: 21040602

College ID: np01nt4a210026

Assignment Due Date: 9th January 2023

Assignment Submission Date: 9th January 2023

Word Count (Where Required): 5102 words

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

List of Figures

List of Tables

Abstract

Cryptography is a means of converting unreadable original communications into readable ones. We'll render the communications illegible. Forms are created utilising two technical processes. It is a replacement and transition approach. Caesar Cipher, as the study's foundation, is a highly researchable issue that is well-suited for evaluation. Caesar Cipher is a replacement method design. Permutation systems refer to the rearranging of plain text characters, whereas substitution technology refers to the technique by which plain

text characters, numerals, and icon characters are changed. The primary objective of this task was to select a cypher and make numerous adjustments to make it more secure. We also talked about CIA Triads and the history of security in this work. We also covered about recent cryptography, including symmetric and asymmetric encryption. This report aims to choose a standard algorithm and further enhance it to address the problems discovered in the standard approach.

1. Introduction

1.1 Security

- Security for information technology (IT) refers to the methods, tools and personnel used to defend an organization's digital assets. The goal of IT security is to protect these assets, devices and services from being disrupted, stolen or exploited by unauthorized users, otherwise known as threat actors. These threats can be external or internal and malicious or accidental in both origin and nature. (Bacon, 2022)

Figure 1: Security

Information technology (IT) security is the safeguarding of computer systems and networks against the theft or destruction of their hardware, software, or information. To

guard against cyber dangers such as malware, hacking, and data breaches, it is critical to have effective IT security procedures in place. Some popular security measures for IT systems include:

- Firewalls: These are used to prevent unauthorised access to a computer or network.
- Encryption is the act of transforming data into a rules and routines that can only be viewed by those who have the appropriate decryption key.
- Strong passwords should be one-of-a-kind and tough for others to discover. ○ Regular updates and patches: To resolve vulnerabilities and avoid attacks, it is critical to maintain software and operating systems up to date.
- Antivirus software: This aids in the prevention of malware such as viruses, worms, and trojans.

In addition to technological safeguards, rules and processes must be in place to guarantee that legitimate people have access to the data they require while prohibiting illegal access or abuse of information.

1.2 Confidentiality, Integrity, and Availability (CIA)

- The CIA Triad of confidentiality, integrity and availability is considered the core

underpinning of information security. Every security control and every security vulnerability can be viewed considering one or more of these key concepts. For a security program to be considered comprehensive and complete, it must adequately address the entire CIA Triad. (Anon., 2022)

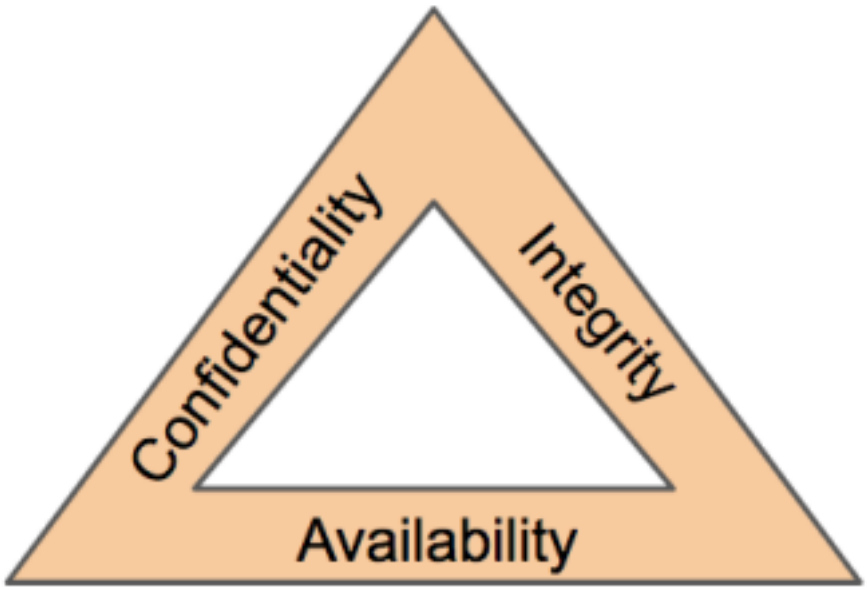


Figure 2: CIA Triad

The CIA Triad is an information security concept that consists of Confidentiality, Integrity, and Availability. The safeguarding of information against unauthorised disclosure is referred to as confidentiality. The protection of information against unauthorised change is referred to as integrity. The ability of allowed users to access information when they need it is referred to as availability. These three components, when combined, lay the basis of an effective information security programme.

Confidentiality refers to personal information shared with an attorney, physician, therapist, accountants, or other individuals that generally cannot be divulged to third parties without the express consent of the client. Lawyers are often required by law to

keep confidential, anything pertaining to the representation of a client. (Anon., 2022)

Data integrity is what the "I" in CIA Triad stands for. This is an essential component of the CIA Triad and designed to protect data from deletion or modification from any unauthorized party, and it ensures that when an authorized person makes a change that should not have been made the damage can be reversed. (Anon., 2022)

This is best ensured by rigorously maintaining all hardware, performing hardware repairs immediately when needed and maintaining a properly functioning operating system (OS) environment that is free of software conflicts. It's also important to keep current with all necessary system upgrades. Providing adequate communication bandwidth and preventing the occurrence of bottlenecks are equally important tactics. (Anon., 2022)

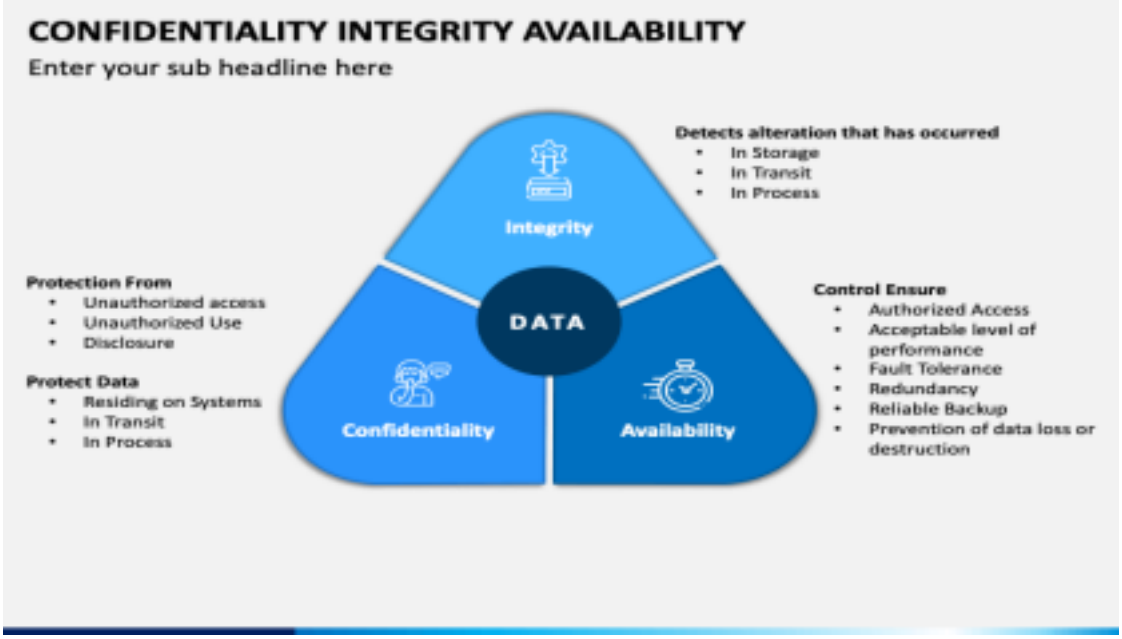


Figure 3: Confidentiality, Integrity, and Availability

1.3 Role of CIA

- The CIA triad provides a simple yet comprehensive high-level checklist for the evaluation of your security procedures and tools. An effective system satisfies all three components: confidentiality, integrity, and availability. An information security system that is lacking in one of the three aspects of the CIA triad is insufficient. (Anon., 2022)

The CIA security triangle is also useful in determining what went horribly wrong what worked-after a negative occurrence. For example, if availability was degraded during a virus assault such as ransomware, but the system in place remained able to guarantee the confidentiality of critical information. This data may be utilised to rectify flaws and duplicate successful policies and implementations.

Figure 4: Role of CIA Triad

2. Background

2.1 History of Cryptography

- The art of cryptography is born along with the art of writing. As civilizations evolved, human beings got organized into tribes, groups, and kingdoms. This led to the emergence of ideas such as power, battles, supremacy, and politics. These ideas further fueled the natural need of people to communicate secretly with selective

recipients which in turn ensured the continuous evolution of cryptography as well. The roots of cryptography are found in Roman and Egyptian civilizations. (Anon., 2022)

There have been three well-defined phases in the history of cryptology. The first was the period of manual cryptography, starting with the origins of the subject in antiquity and continuing through World War I. Throughout this phase cryptography was limited by the complexity of what a code clerk could reasonably do aided by simple mnemonic devices. As a result, ciphers were limited to at most a few pages in size, i.e., to only a few thousands of characters. General principles for both cryptography and cryptanalysis were known, but the security that could be achieved was always limited by what could be done manually. Most systems could be cryptanalyzed, therefore, given sufficient ciphertext and effort. (Anon., 2022)

The ancient Egyptians' use of hieroglyphs is one of the first known examples of cryptography. The development of increasingly complex cryptographic systems, such as the Caesar cypher and the Vigenère encryption, enabled the safe communication of information between military leaders and other strong officials during the Middle Ages.
Cryptography has been an increasingly significant method for securing information in the digital world since the dawn of the computer era. Modern cryptography encodes and decodes data using powerful mathematical methods, and it is critical in guaranteeing the security of internet conversations, business accounts, and other classified info.

The history of cryptography is given below:

- Beginning around 1900 BC with comprehensive Egyptian coding, Greek scrambling, and Romans Caesar moving three spaces to the correct of each letter in the letter set.

- Since the German codebook was sent in 1914, the seizure of Magdeburg affected the course of the war.
- Since the RSA encryption in 1986, Lotus Notes trading apps have been discontinued.
- From 1993 to 1996, Zimmerman researched AES as RSA encryption, which completed the NSA restricting architecture and now had achieved equality in

scholastic encryption for many purposes. RSA encryption is used. The clipper chip enabled NSAs to be implemented in voice decoding devices by 1996. By 1996 PGP was distributed by MIT in a book and on its website.

2.2 Ciphers

- Ciphers, also called encryption algorithms, are systems for encrypting and decrypting data. A cipher converts the original message, called plaintext, into ciphertext using a key to determine how it is done. (Anon., 2022)

A cypher is a form of hidden message that is used to encrypt and decode a message so that it cannot be read by an individual with the appropriate decryption key. Ciphers of many forms have been utilized across history, ranging from basic substitution cyphers to more complicated codes utilizing mathematical algorithms.

Substitution cyphers work by substituting each letter in the plaintext block with a different letter or symbol. In a basic substitution cypher, for example, the letter "a" might be substituted by the letter "b," "b" with "c," and so on. More complicated cyphers may utilise a key to decide how the letters are substituted, or they may encrypt the data using numerous substitution alphabets.

Some of the known historical ciphers are given below:

- Substitution Cipher: Hiding some data is known as encryption. When plain text is encrypted, it becomes unreadable and is known as ciphertext. In a Substitution cipher, any character of plain text from the given fixed set of characters is substituted by some other character from the same set depending on a key. (Anon., 2021)

- Transposition Cipher: Transposition Cipher is a cryptographic algorithm where the order of alphabets in the plaintext is rearranged to form a cipher text. In this process, the actual plain text alphabets are not included. (Anon., 2022)
- Polyalphabetic Cipher: A method to improve monoalphabetic technique is to use different monoalphabetic substitutions as proceeding through the plaintext message. This method is known as polyalphabetic substitution cipher. (Anon., 2022)
- Block Cipher: A block cipher encrypts bits, the smallest unit of computational information, in blocks. In contrast, other types of encryption methods tend to encrypt bits one by one. Block ciphers are frequently used to encrypt large amounts of data into data blocks. (Anon., 2022)
- Public Key Cipher: Public key cryptography involves a pair of keys known as a public key and a private key (a public key pair), which are associated with an entity that needs to authenticate its identity electronically or to sign or encrypt data. Each public key is published, and the corresponding private key is kept secret. Data that is encrypted with the public key can be decrypted only with the corresponding private key. (Anon., 2021)

2.3 Modern Cryptography

- Modern cryptography is the art of securing data during the digital economy by encoding it in such a manner that only someone with the appropriate decryption key may access it. It encodes and decodes data using powerful mathematical methods, and it is critical in ensuring the confidentiality of internet conversations, financial activity, and other

sensitive data.

Modern cryptography is divided into two types: symmetric key cryptography and asymmetric key cryptography. This very same order to encrypt and decrypt the data in symmetric key cryptography. This sort of encryption is quick and safe, but it needs the sender and receiver of the message to share the key. Asymmetric key cryptography, commonly known as cryptographic keys, encrypts and decrypts messages using a pair of keys. The communication is encrypted using one key, known as the public key, and decrypted using the other secret, known as the private key. This kind of encryption is slower than symmetric cryptography, however it has the advantage of not needing the recipient and the sender to exchange the secret.

The Advanced Encryption Standard (AES), the RSA technique, and the Digital Signature with Elliptic Curve Algorithm are three of the most extensively used contemporary cryptographic techniques (ECDSA). These algorithms are used to safeguard a wide variety of data, including financial transactions, sensitive company information, and private letters.

2.4 Symmetric and Asymmetric Encryption

- Symmetric encryption is a type of encryption where only one key (a secret key) is used to both encrypt and decrypt electronic data. The entities communicating via symmetric encryption must exchange the key so that it can be used in the decryption process. (Anon., 2019)

This implies that anybody with the key may read as well as write encrypted communications. AES and Blowfish are two symmetric encryption techniques.

Asymmetric encryption, also known as public key encryption, uses a public key-private key pairing: data encrypted with the public key can only be decrypted with the private key. (Anon., 2022)

This implies that anybody can use the recipient's public key to encrypt a message, while only the author of the encryption key can decode it. RSA and DSA are two examples of asymmetric data encryption.

Because it does not need the exchange of secret keys, asymmetric encryption is thought to be less secure than symmetric encryption. It is, however, often slower than symmetric encryption.

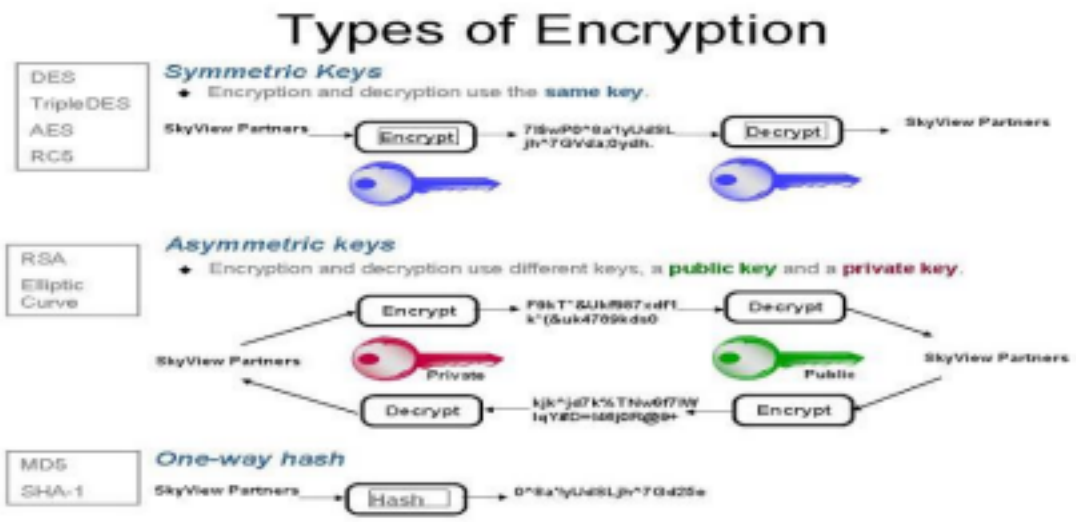


Figure 5: Symmetric and Asymmetric Encryption

3 Caesar Cipher

- The Caesar cipher is the simplest and oldest method of cryptography. The Caesar cipher method is based on a mono-alphabetic cipher and is also called a shift cipher or additive cipher. Julius Caesar used the shift cipher (additive cipher) technique to communicate with his officers. For this reason, the shift cipher technique is called the Caesar cipher. The Caesar cipher is a kind of replacement (substitution) cipher, where all letter of plain text is replaced by another letter. (Anon., 2022)

As an illustration, with a shift of 3, A would become D, B would become E, and so on. Here is an illustration of how to encrypt the word "HELLO" using a shift of three:

H -> K

E -> H

L -> O

L -> O

O -> R

KHOOR would be the encoded message. You would just move the letters back by the same amount to reveal the message. To get the original message "HELLO" in this situation, you would swap K for H, H for E, and so on.

3.1 Advantages using Caesar Cipher

- Even for those without a background in cryptography, it is relatively simple to use and comprehend.
- It is efficient in encrypting and decrypting communications, making real-time communication possible.
- If the shift value is kept a secret, it is reasonably safe.

- It is simple to change it to make it more secure, for as by using a different shift value for each letter or by utilizing a set of Caesar encryption methods. - Its attractiveness and recognition are increased by the fact that it has a lengthy history and has been in use for many years.

3.2 Disadvantages using Caesar Cipher

- It is fairly simple to break, especially if the attacker is familiar with the original message's language or has access to a sizable sample of ciphertext. - It is vulnerable to frequency analysis, a method that includes counting the number of times each letter appears in a ciphertext in order to uncover hidden patterns and infer the original message.
- It is not appropriate for lengthy communications since every letter receives the same shift value, making it simpler for an attacker to decipher the cipher. - As there are only 26 potential shift values (assuming the English alphabet is used), which are readily brute-forced by an attacker, it does not provide much protection. - Since the same message will always generate the same ciphertext when encrypted using the exact shift value, it offers no privacy for the original message.

3.3 Row Transposition Cipher

- In a row transposition cypher, the message is typed in a grid and the rows of the grid are then rearranged to form the ciphertext. This is a straightforward substitution cypher.

Here is an example of how to encode the message "HELLO" using a row transposition cipher with a key of 3:

1 2 3

H E L

L O _

The message is typed in a three-column grid, and the rows are then rearranged using the key (in this case, the rows are rearranged in the order 3, 1, 2). The ciphertext is then obtained by reading the resultant grid row by row:

3 1 2

L H O

_ E L

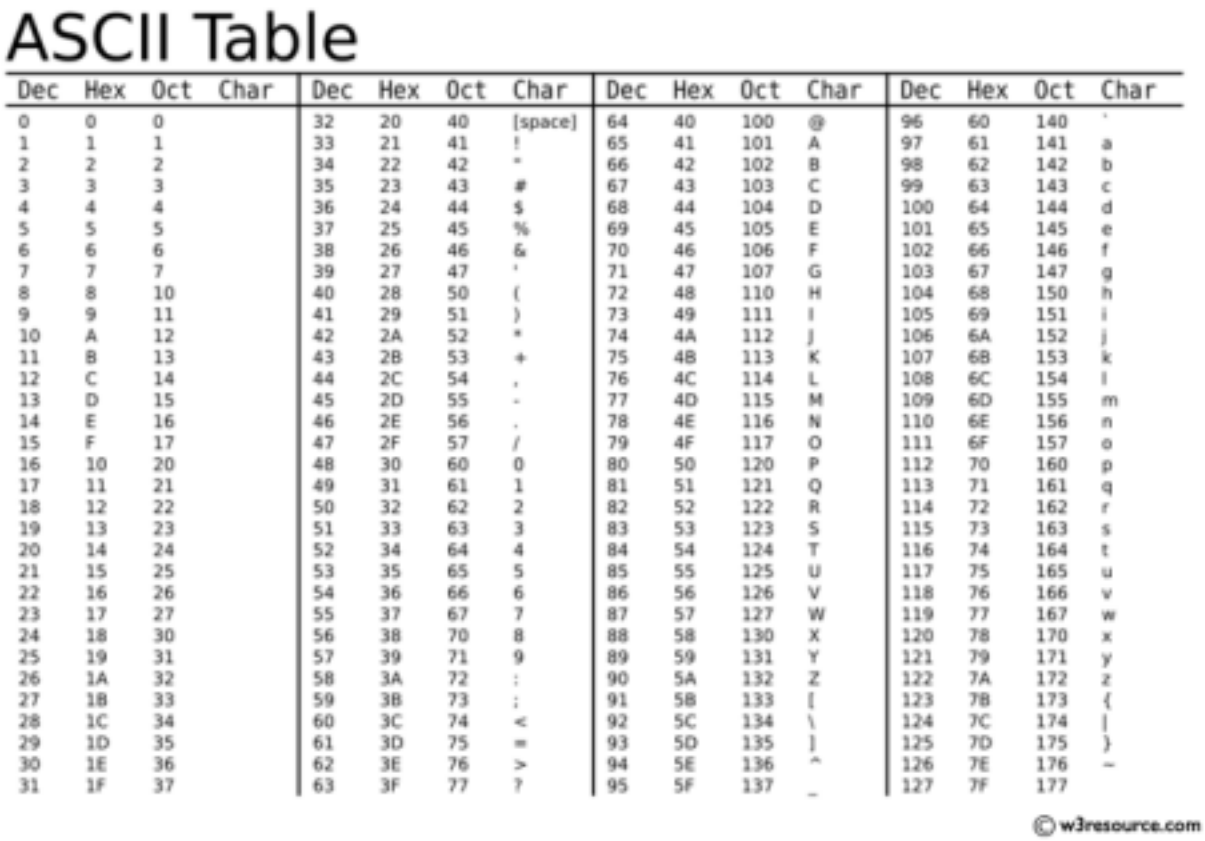
Therefore, "LHOE L" would be the encoded message. You would just rearrange the rows in accordance with the key and read out the message column by column to decode the message.

The row transposition cypher has the drawback of being very simple to crack, especially if the offender is familiar with the original message's language or has access to a sizable sample of ciphertext. Based on how frequently the letters appear in the message, it is also susceptible to assaults.

3.4 ASCII Values

- ASCII (*which stands for American Standard Code for Information Interchange*) is a character encoding standard for text files in computers and other devices. ASCII is a subset of Unicode and is made up of 128 symbols in the character set. These symbols consist of letters (both uppercase and lowercase), numbers, punctuation marks, special characters, and control characters. Each symbol in the character set can be represented by a Decimal value ranging from 0 to 127, as well as equivalent Hexadecimal and Octal

values. (Anon., 2021)



ASCII Table

Dec	Hex	Oct	Char	Dec	Hex	Oct	Char	Dec	Hex	Oct	Char	Dec	Hex	Oct	Char
0	0	0		32	20	40	[space]	64	40	100	@	96	60	140	`
1	1	1		33	21	41	!	65	41	101	A	97	61	141	a
2	2	2		34	22	42	"	66	42	102	B	98	62	142	b
3	3	3		35	23	43	#	67	43	103	C	99	63	143	c
4	4	4		36	24	44	$	68	44	104	D	100	64	144	d
5	5	5		37	25	45	%	69	45	105	E	101	65	145	e
6	6	6		38	26	46	&	70	46	106	F	102	66	146	f
7	7	7		39	27	47	'	71	47	107	G	103	67	147	g
8	8	10		40	28	50	(	72	48	110	H	104	68	150	h
9	9	11		41	29	51	)	73	49	111	I	105	69	151	i
10	A	12		42	2A	52	*	74	4A	112	J	106	6A	152	j
11	B	13		43	2B	53	+	75	4B	113	K	107	6B	153	k
12	C	14		44	2C	54	,	76	4C	114	L	108	6C	154	l
13	D	15		45	2D	55	-	77	4D	115	M	109	6D	155	m
14	E	16		46	2E	56	.	78	4E	116	N	110	6E	156	n
15	F	17		47	2F	57	/	79	4F	117	O	111	6F	157	o
16	10	20		48	30	60	0	80	50	120	P	112	70	160	p
17	11	21		49	31	61	1	81	51	121	Q	113	71	161	q
18	12	22		50	32	62	2	82	52	122	R	114	72	162	r
19	13	23		51	33	63	3	83	53	123	S	115	73	163	s
20	14	24		52	34	64	4	84	54	124	T	116	74	164	t
21	15	25		53	35	65	5	85	55	125	U	117	75	165	u
22	16	26		54	36	66	6	86	56	126	V	118	76	166	v
23	17	27		55	37	67	7	87	57	127	W	119	77	167	w
24	18	30		56	38	70	8	88	58	130	X	120	78	170	x
25	19	31		57	39	71	9	89	59	131	Y	121	79	171	y
26	1A	32		58	3A	72	:	90	5A	132	Z	122	7A	172	z
27	1B	33		59	3B	73	;	91	5B	133	[	123	7B	173	{
28	1C	34		60	3C	74	<	92	5C	134	\	124	7C	174	|
29	1D	35		61	3D	75	=	93	5D	135	]	125	7D	175	}
30	1E	36		62	3E	76	>	94	5E	136	^	126	7E	176	~
31	1F	37		63	3F	77	?	95	5F	137	_	127	7F	177	

© w3resource.com

Figure 6: ASCII Table

4. Development of Modified Caesar Cipher

- In this method, the letters are randomly moved rather than linearly, employing the substitution and permutation box techniques seen in contemporary encryption algorithms like blowfish and DES, among others. Then, using the affine cypher approach, a substitution box has to be made (i.e., Cipher Text = (Plain Text * key1) + key2). The characters are then substituted with their corresponding values, using the replacement box, as a reference. Additionally, use permutation techniques to jumble the cypher text—that is, to randomly rearrange the locations of the letters in the ciphertext—in order to obscure the language's features.

By employing row transposition on the cypher text, cypher text may be permuted. The range of characters that the Caesar cypher cannot encode can be encrypted using the suggested technique.

4.1 Key Generator () Algorithm

1) k1[i]=ASCII value of character in password (key) at position i // k1 is an array of size N.

2) Initialize ckey1=0

3) For I =1 to N do

a. ckey1 = ckey1*10 + k1[i]

b. k1[i] = (k1[i] mod 5) + 1

4) Create visited array of size N and initialize it to 0.

5) For i = 0 to N do

a) If k1[i] is not visited mark as visited

b) Else

I. Find first unvisited value from 1 to N

II. Assign it to k1[i] and mark it as visited

6) ckey2 = k1

4.2 Encryption Algorithm

1) Create a matrix of N x N.

2) Input the plaintext to be encrypted and a password (key) of size N. 3) From the input password (key) generate two sub keys ckey1 and ckey2 using Key Generator() function.

4) Call initialize () function to create two substitution tables.

5) Create ciphertext1 by replacing each character in plaintext by values assigned in the ASCII table - map in step 4.

6) Perform row transformation using ckey2 which was generated by Key Generator() function.

7) Transmit the ciphertext generated in step 6.

4.3 Decryption Algorithm

1) Create a matrix of N x N.

2) Input the ciphertext to be decrypted and a password (key) of size N. 3) From the input password (key) generate two sub keys ckey1 and ckey2 using Key Generator () function.

4) Call initialize () function to create substitution tables.

5) Perform reverse row transformation twice using ckey2 which was generated by Key Generator () function.

6) Generate plaintext by replacing each character in the string obtained by step 5 by values assigned in the ASCII table – map in step 4

5. Testing

- A few examples of modified Caesar Cipher are tested below:

5.1 Test 1

Plain Text - HELLO!

Password – Islington

Key Generator ():

Let, ckey = 0 (Initial)

Using ASCII Table,

I = 73

s = 115

l = 108

i = 105

n = 110

g = 103

t = 116

0 = 111

n = 110

Part – 1:

ckey = 0

N =1 to 9

ckey1 = ckey1 * 10 + k1[i]

ckey1 = 0*10+73 = 73

ckey1 = 73*10+115 = 845

ckey1 = 845*10+108 = 8558

ckey1 = 8558*10+105 = 85685

ckey1 = 85685*10+ 110 = 856960 ckey1 =

856960*10+103= 8569703 ckey1 =

8569703*10+116 =85637146 ckey1 =

85697146*10+111 = 856971571 ckey1 =

856971571*10+110 = 8569715820

Part – 2:

k1[i] = (k1[i] mod5) + 1

ckey2 = (73mod5) +1 = 4

ckey2 = (115mod5) +1 = 1

ckey2 = (108mod5) +1 = 2

ckey2 = (105mod5) +1 = 3

ckey2 = (110mod5) +1 =5

ckey2 = (103mod5) +1 = 6

ckey2 = (116mod5) +1 = 7

ckey2 = (111mod5) +1 = 8

ckey2 = (110mod5) +1 = 9

Key = 412356789

Encryption:

Plain Text – HELLO!

Using inverse map,

Cipher text – G~22p!

Using row transposition method on cipher text,

1	2	3	4	5	6	7	8	9
G	~	2	2	p	!			

Table 1: Test 1

Now,

Key = 412356789

4	1	2	3	5	6	7	8	9
2	G	~	2	p	!			

Table 2: Test 1 Encryption

Encrypted Text – 2G~2p!

Decryption:

Encrypted Text – 2G~2p!

Key – 412356789

Using row transposition method,

4	1	2	3	5	6	7	8	9
2	G	~	2	p	!			

Table 3: Test 1 A

Now,

1	2	3	4	5	6	7	8	9
G	~	2	2	p	!			

Table 4: Test 1 Decryption

Cipher Text – G~22p!

Using Inverse-map,

Plain text – HELLO!

5.2 Test 2

Plain text – Computer.

Password – Islington

Key Generator ():

Let, ckey = 0

(Initial) Using ASCII

Table, I = 73

s = 115

l = 108

i = 105

n = 110

g = 103

t = 116

0 = 111

n = 110

Part – 1:

ckey = 0

N =1 to 9

ckey1 = ckey1 * 10 + k1[i]

ckey1 = 0*10+73 = 73

ckey1 = 73*10+115 = 845

ckey1 = 845*10+108 = 8558

ckey1 = 8558*10+105 = 85685

ckey1 = 85685*10+ 110 = 856960 ckey1 =

856960*10+103= 8569703 ckey1 =

8569703*10+116 =85637146 ckey1 =

85697146*10+111 = 856971571 ckey1 =

856971571*10+110 = 8569715820

Part – 2:

k1[i] = (k1[i] mod5) + 1

ckey2 = (73mod5) +1 = 4

ckey2 = (115mod5) +1 = 1

ckey2 = (108mod5) +1 = 2

ckey2 = (105mod5) +1 = 3

ckey2 = (110mod5) +1 =5

ckey2 = (103mod5) +1 = 6

ckey2 = (116mod5) +1 = 7

ckey2 = (111mod5) +1 = 8

ckey2 = (110mod5) +1 = 9

Key = 412356789

Encryption:

Plain Text – Computer.

Using inverse map,

Cipher text – NvSVnFcR

Using row transposition method on cipher text,

1	2	3	4	5	6	7	8	9
N	v	S	V	n	F	c	R	

Table 5: Test 2

Now,

Key = 412356789

4	1	2	3	5	6	7	8	9
V	N	v	S	n	F	c	R	

Table 6: Test 2 Encryption

Encrypted Text – VNvSnFcR

Decryption:

Encrypted Text – VNvSnFcR

Key – 412356789

Using row transposition method,

4	1	2	3	5	6	7	8	9
V	N	v	S	n	F	c	R	

Table 7: Test 2 A

Now,

1	2	3	4	5	6	7	8	9
N	v	S	V	n	F	c	R	

Table 8: Test 2 Decryption

Cipher Text – NvSVnFcR

Using Inverse-map,

Plain text – Computer.

5.3 Test 3

Plain text – enemy attacks

tonight Password – Islington

Key Generator ():

Let, ckey = 0 (Initial)

Using ASCII Table,

I = 73

s = 115

l = 108

i = 105

n = 110

g = 103

t = 116

0 = 111

n = 110

Part – 1:

ckey = 0

N =1 to 9

ckey1 = ckey1 * 10 + k1[i]

ckey1 = 0*10+73 = 73

ckey1 = 73*10+115 = 845

ckey1 = 845*10+108 = 8558

ckey1 = 8558*10+105 = 85685

ckey1 = 85685*10+ 110 = 856960 ckey1 =

856960*10+103= 8569703 ckey1 =

8569703*10+116 =85637146 ckey1 =

85697146*10+111 = 856971571 ckey1 =

856971571*10+110 = 8569715820

Part – 2:

k1[i] = (k1[i] mod5) + 1

ckey2 = (73mod5) +1 = 4

ckey2 = (115mod5) +1 = 1

ckey2 = (108mod5) +1 = 2

ckey2 = (105mod5) +1 = 3

ckey2 = (110mod5) +1 =5

ckey2 = (103mod5) +1 = 6

ckey2 = (116mod5) +1 = 7

ckey2 = (111mod5) +1 = 8

ckey2 = (110mod5) +1 = 9

Key = 412356789

Encryption:

Plain Text – enemy attacks tonight

Using inverse map,

Cipher text – F^FSk BooBTO] ov^eLMo

Using row transposition method on cipher text,

1	2	3	4	5	6	7	8	9
F	^	F	S	k		B	o	o
B	T	O	]		o	v	^	e

L	M	o						

Table 9: Test 3

Now,

Key = 412356789

4	1	2	3	5	6	7	8	9
S	F	^	F	K		B	o	o
]	B	T	O		O	V	^	e
	L	M	o					

Table 10: Test 3 Encryption

Encrypted Text – SF^FK Boo]BTO OV^e LMo

Decryption:

Encrypted Text – SF^FK Boo]BTO OV^e LMo

Key – 412356789

Using row transposition method,

4	1	2	3	5	6	7	8	9
S	F	^	F	K		B	o	o
]	B	T	O		O	V	^	e

	L	M	o					

Table 11: Test 3 A

Now,

1	2	3	4	5	6	7	8	9
F	^	F	S	k		B	o	o
B	T	O	]		o	v	^	e
L	M	o						

Table 12: Test 3 Decryption

Cipher text – F^FSk BooBTO] ov^eLMo

Using Inverse-map,

Plain text – enemy attacks tonight

5.4 Test 4

Plain text – Islington

College Password –

Islington

Key Generator ():

Let, ckey = 0 (Initial)

Using ASCII Table,

I = 73

s = 115

l = 108

i = 105

n = 110

g = 103

t = 116

0 = 111

n = 110

Part – 1:

ckey = 0

N =1 to 9

ckey1 = ckey1 * 10 + k1[i]

ckey1 = 0*10+73 = 73

ckey1 = 73*10+115 = 845

ckey1 = 845*10+108 = 8558

ckey1 = 8558*10+105 = 85685

ckey1 = 85685*10+ 110 = 856960 ckey1 =

856960*10+103= 8569703 ckey1 =

8569703*10+116 =85637146 ckey1 =

85697146*10+111 = 856971571 ckey1 =

856971571*10+110 = 8569715820

Part – 2:

k1[i] = (k1[i] mod5) + 1

ckey2 = (73mod5) +1 = 4

ckey2 = (115mod5) +1 = 1

ckey2 = (108mod5) +1 = 2

ckey2 = (105mod5) +1 = 3

ckey2 = (110mod5) +1 =5

ckey2 = (103mod5) +1 = 6

ckey2 = (116mod5) +1 = 7

ckey2 = (111mod5) +1 = 8

ckey2 = (110mod5) +1 = 9

Key = 412356789

Encryption:

Plain Text – Islington College

Using inverse map,

Cipher text – _bPe^Lqv^ NvPPFLF

Using row transposition method on cipher text,

1	2	3	4	5	6	7	8	9

_	b	P	e	^	L	q	v	^
	N	v	P	P	F	L	F	

Table 13: Test 4

Now,

Key = 412356789

4	1	2	3	5	6	7	8	9
e	_	b	P	^	L	Q	v	^
p		N	v	P	F	L	F	

Table 14: Test 4 Encryption

Encrypted Text – e_bP^LQv^p NvPFLF

Decryption:

Encrypted Text – e_bP^LQv^p NvPFLF

Key – 412356789

Using row transposition method,

4	1	2	3	5	6	7	8	9

e	_	b	P	^	L	Q	v	^
p		N	v	P	F	L	F	

Table 15: Test 4 A

Now,

1	2	3	4	5	6	7	8	9
_	b	P	e	^	L	q	v	^
	N	v	P	P	F	L	F	

Table 16: Test 4 Decryption

Cipher text – _bPe^Lqv^ NvPPFLF

Using Inverse-map,

Plain text – Islington College

5.5 Strength of modified Caesar cipher

- Each character is shifted by a random integer (Affine cypher generates the random number).
- By distributing the characters across the cypher text, it conceals a language's peculiarities.
- The characters are dispersed throughout the cypher text to hide the quirks of a language.
- It is not possible to attack using frequency analysis attack.
- It eliminates all of the flaws in the conventional Caesar cypher, making it

challenging for cryptanalysts to break it.

5.6 Weakness of Modified Caesar Cipher

- Frequency analysis, a strategy for examining the frequency of letters in the ciphertext, makes it simple to crack the modified Caesar cypher.
- Every letter in the plaintext of the modified Caesar cypher receives the same shift because it only employs one shift value. This makes it simple for an attacker to test every shift value that could exist and rapidly identify the best one.
- Due to the lack of extra security features like key exchanges or authentication, the modified Caesar cypher is vulnerable to assaults like man-in-the-middle attacks. ○ The modified Caesar cypher is straightforward to create and does not need any difficult algorithms or computations, making it simple for attackers to crack.

5.7 Application areas

- A straightforward substitution cipher that is frequently employed as a teaching aid for the fundamentals of cryptography is the modified Caesar cypher. Due to its vulnerability and susceptibility to attack, it is often not employed in real applications.

Substitution cyphers have mostly been supplanted by more sophisticated cryptographic methods since they are not seen to be secure enough for practical usage. There are considerably more sophisticated cyphers that involve key exchanges and intricate algorithms to safeguard the secrecy of the data being conveyed. The modified Caesar cypher can still be applied in situations that are primarily intended to convey

cryptography ideas rather than to offer true security, such as games or puzzles.

6. Conclusion

- By using cryptography, communication may be protected from outside interference or access. It includes encoding and decoding messages using mathematical techniques and protocols to make sure that only the intended receiver can understand the message.

The Caesar cypher, often called the shift cypher, is a straightforward substitution cypher that is simple to use yet prone to intrusion. To construct a ciphertext, the alphabetic letters are moved a predetermined number of times. The Caesar cypher has been mainly supplanted by more secure cryptosystems since it is thought to be slightly

insecure.

In general, modern civilization relies heavily on cryptography to secure communication and safeguard information. It is used for a variety of purposes, including as financial transactions, military communications, and internet communications. However, the strength of the employed algorithms and protocols, as well as the appropriate deployment and administration of the cryptographic systems, all affect how successful cryptography is. As a result, to maintain their security, cryptographic systems need to be continually reviewed and updated.

7. References

Anon., 2019. *CRYPTOMAThIC.* [Online]
Available at: www.cryptomathic.com
[Accessed 8 January 2023].

Anon., 2021. *GeeksforGeeks.* [Online]
Available at: www.geeksforgeeks.org
[Accessed 8 January 2023].

Anon., 2021. *IBM.* [Online]
Available at: www.ibm.com
[Accessed 8 January 2023].

Anon., 2021. *Tech On The Net.* [Online]
Available at: www.techonthenet.com
[Accessed 8 January 2023].

Anon., 2022. *Britannica.* [Online]
Available at: www.britannica.com
[Accessed 8 January 2023].

Anon., 2022. *CertMike.* [Online]
Available at: www.certmike.com
[Accessed 8 January 2023].

Anon., 2022. *Cloudflare.* [Online]
Available at: www.cloudflare.com
[Accessed 8 January 2023].

Anon., 2022. *ContractsCounsel.* [Online]
Available at: www.contractscounsel.com
[Accessed 8 January 2023].

Anon., 2022. *Forcepoint.* [Online]
Available at: www.forcepoint.com
[Accessed 8 January 2023].

Anon., 2022. *Fortinet.* [Online]
Available at: www.fortinet.com
[Accessed 8 January 2023].

Anon., 2022. *HYPR.* [Online]
Available at: www.hypr.com
[Accessed 8 January 2023].

Anon., 2022. *JavaTPoint.* [Online]
Available at: www.javatpoint.com
[Accessed 8 January 2023].

Anon., 2022. *Sangfor.* [Online]
Available at: www.sangfor.com
[Accessed 8 January 2023].

Anon., 2022. *Studocu.* [Online]
Available at: www.studocu.com
[Accessed 8 January 2023].

Anon., 2022. *TechTarget.* [Online]
Available at: www.techtarget.com
[Accessed 8 January 2023].

Anon., 2022. *TutorialsPoint.* [Online]

Available at: www.tutorialspoint.com
[Accessed 8 January 2023].

Anon., 2022. *TutorialsPoint.* [Online]
Available at: www.tutorialspoint.com
[Accessed 8 January 2023].

Bacon, M., 2022. *TechTarget.* [Online]
Available at: www.techtarget.com
[Accessed 8 January 2023].

Appendix

https://arxiv.org/ftp/arxiv/papers/1512/1512.05483.pdf

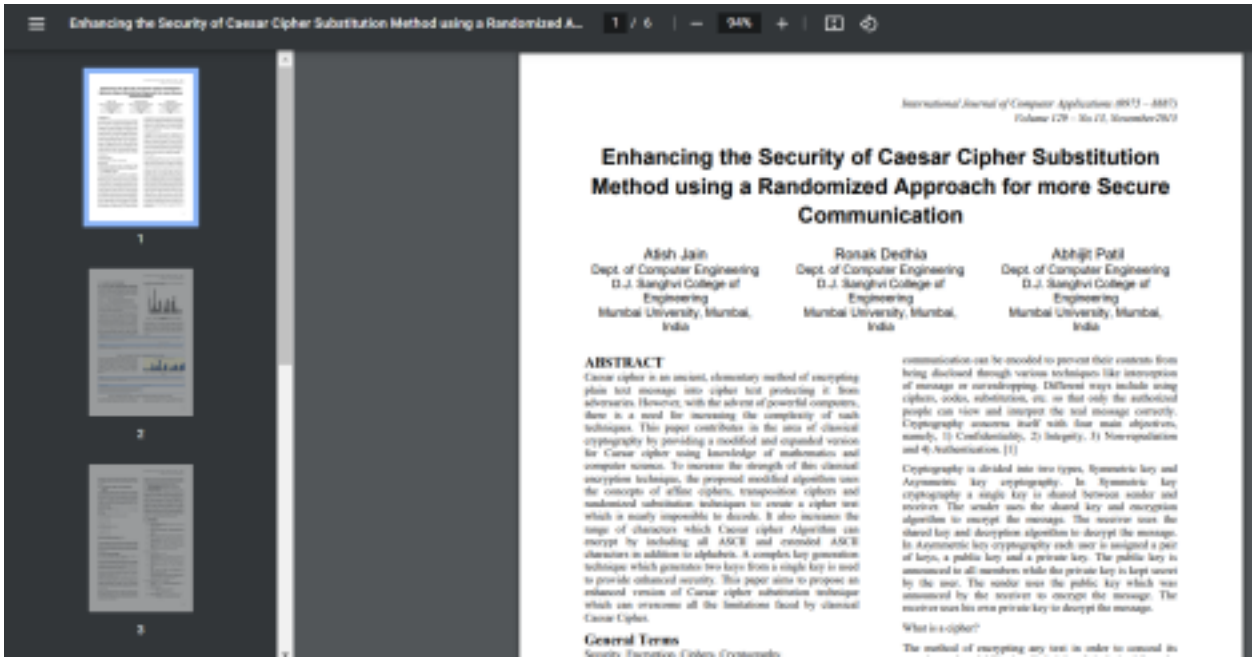


Figure 7: Appendix of pdf

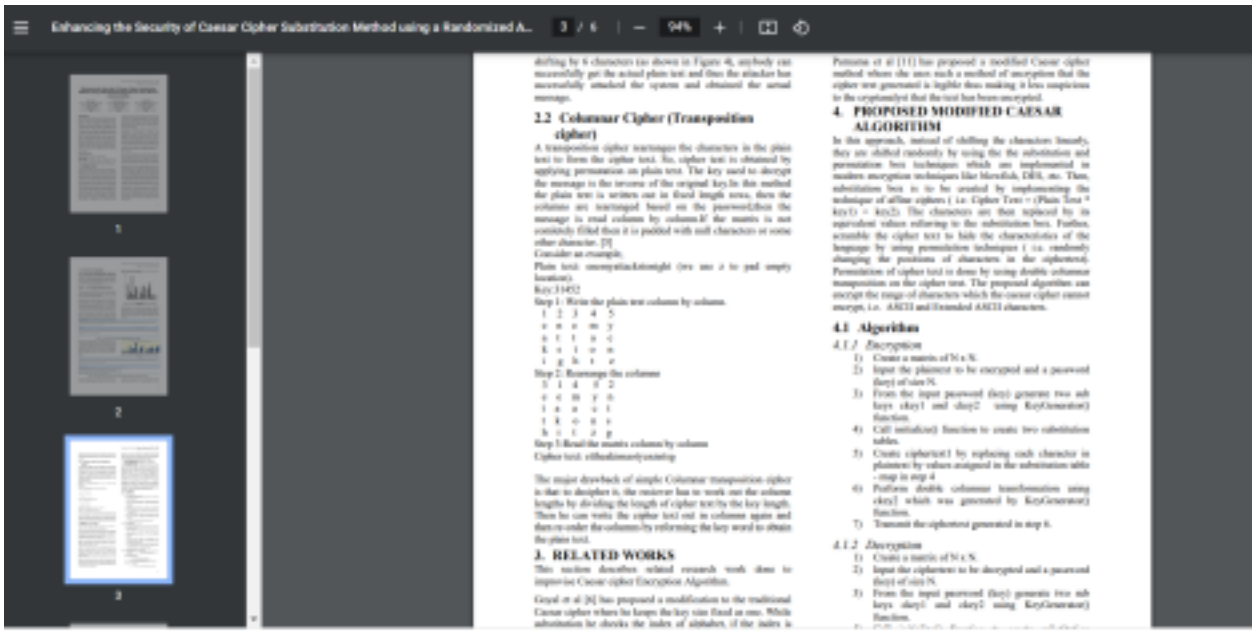


Figure 8: Appendix 2

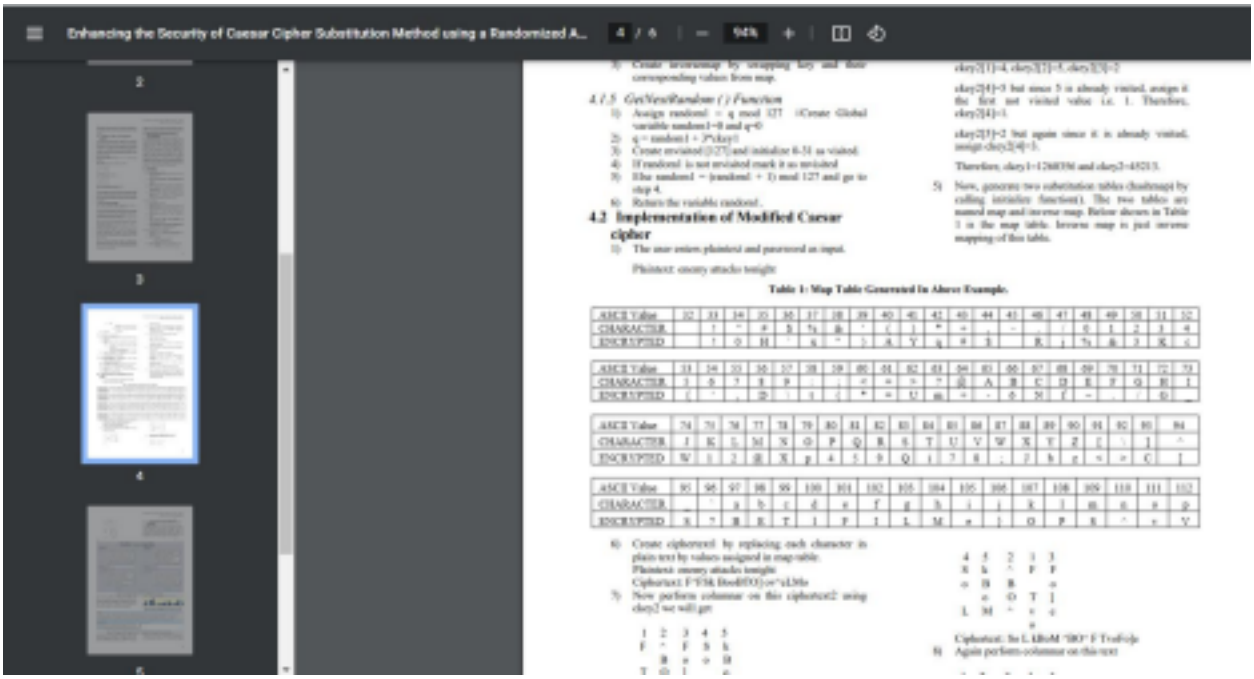


Figure 9: Appendix 3