LONDON METROPOLITAN UNIVERSITY

Islington college
(इस्लिङ्टन कलेज)

Module Code & Module Title

CC5004NI Security in Computing

Assessment Weightage & Type

30% Individual Coursework

Year and Semester

2021 -22 Autumn

Student Name: Aadarsha Muni Shakya

London Met ID: 20049438

College ID: NP01NT4S210023

Assignment Due Date: 10th January 2022

Assignment Submission Date: 10th January 2022

Word Count (Where Required): 4100

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.

Module Code:	**CC5004NI**
Module Title:	**Security in Computing**
Module Leader:	**Mr. Akchayat Bikram Dhoj Joshi (Islington College)**

Coursework Type:	Individual
Coursework Weight:	This coursework accounts for ***30%*** of the overall module grades.
Submission Date:	**Week 12**
Coursework given out:	**Week 4**
Submission Instructions:	Submit the following to the Islington College's RTE department before the due date: • A report (document) in .pdf format in the Google Classroom or through any medium which the RTE department specifies.
Warning:	London Metropolitan University and Islington College takes plagiarism very seriously. Offenders will be dealt with sternly.

Acknowledgement

I am really grateful because the report on the topic Cryptographic system is completed. Also, it would have been impossible to complete this report without the help of the module leader Mr. Akchayat Bikram Dhoj Joshi. The resources provided by the teachers helped me in understanding different cryptographic algorithm. Not just understand but they helped me develop new cryptographic algorithm which is shown further in this report.

Table of Content

Table of Figures

Table of Tables

Abstract

In this report, research on an existing cryptographic algorithm, development of a new cryptographic algorithm called XOR & Key algorithm and testing of XOR & Key algorithm is covered. The importance of the cryptographic algorithm in the domain of information security led to the motivation for this report. Not just existing algorithm but a new algorithm was developed.

While developing a XOR & Key algorithm many problems rose, but by the help of teachers and from the research materials those problems are solved. After this a pride feeling of owning a XOR & Key algorithm which will secure the information which will lead to information security.

1. Introduction to Cryptographic System

Security is a temporary state where the data is secure from malicious entities by using different methods, tools, and personnel to defend digital assets. Cryptography is one of the techniques used for securing data in order to maintain the security triad. So, a cryptographic system helps users to maintain the security triad by encrypting the plain text to cipher text.

Security triad also referred as CIA triad consists of three components. Namely, Confidentiality, Integrity and Availability. If nether of these components are compromised the security of digital assets are also not compromised. However, using a cryptographic system the information is unconditionally secured. This is because it doesn't ensure integrity and availability of data. On the other hand, the information cannot be understood by hackers so its unconditionally secure.

The confidentiality of information is maintained when information is meaningless to unauthorized users. By cryptographic system the hackers might gain control over the encrypted information, but they will not understand the information which will maintain the confidentiality of the information.

Also, cryptography system protects information so, it is very important in the domain of information security. For example, if two people are communicating via internet and their communication is encrypted the communication will be secured. This is because the unauthorize users may have access over the communication they will not understand the accessed data and therefore cryptography is very important in the domain of information security.

For the history of cryptographic algorithm, the concept of cryptography was used in the past as-well. For example, in 1900 BC at Egypt, the form of letter used were different than normal. The purpose was not to hide the message but to make it meaningless for unauthorized users (Sidhpurwala, 2013). This is a form of encryption used in the past. Now based on that purpose the modern world uses cryptographic system to secure information and data.

Similarly, around 100 BC the concept of encryption was done by Julius Caesar which was then named Caesar box or Caesar cipher (GhostVolt, 2021). In this algorithm each letter is replaced by the letter standing 3 places further down the actual letter.

The concept of encryption in the history led to the modern encryption and decryption algorithm. The concept of not letting the information fall under unauthorized personalness has always been the main goal of communicating with a cryptographic algorithm.

In the digital world, cryptographic system is classified into two type symmetric cipher and asymmetric cipher. If the cryptographic system uses a single key to encrypt plain text and decrypt cipher text it is symmetric cipher. Some examples of symmetric cipher are Caesar cipher, Playfair cipher, Rail fence cipher, Row transport cipher, SDES, DES and AES.

However, if one key is used to encrypt the information and a different key is used to decrypt the information the system is asymmetric encryption. While sending the information, it will encrypt the information using a key and on the other side the receiver will decrypt the information using the other key they have.

An example of decryption algorithm is RSA algorithm. In asymmetric cipher the concept of prime numbers and greatest common devisor are used to find the perfect key for encryption and decryption. Public key is used for encryption and private key is used for decryption.

1.1 Aim

The aim of this report is to research on an existing cryptographic algorithm, develop a new cryptographic algorithm and test the algorithm.

1.2 Objectives

Objectives of this report are

- To define cryptographic systems
- To see existing cryptographic algorithm
- To make a XOR & Key algorithm

2. Background of the Selected Cryptographic Algorithm

There are many algorithms of symmetric and asymmetric cryptographic systems namely, Caesar cipher, Playfair cipher, Rail fence cipher, Row transport cipher, SDES, DES, AES, RSA and many more.

Now Row transport cipher will be explained in depth. Row transport cipher is a symmetric where a key is used to determine the way plain text is represented to form the cipher text. For encryption and decryption, a table is required where number of columns is determined by the key.

For encryption, alphabets are assigned a number based on the alphabets. For illustration in the key HACK the order od alphabets is 3124. “A” being 1 because it is the first alphabet and “C” being 2 because “C” is the second alphabet in the key.

Now once the table is set the plain text is filled from the first row all the way until no plain text remains. Then empty boxes might be seen at the last row and those boxes are filled with random letters.

One all the boxes are filled, according to the key number the cipher text is derived. The letters of the column with 1 is written at first then column with 2 and so on is done to derive the cipher text.

For decryption, number of rows should be calculated. To do so, total number of characters in cipher text should be divided by the number of characters in the key. Now the table is formed with fixed rows and columns and according to the key the characters of cipher text is filled column wise. And therefore, decryption is complete.

Every cryptographic algorithm has its own advantages and disadvantages, so does Row transport cipher. The advantages of this cipher are the number of characters is different from plain text to cipher text and key can change the cipher text is formed.

For this cipher's disadvantages, if the key has similar letters this will cause problem because the number assigning through the key will create confusion. For illustration, the key can be BALL here the numeric representation will be 2134 but while encrypting and decrypting the 3 and 4 can interchange and cause problems.

For visual representation of Row transport cipher, the plain text "Security in Computing?" is encrypted and decrypted.

For Encryption

Plain Text = "Security in Computing?"

Key = "SAFE"

Now, Create a blank Table with Key. The number of characters in the key will determine the number of columns in the table.

Table 1: Blank Table

S	A	F	E
4	1	3	2

Now fill the cipher text Row-wise. From the third row and first column the first character is placed. The second character is placed in the third row and second column, and this process is done until there are no characters left. Sometimes in the last row boxes can be empty so using random characters is done until the table is fully filled. In this case "X", "Y", "Z" characters are added to fill the table.

Table 2: Row Transport Encryption

S	A	F	E
4	1	3	2
S	e	c	u
r	i	t	_
i	n	_	C
o	m	p	u
t	i	n	g
?	X	Y	Z

Cipher Text = “einmiXu CugZct pnYSriot?”

For Decryption

Cipher Text = “einmiXu CugZct pnYSriot?”

Key = “SAFE”

Number of rows = Characters in CT / Characters in key

=24/4

=6

Now, Create a blank table with key and number of rows. Key will determine the number of columns and key will determine the number of rows for the table.

Table 3: Blank Table

S	A	F	E
4	1	3	2

Now, fill the table according to the numbers in the second-row column-wise. At first the column with number 1 is filled. “e”, “l”, “n”, “m”, “l” and “X” are filled in that column. And this process is done until the characters finish

Table 4: Row Transport Decryption

S	A	F	E
4	1	3	2
S	e	c	u
r	i	t	_
i	n	_	C
o	m	p	u
t	i	n	g
?	X	Y	Z

Plain Text = “Security in Computing?XYZ”

Now remove the Random letters from the last to get the final plain text. While encrypting to fill the table random texts were added and just reading the plain text the meaning less characters can be removed to finalize the plain text.

Plain Text = “Security in Computing?”

3. Development of a XOR & Key algorithm

This XOR & Key algorithm is a symmetric cipher which used a 5-bit key to encrypt as-well-as decrypt. A predefined table with characters and their respective binary value are defined which is used to encrypt plain text and decrypt cipher text. The binary values are 5-bit which means only 32 numbers can be encrypted and decrypted.

While communicating the most frequently used characters like Space, alphabets, some symbols like "@" and "&" and punctuation marks like ".", "," and "?" have respective binary values to encrypt and decrypt.

Table 5: Predefined Table

Number	Character	Binary value	Number	Character	Binary value
1	Space	00000	17	P	10000
2	A	00001	18	Q	10001
3	B	00010	19	R	10010
4	C	00011	20	S	10011
5	D	00100	21	T	10100
6	E	00101	22	U	10101
7	F	00110	23	V	10110
8	G	00111	24	W	10111
9	H	01000	25	X	11000
10	I	01001	26	Y	11001
11	J	01010	27	Z	11010
12	K	01011	28	@	11011
13	L	01100	29	?	11100
14	M	01101	30	,	11101
15	N	01110	31	.	11110
16	O	01111	32	&	11111

Also, while encrypting ad decrypting steps like XOR, LS and RS are used. In XOR, if two bits are passed it gives a single output. If the bits are same as 0 and 0 or 1 and 1 the output will always be 0. And if the bits are different as 0 and 1 or 1 and 0 the output is always 1.

In order for this to work the bit size of both binary values should be the same. For example, 1010 and 111 cannot be XORed because the last bit of 1010, which is 0 won't have a bit to XOR and this will cause problems.

For LS and RS, LS means left shift and RS means right shift. Moreover LS 1 means moving the first bit to the last making the second bit the first bit. Similarly, If RS 1 is used the last bit will be the first bit and the first bit will be the second bit. If LS 1 is followed by RS 1 their will be no change in the binary value.

For Encryption

Step 1: Start

Step 2: Find plain text

Step 3: Covert to 5-bit binary from predefined table

Step 4: XOR PT with Key to find CT

Step 5: Left shift one on CT

Step 6: Find the CT from the predefined table

Step 7: Stop

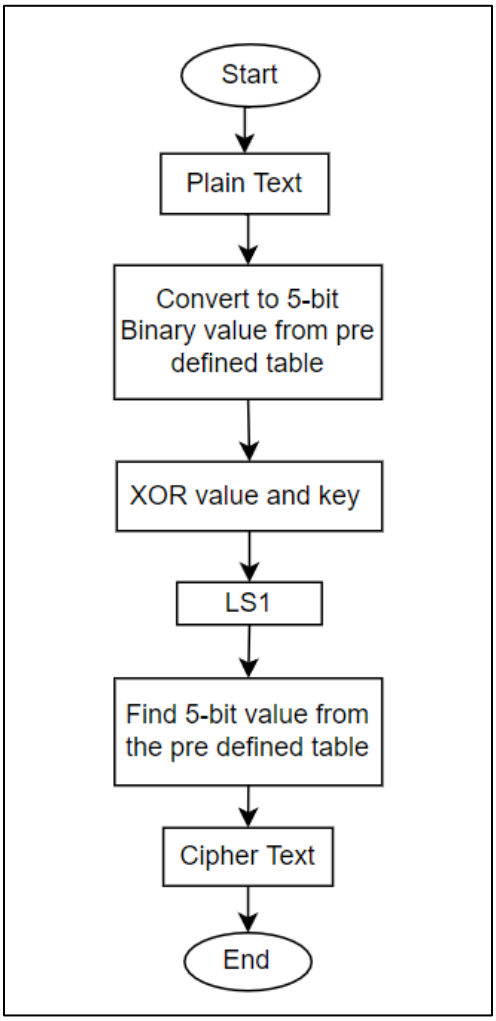

Figure 1: Flowchart for Encryption

For Encryption, every letter of the plain text is split into individual character. Then the respective binary value for the character is searched from the pre-defined table. Then the 5-bit binary value and 5-bit key are XORed. After this step Left shift 1 is done to make the algorithm more complex. Lastly, the cipher text is derived from the binary value from the predefined table.

For Decryption

Step 1: Start

Step 2: Find Cipher Text

Step 3: Covert to 5-bit binary from predefined table

Step 4: Right shift 1

Step 5: XOR CT with Key to find PT

Step 6: Find the PT from the predefined table

Step 7: Stop

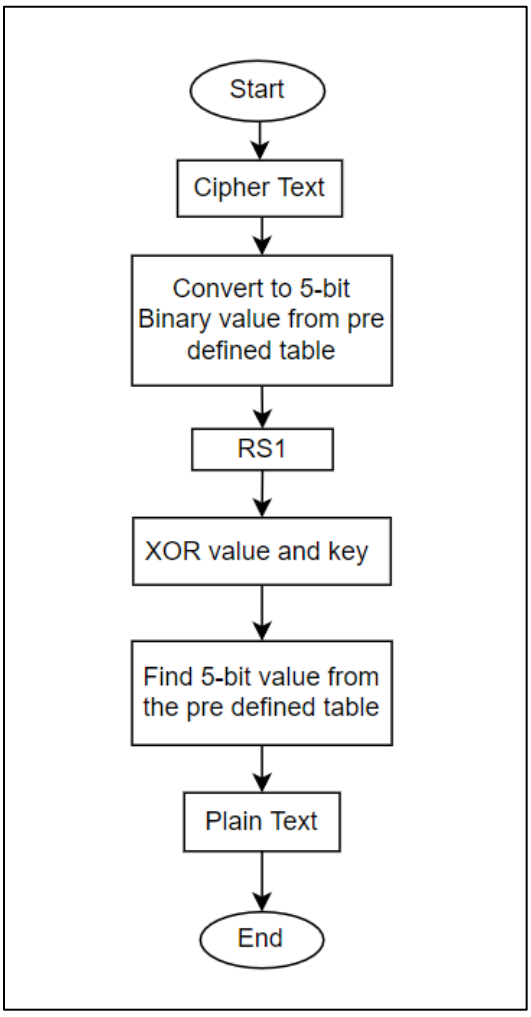

Figure 2: Flowchart for Decryption

For Decryption, every letter of the cipher text is split into individual character. Then the respective binary value for the character is searched from the pre-defined table. Then the step Right shift 1 is don't to the binary value. After this 5-bit binary value and 5-bit key are XORed. Lastly, the plain text is derived from the binary value from the predefined table.

4. Test Cases

4.1 Test 1

For Encryption

Plane Text (PT) = “aadarshakya23@gmail.com”

Key = 11000

For “a”

Step 1: Covert to 5-bit binary from predefined table

PT = 00001

Step 2: XOR PT with Key to find CT

00001

11000

11001

CT = 11001

Step 3: Left shift one on CT

CT = 10011

Step 4: Find the CT from the predefined table

CT = s

Cipher Text (CT) = s

For “d”

Step 1: Covert to 5-bit binary from predefined table

PT = 00100

Step 2: XOR PT with Key to find CT

00100

11000

11100

CT = 11100

Step 3: Left shift one on CT

CT = 11001

Step 4: Find the CT from the predefined table

CT = y

Cipher Text (CT) = y

For “r”

Step 1: Covert to 5-bit binary from predefined table

PT = 10010

Step 2: XOR PT with Key to find CT

10010

11000

01010

CT = 01010

Step 3: Left shift one on CT

CT = 10100

Step 4: Find the CT from the predefined table

CT = t

Cipher Text (CT) = t

For “s”

Step 1: Covert to 5-bit binary from predefined table

PT = 10011

Step 2: XOR PT with Key to find CT

10011

11000

01011

CT = 10110

Step 3: Left shift one on CT

CT = 10110

Step 4: Find the CT from the predefined table

CT = v

Cipher Text (CT) = v

For “h”

Step 1: Covert to 5-bit binary from predefined table

PT = 01000

Step 2: XOR PT with Key to find CT

01000

11000

10000

CT = 10000

Step 3: Left shift one on CT

CT = 00001

Step 4: Find the CT from the predefined table

CT = a

Cipher Text (CT) = a

For “k”

Step 1: Covert to 5-bit binary from predefined table

PT = 01011

Step 2: XOR PT with Key to find CT

01011

11000

10011

CT = 10011

Step 3: Left shift one on CT

CT = 00111

Step 4: Find the CT from the predefined table

CT = g

Cipher Text (CT) = g

For “y”

Step 1: Covert to 5-bit binary from predefined table

PT = 11001

Step 2: XOR PT with Key to find CT

11001

11000

00001

CT = 00001

Step 3: Left shift one on CT

CT = 00010

Step 4: Find the CT from the predefined table

CT = b

Cipher Text (CT) = b

For “@”

Step 1: Covert to 5-bit binary from predefined table

PT = 11011

Step 2: XOR PT with Key to find CT

11011

11000

00011

CT = 00011

Step 3: Left shift one on CT

CT = 00110

Step 4: Find the CT from the predefined table

CT = f

Cipher Text (CT) = f

For “g”

Step 1: Covert to 5-bit binary from predefined table

PT = 00111

Step 2: XOR PT with Key to find CT

00111

11000

11111

CT = 11111

Step 3: Left shift one on CT

CT = 11111

Step 4: Find the CT from the predefined table

CT = &

Cipher Text (CT) = &

For “m”

Step 1: Covert to 5-bit binary from predefined table

PT = 01101

Step 2: XOR PT with Key to find CT

01101

11000

10101

CT = 01011

Step 3: Left shift one on CT

CT = 01011

Step 4: Find the CT from the predefined table

CT = k

Cipher Text (CT) = k

For “i”

Step 1: Covert to 5-bit binary from predefined table

PT = 01001

Step 2: XOR PT with Key to find CT

01001

11000

10001

CT = 10001

Step 3: Left shift one on CT

CT = 00011

Step 4: Find the CT from the predefined table

CT = c

Cipher Text (CT) = c

For “l”

Step 1: Covert to 5-bit binary from predefined table

PT = 01100

Step 2: XOR PT with Key to find CT

01100

11000

10100

CT = 10100

Step 3: Left shift one on CT

CT = 01001

Step 4: Find the CT from the predefined table

CT = i

Cipher Text (CT) = i

For “.”

Step 1: Covert to 5-bit binary from predefined table

PT = 11110

Step 2: XOR PT with Key to find CT

11110

11000

00110

CT = 01100

Step 3: Left shift one on CT

CT = 01100

Step 4: Find the CT from the predefined table

CT = l

Cipher Text (CT) = l

For “c”

Step 1: Covert to 5-bit binary from predefined table

PT = 00011

Step 2: XOR PT with Key to find CT

00011

11000

11011

CT = 11011

Step 3: Left shift one on CT

CT = 10111

Step 4: Find the CT from the predefined table

CT = w

Cipher Text (CT) = w

For “o”

Step 1: Covert to 5-bit binary from predefined table

PT = 01111

Step 2: XOR PT with Key to find CT

01111

11000

10111

CT = 10111

Step 3: Left shift one on CT

CT = 01111

Step 4: Find the CT from the predefined table

CT = o

Cipher Text (CT) = o

Therefore, “aadarshakya23@gmail.com” will be “ssystvasgbs23f&kscilwok”

For Decryption

Cipher Text = “ssystv sgbs23f&kscilwok”

Key = 11000

For “s”

Step 1: Covert to 5-bit binary from predefined table

CT = 10011

Step 2: Right shift 1

11001

Step 3: XOR CT with Key to find PT

11001

11000

00001

PT = 00001

Step 4: Find the PT from the predefined table

PT = a

Plane Text (PT) = a

For “y”

Step 1: Covert to 5-bit binary from predefined table

CT = 11001

Step 2: Right shift 1

11100

Step 3: XOR CT with Key to find PT

11100

11000

00100

PT = 00100

Step 4: Find the PT from the predefined table

PT = d

Plane Text (PT) = d

For “t”

Step 1: Covert to 5-bit binary from predefined table

CT = 10100

Step 2: Right shift 1

01010

Step 3: XOR CT with Key to find PT

01010

11000

10010

PT = 10010

Step 4: Find the PT from the predefined table

PT = r

Plane Text (PT) = r

For “v”

Step 1: Covert to 5-bit binary from predefined table

CT = 10110

Step 2: Right shift 1

01011

Step 3: XOR CT with Key to find PT

01011

11000

10011

PT = 10011

Step 4: Find the PT from the predefined table

PT = s

Plane Text (PT) = s

For a

Step 1: Covert to 5-bit binary from predefined table

CT = 00001

Step 2: Right shift 1

10000

Step 3: XOR CT with Key to find PT

10000

11000

01000

PT = 01000

Step 4: Find the PT from the predefined table

PT = h

Plane Text (PT) = h

For “g”

Step 1: Covert to 5-bit binary from predefined table

CT = 00111

Step 2: Right shift 1

10011

Step 3: XOR CT with Key to find PT

10011

11000

01011

PT = 01011

Step 4: Find the PT from the predefined table

PT = k

Plane Text (PT) = k

For “b”

Step 1: Covert to 5-bit binary from predefined table

CT = 00010

Step 2: Right shift 1

00001

Step 3: XOR CT with Key to find PT

00001

11000

11001

PT = 11001

Step 4: Find the PT from the predefined table

PT = y

Plane Text (PT) = y

For “f”

Step 1: Covert to 5-bit binary from predefined table

CT = 00110

Step 2: Right shift 1

00011

Step 3: XOR CT with Key to find PT

00011

11000

11011

PT = 11011

Step 4: Find the PT from the predefined table

PT = @

Plane Text (PT) = @

For “&”

Step 1: Covert to 5-bit binary from predefined table

CT = 11111

Step 2: Right shift 1

11111

Step 3: XOR CT with Key to find PT

11111

11000

00111

PT = 00001

Step 4: Find the PT from the predefined table

PT = g

Plane Text (PT) = g

For “k”

Step 1: Covert to 5-bit binary from predefined table

CT = 01011

Step 2: Right shift 1

10101

Step 3: XOR CT with Key to find PT

10101

11000

01101

PT = 00001

Step 4: Find the PT from the predefined table

PT = m

Plane Text (PT) = m

For “c”

Step 1: Covert to 5-bit binary from predefined table

CT = 00011

Step 2: Right shift 1

10001

Step 3: XOR CT with Key to find PT

10001

11000

01001

PT = 00001

Step 4: Find the PT from the predefined table

PT = i

Plane Text (PT) = i

For “i”

Step 1: Covert to 5-bit binary from predefined table

CT = 01001

Step 2: Right shift 1

10100

Step 3: XOR CT with Key to find PT

10100

11000

01100

PT = 01100

Step 4: Find the PT from the predefined table

PT = l

Plane Text (PT) = l

For “l”

Step 1: Covert to 5-bit binary from predefined table

CT = 01100

Step 2: Right shift 1

00110

Step 3: XOR CT with Key to find PT

00110

11000

11110

PT = 11110

Step 4: Find the PT from the predefined table

PT = .

Plane Text (PT) = .

For “w”

Step 1: Covert to 5-bit binary from predefined table

CT = 10111

Step 2: Right shift 1

11011

Step 3: XOR CT with Key to find PT

11011

11000

00011

PT = 00011

Step 4: Find the PT from the predefined table

PT = c

Plane Text (PT) = c

For “o”

Step 1: Covert to 5-bit binary from predefined table

CT = 01111

Step 2: Right shift 1

10111

Step 3: XOR CT with Key to find PT

10111

11000

01111

PT = 01111

Step 4: Find the PT from the predefined table

PT = o

Plane Text (PT) = o

Therefore, “aadarshakya23@gmail.com” will be “ssystvasgbs23f&kscilwok”

4.2 Test 2

For Encryption

Plane Text (PT) = r

Key = 11010

Step 1: Covert to 5-bit binary from predefined table

PT = 10010

Step 2: XOR PT with Key to find CT

10010

11010

01000

CT = 01000

Step 3: Left shift one on CT

CT = 10000

Step 4: Find the CT from the predefined table

CT = p

Cipher Text (CT) = p

For Decryption

Cipher Text (CT) = p

Key = 11010

Step 1: Covert to 5-bit binary from predefined table

CT = 10000

Step 2: Right shift 1

01000

Step 3: XOR CT with Key to find PT

01000

11010

10010

PT = 10010

Step 4: Find the PT from the predefined table

PT = r

Plane Text (PT) = r

4.3 Test 3

For Encryption

Plane Text (PT) = space

Key = 11111

Step 1: Covert to 5-bit binary from predefined table

PT = 00000

Step 2: XOR PT with Key to find CT

00000

11111

11111

CT = 11111

Step 3: Left shift one on CT

CT = 11111

Step 4: Find the CT from the predefined table

CT = &

Cipher Text (CT) = &

For Decryption

Cipher Text (CT) = &

Key = 11111

Step 1: Covert to 5-bit binary from predefined table

CT = 11111

Step 2: Right shift 1

11111

Step 3: XOR CT with Key to find PT

11111

11111

00000

PT = 00000

Step 4: Find the PT from the predefined table

PT = “ ”(space)

Plane Text (PT) = “ ”(space)

4.4 Test 4

For Encryption

Plane Text (PT) = &

Key = 11000

Step 1: Covert to 5-bit binary from predefined table

PT = 11111

Step 2: XOR PT with Key to find CT

11111

11000

00111

CT = 00111

Step 3: Left shift one on CT

CT = 01110

Step 4: Find the CT from the predefined table

CT = n

Cipher Text (CT) = n

For Decryption

Cipher Text (CT) = n

Key = 11000

Step 1: Covert to 5-bit binary from predefined table

CT = 01110

Step 2: Right shift 1

00111

Step 3: XOR CT with Key to find PT

00111

11000

11111

PT = 11111

Step 4: Find the PT from the predefined table

PT = &

Plane Text (PT) = &

4.5 Test 5

For Encryption

Plane Text (PT) = @

Key = 00000

Step 1: Covert to 5-bit binary from predefined table

PT = 11011

Step 2: XOR CT with Key to find PT

11011

00000

11011

CT = 11011

Step 3: Left shift one on CT

CT = 10111

Step 6: Find the PT from the predefined table

CT = w

Cipher Text (CT) = w

For Decrypting

Cipher Text (CT) = w

Key = 00000

Step 1: Covert to 5-bit binary from predefined table

CT = 10111

Step 2: Right shift 1

11011

Step 3: XOR CT with Key to find PT

11011

00000

11011

PT = 11011

Step 4: Find the PT from the predefined table

PT = @

Plane Text (PT) = @

5. Critical Evaluation of the XOR & Key algorithm

Just like other algorithms the XOR & Key algorithm also has its own strengths and weakness. The strengths include hard to guess and has a lengthy process. Whereas the weakness are limited characters, simple algorithm and number of characters are the same.

More into strengths, this algorithm uses its own predefined table which has respective binary values for limited characters. This means the information will be more secure because the character can have any binary value. Unlike ASCII table where binary value is fixed, the binary value in this algorithm can change.

Similarly, different key leads to different output. This will also make the cryptographic algorithm hard to guess. A 5-bit key can make 32 different keys which makes it more complex to guess.

Also, the cryptographic algorithm is very lengthy. Each word of the plain text has to go through the steps shown before. So, even if the malicious entities know the process of decryption, it will be time consuming and therefore might not decrypt the information. Therefore, this cryptographic algorithm is computationally secure.

However, the cryptographic algorithm can encrypt only 32 different characters. So, if more than 32 characters are used in a plain text there will be letters which were never encrypted. Also, while encryption and decrypting the letter “o” is unchanged.

Similarly, the algorithm is very simple. So, if the malicious entities have sufficient time to decrypt the information this algorithm cannot be used. And lastly, the number of characters in plain text and cipher text is the same which will make the algorithm weak.

Based on this cryptographic algorithm’s strengths and weaknesses this can be used in long texts which will bring the best of this algorithms strengths and can be used for information which will be meaningless after some time.

6. Conclusion

For conclusion, cryptographic system helps convert plain text to cipher text and vice versa. This allows users to maintain unconditional security where the malicious entities might gain access over the file but cannot understand the information.

References

Bacon, M., 2021. *What is Security?.* [Online] Available at: https://www.techtarget.com/searchsecurity/definition/security [Accessed 9 January 2022].

Geeks for Geeks, 2019. *Columnar Transposition Cipher - GeeksforGeeks.* [Online] Available at: https://www.geeksforgeeks.org/columnar-transposition-cipher/ [Accessed 9 January 2022].

GhostVolt, 2021. *The Story of Cryptography : Historical Cryptography.* [Online] Available at: https://ghostvolt.com/articles/cryptography_history.html [Accessed 9 January 2022].

Shashank, 2020. *What is Cryptography? | Cryptographic Algorithms | Types of Cryptography |Edureka.* [Online] Available at: https://www.edureka.co/blog/author/shashankedureka-co/ [Accessed 9 January 2022].

Sidhpurwala, H., 2013. *A Brief History of Cryptography.* [Online] Available at: https://www.redhat.com/en/blog/brief-history-cryptography#:~:text=The%20first%20known%20evidence%20of,place%20of%20more%20ordinary%20ones. [Accessed 9 January 2022].