International Journal of Scientific & Engineering Research, Volume 8, Issue 1, January -2017
ISSN 2229-5518

Encryption Using Timing Clock

YAHYA LAYTH KHALEEL, MUSTAFA ABDULFATTAH HABEEB, RAGHAD ABDULRAHMAN SHABAN

Abstract— In this research will be work to encryption algorithm based on a new idea to encrypt text data, which depends on the architectural and mathematical operations and then generate the cipher text output the these operations where we will be the removal of the letters and replace letters, numbers and symbols depending on the specific algorithm indicated the pulses time, finally this research It includes clarification of a new way to encrypt data using architectural thought to get rid the frequencies of letters, in addition to the algorithm will be the launch of its name (Clock encryption).

Index Terms— Computer Security, Data Encryption, Clock, CTE, Symmetric, Substitution, Key, Frequency, shifting, Characters, Cipher.

1 Introduction

Led the increasing growth of multimedia applications on a communication networks to the increase in the need to provide efficient modalities Which works to protect data and private ownership of the individual and therefore had to be a means to act providing for the security of these media To protect it from theft hacking and tampering with counterfeiting and dissemination of sensitive information.

Hence the need for the provision of data security, and this means the encryption flag who cares to provide protection for the storage and transfer the data through the use of a secret key, therefore encryption still successful way to protect data stored that sent across the network, but with an increase in high traffic areas networks and information network internet world, it has become difficult to keep these data, particularly that it always be accessible through the Internet in the clear wording sends that Doubt The attention of the intruder to open this encryption or destruction of the information transmitted.The hide of information means include information in the information apparently does not call into doubt and draw attention, and not be aware of before hackers and attackers, so the information will not be rumored to users of the network, but remains content exclusive to the relevant authorities, which are familiar with how to extract this content.

2 Shifting and Frequency in Encryption

The ciphertext generated by using keys,the are two types of keys, The first called a similar switch, which uses the same key in the encryption and decryption [1], an example of this type of keys (Caesar) encryption which uses Shifting or the so-called "shift chiper" where each character in the message replaced with the another letter in the alphabet [2], In this type will be very easy to break the key because its used constant key and the character shift in the letter to the another character. For example, when using the 4 key and when there is a character in the letter A to the letter will Encrypts E, its easy to decryption by using the same key [1], This case is easy to break through the use of key characters frequencies by calculate these frequencies in the encrypted message the knowledge of the frequency highest in the ciphertext and returned what is being compensated by the letter E in the original text of the letters that the Supreme frequency and the proportion of its frequency in the texts approximately 12.7, and the character that followed in frequency is the letters t,...Etc, the figure below shows the frequencies of the letters in the language and knowledge of the ciphertext frequencies we can knowledge of the key and break the encryption [3].

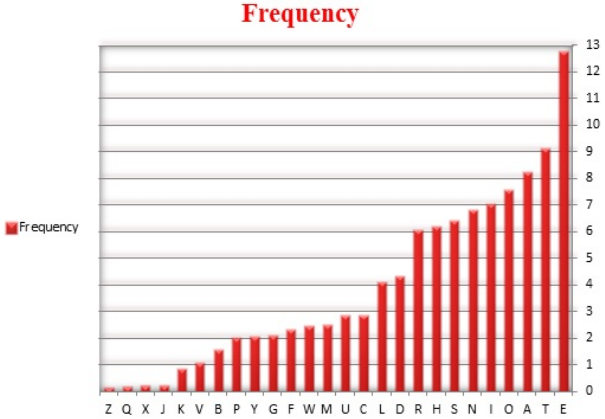

Figure.1. Frequencies of the letters

- ***YAHYA LAYTH KHALEEL*** *has been awarded the degree of BSc in Computer Sciences Department from College of Computer Sciences and Mathematics from Tikrit University, Iraq, in 2012, Currently working in Computer and Informatics Center, Tikrit University, Iraq.*
  E-mail: yahya@ tu.edu.iq
- ***MUSTAFA ABDULFATTAH HABEEB*** *has been awarded the degree of BSc in Computer Sciences Department from College of Computer Sciences and Mathematics from Tikrit University, Iraq, in 2012, Currently working in Computer and Informatics Center, Tikrit University, Iraq.*
  E-mail: mustafa@ tu.edu.iq
- ***RAGHAD ABDULRAHMAN SHABAN*** *has been awarded the degree of BSc in Computer Sciences Department from College of Computer Sciences and Mathematics from Tikrit University, Iraq, in 2009, Currently working in dentistry college, Tikrit University, Iraq.*
  E-mail: rw@ tu.edu.iq

International Journal of Scientific & Engineering Research, Volume 8, Issue 1, January -2017
ISSN 2229-5518

The second type of keys is a different key, used different key encryption from the decryption, an example of this type of algorithm key is (RSA) encryption, which uses two keys a public key and a private key, in this kind scientists were able to get rid of the frequencies of letters and break the encryption and this type of keys to be the toughest in the decoding of the second type, but this kind exhibition vandalized easily by change the public key [2].

3 Clock Encryption

3.1 Encryption Method

Before starting the encryption we will re-arrange all the 96 characters used.

The characters in the standard order of ASCII code is shown in the table below:

TABLE 1
ASCII PRINTABLE CHARACTERS+ ENTER / CARRIAGE RETURN CHARACTER [5]

index	Dec	Hex	Binary	Character	Description
0	32	20	00100000	Space	space
1	33	21	00100001	!	exclamation mark
2	34	22	00100010	"	double quote
3	35	23	00100011	#	number
4	36	24	00100100	$	dollar
5	37	25	00100101	%	percent
6	38	26	00100110	&	ampersand
7	39	27	00100111	'	single quote
8	40	28	00101000	(	left parenthesis
9	41	29	00101001	)	right parenthesis
10	42	2A	00101010	*	asterisk
11	43	2B	00101011	+	plus
12	44	2C	00101100	,	comma
13	45	2D	00101101	-	minus
14	46	2E	00101110	.	period
15	47	2F	00101111	/	slash
16	48	30	00110000	0	zero
17	49	31	00110001	1	one
18	50	32	00110010	2	two
19	51	33	00110011	3	three
20	52	34	00110100	4	four
21	53	35	00110101	5	five
22	54	36	00110110	6	six
23	55	37	00110111	7	seven
24	56	38	00111000	8	eight
25	57	39	00111001	9	nine
26	58	3A	00111010	:	colon
27	59	3B	00111011	;	semicolon
28	60	3C	00111100	<	less than
29	61	3D	00111101	=	equality sign
30	62	3E	00111110	>	greater than
31	63	3F	00111111	?	question mark
32	64	40	01000000	@	at sign
33	65	41	01000001	A	
34	66	42	01000010	B	
35	67	43	01000011	C	
36	68	44	01000100	D	
37	69	45	01000101	E	
38	70	46	01000110	F	
39	71	47	01000111	G	
40	72	48	01001000	H	
41	73	49	01001001	I	
42	74	4A	01001010	J	
43	75	4B	01001011	K	
44	76	4C	01001100	L	
45	77	4D	01001101	M	
46	78	4E	01001110	N	
47	79	4F	01001111	O	
48	80	50	01010000	P	
49	81	51	01010001	Q	

International Journal of Scientific & Engineering Research, Volume 8, Issue 1, January -2017
ISSN 2229-5518

index	Dec	Hex	Binary	Char-acter	Description
50	82	52	01010010	R	
51	83	53	01010011	S	
52	84	54	01010100	T	
53	85	55	01010101	U	
54	86	56	01010110	V	
55	87	57	01010111	W	
56	88	58	01011000	X	
57	89	59	01011001	Y	
58	90	5A	01011010	Z	
59	91	5B	01011011	[	left square bracket
60	92	5C	01011100	\	backslash
61	93	5D	01011101	]	right square bracket
62	94	5E	01011110	^	caret / circumflex
63	95	5F	01011111	_	underscore
64	96	60	01100000	`	grave / accent
65	97	61	01100001	a	
66	98	62	01100010	b	
67	99	63	01100011	C	
68	100	64	01100100	d	
69	101	65	01100101	E	
70	102	66	01100110	F	
71	103	67	01100111	g	
72	104	68	01101000	h	
73	105	69	01101001	I	
74	106	6A	01101010	J	
75	107	6B	01101011	K	
76	108	6C	01101100	L	
77	109	6D	01101101	m	
78	110	6E	01101110	n	
79	111	6F	01101111	o	
80	112	70	01110000	p	

index	Dec	Hex	Binary	Char-acter	Description
81	113	71	01110001	q	
82	114	72	01110010	R	
83	115	73	01110011	S	
84	116	74	01110100	T	
85	117	75	01110101	u	
86	118	76	01110110	V	
87	119	77	01110111	w	
88	120	78	01111000	X	
89	121	79	01111001	Y	
90	122	7A	01111010	Z	
91	123	7B	01111011	{	left curly bracket
92	124	7C	01111100	|	vertical bar
93	125	7D	01111101	}	right curly brack-et
94	126	7E	01111110	~	tilde
95	13	0D	00001101	CR	enter / carriage return

The number of characters that will be used in encryption is 16 characters because we will use the hexadecimal system, for this it must be rearranged with the remaining 80 characters to avoid the juxtaposition between the characters and the purpose of using the largest number of characters when using the shifting indexes of characters as much as possible.

The mechanism of re-arrange characters will be as follows:

- Finding prime numbers between 1 to 96, which are:2,3,5,
- Divide the prime numbers that have been created in the previous point to other groups where we will take the first set of numbers The lowest 10 and we take the second set numbers between 10 and 20 ... etc. as shown in the table below:
- Give the numbers that will be encrypted (1 ... 9) the first number of each group that have been created in the previous point (located in the left hand in each group).
- Give the numbers that will be encrypted (A ... F) the first number of each group that have been created in the second point (from the right) on condition that is the difference between the number and another number at least ten.

The re-arrange the characters will be as in the following table:

International Journal of Scientific & Engineering Research, Volume 8, Issue 1, January -2017
ISSN 2229-5518

TABLE 2
ASCII PRINTABLE CHARACTERS+ ENTER / CARRIAGE RETURN CHARACTER AFTER RE-ARRANGING

index	Dec	Hex	Binary	Character	Description
0	32	20	00100000	Space	space
1	33	21	00100001	!	exclamation mark
2	48	30	00110000	0	zero
3	34	22	00100010	"	double quote
4	35	23	00100011	#	number
5	36	24	00100100	$	dollar
6	37	25	00100101	%	percent
7	70	46	01000110	F	
8	38	26	00100110	&	ampersand
9	39	27	00100111	'	single quote
10	40	28	00101000	(	left parenthesis
11	49	31	00110001	1	one
12	41	29	00101001	)	right parenthesis
13	42	2A	00101010	*	asterisk
14	43	2B	00101011	+	plus
15	44	2C	00101100	,	comma
16	45	2D	00101101	-	minus
17	46	2E	00101110	.	period
18	47	2F	00101111	/	slash
19	69	45	01000101	E	
20	58	3A	00111010	:	colon
21	59	3B	00111011	;	semicolon
22	60	3C	00111100	<	less than
23	50	32	00110010	2	two
24	61	3D	00111101	=	equality sign
25	62	3E	00111110	>	greater than
26	63	3F	00111111	?	question mark
27	64	40	01000000	@	at sign
28	71	47	01000111	G	
29	72	48	01001000	H	
30	73	49	01001001	I	
31	51	33	00110011	3	three
32	74	4A	01001010	J	
33	75	4B	01001011	K	
34	76	4C	01001100	L	
35	77	4D	01001101	M	
36	78	4E	01001110	N	
37	68	44	01000100	D	
38	79	4F	01001111	O	
39	80	50	01010000	P	
40	81	51	01010001	Q	
41	82	52	01010010	R	
42	83	53	01010011	S	
43	52	34	00110100	4	four
44	84	54	01010100	T	
45	85	55	01010101	U	
46	86	56	01010110	V	
47	87	57	01010111	W	
48	88	58	01011000	X	
49	89	59	01011001	Y	
50	90	5A	01011010	Z	
51	91	5B	01011011	[	left square bracket
52	92	5C	01011100	\	backslash
53	53	35	00110101	5	five
54	93	5D	01011101	]	right square bracket
55	94	5E	01011110	^	caret / circumflex
56	95	5F	01011111	_	underscore
57	96	60	01100000	`	grave / accent
58	97	61	01100001	a	
59	67	43	01000011	C	

International Journal of Scientific & Engineering Research, Volume 8, Issue 1, January -2017
ISSN 2229-5518

index	Dec	Hex	Binary	Character	Description
60	98	62	01100010	b	
61	99	63	01100011	C	
62	100	64	01100100	d	
63	101	65	01100101	E	
64	102	66	01100110	F	
65	103	67	01100111	g	
66	104	68	01101000	h	
67	54	36	00110110	6	six
68	105	69	01101001	I	
69	106	6A	01101010	J	
70	107	6B	01101011	K	
71	55	37	00110111	7	seven
72	108	6C	01101100	L	
73	109	6D	01101101	m	
74	110	6E	01101110	n	
75	111	6F	01101111	o	
76	112	70	01110000	p	
77	113	71	01110001	q	
78	114	72	01110010	R	
79	66	42	01000010	B	
80	115	73	01110011	S	
81	116	74	01110100	T	
82	117	75	01110101	u	
83	56	38	00111000	8	eight
84	118	76	01110110	V	
85	119	77	01110111	w	
86	120	78	01111000	X	
87	121	79	01111001	Y	
88	122	7A	01111010	Z	
89	65	41	01000001	A	
90	123	7B	01111011	{	left curly bracket
91	57	39	00111001	9	nine
92	124	7C	01111100	|	vertical bar
93	125	7D	01111101	}	right curly bracket
94	126	7E	01111110	~	tilde
95	13	0D	00001101	CR	enter / carriage return

After rearranging the characters being starting the encryption, which can be summarized as follows:

1. Taking the original text and convert it to the ASCII Code.
2. Convert all the 0 to 1 and vice versa.
3. Took all four bits and converted to hexadecimal system.
4. Find the number of result characters.
5. Taking the first four places of the number of result characters, if the number of resulting characters less than four ranks being as the following:

- If the number consists of three ranks, the one remaining rank compensates 0 (in place of the fourth rank).
- If the number consists of two ranks, the two remaining ranks compensate 0 (in place of the third and fourth ranks).
- If the number consists of one rank, the three remaining ranks compensate 0 (in place of the second, third and fourth ranks).
- If the first and second ranks of the number of result characters more than 12 characters being the result of finding the rest of the division by 12.
- If the third and fourth ranks of the number of result characters more than 60 being the result of finding the rest of the division by 60.

6-The resulting number (from 4,5) converted to the time format (The first and second ranks from left refer to the hours, and the third and fourth ranks from left refer to the minutes).

7- being start encryption by using a clock where Put the time that was obtained in the previous step (point 6), where will indicate the minutes to the number of shifting positions and will start from the first letter, With each character are added minutes, the number of shifting positions increases one by the value of the hour for every adding minute while the times of shifting positions remain fixed until the start of a new hour, as it is shown in the following figure:

Fig. 2. Example of Cock Encryption.

International Journal of Scientific & Engineering Research, Volume 8, Issue 1, January -2017
ISSN 2229-5518

8-Obtaining the cipher text.

3.2 Encryption Algorithm

The following figure shows the encryption algorithm after rearranging the characters:

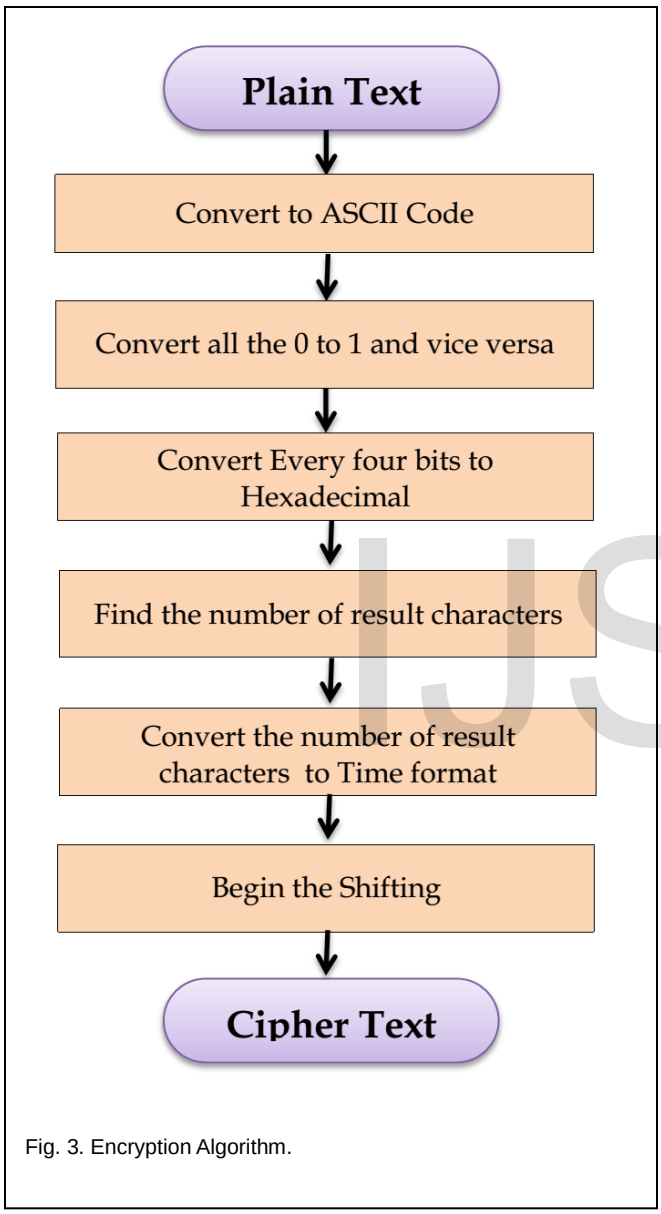

Fig. 3. Encryption Algorithm.

3.3 Example

The Plain Text: Hello

- Convert to ASCII Code: 01001000 01100101 01101100 01101100 01101111
- Convert every 0 to 1 and vice versa: 10110111 10011010 10010011 10010011 10010000
- Convert to Hexadecimal: B79A939390
- Convert to Time: 10:00
- Begin the Shifting from 10:01 as

B= index of B+10*1
7=index of 7+10*2
0=index of 9+10*3
A=index of A+10*4
9=index of 9+10*5
3=index of 3+10*6
9=index of 9+10*7
3=index of 3+10*8
9=index of 9+10*9
0=index of 0+10*10

- The Cipher Text: A9JKU9g,w%

4 Conclusion

Although a huge development in technology, but the encryption in this manner is characterized by the high security addition to the possibility be used manually, it reduces the difference frequency between the characters In addition it is composed of more than one method nested encryption and thus it gives the algorithm for high-security feature and the difficulty of breaking it.

References

[1] Kushwahaa, A. , Sharmab,H. R., Ambhaikarc, A. (2016). A Novel Selective Encryption Method for Securing Text over Mobile Ad hoc Network. Procedia Computer Science, 79(2016)16–23.

[2] Verma, P., Gaba, G. S. (2016). EXTENDED CAESAR CIPHER FOR LOW POWERED DEVICES. International Science Press, 9(11)2016, pp. 5391-5400.

[3] Algorithm [Online]. Available: https://www.programming-algorithms.net

[4] Kaur, D., Kaur, R. (2016). Secure and Optimized Data Migration Scheme over Cloud Severs using ABC Optimization and RSA Encryption. INTERNATIONAL JOURNAL OF RESEARCH IN ELECTRONICS AND COMPUTER ENGINEERING, ISSN: 2348-2281.

[5] ASCII Table [Online]. Available: http://www.rapidtables.com/code/text/ascii-table.htm