Journal of Computer and Mathematical Sciences, *Vol.11(11),72-87 November 2020* *ISSN 0976-5727 (Print)*
(An International Research Journal), *www.compmath-journal.org* *ISSN 2319-8133 (Online)*

A Novel approach of Dynamic Cryptography using Random virtual 2D Data Tokens

Rahul Kumar[1] and Anurag Sinha[2]

[1,2]Department of Computer Science and IT,
Student, Amity University Jharkhand Ranchi, Jharkhand, 834001 INDIA.
email:rahulkkumar1997@gmail.com, anuragsinha257@gmail.com.

(Received on: October 25, 2020)

ABSTRACT

In today's world, data security is the main concern for anyone. Information security is the most extreme basic issue in guaranteeing safe transmission of data through the web. Data security ensures that our data is only accessible by the intended receiver and prevents any modification or alteration of data. In order to achieve this level of security, various cryptography algorithms and methods have been developed. This paper proposes a new Dynamic Cryptography technique through which Security can be enhanced as it increases the complexity of solving the cipher text when handled by intruders.

Keywords: Encryption, Decryption, Computer Security, Cryptography, DES, AES, Blowfish, RSA, CL-PKC, Securing Data, Hacking.

1. INTRODUCTION

1.1 State of the art

With the web having arrived at a level that converges with our carries on with, developing dangerously during the most recent quite a few years, information security has become a primary worry for anybody associated with the web. Security is a significant in ensuring information against interlopers. One of the most significant techniques for guaranteeing information mystery is cryptography. Cryptography is mystery composing for information security insurance. All around shrouded information can only with significant effort be perused, changed or created. Cryptography ensures pivotal information by means of transforming it into hazy information that must be gotten to through approved collectors, who at that point changes over the unsure information into the first literary substance. The way toward changing unique content into muddled content (figure text) with a specific key alluded to as encryption, and something contrary to encryption measure is alluded to as unscrambling Cryptography gives number of security objectives to guarantee of protection of information, on-adjustment of information, etc. Cryptography is utilized to guarantee that the substance of a message is very classification communicated and would not be adjusted. The development of encryption is moving towards an eventual fate of perpetual type of potential outcomes. As it is difficult to quit hacking, we can make sure about our touchy information even it is hacked utilizing encryption methods and which ensuring the data security? In this paper we present another technique for Dynamic Cryptography.

2. LITERATURE SURVEY

DNA encryption technique relies upon mathematical system control where they used an ensured age estimation to make new key for encryption measure. The upside of this key age plot is that they by and large get another code data for same plaintext and same key. It gives a nice security layer which doesn't give any infer about plaintext. DNA cryptography can be gotten together with standard cryptography to give cross variety security. It is so far making its fundamental steps, so there is a lot of degree to work around there of cryptography and need more works and explores to show up at the affirmation and to overhaul the particular issues.[1]

A cross variety approach of cryptography by using traditional symmetric code to encode part of message while covering other part inside a DNA microdot to ensure the aggressor can't get the message without haggling the two areas. This will in itself be made shaky for the assailant by covering data holding DNA behind a swarm of similar DNA strands which would be acting like spread authorities. Thusly, given the secret keys are moved securely we can expect that the count will ruin any sort of assailant to deal the correspondence by raising his level of attempts and cost of productive attack a ton past the standard PC based estimations.[2]

A couple of tries have been made to dispense with the deficiencies in the arrangement of DNA steganography and cryptography. A data hiding computation has been arranged by using DNA progressions thought and customary steganography technique. Using steganography they cover the data into the DNA groupings and send mixed DNA courses of action close by a key to the beneficiary side. Using this key worth and mixed substance the recipient with no issue recovers the plain substance. Using this strategy they send and get the data with no insufficiency. In case any undertaking is made to make a fake data then the beneficiary can know after applying the computation into fake data since it can't gives the same results when we apply key on it. This estimation is very profitable and easy to use. DNA enlisting has more splendid improvement possibilities in field of Steganography and approval, which have a more layer protection than a singular encryption.[3]

A couple of procedures weight on utilizing DNA cryptography for giving security in correspondence, especially in data transmission in distant sensor associations. SSL (Secure

Socket Layer) is used to decide the issue of sharing keys in a WSN. Digressed key encryption is followed, for which the keys are created using RSA figuring. Right when the sensor center points are passed on, each center point is given out a key pair and progressed support, inferable from its microscopic accumulating and low power. Public keys are exchanged through SSL. Security here is cultivated in 3 stages - information, computation and DNA depiction. The ideal situation of this procedure lies in the achievement of access control, openness and imprint. The primary drawback observed, is the errand of key sets and thesignature to each and every center in the WSN, before game plan.[4]

The current paper give the security at two levels for such a record. Regardless of the two fold level encryption and second, at the DNA change. The equivalent encryption is finished by doing the delivering of 8x8 organizations spirally by social event the 4 zones at an event to stir up the twofold characteristics. The following advance is change of the essential piece into ASCII plan and scrambling the information as shown by the static DNA word reference table. This outcomes in the blended record.[5]

2. RELATED WORK

Cryptology is the investigation of cryptosystem [Goldreich, 2000; Katz and Lindell, 2014]. It is the science for data security which changes over conventional plain content into human indiscernible codes for example figure text and the other way around. Cryptology has two subfields, viz., cryptography and cryptanalysis.

Cryptography is the method created by applying science and rationale to store and send information in coded and made sure about structure with the goal that solitary the planned beneficiary can peruse and measure it. The technique for making sure about information by producing figure text from plain content is otherwise called encryption. Cryptography shields information from the outsiders for example enemies and furthermore it is utilized for client verification. Cryptanalysis or unscrambling is the science or strategy to disentangle the figure text. The fundamental model of cryptosystem is spoken to in Fig. 1.

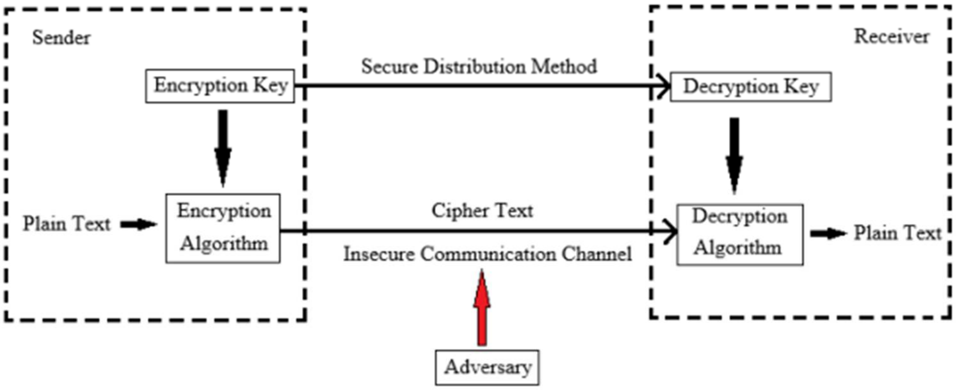


Figure 1: Model for Cryptography

Commonly used terms in Cryptography

- Plaintext: The first and justifiable content. As an occurrence, 'Y' needs to communicate a "PC" message to 'Z'. Here, "PC" is the plaintext or the first message.
- Cipher text: The content that can't be perceived by method of anyone or a hogwash text, model "A@$&J9."
- Encryption: A cycle of changing clear content into indistinct content. The way of decipherment needs an decipherment calculation and a key. Decipherment happens on the sender side.
- Decryption: An opposite strategy for encode. It is a way of changing over cipher text into plaintext.
- Key: A key is character, number, or an uncommon character. It is utilized at the hour of decipherment on the first content and at the hour of translate on the cipher text.

3. PRELIMINIARY

Purpose of Cryptography

Authentication: The capability of a framework to test the character of the sender.
Confidentiality: Information communicated should be gotten to handiest by utilizing lawful gatherings and not through any other individual.
Integrity: Only the approved gatherings are allowed to adjust on sent data.
Non-renouncement: Is the assurance that somebody can't prevent the legitimacy from getting something.
Access Control: Just the approved people are skilled to get right of section to the given data

Techniques of Cryptography

The two key strategies for encoding information are "symmetric cryptography," which involves the use of a similar key to scramble/translate data; and "topsy-turvy cryptography," which utilizes public and private keys to encode/disentangle data. Instances of symmetric calculations are Data Encryption Standard (DES), Triple-DES (3DES), Blowfish, and Advanced Encryption Standard (AES)[20]. The most notable deviated calculations are RSA and ELGAMAL Schema.

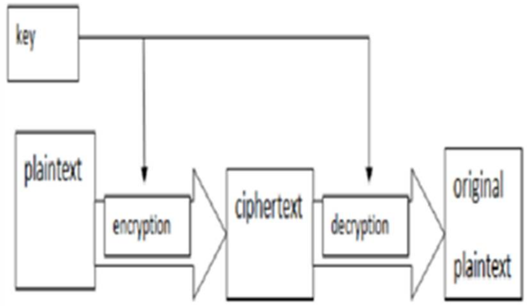


Figure 2: Symmetric cryptosystem

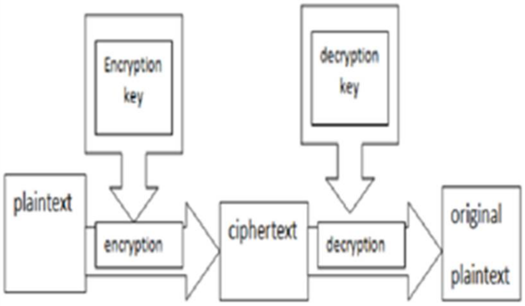


Figure 3: Asymmetric cryptosystem

Types of Cryptography

Secret Key Cryptography: At the point when a similar key is utilized for both encryption and unscrambling, DES, Triple DES, AES, RC5 and so forth, might be the instances of such encryption, at that point that component is known as mystery key cryptography.

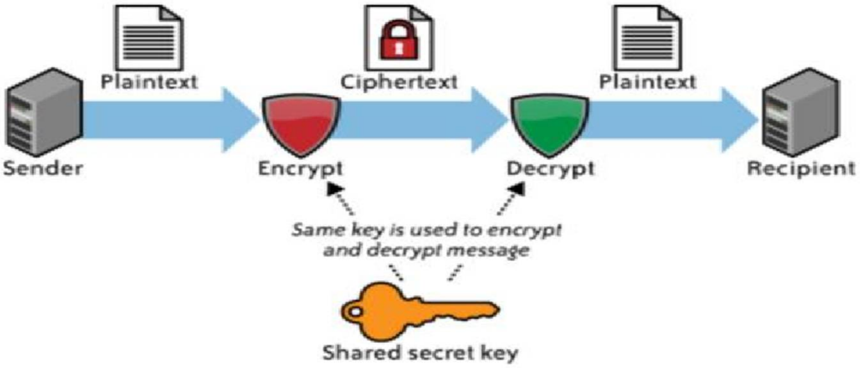


Figure 4: Secret Key Cryptography

Public Key Cryptography: the point when two distinct keys are utilized, that is one key for encryption and another key for decoding, RSA, Elliptic Curve and so forth, might be the instances of such encryption, at that point that instrument is known as open key cryptography.

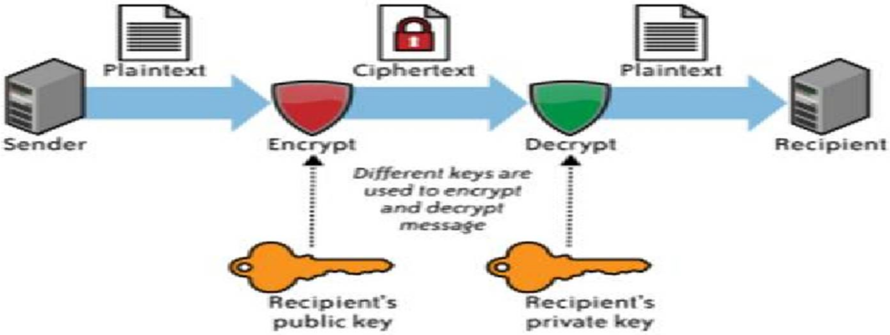


Figure 5: Public Key Cryptography

4. ENCRYPTION ALGORITHM

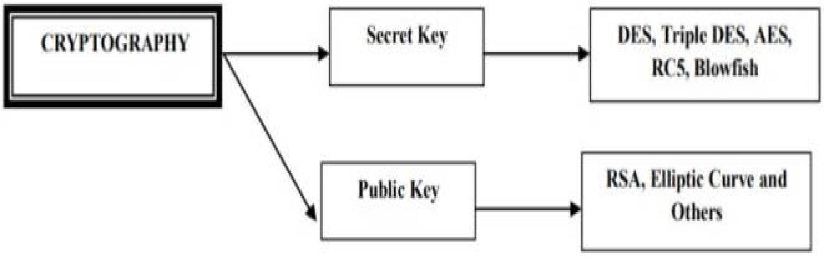

CRYPTOGRAPHY
Secret Key
DES, Triple DES, AES, RC5, Blowfish
Public Key
RSA, Elliptic Curve and Others

Figure 6: process of cryptography

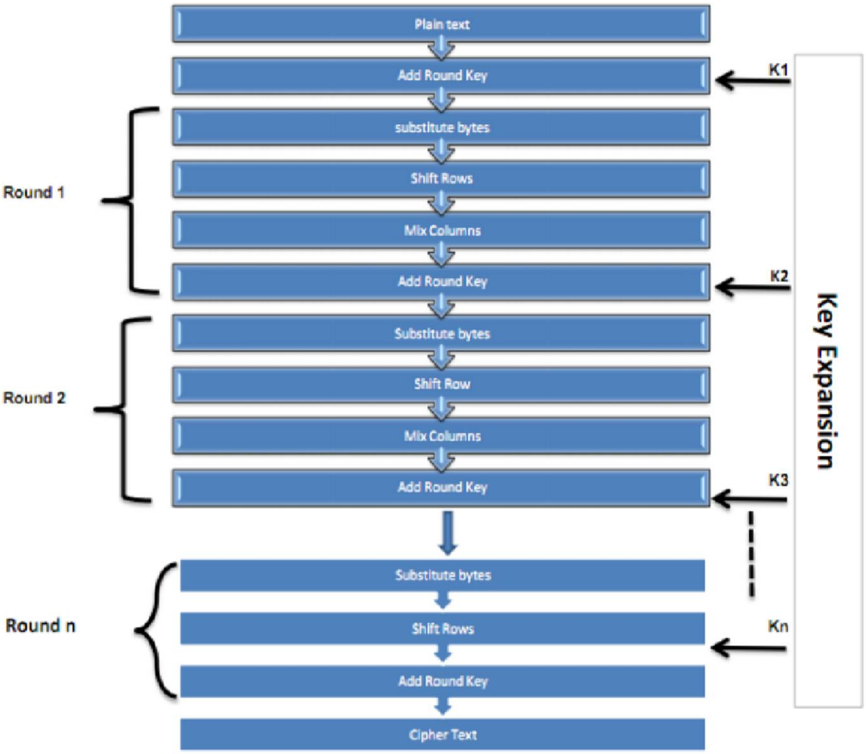


Figure 7: AES algorithm

DES: DES is the soonest symmetric decipherment calculation presented in 1972 by International Business Machines Corporation and in 1977 it has been Agreed as Federal Information Processing Standard through the National Bureau of Standard[3]. It involves similar strides as SDES and cycles a 64-digit contribution with a starter change. In DES, the quantity of rounds is 16 while in SDES is two adjusts additionally the S-DES utilizes 8 pieces for input.

Triple DES (3DES):3DES was recommended by IBM (International Business Machines Corporation) in 1998. A substitute for DES, 3DES shows improved key size and applies the DES calculation 3 rounds in every information block. The key length for the 3DES is 112 and 168 pieces, the quantity of rounds is 48 and the square length is 64 pieces[4]. This calculation means to expand insurance and security through its more drawn out key size comparative with DES. Nonetheless, it is additional tedious than DES is when applied to the encryption cycle.

Blowfish: Blowfish is a kind of symmetric square code produced by B. Schneier in 1993. Blowfish is quick calculation, permit free, and unpatented. It utilizes a key length in the scope of 32–448 and a 64 cycle block. The Blowfish calculation makes utilize 16 round for the encipherment strategy Fig. 6. Blowfish conventionally utilizes 4 S-boxes as opposed to of one S-box. It requires extra handling time since it depends on key length, anyway it gives solid wellbeing[4]. Keep your content and realistic documents separate until after the content has been arranged and styled. Try not to utilize hard tabs, and breaking point utilization of hard re-visitations of just one return toward the finish of a passage. Try not to include any sort of pagination anyplace in the paper. Try not to number content heads-the layout will do that for you.

Advanced Encryption Standard (AES): AES was sending by the National Institute of Standards and Technology in 2001; it is additionally called "Rijndael"[5]. AES is a square code with a square size of 128 pieces. The key length can be 128, 192 or 256 pieces. Encipherment incorporates ten rounds of handling for 128-digit keys, 12 rounds for 192-piece keys and 14 rounds for 256-cycle keys. The calculation is called AES-128, AES-192 or AES-256 depending on the key size[5]. The means for each round incorporate of 4 layers, especially, substitution byte, move lines, mix segment and include round key as show up in Fig.5 [4].

Comparison of Cryptography Algorithms

E. Thambiraja, G. Ramesh, Dr. R. Umarani[8] have done review on most basic encryption methods. Monika Agrawal and Pradeep Mishra[9] in have likewise done a similar review on Secret Key Encryption Techniques. Gurujeevan Singh, Ashwani Kumar Singla, K.S.Sandha[6] in have given examination of different cryptography strategy calculations.

Table 1. Cryptography Algorithms – A Comparison

Algorithm	Developed (Year)	KeySize(inbits)	BlockSize(bits)
DES	IBM1975	56	64
3DES	IBMinyear1978	112(or)168	64
AES	JoanDaemenandVincentRijmen1998	256	128
Blowfish	BruceSchneier1993	32(or)448	64

5. METHODOLOGY

Proposed Algorithm

In this algorithm, data set is taken and encryption will occur only with the help of these data tokens. Algorithm is divided into three stages:

- Generation of Virtual Keyboard: A KEYBOARD 2- D array is generated which will act as the keyboard for encryption.
- ➢ Encryption: Takes the data to be encrypted in the form of array named text array.
- ➢ Decryption: Reading the encrypted_data1_file file and copying the contents to another array named encrypted_data2_array

Step 1: (Virtual Keyboard)

1. Data set is taken as mentioned below and encryption will occur only with the help of these data tokens.

Data Tokens – a-z, A-Z, 0-9, !@#$%^&*(){}

1. Taking all the possible data set (character, numbers, and special characters) on which encryption will take place. The available data token is taken in a 1-D array. (These data tokens can also be kept in a file for easy reading and writing of data.)

    1. Deciding the dimension of the keyboard (here 128). Possible dimensions:
        - i. 1 x 128
        - ii. 2 x 64
        - iii. 4 x 32
        - iv. 8 x 16
        - v. 16 x 8
        - vi. 4 x 32
        - vii. 2 x 64
        - viii. 128 x 1

2. As the virtual keyboard cannot be 1-D so 1 x 128 and 128 x 1 will be eliminated. Considering the rest value and Using random function to select any dimensions.
3. Creating a KEYBOARD 2 -D array m x n.
4. Filling data in the 2-D array.
    - i. Initializing whole 2-D array with a pre known value. (This value may be any value other than that available in the 1- D data set. Assuming it to be Z1).
    - ii. While loop will run until all the blocks of 1-D array is copied to the 2-D array.

(Beginning of loop)

```
1.      WHILE (TRUE)
2.      Initialize X = random (m)
3.      Initialize Y= random (n)
4.      Initialize COUNTER = 0
5.      IF (KEYBOARD [X, Y] == Z1)
                Copy element in sequential manner from
                1-D array. Increment the COUNTER++.
6.      ELSE
                Don't copy element rather.
7.      END IF
        (Check the if the counter is size of 1-D array.)
8.      IF(COUNTER==128)
        Terminate.
```

(End of While Loop)

Step 2: (Encryption)

```
1.      ENCYPT (FILE)
2.      Takes the data to be encrypted in the form of array named text_array.
```

3. While loop will run until there is no data left in the text_array.

(**Beginning of While loop)**

4. Data will be taken from the text_array in a sequential manner and compared to characters in the KEYBOARD 2-D array.
5. The co-ordinates of the character will be stored in another array named encrypted_data1_array.
   encrypted_data1_array[i] = x co-ordinate.
   encrypted_data1_array[i+1] = y co-ordinate.
   i=i+2

(**End of While loop**)

6. Delete the current data of text_array.
7. The encrypted_data1_array is then copied to a file named encrypted_data1_file for easy read and write operations.

Step 3: (Decryption)

1. DECRPT (encrypted_data1_file)
2. Reading the encrypted_data1_file file and copying the contents to another array named encrypted_data2_array.
3. While loop will run until there is no data left in the encrypted_data2_array.

(**Beginning of While loop)**

4. Data will be taken from the encrypted data-array in a sequential manner and compared to characters in the 2-D array.
   x co-ordinate= encrypted_data2_array[i]
   y co-ordinate=encrypted_data2_array[i+1]
   i=i+2

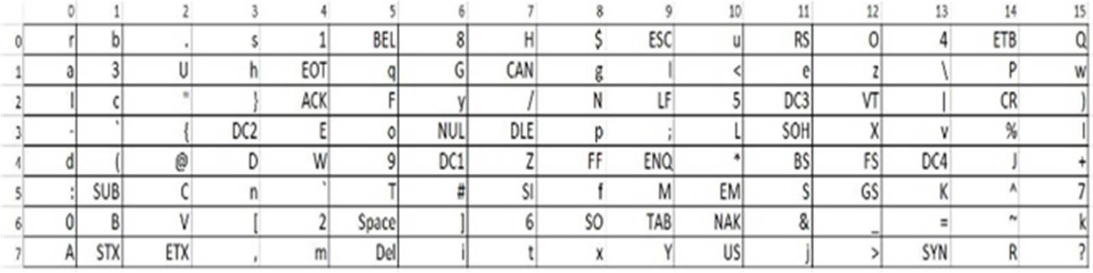
These co-ordinates are then searched in the 2-D array (Virtual Keyboard). The character of the corresponding co-ordinates is returned and stored in another array named decrypted_data2_array.

(End of While loop)

5. Delete the current data of encrypted_data2-array (i.e. i and i+1).
6. The decrypted_data_array is then copied to a file named decrypted_data_file for easy read and write operations.

Analysis

To evaluate the efficiency of the suggested algorithm, let us consider some cases:
Case 1: Taking an input of string "Ht4%a".
Step 1: Generating KEYBOARD 2D array. Using random function to select any dimensions.
Creating a KEYBOARD 2 -D array 8 x 16



	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	r	b	.	s	1	BEL	8	H	$	ESC	u	RS	O	4	ETB	Q
1	a	3	U	h	EOT	q	G	CAN	g	I	<	e	z	\	P	w
2	l	c	"	}	ACK	F	y	/	N	LF	5	DC3	VT	|	CR	)
3	-	'	{	DC2	E	o	NUL	DLE	p	;	L	SOH	X	v	%	I
4	d	(	@	D	W	9	DC1	Z	FF	ENQ	*	BS	FS	DC4	J	+
5	:	SUB	C	n	`	T	#	SI	f	M	EM	S	GS	K	^	7
6	0	B	V	[	2	Space	]	6	SO	TAB	NAK	&	_	=	~	k
7	A	STX	ETX	,	m	Del	i	t	x	Y	US	j	>	SYN	R	?

Step 2: Encrypting

H	t	4	%	A

text array

(Beginning of While loop)

Pass 1

i=0

Co-ordinate of H (0,7)

encrypted_data1_array [0] = 0

0	7								

encrypted_data1_array

Pass 2

i =2

Co-ordinate of t (7,7)

encrypted_data1_array [2] = 7

encrypted_data1_array [3] = 7

i = 4

0	7	7	7						

encrypted_data1_array

Pass 3

i=4

Co-ordinate of 4 (0,13)

encrypted_data1_array [4] = 0

encrypted_data1_array [5] = 13

i = 6

0	7	7	7	0	13				

encrypted_data1_array

Pass 4

i=6

Co-ordinate of % (3,14)

encrypted_data1_array [6] = 3

encrypted_data1_array [7] = 14

i = 8

0	7	7	7	0	13	3	14		

encrypted_data1_array

Pass 5
i=8
Co-ordinate of a (1,0)
encrypted_data1_array [8] = 1
encrypted_data1_array [9] = 0
i = 10

0	7	7	7	0	13	3	14	1	0

encrypted_data1_array
(no data left in the text_array. End of while loop.)

The encrypted_data1_array is then copied to a file named encrypted_data1_file.

0	7	7	7	0	13	3	14	1	0

encrypted_data1_file

Step 3: Decrypting the file.

0	7	7	7	0	13	3	14	1	0

encrypted_data1_file
(Reading the encrypted_data1_file file and copying the
contents to another array named encrypted_data2_array)

0	7	7	7	0	13	3	14	1	0

encrypted_data2_array

(Beginning of While loop)
Pass 1
i=0
x co-ordinate= encrypted_data2_array [0]
y co-ordinate=encrypted_data2_array [1]
i=i+2
(These co-ordinates are then searched in the 2-D array (Virtual Keyboard). The character of the corresponding co-ordinates is returned and stored in another array named decrypted_data2_array.)

H				

decrypted_data2_array

Pass 2
i=2
x co-ordinate= encrypted_data2_array [2]
y co-ordinate=encrypted_data2_array [3]
i=4

(These co-ordinates are then searched in the 2-D array (Virtual Keyboard). The character of the corresponding co-ordinates is returned and stored in another array named decrypted_data2_array.)

H	t			

decrypted_data2_array

Pass 3

i=4

x co-ordinate= encrypted_data2_array [4]

y co-ordinate=encrypted_data2_array [5]

i=6

(These co-ordinates are then searched in the 2-D array (Virtual Keyboard). The character of the corresponding co-ordinates is returned and stored in another array named decrypted_data2_array.)

H	t	4		

decrypted_data2_array

Pass 4

i=6

x co-ordinate= encrypted_data2_array [6]

y co-ordinate=encrypted_data2_array [7]

i=8

(These co-ordinates are then searched in the 2-D array (Virtual Keyboard). The character of the corresponding co-ordinates is returned and stored in another array named decrypted_data2_array.)

H	t	4	%	

decrypted_data2_array

Pass 5

i=8

x co-ordinate= encrypted_data2_array [8]

y co-ordinate=encrypted_data2_array [9]

i=10

(These co-ordinates are then searched in the 2-D array (Virtual Keyboard). The character of the corresponding co-ordinates is returned and stored in another array named decrypted_data2_array.)

H	t	4	%	a

decrypted_data2_array

(no data left in the encrypted_data2_array. End of while loop)

Ht4%a

decrypted_data2_file
The decrypted data array is then copied to a file named decrypted data file

Plaintext	**Cipher text**
Ht4%a	077701331410

Case 2: Taking an another input of string “S(,gyi`]WUs03”.
We get:

Plaintext	**Cipher text**
S(,gyi`]WUs03	511417316267631664412

*Case 3:*Similarly, Taking an another input of string “N2F#GidR^QX*”.
We get:

Plaintext	**Cipher text**
N2F#GidR^QX*	53642556187640714514015312410

5. RESULT AND ANALYSIS

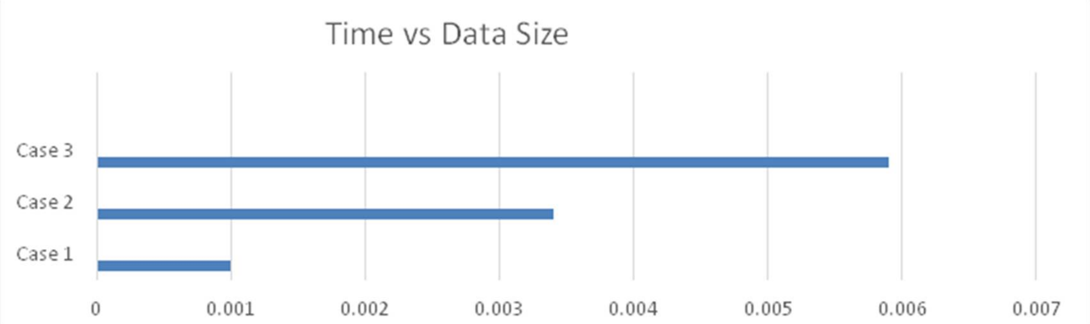
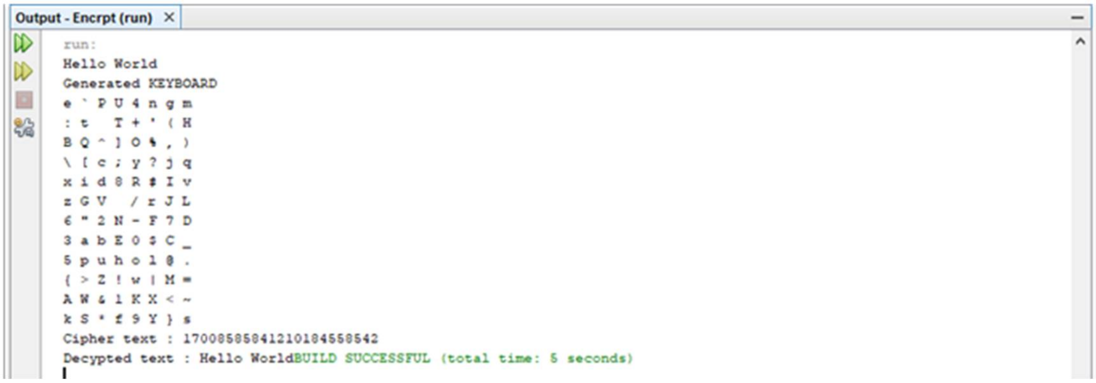
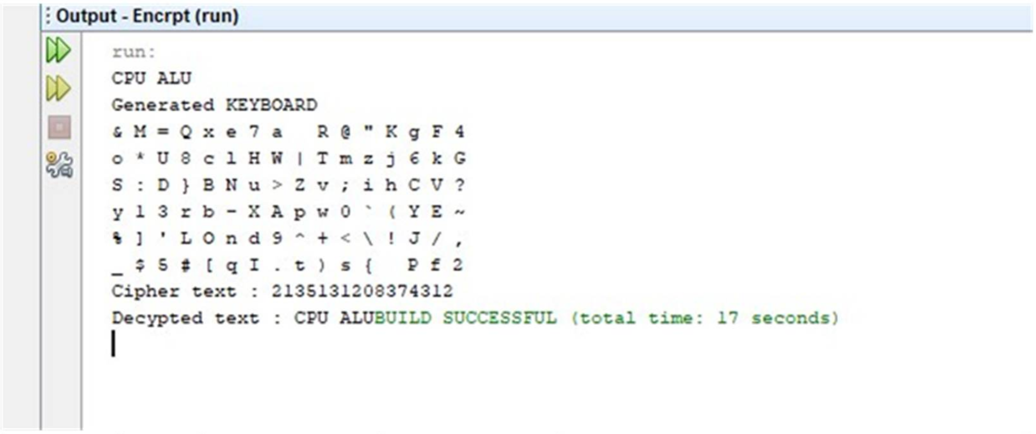


Figure 8: Relationship between times vs. Data size

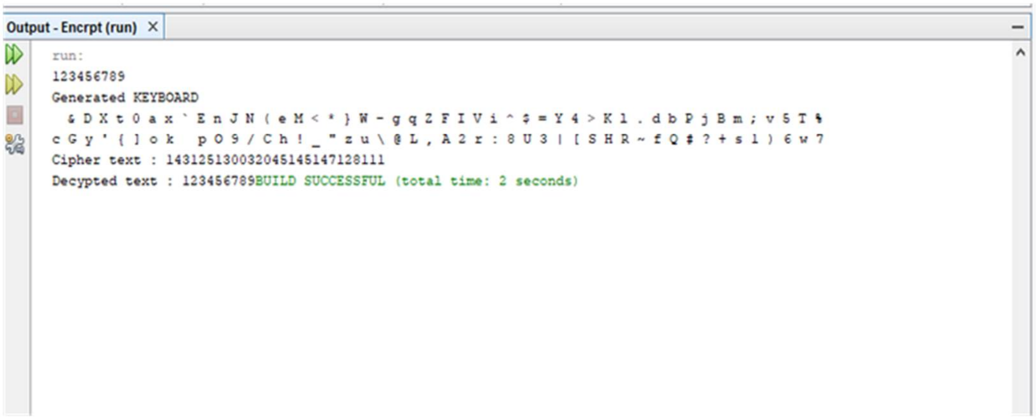
The following experimental output is shown below:-



```
run:
Hello World
Generated KEYBOARD
e ` P U 4 n g m
: t   T + ' ( H
B Q ^ ] O % , )
\ [ c ; y ? j q
x i d 8 R # I v
z G V   / r J L
6 " 2 N - F 7 D
3 a b E 0 $ C _
5 p u h o 1 @ .
{ > Z ! w | M =
A W & 1 K X < ~
k S * f 9 Y } s
Cipher text : 17008585841210184558542
Decypted text : Hello WorldBUILD SUCCESSFUL (total time: 5 seconds)
```



```
run:
CPU ALU
Generated KEYBOARD
& M = Q x e 7 a   R @ " K g F 4
o * U 8 c l H W | T m z j 6 k G
S : D } B N u > Z v ; i h C V ?
y 1 3 r b - X A p w 0 ` ( Y E ~
% ] ' L O n d 9 ^ + < \ ! J / ,
_ $ 5 # [ q I . t ) s {   P f 2
Cipher text : 2135131208374312
Decypted text : CPU ALUBUILD SUCCESSFUL (total time: 17 seconds)
```



```
run:
123456789
Generated KEYBOARD
  & D X t 0 a x ` E n J N ( e M < * } W - g q Z F I V i ^ $ = Y 4 > K 1 . d b P j B m ; v 5 T %
c G y ' { ] o k  p O 9 / C h ! _ " z u \ @ L , A 2 r : 8 U 3 | [ S H R ~ f Q # ? + s l ) 6 w 7
Cipher text : 14312513003204514514712811l
Decypted text : 123456789BUILD SUCCESSFUL (total time: 2 seconds)
```

6. CONCLUSION

Encryption of data is very important in order to protect it when it is being transmitted over any network. These Encryption and Decryption algorithm plays a very important role in keeping the user data secured. The above stated algorithm is quite secured because even if the data is compromised, the unauthorised user will not be able to access the data as the virtual keyboard is only provided to authorised user.

This is a very light weight but as well as sophisticated algorithm. It can easily be applied in communication applications where user private data cannot be compromised. It is very efficient in textual data without much overhead, thus can be implemented anywhere textual data is included.

7. FUTURE SCOPE

Digital assaults are continually developing, so security pros must remain occupied in the lab creating new plans to keep them under control. Master onlookers are cheerful that another technique called Honey Encryption will stop programmers by presenting counterfeit information for each off base speculation of the key code. This exceptional methodology eases back aggressors down, however possibly covers the right key in a bundle of bogus expectations. The encryption can additionally be improved and upgraded for greater security. This should be possible by taking irregular number of occurrences of each character. It will prompt questionable co-ordinate estimations of a solitary character which will be hard to hack.Also the encryption algorithm can be called recursively so that the bitwas security increases. This can be achieved by creating virtual keyboard at each random call. The keyboard can be backed up of encryption and decryption. Also considering the communication channel the virtual keyboard can bereplaced from time to time, which will further lower the risk of data hacked anywhere textual data is involved.

REFERENCES

1. Mandge, Tushar, and Vikas Choudhary. “A DNA encryption technique based on matrix manipulation and secure key generation scheme”. Information Communication and Embedded systems (ICICES), 2013. International Conference on. *IEEE*, (2013).
2. Chaudhary, Himanshu, and Vishal Bhatnagar. “ Hybrid approach for secure communication of data using chemical DNA.” Confluence The Next Generation Information Technology Summit (Confluence), 2014 5th International Conference. *IEEE*, (2014).
3. Kumar, dinesh, and Sushil Sing. “Secret data writing using DNA Sequence.” Emerging Trends in Network and computer Communications (ETNCC), 2011 International conference on. *IEEE*, (2011).
4. Sundaram, G. Shanmuga, *et al.* “ Cellular automata based DNA cryptography algorithm.” Intelligent System and Control (ISCO), 2015 IEEE 9th International Conference on. *IEEE*, (2015).
5. Shipra Jain, Dr.Vishal Bhatnagar. “A novel DNA sequence Dictionary method for securing data in DNA using Spiral Approach and Framework for DNA Cryptography”. *IEEE International conference on advances in Engineering & Technology Research.*, (2014).
6. C. P. Pfleeger, S. L. Pfleeger, and J. Margulies, Security in Computing. New Jersey: Prentice Hall, 2015N. Koblitz, A. Menezes, and S. Vanstone, “The state of elliptic curve cryptography”, Towards a quarter-century of public key cryptography. *Springer*, pp. 103–123 (2000).
7. M. Mushtaq Faheem, S. Jamel, A. Hassan Disina, Z. A. Pindar, N. Shafinaz Ahmad Shakir, and M. Mat Deris, "A survey on the cryptographic encryption algorithms," *Int. J. Adv. Comput. Sci. Appl.*, 8(11), pp. 333-344 (2017).
8. G. Suman, C. Krishna, and M. T. Se, "Improved cryptosystem using SDES algorithm with substitution ciphers," *International Journal of Advanced Research in Computer Science and Software Engineering*, 3(7), pp. 131-136 (2013).

9. Gurjeevan Singh, Ashwani Kumar Singla, K.S. Sandha “Performance Evaluation of Symmetric Cryptographic Algorithms”, *International Journal of Electronics and Communication Technology* Vol 2 Issue 3, Sep (2011).
10. Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, “Electron spectroscopy studies on magneto-optical media and plastic substrate interface,” *IEEE Transl. J. Magn. Japan*, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].
11. E.Thmbiraja, G.Ramesh, Dr.R.Umarani, “A survey on various most common encryption techniques”, *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol 2, Issue 7, July (2012).
12. Monika Agrawal, Pradeep Mishra”, A Comparative Survey on Symmetric Key Encryption Techniques”, *International Journal on Computer Science and Engineering (IJCSE)*, Vol.4 May (2012).
13. M. Young, The Technical Writer’s Handbook. Mill Valley, CA: University Science, (1989).
14. S. Karthik, and A. Muruganandam, "Data Encryption and Decryption by using Triple DES and performance analysis of crypto system," *Int. J. Sci. Eng. Res*., 2(11), pp. 24-31, (2014).
15. V. Agrawal, S. Agrawal, and R. Deshmukh, "Analysis and review of encryption and decryption for secure communication," *Int. J. Sci. Eng. Res*., 2(2), pp. 2347-3878 (2014).
16. R. Malik, and P. Kumar, "Cloud computing security improvement using Diffie Hellman and AES," *Int. J. Comput. Appl*., 118(1), pp. 975-8887 (2015).
17. M. Ahmed, B. Sanjabi, D. Aldiaz, A. Rezaei, and H. Omotunde, "Diffie-Hellman and its application in security protocols," *Int. J. Eng. Sci. Innov. Technol*., 1(2), pp.69-73 (2012).
18. B. L. Srinivas, A. Shanbhag, and A. S. D. Souza, "A comparative performance analysis of DES and BLOWFISH symmetric algorithm," *International Journal of Innovative Research in Computer and Communication Engineering*, 2(5), pp. 77-88 (2014).
19. M. A. Hameed, A. I. Jaber, J. M. Alobaidy, and A. Alaa, "Design and simulation DES algorithm of encryption for information security," *American Journal of Engineering Research*, 7(4), pp. 13-22. 17 (2018).
20. S. Ramanujam, and M. Karuppiah, "Designing an algorithm with high avalanche effect," *Int. J. Comput. Sci. Netw. Secur*., 11(1), pp. 106-111. 18 (2011).
21. R. Divya, and M. Kumar, "Enhanced digital assessment of examination with secured access," *International Journal of Advanced Studies in Computers, Science and Engineering*, 3(10), pp. 33-37. 19 (2014).
22. M. M. Al-Laham, "Reducing security concerns when using cloud computing in online exams case study: General Associate Degree Examination (Shamel) in Jordan," *Int. J. Comput. Sci. Inf. Technol*., 7(6), pp. 131-144. 20 (2015).
23. N. Singhal, and J. P. S. Raina, "Comparative analysis of AES and RC4 algorithms for better utilization," *Int. J. Comput. Trends Technol*., 2(6), pp. 177-181 (2011).