Secure Sharing of Data using an Algorithm Namely KAN

Sadhu Narayana Naidu, Itha Aravinda Kousik, SumaiyaThaseen

Abstract: Large amount of data is transferred through the internet, which is highly insecure. This can cause disruption of data due to attacks. To resist those attacks, the analysts are centered on the distinctive sort of systems to verify the information from assaults. Some of the techniques are AES, DES, and Digital Signatures etc. These techniques are not providing abnormal state proficient of security. So, in order to increase the efficiency level, we proposed a new method called KAN algorithm which is an extension of RSA algorithm to enhance the security of normal data by utilizing graph theory approach. This algorithm can be applicable for military basis and highly information secure system.

Keywords: Encryption, Decryption, Graph, Periodic Elements, Security.

I. INTRODUCTION

The data security is a fundamental part while transferring the information through the internet in an insecure channel because the maximum data transformation will occur through the digital format. The information can confront several assaults with various threats based on the application. The information can be secured by encrypting the information, which is unreadable by the third party. Kripa N Bangera et al in 2017[1] portrays a high level of security to the information by combining the RSA cryptographic algorithm and audio steganography algorithm. The output is in the form of Waveforms, which says no modifications can occur. Prabht k. panda and Sudipta Chattopadhyay in 2017 [2] portrays the Hybrid RSA algorithm where public and private key computed based on four prime numbers. Along these lines, the intricacy of the message increases and another approach to increase the complexity is computing the intermediate factors. Prabhat k Panda and Sudipta Chattopadhyay in 2017[3] describes Hybrid RSA by using four prime numbers to generate a public and private key to encrypt and decrypt the data. In addition, they analyzed conventionally and Enhanced RSA by Key generation time, encryption time and decryption time. Finally, Hybrid RSA provides better security than the CRSA and ERSA. Narander Kumar and Priyanka Chaudhary in 2016[4] portrays RSA to improve security.

Revised Manuscript Received on July 05, 2019.

Sadhu Narayana Naidu, School of Information Technology and Engineering, Vellore Institute of Technology, Vellore.

IthaAravindaKousik, School of Information Technology and Engineering, Vellore Institute of Technology, Vellore.

SumaiyaThaseen, School of Information Technology and Engineering, Vellore Institute of Technology, Vellore.

Basically, RSA relies upon the factorization of prime numbers. By using large prime numbers we can boost the security of information. Because factorization of a large prime number isn't a simple errand.A Manimaran et al in 2015[5] portrays the secure sharing of telephone numbers by using pack cards. To encrypt the telephone numbers by doling out 13 cards for 13 digits and by converting the decimal to hexadecimal. The encrypted message and decrypted message by converting hexadecimal to decimal and by contrasting and doled out 13 digits in 13 cards, the receiver can decrypt the telephone number. It is one of the approaches to secure the exchange of telephone numbers. Wael Mahmoud Al Etaiwi in 2014[6] have proposed an algorithm which represents the new encryption algorithm to encrypt and decrypt the information securely with the benefits of graph properties, the new symmetric encryption algorithm uses the concept of cycle graph, complete graphs, and minimum spanning trees to generate a complex ciphertext using a shared key. DebajitSensaram et.al in 2014[7] has proposed a graph-based algorithm. Graphs can be used for designing block ciphers, stream cipher or public key cipher. The graph encryption is based on the secret key and generates different ciphertext by using a symmetric key on the same plain text. Saranya et al. in 2014[8] proposed an algorithm to improve the security of the information by using the RSA algorithm but existing RSA algorithm gives the high-security level of the data. In order to produce better security of the data, they introduced an exponential in RSA. M P Radhini et al in 2014[9] trace secure sharing of restorative data, for that they acquainted a multi-authority characteristic with encryption of medical records. In this way, PMR can be assessed from any hospital by using a single key. This will reduce the complexity of key management. M Preetha and M Nithya in 2013[10] portrays that the present requirement for security and the correlation of public key generation algorithms. Both RSA and enhanced RSA algorithm provides the execution period and the security concern applications using RSA - OAEP. K. Govindan in 2011[11] describes multilevel cryptography techniques for data encryption-decryption using graceful codes, which will concern multiple levels of encryption. With the goal of that, it gives the different value for each character in the string, while decrypt it gives us a unique kind of dataset. In addition, the length of the initial string and the encrypted should be varied because it goes multiple encryptions of the data value, which is inserted in between the string and it is randomly chosen by the user or system can automatically give the computer. So that security can be maximized. AnishaKumari and Kirubanad V. B in 2008[12] depicts the encryption and decryption of data using graphs, they used an affine cipher to encrypt the data, the user can use the symmetric key to encrypt the data and plot on a graph. At that point, the graph will change over to a picture. The receiver uses the symmetric key to decrypt the data. This provides better security while storing the data in the cloud. This paper describes the KAN algorithm for encryption and decryption of data along with the RSA algorithm for key encryption, for both the text as well as graphs.

II. PROBLEM DEFINITION

The majority of the people are using the internet to transfer the data. In data transformation security act as a vital role to make the data more secure and confidential. Nowadays, security hijackers are good enough to make the data modification or threat.

III. EXISTING ENCRYPTION & DECRYPTION

The success rate of any software product depends on the security of the application. To secure the data from the attackers, some of the techniques are introduced, but by using the same algorithm for many applications and with many years. There might be conceivable to hack your data because aggressors are having more knowledge than the security scientists. By using the RSA algorithm with KAN algorithm, we can sustain or reduce the assault rate.

IV. PROPOSED METHOD

The proposed algorithm is implemented by using the Java program and the python program. In this algorithm, Based on the length of the string and the space values can generate a key message. Based on the key, the message string encrypted and the message key encrypted by using the RSA algorithm called the cipher text. At the receiver side, the key message decryption by using the RSA algorithm and after that every single character in the string message decrypted by using key message.

V. RSA ALGORITHM

A. *Key generation*

i. Select the two random prime numbers as p and q.

ii. Calculate $N = p * q$

iii. $\Phi = (p-1)(q-1)$

iv. Choose the number e(public key exponent), where $1 < e < \Phi$ (Or) $\gcd(e, \Phi) = 1$

v. Calculate secret key d (private key exponent) $where\ 1 < d < \Phi$ (Or) $\mathrm{e} * \mathrm{d} \bmod \Phi = 1$

vi. Public key$(\mathrm{N}, \mathrm{e})$and private key (N, d)

B. *Key message encryption*

i. If the message sends A to B

ii. Get the recipient B's public key (N, e)

iii. Compute the cipher text of key message encryption, Cipher $\text{text}(\mathrm{C}) = \mathrm{M}^{\mathrm{e}} mod\ N$

iv. Sender sends the cipher text to B.

v. Key message decryption

vi. B has its own private key (N, d)

vii. Compute the key message of cipher text, $\text{Message}(\mathrm{M}) = \mathrm{c}^{\mathrm{d}} mod\ N$

VI. KAN ALGORITHM

A. *Message encryption*

If A sends the message to recipient B

i. Get the string message from A

ii. Choose the arbitrary(random) space value.

iii. Insert the space number of random chemical names or alphabets from Table .5 between the string characters.

iv. Compute a Key message based on length of the string "n" and Space value.

v. $TN = n * space\ value$

vi. Key $\text{message}(X) = (Space\ value - 1) * TN.$

vii. Encrypt the each character in the string based on X

$$\frac{\text{key message value} * \text{character value}}{\text{TN}} = \text{encrypted message value}$$

Where key message value and character value are the positions of key message and character from Table .5

viii. Compute the RSA for the key message value.

ix. Concatenate key message value to the encrypted message.

x. Plot a graph.

B. *String message decryption*

i. Get the graph from sender.

ii. Decrypt the key message using RSA algorithm.

iii. Decrypt the each character in the string based on key message.

$$\frac{\text{TN} * \text{ character value}}{key\ message\ value} = \text{decrypted message value}$$

iv. Compute the space value

$$1 + \frac{X(key\ message)}{TN} = \text{Space value}$$

v. Remove the final key message value.

vi. Remove the random chemical names and alphabets in between the two characters based on space value.

vii. Get the original plain text.

viii. Similarly for graph encryption and decryption

ix. Compute the nodes(n)

x. Compute edges for each node. For example, if node 1 having 3 edges means character in the position 3 is C.

xi. Proceed the KAN algorithm.

VII. DIAGRAMMATIC REPRESENTATION

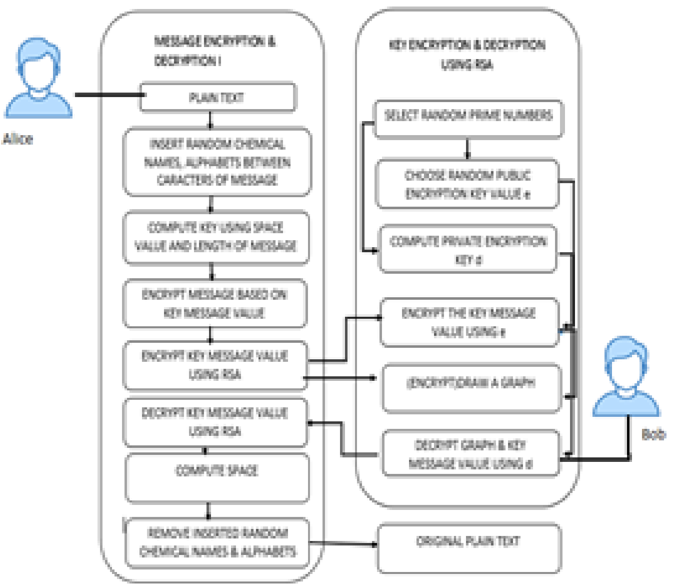

Fig. 1 Architecture Diagram for KAN

VIII. ENCRYPTION & DECRYPTION:

Fig. 1 shows the encryption and decryption of message using RSA enhancing algorithm called KAN algorithm. Here Alice sending the message to Bob by encrypting the message using KAN algorithm and RSA key generation algorithm. Bob decrypt the message by using the KAN algorithm and the RSA algorithm to get the original message.

A. *Encryption:*

It is a process to convert original message to an encrypted message by Alice so that the unauthorized users cannot able to access the data. The KAN algorithm provides on of the way to save the data from an unauthorized user. Convert the message as follows:

1. Insert the space number of random alphabets and chemical names in between the two characters of a message.
2. Compute the key, based on the size of the randomly inserted alphabets and chemical names.
3. Again, encrypt the message based on the generated key and the positions of each character from the message.
4. Encrypt the generated key by using RSA and selecting the two large prime numbers.
   4.1 Compute the public and private keys are KU= {N,e} and KR= {N,d}
5. Concatenate the encrypted key message with encrypted message.
6. Plot a graph based on the positions of encrypted message along with encrypted key.

B. *Decryption:*

Decryption is a reverse process of encryption in which cipher text will convert to normal message by Bob as follows:

1. Convert the graph into integer values based on the crust and troughs in the graph in sequence.
2. Convert the integer value as a position of character to message.
3. Consider the last position value as key.
4. Decrypt the key value using RSA by private or public keys respectively.
5. Decrypt the message with their positions from Table .5 by key message value.
6. Compute space value using size of message, key.
7. Remove randomly inserted alphabets and chemical names between the two characters.

IX. EXAMPLE1 CONSIDER NORMAL TEXT MESSAGE

Suppose the plain text message is BOB SENDS MESSAGE TO ALICE

Step1: Insert random characters from Table .5

Let take Space value is 3 , then we will get the text is

BJKLOWHGBOHJ@TTRSDUYECIONQFJDBSLSHOC@RTEMYRCEJKLSWHGSOHJATTRGDUYECIO@QFJTBSLOHOC@RTEAYRCLJKLIWHGCOHJE(X)

Step2: Compute key message value X

$$1+\frac{X}{TN}=\text{Space } value ------- (1)$$

Here TN= product of string message length, space value, X Is the key message. For Example1 TN=104, space value= 3. By substituting TN, space value in Equation (1), we will get key messagevalue.

$1+\frac{X}{104}$ = 3=208. i.e., TH+ from Table .5 Replace the key value X to TH+ in step1 output.

BJKLOWHGBOHJ@TTRSDUYECIONQFJDBSLSHOC@RTEMYRCEJKLSWHGSOHJATTRGDUYECIO@QFJTBSLOHOC@RTEAYRCLJKLIWHGCOHJETH+

Step3: Encrypt the plain text

$$\frac{\text{key message value} * \text{character value}}{TN} = \text{Encrypted message value} ----------- (2)$$

By substituting the key message value= TH+=208 and TN=104 in Equation (2), for character

B= $\frac{208*2}{104}$ = 4=D from Table .5

Similarly, for all the characters in the step 2 output except the key, we get the encrypted message as DTVXNeGaPNDNePTBCd+MnMnCaTiHCoBrJFRNeLiSiLTHDTiXTiPNeFBBCd+CaMnJ

ZBrCaFJTVXTiGaPTBMnMnCaNHCoBrJFRNeBCd+SiLTMnDTiXNePNeFBCd+CaMnJBBrCaFXTVXRGaPNFNePTJEDTKTH+

Encrypt the key based on RSA algorithm

Step4: Take the two large random prime numbers

Let us consider P= 13 and Q=17 and whose product is $N = 13 * 17 = 221$

Step 5: Compute totient value

Here $Totient\ \Phi = (P - 1) * (Q - 1) = 192$

Step6: Select random public encryption key e

Public key exponent e, where $1 < e < \Phi$ (Or) $\gcd(e, \Phi) = 1$. Here we assumed e as 11 which is coprime of Φ and gcd(11,192)=1.

Step7: Compute private encryption key d, by using extended Euclidean's algorithm

Table 1. Private encryption key generation

Q(quotient)	Φ	E	R(remainder)	T1	T2	T=T1-Q(T2)
17	192	11	5	0	1	-17
2	11	5	1	1	-17	1+34=35
5	5	1	0	-17	35	-17-175=-192
0	1	0	0	35	-192	35

Here the T is 35. So, private encryption key d=35. If you get negative value as d, you have to subtract the d value fromΦ .

Step7: Encryption key message

For Example 1 Public key KU=$(N, e) = (221,11)$ and the Message M is 208 by substituting in Cipher text $C = M^e mod\ N = 208^{11}\ mod\ 22 = 13\ mod\ 221 = 13$

i.e., Cipher text C=13=M from Table .5.. By replacing TH+ with M we will get final encrypted message as

DTVXNeGaPNDNePTBCd+MnMnCaTiHCoBrJFRNeLiSiLTHDTiXTiPNeFBBCd+CaMnJZBrCaFJTVXTiGaPTBMnMnCaNHCoBrJFRNeBCd+SiLTMnDTiXNePNeFBCd+CaMnJBBrCaFXTVXRGaPNFNePTJEDTKM.

Plot on a graph:

Based on the final encrypted message with their corresponding position values from Table .5., the graph plotted. In addition, this graph is sent to the receiver.

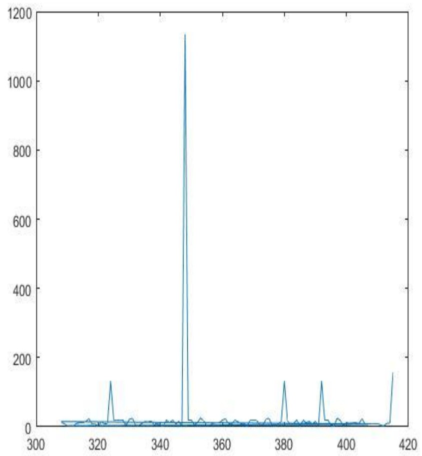

Fig 2. Encrypted message in graph.

The graph is obtained by using MATLAB. Then the receiver can decrypt the graph into message by identifying the key value based line from starting point on X-axis and line ending point on Y- axis will shows the key value in Fig2. Therefore, the receiver can take the crust and trough values, which will gives the encrypted message values. Based on these values, the receiver can decrypt the graph into message as

DTVXNeGaPNDNePTBCd+MnMnCaTiHCoBrJFRNeLiSiLTHDTiXTiPNeFBBCd+CaMnJZBrCaFJTVXTiGaPTBMnMnCaNHCoBrJFRNeBCd+SiLTMnDTiXNePNeFBCd+CaMnJBBrCaFXTVXRGaPNFNePTJEDTKM

Step8: Decryption of key message

Private Key $KR = (N, d) = (221,35)$ and Cipher text from decrypt message M as 13 from Table .5,then decrypt the key message value

$$M = C^d mod\ N$$

$= 13^{35} mod\ 221$

$= 208\ mod\ 221$

$= 208.$

Key message valueM=208. i.e., TH+ from Table .5

We get the decrypted message as

DTVXNeGaPNDNePTBCd+MnMnCaTiHCoBrJFRNeLiSiLTHDTiXTiPNeFBBCd+CaMnJZBrCaFJTVXTiGaPTBMnMnCaNHCoBrJFRNeBCd+SiLTMnDTiXNePNeFBCd+CaMnJBBrCaFXTVXRGaPNFNePTJEDTKTH+

Step9: Decrypt the message

$$\frac{\text{TN} * \text{Character value}}{key\ message\ value} = \text{decrypted message} - - - - - - - - - - - - (3)$$

From decrypted message, TN=104, key message value=208 and D is 4. Substituting TN, key message value and Character value in Equation (4),

For D = $\frac{104*4}{208}$ = 2 = B from Table .5.Similarly, for all decrypted message characters, we will get Decrypted message as

BJKLOWHGBOHJ@TTRSDUYECIONQFJDBSLSHOC@RTEMYRCEJKLSWHGSOHJATTRGDUYECIO@QFJTBSLOHOC@RTEAYRCLJKLIWHGCOHJEBJKTH+

Step10: Compute Space value.

$$\text{Space value} = 1 + \frac{X(key\ message\ value)}{TN} = 1 + \frac{208}{104} = 3$$

Step11: Removing Characters from the decrypted message

Here we removed 3 letters as follows BJKLOWHGBOHJ@TTRSDUYECIONQFJDBSL SHOC@RTEMYRCEJKLSWHGSOHJATTRGDUYECIO @QFJTBSLOHOC@RTEAYRCLJKLIWHGCOHJEBJKTH+. We will get the original message as BOB SENDS MESSAGE TO ALICE

X. EXAMPLE 2: BASED ON GRAPHS

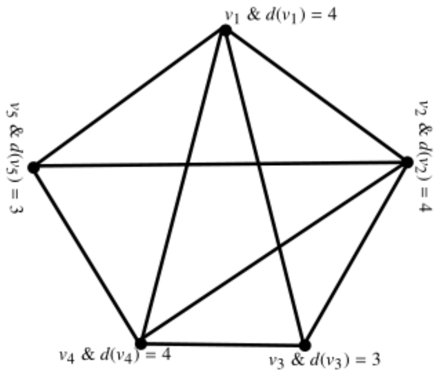

Fig 3. Graph message sending from A to B

Let us consider the above graph as a simple graph

Convert the vertices of degrees to normal plain text message. Here vertices are 5 (v1,v2,v3,v4,v5) and their corresponding degrees 4, 4,3,4,3 as D, D, C, D, C from Table .5 respectively. We will get normal message as DDCDC.

Step1: Inserting random chemical names from Table .5.

Suppose space value=4, insert the 4 random chemical names and alphabets from Table.5 We will get DATBFDCDXYCPQTRDFTSDCEKJI (X)

Step2: Compute key message value X

$$1 + \frac{X}{TN} = \text{Space} \qquad ---------(1)$$

Here TN= product of message length and space value. For Example 2, substitute TN=25, space value= 4 in Equation (i).$1 + \frac{X}{25} = 4 = 75$ = Pt from Table .5.. Replace key message value X from output of step1 to Pt, we will get DATBFDCDXYCPQTRDFTSDCEKJI (Pt)

Step3: Encrypt the plain text

$$\frac{\text{key message value} * \text{character value}}{\text{TN}} = \text{encrypted message value} ----(2)$$

Substitute key message value= Pt =75 from Table .5. and TN= 25 in Equation (ii). For D = $\frac{75*4}{25}$ = 12 = L from Table .5..Similarly, for all the Characters from the output of step 2 except key message value we will get encrypted message as

LCPdFRLILRePtIAsKrPdZrLRPdTcLIOAlNeHe (Pt)

Encrypt the key based on RSA algorithm

Step4: Take the two large random prime numbers

Let us consider the large random prime number are P= 13 and Q=17 and whose product N = 13 * 17 =221.

Step 5: Compute totient value Φ

Here $\Phi = (P-1)*(Q-1) = 12*16 = 192$

Step6: Selecting random public encryption key e

Public key exponent e, where $1 < e < \Phi$ (Or) $\gcd(e, \Phi) = 1$. Here we assumed e as 7 which is coprime of Φ and gcd(7,192)=1.

Step7: Compute private encryption key d, by using extended Euclidean's algorithm

Table 2. Private encryption key generation

Q(quotient)	Φ	E	R(reMainder)	T1	T2	T=T1-Q(T2)
27	192	7	3	0	1	-27
2	7	3	1	1	-27	55
3	3	1	0	-27	55	-192
0	1	0	0	55	-192	55

Here T= 55. Therefore, the private encryption key is 55. If you get negative value as d, you have to subtract the negative value from Φ

Step7: Encrypt the key message

Here Public key $KU = (N, e) = (221,7)$ with key message Pt is 75 from Table .5. Then the

$$\text{Cipher text} = M^e mod\ N$$

$$= 75^7 \bmod 221$$

$$= 114 \bmod 221$$

$$= 114.$$

Here 114 is Yb from Table .5.. We will get final encrypted message by replacing Pt to Yb as key message value.

LCPdFRLILRePtIAsKrPdZrLRPdTcLIOAlNeHe(Yb)

Plot in graph:

Graph is plotted, based on the final encrypted message and their corresponding positional values from Table.5 and this message can be send to receiver.

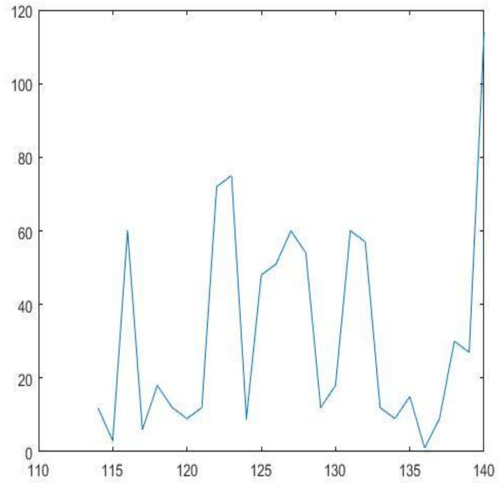

Fig 4. Encrypted message of Fig 3

The graph we obtained by using MATLAB. Then the receiver can identify the key message value based line starting point on X-axis and line-ending point on Y- axis gives key message value from Fig4. In addition, the receiver can take the crust and trough values, which will, gives the encrypted message values. Based on the values the receiver can decrypt the graph to message as

LCPdFRLILRePtIAsKrPdZrLRPdTcLIOAlNeHe(Yb)

Step8: Decryption of private encryption key

Here Private Key: $KR = (N, d) = (221,55)$ and Cipher text is Yb as 114 from Table .5.. Then decrypt the key message value

$$M = C^d mod\ N$$

$$= 114^{55} mdo\ 221$$

$$= 75\ mod\ 221$$

$$= 75$$

. i.e., 75 is Pt from Table .5.. We get the decrypted message as

LCPdFRLILRePtIAsKrPdZrLRPdTcLIOAlNeHe (Pt).

Step9: Decrypt the cipher text of a plain text using key

$$\frac{\text{TN} * \text{character value}}{key\ message\ value} = \text{decrypted message value} \qquad -------- (3)$$

Substitute TN= 25 and the key message value 75 in Equation (3).

For L= $\frac{12*25}{75}$ = 4= D. Similarly, for all characters in decrypted message, we will get

DATBFDCDXYCPQTRDFTSDCEKJI (Pt)

Step10: Compute Space value

Space value $= 1 + \frac{X(key)}{N} = 1 + \frac{75}{25} = 4$

Step11: Remove random chemical names and Alphabets

Here we remove 4 characters as follows. D~~ATBF~~D~~CDXY~~C~~PQTR~~D~~FTSD~~C~~EKJI~~(Pt)

In addition, remove the key, we will get the plain text as DDCDC, finally we get the original graph as

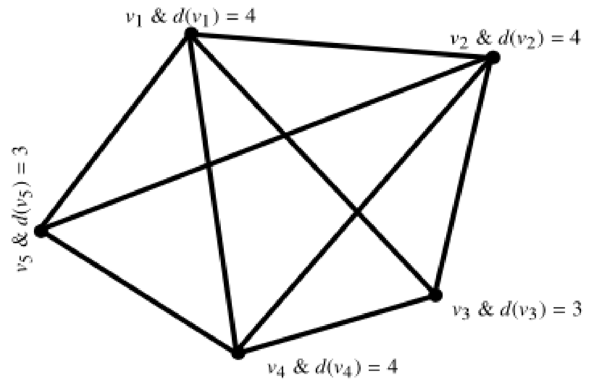

Fig 5. Graph received from sender A

XI. RESULT & DISCUSSION

Here we implement both KAN and RSA algorithm to encrypt and decrypt information in java. There we provide a input message is VIT UNIVERSITY. The corresponding cipher text that obtained an

A. Encrypted Message In KAN:

qBB$RDDDmHBD#DBDoFBHaDF$RDHBqDDJDHi$$ kBBRHBBmHBDwDHF,

B. Decrypted Message In KAN:

VAACICDDT$$A@AD$UBCAN$BDIAD$GVAD$EDBARBAAIADCSBACIDDDT$$CGYADBADBARBAAIADCSBACIDDDT$$CG.

By removing the key and randomly inserted chemical names and Alphabets, we will get VIT UNIVERSITY as our original message.

XII. COMPARISON BETWEEN THE KAN & RSA EXECUTION TIME: -

Table 3. Time performance of both KAN & RSA

KAN algorithm		RSA algorithm
Input Size	**Total Execution Time**	**Total Execution Time**
1kb	2 seconds	26 seconds
14kb	50 seconds	1 minute 18 seconds
24kb	1 minute	1 minute 32 seconds

Retrieval Number: I8523078919/19©BEIESP
DOI:10.35940/ijitee.I8523.078919

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

30kb	1 minute 16 seconds	1 minute 33 seconds
39kb	2 minutes 15 seconds	3 minutes 5 seconds
62kb	3 minutes 25 seconds	3 minutes 26 seconds

Encryption and Decryption of data using RSA is suitable for only the small amount of data. For large data, it is not possible to encrypt and decrypt. It takes lesser time to key generation, compared to our KAN algorithm. But the encryption and decryption of data will takes more time in RSA than KAN. That represented in fig 6. The key generation time in KAN is higher. So, that the time required to break the KAN is also high. KAN will enhances, the security. So, that the proposed algorithm is best suitable for medical data sharing, military data and so on.

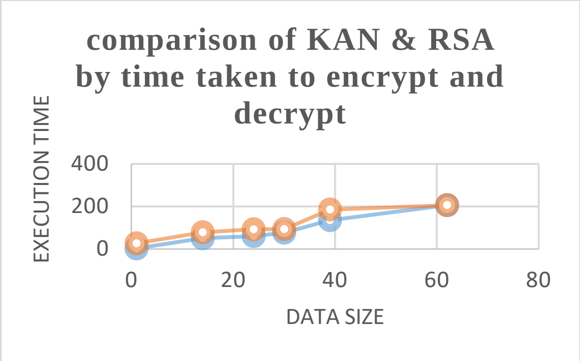

Fig 6 Time performance of KAN & RSA.

Table 4. Accuracy table.

words	Accuracy
10	100%
15	100%
20	100%
50	100%

Accuracy table shows whether the message is received by the receiver is same as original message or not. Here the KAN method can provide 100% accuracy even the data size is to large in a message

XIII. CHEMICAL AND ALPHABETIC TABLE:

This table is prepared by using the chemical names and alphabets.it is useful toeasy transfer of medical data.

Table.5 alphabetic and chemical names

ALPHABET	VALUE	ALP	VAL	ALP	VAL	ALP	VAL	ALP	VAL	ALP	VAL	ALP	VAL
A	1	U	21	Fe	41	Ag	61	Po	81	La	101	PU	121
B	2	V	22	Co	42	cd	62	At	82	Ce	102	AM	122
C	3	W	23	Ni	43	In	63	Rn	83	Pr	103	CM	123
D	4	X	24	Cu	44	Sn	64	Fr	84	Nd	104	BK	124
E	5	Y	25	Zn	45	Sb	65	Ra	85	Pm	105	CF	125
F	6	Z	26	Ga	46	Te	66	Rf	86	Sm	106	ES	126
G	7	He	27	Ge	47	Xe	67	Db	87	Eu	107	FM	127
H	8	Li	28	As	48	Cs	68	Sg	88	Gd	108	MD	128
I	9	Be	29	Se	49	Ba	69	Bh	89	Tb	109	NO	129
J	10	Ne	30	Br	50	Hf	70	Hs	90	Dy	110	LR	130
K	11	Na	31	kr	51	Ta	71	Mt	91	Ho	111	@	131(space)
L	12	Mg	32	Rb	52	Re	72	Ds	92	Er	112	+	Concat
M	13	Al	33	Sr	53	Os	73	Rg	93	Tm	113	-	Subtract
N	14	Si	34	Zr	54	Ir	74	Cn	94	Yb	114	*	Multiply
O	15	Ar	35	Nb	55	Pt	75	Nh	95	Lu	115		
P	16	Ca	36	Mo	56	Au	76	Fi	96	Ac	116		
Q	17	Sc	37	Tc	57	Hg	77	Mc	97	Th	117		
R	18	Ti	38	Ru	58	Ti	78	Lv	98	Pa	118		
S	19	Cr	39	Rh	59	Pb	79	Ts	99	U	119		
T	20	Mn	40	Pd	60	Bi	80	Og	100	Np	120		

XIV. CONCLUSION

The proposed algorithm is a standout amongst the various approaches to secure the message by using graph theory. The portrayal of graphs with chemical values and alphabets isn't broadly used for encryption and decryption. Nonetheless, it is a simple method for representation in computers. In this paper, we introduce a new concept of integrating the concept of RSA with KAN algorithm. KAN algorithm imposes graph encryption and decryption on the message based on the chemical names and alphabets. This will provide more security to the data from the assailants. However the complexity of the KAN is high compared to RSA, hence it is difficult to decrypt the cipher text message but appropriate for capital letters and it is the best ideal approach to secure our Information. In RSA algorithm, we have to use sub key generation of each character is required. But, In the KAN algorithm no need to use sub key generation. For the Sub key generation, the execution time factor is more. So, this is the main reason for removal of sub key generation.

XV. REFERENCES

1. Saranya, V. (2014). Vasumathi,"A Study on RSA Algorithm for cryptography". *International Journal of Computer Science and Information Technologies (IJCSIT)*, *5*(4), 5708-5709.
2. Panda, P. K., & Chattopadhyay, S. (2017, January). A hybrid security algorithm for RSA cryptosystem. In *2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS)* (pp. 1-6). IEEE.
3. Govinda, K. (2011). Multilevel cryptography technique using graceful codes. *Journal of Global Research in Computer Science*, 2(7), 1-5.
4. Al Etaiwi, W. M. (2014). Encryption algorithm using graph theory. *Journal of Scientific Research & Reports*, *3*(19), 2519-2527.
5. Sensarma, D., &Sarma, S. S. (2014). Gmdes: a graph based modified data encryption standard algorithm with enhanced seurity. *Int J Res EngTechnol*, *3*(3), 653-60.
6. Manisha Kumari, Kirubanad V.B(2018,Febrauary).data encryption and decryption using graph plotting. *International Journal of Civil Engineering and Technology* (Vol 9,pp. 36–46).
7. Preetha, M., &Nithya, M. (2013). A study and performance analysis of RSA algorithm. *International Journal of Computer Science and Mobile Computing*, *2*(6), 126-139.
8. Bangera, K. N., Reddy, N. S., Paddambail, Y., &Shivaprasad, G. (2017, May). Multilayer security using RSA cryptography and dual audio steganography. In *2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)* (pp. 492-495). IEEE.
9. Panda, P. K., & Chattopadhyay, S. (2017, January). A hybrid security algorithm for RSA cryptosystem. In *2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS)* (pp. 1-6). IEEE.
10. Kumar, N., & Chaudhary, P. (2016, March). Implementation of Modified RSA Cryptosystem for Data Encryption and Decryption based on n Prime number and Bit Stuffing. In *Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies* (p. 120). ACM.
11. Radhini, M. P., Ananthaprabha, P., &Parthasarathi, P. (2014). Secure Sharing of Medical Records Using Cryptographic Methods in Cloud.
12. A.Manimaran,V.M. Chandrasekaran, VivekMallineni, GangireddyKoushik Reddy, P. M. Karthick (2015). A new approach for encrypting and decrypting phone numbers. In *International Journal Of Pharmacy & Technology* (Vol. 7, pp. 9904-9908).
13. M. Yamuna, K. Karthika(2014).Periodic table as a Binary table for Drug Encryption. *Scopus International Journal of Pharma Tech Reserch*, 6(3), 1002-1006.
14. P.suresh(2017). Secure Cloud Environment Using RSA Algorithm *.International Research Journal of Engineering and Technology (IRJET)*,Vol 03
15. B. persis Urbana in (2018), A Simple and Efficient Counting Algorithm for Data Encryption and Decryption *TAGA JOURNAL* (Vol 14)

AUTHORS PROFILE

Sadhu Narayana Naidu is currently pursuing his 3rd. Year M.Tech (S.E) in Vellore Institute of Technology, Vellore.

Itha Aravinda Kousik is currently pursuing his 3rd. Year M.Tech (S.E) in Vellore Institute of Technology, Vellore. He is also the Director of External Affairs and Social Outreach-Health Club VIT.He completed Dakshina Bharatha Hindi Prachara Sabha.

Dr. Sumaiya Thaseen has fourteen years of teaching and research experience in VIT University. She completed her PhD in the domain of "Intrusion Detection Models using feature selection and ensemble of classifiers". She has publications in the domain of intrusion detection having good citations. She has more than ten publications in the domain of intrusion detection, few of which are indexed in Elsevier and SCI. According to Google Scholar, Sumaiya has over 248 citations and the H-Index is 8. Sumaiya is a reviewer for Artificial Intelligence Review Journal