A New Variable Length Key Block Cipher Technique for Network Security in Data Transmission

A.V.N. Krishna[1] *A.Vinaya Babu*[2]

Abstract

The algorithm that is going to be discussed in this work will consider a random matrix key which on execution of sequence of steps generates a sequence. Based on the equality of values, this sequence is being divided into basins. The basins with minimum values will be eliminated. Remaining each basin represents one block of data. Depending on starting input value of plain text character, corresponding basin is considered as a key. The procedure is repeated for certain plain text depending on chosen value. Thus the cipher text obtained becomes very difficult to be broken with out knowing the key.

Keywords : Cryptography, Variable length key, Encryption Algorithm, Example, Add function.

1. Introduction

A crypto system [ref 1-5] is an algorithm, plus all possible plain texts, cipher texts and keys. There are two general types of key based algorithms: symmetric and public key. With symmetric-key encryption, the encryption key can be calculated from the decryption key and vice versa. With most symmetric algorithms, the same key is used for both encryption and decryption, as shown in Figure 1.

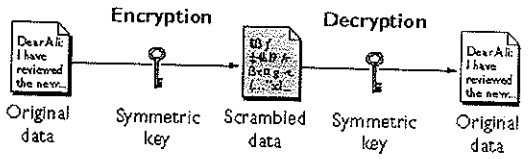


Figure 1: Symmetric-Key Encryption

Implementations of symmetric-key encryption can be highly efficient, so that users do not experience any significant time delay as a result of the encryption and decryption. Symmetric-key encryption also provides a degree of authentication, since information encrypted with one symmetric key cannot be decrypted with any other symmetric key. Thus, as long as the symmetric key is kept secret by the two parties using it to encrypt communications, each party can be sure that it is communicating with the other as long as the decrypted messages continue to make sense.

Symmetric-key encryption is effective only if the symmetric key is kept secret by the two parties involved. If anyone else discovers the key, it affects both confidentiality and authentication. A person with an unauthorized symmetric key not only can decrypt messages sent with that key, but can encrypt new messages and send them as if they came from one of the two parties who were originally using the key.

2. A New Algorithm [6-12 &18-19]

2.1 The New Algorithm Has the Following Features

1. A set of poly alphabetic substitution rule is used.
2. A Random matrix Key is used as a key.

[1]Professor, Department of Computer Science, Indur Institute of Engineering & Technology, Siddipet, Andhra Pradesh, India . Mob.No: 9849520995. Email: hari_avn@Rediffmail.com

[2]Director, School For Continues & Distance Education, J.N.T.U, Hyderabad.

3. A sequence is generated from a product of ternary vector and the key.
4. Based on equality of values, the sequence is divided into basins.
5. These basins are used as variable length keys to the characters in the plain text by a particular chosen rule.

2.2 The New Algorithm Is Combination Of

a. Substitution cipher
b. A Random Matrix key
c. Development of basins.
d. Each basin with unequal number of values.
e. Modified Caesar algorithm.
f. Coding method.

Thus this algorithm is a combination of

1. A Random vector of 27 values to few basin values.
2. Each basin containing different number of values.
3. Corresponding basin is considered as key depending on first character of plain text.

2.3 The Steps That Are Involved In the Proposed Algorithm

1. The letters of the alphabet were given numerical values starting from 0
2. A random matrix used as a key. Let it be A.
3. A ternary vector of 27 values is considered.
4. Ternary vector is multiplied with Random matrix key.
5. A Sign function is applied on the product to make it more secure.[14-17]
6. A sequence is generated.
7. Basins will be developed from this sequence which contains similar values.
8. Thus each basin contains unequal number of values.
9. Basins with minimum values (say 1 value) are eliminated.
10. Each basin is represented by one character.
11. The plain text being converted to equivalent numerical value.
12. The alphanumerical value of the first character of plain text is considered.
13. The mod of the first value with the number of basins is calculated.
14. Depending on the value of the remainder, the corresponding basin is considered as a key.
15. The key is added to the plain text to generate cipher text.
16. The procedure is repeated for successive plain texts depending on chosen value.

3. Advantages

1. It is almost impossible to extract the original information.
2. Even if the algorithm is known, it is difficult to extract the information.
3. Versatile to users. Different users of internet can use different modified versions of the new algorithm.
4. As per basin values, the same character is substituted by different alpha numerical value which provides more security for the message.

4. Example: n= 0 : 26 ;

r = ternary vector 0:26

n = 0 1 2 3 4 5 26

r = 0 0 0 0 0 0 2

0 0 0 1 1 1 2

0 1 2 0 1 2 2

r = r-1;

r = -1 -1 -1 -1 -1 -1 1

-1 -1 -1 0 0 0 1

-1 0 1 -1 0 1 1

A= key = 2 5 -6

3 1 3

4 -2 -3

r = multiply (A*r).

r = -1 -7 -13 4 -2 -8 .....

-7 -4 -1 -6 -3 0 .....

1 -2 -5 -1 -4 -7.....

Convert all positive values to 1, all negative values to –1 , and zero by 0.

Thus r = -1 -1 -1 1 -1 1 1

-1 -1 -1 -1 -1 0 1

1 -1 -1 -1 -1 -1 .....-1

r=r+1;

r = 0 0 0 2 0 0 2

0 0 0 0 0 1 2

2 0 0 0 0 0 0

r=r(3,1)+r(2,1)*3+r(1,1)*9;

thus for N = 0 ; r = (2 0 0) = 2 + 0 * 3 + 0 * 9 = 2 ;

Ternary vector n=0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26

Random Sequence generated

r=2 0 0 18 0 3 18 18 6 20 2 6 20 13 6 20 24 6 20 8 8 23 26 8 26 26 24.

The basins that can be formed using this sequence are

b(0)=(0,1,2,4,10)

b(1)=(3,5,6,7,8,9,11,12,14,15,17,18,19,20,23)

b(2)=(16,21,22,24,25,26)

Plain text avnkrishna

Considering the first character of the plain text, a = 10, 10 mod 3=1. So the basin considered is b(1)

1. Encryption

1. Plain text

a v n k r I s h n a

10 31 23 20 27 18 28 17 23 10

2. Basin Considered. b(1)

3 5 6 7 8 9 11 12 14 15

3. Add Function

13 36 29 27 35 27 39 29 37 25

4. Mod 36

13 0 29 27 35 27 10 29 10 25

5. Cipher text

d 0 t r z r a t a p

2. Decryption

1. Cipher text

d 0 t r z r a t a p

13 0 29 27 35 27 10 29 10 25

2. Mod 36

13 36 29 27 35 27 39 29 37 25

3. Basin Considered. b(1)

3 5 6 7 8 9 11 12 14 15

4. Subtract function

10 31 23 20 27 18 28 17 23 10

5. Plain text

a v n k r I s h n a.

After some part of plain text, the procedure is repeated.

5. Total Number Of Computations

Considered in the given model for converting plain text to cipher text.

1 computation: converting n=0:26 to ternary vector. Let it be r.

2 computation: calculating r-1.

3 computation: multiplying r with the key considered.

4 computation: applying sign function on the product. Store it in r.

5 computation: calculating r+1

6 computation: converting output ternary vector to integer form. Let this be s,the sequence generated.

7 computation: Different basins will be formed by placing similar values of the sequence in one basin.

8 computation: converting plain text to alphanumerical value.

9 computation: considering the first character of plain text and applying a mod function of the order of number of basins formed.

10 computation: depending on the output of the mod function, the corresponding basin be used as a key.

11 computation: add the key to the alphanumerical value of the plain text.

12 computation: applying mod function on the output.

13 computation: converting the output to characters of the alphabet to get cipher text.

14 computation: The procedure being repeated for chosen part of plain text.

Thus the total number of computations in the first proposed model are 15.

Computation overhead for a 27 character key.

1 computation: 27 calculations.

2 computation: 27 calculations

Key considered : 9 character key.

3 computation: 27*9 calculations.

4 computation: 27 calculations.

5 computation: 27 calculations

6 computation: 27 calculations

7 computation: 27*27 calculations +27*27 calculations

8 computation: 27 calculations.

9 computation: 03 calculations depending on chosen rule.

10 computation 03 calculations.

11 computation: 27 calculations

12 computation: 27 calculations

13 computation: 27 calculations

14 computation: 03 calculations depending on the chosen rule.

Thus the total computational overhead by the proposed model is 1953 calculations

6. Security Analysis by Construction

6.1 If We Go By the Construction of the Algorithm

1 computation : converting n=0:26 to ternary vector. Let it be r. The complexity is multiples of n.

2 computation: calculating r-1. The complexity is multiples of n

3 computation: multiplying r with the key considered. The complexity is multiples of n

4 computation: applying sign function on the product. Store it in r. The complexity is multiples of n

5 computation: calculating r+1 The complexity is multiples of n

6 computation: converting output ternary vector to integer form. Let this be s,the sequence generated. The complexity is multiples of n

7 computation: 27*27 calculations +27*27 calculations . The complexity is multiples of n*n.

8 computation: 27 calculations. The complexity is multiple of n

9 computation: 03 calculations depending on chosen rule. The complexity depends on chosen rule.

10 computation 03 calculations. The complexity depends on chosen rule.

11 computation: 27 calculations The complexity is multiple of n..

12 computation: 27 calculations The complexity is multiple of n..

13 computation: 27 calculations The complexity is multiple of n..

14 computation: 03 calculations depending on the chosen rule.

The complexity depends on chosen rule

Thus the total computational complexity of the model by its construction is of the order of $O(n^2)$

6.2 Complexity of the Algorithm by Its Strength

In the given algorithm a matrix key is used. This matrix key is multiplied with ternary vector. On the generated values a sign function is used to convert all positive values to 1 , negative values to –1 and zero to 0. This provides the necessary strength to the algorithm. Thus known the algorithm, known the plain text & cipher text pairs, it is computationally infeasible to generate the matrix key. Thus this algorithm is supposed to be safe in real time environment. Thus if we go by the security of the algorithm, the complexity is exponential in nature.

7. Avalanche Effect

In this model a sequence is generated and this sequence is used to generate basins of variable length. These basins will be used as keys for the plain text to generate the cipher text Depending on the key; the sequence will be used to generate the basins. We will identify the variations in the basins generated, by slight variations in the key .Thus we can identify the variations in the cipher text by slight variations in the key considered. We will also identify the variations in the cipher text by slight variations in the plain text. For example,

Case 1:

$$A=key \quad \begin{vmatrix} 2 & 5 & -6 \\ 3 & 1 & 3 \\ 4 & -2 & -3 \end{vmatrix}$$

Sequence generated from the proposed model

n=0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18

r=2 0 0 18 0 3 18 18 6 20 2 6 20 13 6 20 24 6 20

n= 19 20 21 22 23 24 25 26

r= 8 8 23 26 8 26 26 24.

Thus the basins that can be formed using this sequences which are used as key are

b(0)=(0,1,2,4,10)

b(1)=(3,5,6,7,8,9,11,12,14,15,17,18,19,20,21,23)

b(2)=(13)

b(3)=(16,22,24,25,26)

Case 2 : By increasing the values of key by 1at each row

$$A = key = \begin{matrix} 3 & 5 & -6 \\ 4 & 1 & 3 \\ 5 & -2 & -3 \end{matrix}$$

Sequence generated

r= 1 0 0 18 0 0 18 18 3 20 2 6 20 13 6 20 24 6 23 8 8 26 26 8 26 26 25.

Thus the basins formed which are used as key are

b(0)= (0,1,2,4,5,10)

b(1)= (3,6,7,8,9,11,12,14,15,17,18,19,20,23)

b(2)=(13)

b(3)= (16,21,22,24,25,26);

Case 3 :

By decreasing the key values by 1 at each row.

$$A = key = \begin{matrix} 1 & 5 & -6 \\ 2 & 1 & 3 \\ 2 & -2 & -3 \end{matrix}$$

Sequence generated by the model.

r=11,1,3,20,0,6,18,18,6,20,2,6,20,13,6,20, 24,6,20,8,8,20,26,6,23,25,15.

Basins formed which are used as key are

b(0) = (0,11,4)

b(1) = (1);

b(2)= (2,3,10);

b(3)=(5,6,7,8,9,11,12,14,15,17,18,19,20,21,22,23,24,26)

b(4)=(13)

b(5)=(25).

For example

By converting the characters of the alphabet to alphanumerical values, starting from 1,

if the plain text considered is	a b c d e
its equivalent alphanumerical value is	01 02 03 04 05.
As per the algorithm key is b(0)	0 1 2 4 10
The cipher text formed will be	01 03 05 08 15
	a c e h o.

If the key is decreased by 1 at each row,

if the plain text considered is	a b c d e
its equivalent alphanumerical value is	1 2 3 4 5
As per the algorithm key is b(0)	0 11 4 0 11
The cipher text formed will be	1 13 7 4 16
	a m g d p

Thus we can see that, by changing the key slightly, there are a lot of variations in the basins generated. Since these basins will form the keys for the given model, they provide maximum avalanche effect to the algorithm. Thus this model provides for good variations in cipher text for slight variations in the key. This provides for maximum strength and security to the algorithm.

If the plain text is slightly varied, a different basin will be considered as key depending on the first value of plain text.

For example if the plain text considered is	a b c d e
Its equivalent alphanumerical value is	01 02 03 04 05.
As per the algorithm key is b(0)	0 1 2 4 10
The cipher text formed will be	01 03 05 08 15
	a c e h o.

If the plain text is slightly varied by one value,

if the plain text considered is	b b c d e
its equivalent alphanumerical value is	02 02 03 04 05.
As per the algorithm key is b(1)	3 5 6 7 8

The cipher text formed will be 5 7 9 11 13
e g I k m

We will see a lot of variations in the cipher text generated for slight variations in the plain text. Thus it provides a maximum avalanche effect to the algorithm which provides for more strength and security.

8. Security Analysis

1. A Variable length key is used which makes the algorithm free from linear cryptanalysis.
2. A sign function is used for development of sequence which is used to generate basins. This sign function converts all positive values to 1, negative values to -1 & zero to 0. This makes the algorithm free from differential crypto analysis.
3. A mod function is used on selective plain text values to choose corresponding basin. This provides for better avalanche effect with a small change in plain text will produce a significant variations in cipher text.
4. A small change in key values will have a considerable change on the values of basins, which provides for better avalanche effect.

9. Comparative Study Of The Proposed Variable Length Key Encryption Algoritham With Standard Algorithms Like Des and RSA In Terms Of Computational Overhead, Complexity And Security Analysis

Algorithm	Computational overhead
DES	6424 for a56 bit key
RSA	1,26,072 for a 200 bit key
A new variable leng th key encryption algorithm.	1953 for a 9 character key.

10. Conclusion

The present work is compared with standard algorithms like DES & RSA. It is observed that the proposed algorithm is having equal security with respect to DES & RSA algorithms at low computational overhead. Thus in applications like Broad casting applications, wireless sensor networks the proposed algorithm can well be used. The proposed work along with public key distribution mechanism can well be used in secure electronic transactions, digital cash where security to data is of higher importance. It is also observed that by changing the key by one value, the number of basins formed is varying in nature, which provides a better avalanche effect. This provides more security and strength to the algorithm.

References

1. Brics, *"Universally comparable notions of key exchange and secure channels"*, Lecture Notes in Computer Science, Springer, Berlin, March 2004.
2. Bruce Scheneier, *"Applied cryptography"* (John Wiley & sons (ASIA) Pvt. Ltd.
3. Brassard .G, *"Modern cryptology"*, a tutorial lecture Notes on computer science , (325) ,(spring-verlas) , Vol. 10, No.1, PP. 71-84, Jan 99.
4. Henry Baker and Fred Piper , *"Cipher systems"*(North wood books, London 1982).
5. J.William Stalling , *"Cryptography and network security"* (Pearson Education,ASIA1998)
6. Krishna A.V.N, *"A new algorithm in network security"*, International Conference Proc. Of CISTM-05, 24-26, Gurgoan, India, July 2005.
7. Krishna A.V.N, Vishnu Vardhan.B, *"Utility and Analysis of some Encryption algorithms in E*

learning environment", International Convention Proc. of CALIBER 2006, Gulbarga, India, 02-04, Feb. 2006.

8. Krishna A.V.N, S.N.N.Pandit, *"A new Algorithm in Network Security for data transmission"*, Acharya Nagarjuna International Journal of Mathematics and Information Technology, Vol.1, No. 2, PP.97-108, 2004.

9. Krishna A.V.N, S.N.N.Pandit, A.Vinaya Babu, *"A generalized scheme for data encryption technique using a randomized matrix key"*, Journal of Discrete Mathematical Sciences & Cryptography, Vol.10, No. 1, PP.73-81, Feb 2007.

10. Krishna A.V.N, A.Vinaya Babu, *"Web and Network Communication security Algorithms"*, Journal on Software Engineering, Vol.1,No.1, PP.12-14, July 06.

11. Krishna A.V.N, A.Vinaya Babu, *"Pipeline Data Compression & Encryption Techniques in e-learning environment"*, Journal of Theoretical and Applied Information Technology, Vol .3, No.1, PP.37-43, Jan 2007.

12. Krishna A.V.N, A.Vinaya Babu, *"A Modified Hill Cipher Algorithm for Encryption of Data in Data Transmission"*, Georgian Electronic Scientific Journal: Computer Science and Telecommunications 2007 , No. 3(14) PP. 78-83.

13. Lester S. Hill, *"Cryptography in an Algebraic Alphabet"*, The American Mathematical Monthly 36, PP.306–312, June-July 1929.

14 Lester S. Hill, *"Concerning Certain Linear Transformation Apparatus of Cryptography"*, The American Mathematical Monthly 38, PP.135–154, 1931.

15. Maybec.J.S, Sign Solvability, *"Proceedings of first symposium on computer assisted analysis and model simplification"*, Academic Press, NY, 1981.

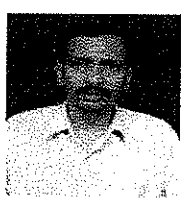
16. Pandit S.N.N, *"Some quantitative combinatorial search problems"*, (Ph.D. Thesis) (1963).

17. Pandit S.N.N, *"A New matrix Calculus"*, J Soc., Ind. and Appl. Math., PP. 632-637, 1961.

18. Phillip Rogaway , *"Nonce Based Symmetric Encryption"*, www.cs.ucdavis.edu/rogeway.

19. Ronald Rivest of RSA , *"The RC4 algorithm"*, Modern cryptology, a tutorial lecture Notes on computer science , (325) ,(spring-verlas) .

Author's Biography



A.V.N.Krishna, Professor, Computer Science, Indur Institute of eng. & Tech., Siddipet, India. He has 19 yrs of teaching Experience at UG & PG level and actively involved in Research. His fields of interest are Cryptography, Mathematical modeling & Data Mining. He has Published Papers at Journals of National & International repute and presented work at International Conferences.