ISSN: 2321-7782 (Online)
Volume 2, Issue 10, October 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Modified Related Key Algorithm for Data Transmission

Tarun Mahajan[1]
Assistant Professor(CSC)
R.R.M.K Arya Mahila Mahavidyalaya
Pathankot – India

Sheetal[2]
R.R.M.K Arya Mahila Mahavidyalaya
Pathankot – India

Sumiti Duggal[3]
R.R.M.K Arya Mahila Mahavidyalaya
Pathankot – India

Abstract: ***Data is being transmitted from source to destination on the network. Data can be delivered successfully to the destination or data can be corrupted and lost. Data may of prime importance to an organization so there must be mechanisms in order to solve this problem. These problems can be referred to as attacks. Attacks could of many types. In this case we are focusing on WEP(Wired Equivalent Privacy). This protocol is vulnerable to related-key attack. WEP is generally used to protect WiFi internet devices. In order to prevent the related key attack we will use complex relationships between encryption keys. The protocol we will suggest is Complex Relation Model. In this model random number generator will be used along with distance calculator. This model will use asymmetric encryption.***

Keywords: Related Key, WiFi, WEP, Asymmetric Encryption, Complex Relation Model.

I. INTRODUCTION

Now days, Information is very important for an organization. Accurate information will lead to the success and inaccurate information will lead to failure of an organization. There are secure and unsecure medium of data transmission. If unsecure medium like Computer Networks, Telephone lines etc, are used to transmit the data then hackers may intercept the data and read the important information. They may change or modify the message during its transmission in such a way that receiver may not able to discover the change. In related key attacks hacker will determine one of the keys and then use that key to decrypt entire message. In our algorithm we will use random number generator along with the distance calculator to design a key which will stop such attacks. The message will be considered as group of numbers and complex calculations mechanisms will be used to generate key. Hence this algorithm will be asymmetric in nature.

1.1 Goals

There are number of goals which are associated with the Complex Relation Model.

a) Confidentiality: It is one of the most important goals associated with this algorithm. No one can decrypt the message except for the person having the key.

b) Data Integrity: The term integrity means validity of data. With the help of this protocol hacker cannot decrypt the data and hence data cannot be changed.

c) Non-Repudiation: This is a mechanism which is used to ensure that receiver cannot claim that message is not being delivered to the destination.

1.2 Basic Terminology

There are following terminology which is associated with Complex Relation Model

Cryptography: The word Cryptography is derived from the Greek word"KRYPTOS", which means hidden and "GRAPHIKOS" which means writing, it is a technique to change original form of text into some other form that looks meaningless to others.

Plain Text: The original text which is transmitted is known as plain text.

Cipher Text: The text which we get after encryption (converted text) is known as cipher text.

Network Security: it ensures to protect the usability, integrity, reliability and safety of data during their transmission on a network.

Random Number Generator: Random Number Generator will generate the number corresponding to given character in the message.

Distance Calculator: This will give us the actual distance of the character from the character in cipher text.

II. Symmetric and Asymmetric Algorithm

The symmetric algorithm will be the one in which single key is used in order to perform encryption and decryption of data. This method was followed before public key was discovered. The safe way to move the data from sender to receiver is transfer secret key by using secure channels.

The Example of symmetric key algorithm will be Caesar cipher model. In this case at Encryption side following formula

E(x)=(x+n)mod p

At decryption side following formula will be used

E(x)=(x-n)mod p

The Asymmetric algorithm will assume numbers in place of the characters. Complex calculations are performed in order to calculate the characters in cipher text corresponding characters in plain text. RSA algorithm will be example of Asymmetric Algorithm.

III. Purposed algorithm

The algorithm which we are purposing in here will use random number generator at encryption side. The numbers will have a range(0-100). Out of these number generator can select any number.

Y=Random(100);

Random method will give any value between 0-100 and result will be stored with in Y variable.

Now at encryption side position of this character will be added with this number and then will be divided by total numbers of characters in the character set.

Let message to be transferred is "Name". Let random numbers corresponding to the above numbers are:10,5,20,3.

The position of numbers within the message is: 14, 1,13,5

These position values are added with the random numbers and result will be: 24, 6,33,8

First character of the message will give total number of characters in the message.

Key will be obtained as:42101522013224162331 8

First four positions will corresponds to original message position and next four key position values.

Characters are stuffed in order to determine the length of key element.

Now, at Decryption side the receiver will decrypt the key by the following

Key received =42101522013224162331 8

The receiver will decrypt it by selecting first digit as character count for the total number of characters in original message. Stuffed characters and distances are removed at receivers end.

Decryption Process:

A1) First of all 4 is received that will suggest total number of characters in original message.

A2) '2' will indicate total numbers of characters in the first key element. Which means '10' will be extracted. After that 1 will indicate single keyed element which means '5'. This process continues until entire message is read. After extraction message will become 10 5 20 3 24 6 33 8

A3) After character stuffing is removed subtract first 4 numbers from next four numbers as (24-10 6-5 33-20 8-3) =14 1 13 5

A4) Through subtraction original message character positions are again obtained. So in the above steps it is clear that generated key will be very difficult to be hacked.

The generalized algorithm at encryption side will be as follows:

COMPLEX_PART1(N)

a) Read Message(str)

b) Calculate length

N=strlen(str)

c) Convert characters to corresponding number values

I=0

Repeat While(I<N) Loop

X=Ascii(str[I])

X=X-39

Str1[I]=X

End of While

d) Generate Random Numbers and add it with digits of the characters in original message

I=0

Repeat while(I<N)Loop

Y=random[1-100]

Str2[I]=Str1[I]+Y

I=I+1

End of While

e) Now perform character stuffing

I=0

K=0

Final[I]=N

I=1

Z=strlen(str2[I])

Final[I]=Z

I=I+1

K=I

While(I<=N) Loop

Z=strlen(str2[K])

Final[I]=Z

Final[I+1]=str2[K]

I=I+1

K=K+1

End of While Loop

f) Final[N] will be the key to be transmitted.

At Decryption Side

COMPLEX_PART2(FINAL[N])

a) Read Final[N]

b) K=Final[0]

c) I=1 J=0

d) While (I<K) Loop

W=Final[I]

I=I+1

While(J<W) Loop

Code[J]=Final[I]

J=J+1

I=I+1

End of While Loop

End of While Loop

e) P=0,I=0

f) While (P<K)

Decrypt[I]=Code[K+I]-Code[I]

I=I+1

P=P+1

End of While Loop

g) Character corresponding to Decrypt[N] will be the original character

Complex_part1 algorithm will be used at encryption side and Complex_part2 algorithm will be used at decryption side.

IV. Conclusion and Results

The purposed algorithm will going to enhance the security of data. The scheme which is purposed in this paper can be implemented as asymmetric algorithm. Key value in this case is lengthy and complex. So it is not easy to hack. The cost and effort associated with this algorithm is high. This algorithm will increase efficiency and ensure integrity of data can be maintained.

V. Future Work

There is still a great deal of work which is required in this area. The purposed algorithm although increases security still its key value is difficult to generate. So encryption as well as decryption will require huge cost. In the future we wish to modify the above algorithm so that key can be easily calculated and cost can be reduced.

References

1. Ayushi, Lecturer Hindu College,"A Symmetric Key Algorithm" Vol-I-No.15.
2. Mohamad Abutaha, Mousa Farajalla, Radwa Tahboub, Mohmad Adeh,"Cryptography is the Science of Information Security",Vol-5:Issue-3,2011.
3. Ajit Singh, Rimple Glhotra," Data Security Using Private Key Encryption System Based On Arthmetic Coding", Vol-3,No,3,May 2011.
4. Yogesh Kumar, Rajni Munjal, Harsh Sharma, "Comparison Of Symmetric And Asymmetric Cryptography With Existing Vulnerabilities And Countermeasures",Vol-11,Issue-03,Oct 2011.
5. Vishwa Gupta, Gajendra Singh, Ravinder Gupta," Advanced Cryptography Algorithm", Vol-2 Issue 1.
6. Pratap Chanadra Mandal, " Superiority Of Blowfish Algorithm", Vol-2, Issue 9.
7. Bibash Roy , Gautam Rakshit, Ritwik Chakrobarty," Enhanced Key Generation Scheme Based Cryptography With Dna Logic", Vol -1,No.8.
8. Gehani Ashish, La Bean, Thomas H. Reit, John H," DNA Based Cryptography", Department Of Computer Science, Duke University, June 1999.
9. Dan Boneh, Matthew Frankin," Identity Based Encryption From Weil Pairing",Vol-32,No.3,Pp.586-615,2003.
10. Mansoor Ebrahim, Shujeet Khan, Umer Bin Khalid," Symmetric Algorithm Survey:A Comparative Analysis" ,Vol-61,No.20,2013.
11. Hansche,"Cryptography",(ISC)2 Press,2003.
12. Wheeler D.J & Needham R.J (1994),"Tea,A Tiny Encryption Algorithm",Proceeding Of The 2nd International Workshop,1008.
13. Heys H.M,Tavaser.E,"Security Of The Cast Encryption Algorithm", Electrical And Computer Engg.
14. Michael J. Wiener," CRYPTOBYTES" ,Vol-4,No.1,1998.
15. Sri Rangarajan, N. Sai Ram, N. Vamshi Krishna," Securing Sms Using Cryptography ", Vol. 4 (2) , 2013, 285 – 288.

