International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 3, Issue 5, September-October 2014 **ISSN 2278-6856**

Crypt Analysis Using Simple Logical and Complement Operation

Dr S Kiran[1] ,Dr T.BhaskaraReddy[2], Hema Suresh Yaragunti [3], Dr B.G.Prashanthi [4]

[1] Assistant Professor in the Dept of Computers Applications, Y.V. University, Kadapa.

[2] Associate Professor in the Dept of Computer Science & Technology, S.K.U., Anantapuram

[3]. Research scholor, Dept.of Computer Science & Technology, S.K.U.Anantapuram

[4] Asst.Professor & Head of the Department, Computer Science in S.R.N.Adarsh College,Bangalore

Abstract

Communication is a basic process of exchanging information. Secure communication includes means by which people can share information with varying degrees of certainty that third parties cannot intercept what was said. Information security is a very important aspect now a day. The introduction of internet and distributed system made the information security issue more challenging and complex. Cryptography plays a crucial role in providing security to data transmitted over the internetwork. In our proposed scheme, we have suggested a method for developing poly substitution method and applying traditional XOR operation and then performing 2's complement which makes a reversible process. This method converts plain data into cipher value by performing above operations which involves less coding, doesn't involve complex mathematical operations and hence works very fast and occupies less amount of space.

Keywords:- Information security, Plaintext, Encryption, Decryption, Poly substitution, Key, XOR operation, 2's compliment, Cipher value.

1. INTRODUCTION

Industrial wireless transmission has arrived providing clear and significant advantages. Nevertheless, security is always an important issue and a question often arises is " Will information be secure when broadcast via wireless networks ?" the answer can be found in understanding the technologies and algorithms employed in these products and, to that end, this paper will provide the understanding needed with simple algorithm of Cryptography.

a. Why Cryptography ?

Cryptography is necessary when communicating over an un trusted medium, which includes just about by any new network, particularly the internet. Within the context of any application-to-application, there are some specific requirements, including:

- Authentication: The process of proving one's identity.
- Privacy/Confidentiality: Ensuring that no one can read the message except the intended receiver.
- Integrity: Assuring the receiver that he received message has not been altered in any way from the original.
- Non-repudiation: A mechanism to prove that the sender really sent his message.

Cryptography, then, not only protects data from theft or alteration. There are in general three types of cryptographic schemes typically used to accomplish these goals: Secret key (or symmetric)cryptography, public-key (or asymmetric)cryptography, and hash functions. Encryption[1,4] is the conversion of data into a form, called a cipher[2,3] that appears to be random and meaningless cannot be understood by unauthorized people. Decryption[1,4] is the process of converting cipher text back to plain text. To encrypt more than a small amount of data, symmetric encryption is used. A symmetric key is used during both encryption and decryption processes. To Decrypt a particular piece of cipher text, the key that was used to encrypt the data must be used. In this paper, an Algorithm which incorporates poly substitution method[5], logical and mathematical operations. To encrypt a message, convert the text characters into its ASCII values and ASCII values are converted into binary number form, change the LSB and MSB bits. Consider a key element and convert the key into binary form. Perform XOR operation for the key element in binary form to the text resulted after changing LSB and MSB. Arrange all the obtained bits in reverse order, take 2's complement and then convert the result into decimal form which is the required cipher value. The reverse of the encryption process called decryption which obtains the original message from the cipher text.

2. PROPOSED METHOD

A.Encryption Process

Consider a plain text message say "SECURE". Now consider the first character 'S' of the plain text, take the ASCII value of the character and convert it into binary form. Change the LSB and MSB bits as 1 to 0 or 0 to 1. Then consider a key between 1 to 128 element which is used to encrypt the message and then take the binary form of that key. Next perform XOR operation for the binary form key element to the resultant obtained for the character.

B. Encryption Algorithm:

The Encryption Algorithm is as follows:

step1: Start

step2: Input the plain text message to be transmitted.

step3: Read the character from the plain text message and take the ASCII value..

step4: Convert the ASCII value into binary number form.

step5: change MSB and LSB bits as 1 to 0 (or) 0 to 1.

step6: Consider a key element of ASCII value in between 1 to 128 numbers and convert that into binary number.

step7: perform XOR operation for key element to the character which are obtained in binary form, arrange all the bits in reverse order.

Step8: Take 2's compliment for the resultant in step8 and convert into Decimal number which is the required cipher value .

step9: Stop.

C. Decryption Process:

To Decrypt the cipher text Follow steps in given decrypt algorithm.

D. Decryption Algorithm :

step1: Convert the cipher value into binary

step2: Arrange the bits in reverse order and take the 2's compliment.

step3: Consider a key element and convert it in to Binary form and Perform XOR with the above step2 resultant.

step4: Change the LSB and MSB as 1 to 0 (or) 0 to 1.

step5: Convert the step4 result into ASCII value.

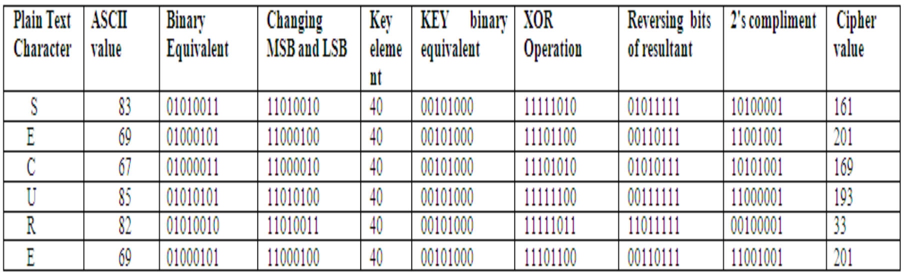
step6: Convert the ASCII value into Character which is the required original plain text.

step7: Stop.

C. Result:

Example: Consider a plain text message "SECURE". The Encryption and Decryption results produced by the algorithm are as follows .

TABLE 1. ENCRYPTION



Plain Text Character	ASCII value	Binary Equivalent	Changing MSB and LSB	Key element	KEY binary equivalent	XOR Operation	Reversing bits of resultant	2's compliment	Cipher value
S	83	01010011	11010010	40	00101000	11111010	01011111	10100001	161
E	69	01000101	11000100	40	00101000	11101100	00110111	11001001	201
C	67	01000011	11000010	40	00101000	11101010	01010111	10101001	169
U	85	01010101	11010100	40	00101000	11111100	00111111	11000001	193
R	82	01010010	11010011	40	00101000	11111011	11011111	00100001	33
E	69	01000101	11000100	40	00101000	11101100	00110111	11001001	201

Table2 . Decryption

cipher value	Binary equivalent	2's compliment	Reversing bits	Key	Key Binary equivalent	XOR	Changing LSB and MSB bits	Resultant ASCII value	Resultant plain text
161	10100001	01011111	11111010	40	00101000	11010010	01010011	83	S
201	11001001	00110111	11101100	40	00101000	11000100	01000101	69	E
169	10101001	01010111	11101010	40	00101000	11000010	01000011	67	C
193	11000001	00111111	11111100	40	00101000	11010100	01010101	85	U
33	00100001	11011111	11111011	40	00101000	11010011	01010010	82	R
201	11001001	00110111	11101100	40	00101000	11000100	01000101	69	E

C. Features :

- Involves simple coding.
- Low processing delay.
- Simple to analyze.
- Incorporates the substitution, simple logical operations.
- Fast response.
- More secure.
- Simple to Encrypt and Decrypt with key element.

D. Limitations :

- Applicable for only small Scale of Data, Time taken is more for large scale of data.

E. Conclusion :

Information security is the ongoing process of exercising due care and due diligence to protect information, and information systems, from unauthorized access, use, disclosure, destruction, modification, or disruption or distribution. Active attacks involve both modification and fabrication of messages. The goal of the encryption algorithm designing is to frustrate the hackers and makes the cryptanalysis difficult. The key value play more important role in encryption process. Altering each value of the cipher text generated to get the final cipher text make the cryptanalysis still more complex. The algorithm provides appreciable data security and requires minimum coding .The algorithm can be applied to message of any length.

References:

[1] Information Security: Text Encryption and Decryption with Poly Substitution method and combining features of cryptography.-R.Venkateswaram, Dr.V.Sundaram ,June 2010. U. K.Sastry, Prof. D. S. R. Murthy, Dr. S. Durga Bhavani .

[2] Cryptography and Network Security Principles and

Practices, Third Edition – William Stallings

[3] Introduction to Modern Cryptography, Jonathan Katz, Yehuda Lindell Chapman & Hall /CRC Taylor RFrancisGroup

[4] A modified Hill cipher Involving Interweaving and Iteration.- V. Umakanta Sastry, N. Ravi Shankar and S. Durga Bhavani , July 2010.

[5] A block cipher having a key on one side of plain text Matrix and its Inverse on the other side. Dr. V.

[6] Applied Cryptography Protocols, Algorithms and Source Coding BRUE SCHNEIER, Second Edition, John Wiley & Sons, Inc

AUTHORS

Dr.S.Kiran is an Assistant Professor in the department of Computer Science and Engineering at Yogivenama University, Kadapa, A.P. He has completed his M.Sc and Ph.D in computer science from S.K.University. He has acquired M.Tech from Nagarjuna University. He has been continuously imparting his knowledge to several students from the last 5 years. He has published 10 National and International publications.. His research interests are in the field of image Processing, computer networks, data mining and data ware house.

Dr.T.Bhaskara Reddy is an Associate Professor in the department of Computer Science and Technology at S.K. University, Anantapur A.P. He holds the post of Deputy Director of Distance education at S.K.University and He also the CSE Cocoordinator of Engineering at S.K. University. He has completed his M.Sc and Ph.D in computer science from S.K.University.He has acquired M.Tech from Nagarjuna University. He has been continuously imparting his knowledge to several students from the last 17 years. He has published 47 National and International publications. He has completed major research project (UGC). Four Ph.D and Three M.Phil have been awarded under his guidance. His research interest are in the field of image Processing, computer networks, data mining and data ware house.

Dr.B.G.Prasanthi M.Sc.M.tech.,M.phil (CS) from Sri Rama krishna PG college ,Nandyal and M.phil from algappa university and doing Ph.D in computer science at S.K.University Anantaput. she has 8 years of teaching experience and 2 years of industry. She has published 20 national and international papers in wireless networks, routing techniques She is currently working as Asst.Professor & head of the department, Computer Science in S.R.N.Adarsh College,Bangalore.

Mrs.Hema Suresh Yaragunti is research scholar in the department of Computer Science Technology at S.K.University. She acquired M.Sc in Computer Science from Karnataka University Dharwad. She has 5 years of experience in teaching and 2years of experience in software field. Her research interest is in the field of Imag Processing