Volume 1, No. 2, July-August 2010

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Implemented Encryption Scheme (One Time Pad) using 9'S Complement

Sharad Patil [*]
GMC Polytechnic , Shahada
Research Student, Bharti Vidyapeeth, University
Pune(MS), India
sd_patil057@rediffmail.com

Ajay Kumar
D.Y. Patil Institute of Mgt.
Research Guide, Bharti Vidyapeeth, University
Pune(MS), India
ajay19_61@rediffmail.com

Abstract: In this articles we show how implemented one time security encryption scheme is more lucid , effective , However it is more complex in nature of attacker view. The one-time pad encryption scheme itself is mathematically unbreakable. (see Claude Shannon's "Communication Theory of Secrecy Systems"). Therefore, the attacker will focus on breaking the key instead of the cipher text. Random key stream can be used to create lifetime supply of keys for one time pads. Here we provided the practical approach that you can use to set up your own one-time pad encryption. Permutation techniques can be used in conjunction with other technique includes substitution, encryption function etc. for effective performance. The goal of this article to show how the one-time pad encryption technique can be achieved including complement approach technique.

Keywords: Cryptography, One-time pad, Encryption, Key -Enhancement, Network Security, Computer Security.

I. INTRODUCTION

Computer tend now a days to be organized in large networks connected to Internet, and are used in an increasing number of sensitive applications, such as online banking and shopping , control of hardware installations and public infrastructure . Meanwhile ,as more and more critical tasks are delegated to computers, computer security becomes a matter of first importance, hence the interest of understanding what everyday practical computer security consist.

The Network security is concerned with the security of information.[Good security means that the system and users are protected from attacks originating from inside the network just as well as they from outside attacks.] Security- guarding against interference by entities external to a system. The main aim is to protect the information, which are sent from one computer to another computer through network. The information security is defined as follows.

Information security = Confidentiality + integrity + availability + authentication

There can be no information security without confidentiality. Confidentiality ensures the unauthorized users do not intercept, copy or replicate the information. The integrity is necessary so that the accurate information can flow over the network The information security is also required during the retrial of the data. The users should be authenticated to retrieve data and the information is not secure without authentication.

There is no such thing as a completely secure computer network. The nature of a network is to allow communication. Any communication can fall into the wrong hands. The purpose of this guide is to help you secure your network without putting a halt to its use and put in place the safeguards to detect when your security is breached.

Today's corporate networks are complex and diverse. They connect mainframes, minis, PC's, LAN's and peripherals over ever-widening geographic boundaries. This diversity, both technically and geographically, means that devising an effective corporate-wide security plan involves adapting security techniques and procedures from the various systems currently incorporated in your company. Control access to your network and all its related parts. (This means terminals, switches, modems, gateways, bridges, routers, even printers)

A. *Objectives of Network Security*

Ensure that any message sent, arrives at the proper destination.

Ensure that any message received was in fact the one that was sent. (nothing added or deleted) they refer to as Minimal Security Functional Requirements for Multi-User Operational Systems. The major functions are listed below.

Protect information in-transit, from being seen, altered, or removed by an unauthorized person or device.

Any breaches of security that occur on the network should be revealed, reported and receive the appropriate response.

Have a recovery plan, should both your primary and backup communications avenues fail.

Network security is the effort to create a secure computing platform, designed so that agents (users or programs) cannot perform actions that they are not allowed to perform, but can perform the actions that they are allowed to. The actions in question can be reduced to operations of access, modification and deletion. Network security can be seen as a subfield of security engineering, which looks at broader security issues in addition to network security.

B. *One Time Pad*

One well known realization of perfect secrecy is the One-time Pad, which was first decscibed by Gillbert Vernam in 1917 for use in automatic encryption and decryption of telegraph messages. It is interesting that the One-time Pad was thought for many years to be an "unbreakable" cryptosystem, but there was no mathematical proof of this until Shannon developed the concept of perfect secrecy over 30 year later.

We can only talk about OTP if four important rules are followed. If these rules are applied correctly, the one-time pad can be proven to be unbreakable (see Claude Shannon's "Commu-

nication Theory of Secrecy Systems"). However, if only one of these rules is disregarded, the cipher is no longer unbreakable.
1. The key is as long as the plaintext.
2. The key is truly random (not generated by simple computer Rnd functions or whatever!)
3. There should only be two copies of the key: one for the sender and one for the receiver (some exceptions exist for multiple receivers)
4. The keys are used only once, and both sender and receiver must destroy their key after use.

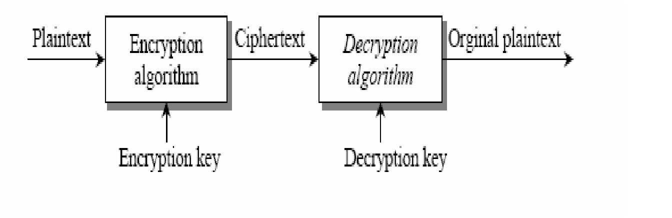
For practical application, the key used for one time pad cipher is a string of random bits, usually generated by a Cryptographically Strong Pseudo-Random Number Generator. However for ultimate security, it is suggested to generate the key by using the natural randomness of quantum mechanical events, since quantum events are believed scientifically to be the only source of truly random information in the universe.

If the key is truly random an XOR operation based one – time pad encryption scheme is perfectly secure against cipher text-only cryptanalysis.

We come to the point that if the hackers do not know the sender or receiver key, then the one time pad encryption scheme is 100 % secure.

A one-time pad is essentially a pad of paper on which each page has a unique set of random letters. The sender and receiver have identical pads. Each letter on the pad is used to determine a single letter of the enciphered message. Since the letters on the pad are random, there is no formula that can be determined by studying the letters. Assuming that the pad is not compromised, and each page is used only once, then the OTP system is unbreakable. One-time pads are "information-theoretically secure" in that the encrypted message (i.e., the cipher text) provides no information about the original message to a cryptanalyst (except the length of the message). This is a very strong notion of security first developed during WWII by Claude Shannon and proved, mathematically, to be true of the one-time pad by Shannon about the same time. His result was published in the Bell Labs Technical Journal in 1949. Properly used one-time pads are secure in this sense even against adversaries with infinite computational power.

II. METHODOLOGY



In this article we consider the basic fact of one time pad encryption scheme with little bit concept of 9’s complement is added and then evaluate the scheme. Here we use concept like key size must be same as long as the plaintext. Key must be truly random and at last keys are used only once, and both sender and receiver must destroy their key after use. Here we first create the chart for alphabet 1-26 that shown in Table-1 and then take the decimal equivalent value of the text message from table then take the 9’s complement of decimal value , convert the 9’s complemented decimal value in to 6 bit binary , generate the random number key , then after apply EX-OR properties , [i.e. 1-1=0, 0-0=0 and 1-0=1,0-1=1] after ex-oring take the 1’ complement of result , after that convert the complement value into decimal digit, if digit value is more that 26 then subtract the value form 26 and write equivalent alphabet which is the encrypted message sent to the recipient, then recipient apply reverse process and get the plain text .

Table-I

Alphabet	*Number*	*Binary 6 bit Eq. Decimal Value*
A	1	000001
B	2	000010
C	3	000011
D	4	000100
E	5	000101
F	6	000110
G	7	000111
H	8	001000
I	9	001001
J	10	001010
K	11	001011
L	12	001100
M	13	001101
N	14	001110
O	15	001111
p	16	010000
q	17	010001
r	18	010010
s	19	010011
t	20	010100
u	21	010101
v	22	010110
w	23	010111
x	24	011000
y	25	011001
z	26	011010

III. ALGORITHM

Steps:
1 Consider the Plain text
2. Take decimal value of the text message from table
3. Take 9’s complement of the decimal value
4. Convert 9’s complemented value into 6 bit binary.
5. Apply 6 bit key
6. Apply property of X-OR
7. Take the 1’s complement of resulted X-OR
8. Convert X-OR resulted value into decimal. If decimal value is more than 26 subtract it from 26 and then write equivalent alphabet from table shown.
9 Write equivalent alphabet [Which is encrypted text].
10 Send encrypted text again converted into 6 bit binary from table
11 Apply the same key and X-OR Properties.
12 Take the 1’s and 9’s complement
13 Convert into equivalent alphabet which is not but the plain text.

IV. IMPLEMENTATION AND ANALYSIS

Here we consider one simple example for wide understanding.

Encrypted Process from Sender Side :-

Take the example here as a plain text GOD

G O D

Decimal equivalent from table G=7, O=15 and D=4

Take the 9's complement i.e. 9-7= 2, 9-1 =8, 9-5 =4 and 9-4 =5

So 2 8 4 5

Convert 6 bit binary and apply 6 bit key

6 bit	000010	001000	000100	000101
Key	101010	101010	101010	101010
	----------	-----------	-----------	----------
X-OR	101000	100010	101110	101111
1' Complement	010111	011101	010001	010000
Decimal Equi.	23	3	17	16
Alphabet From Table	w	c	q	p

Encrypted text is WCQP of GOD

This encrypted text WCQP is send to the recipient

B] Decrypted Process from Recipient Side

	w	c	q	p
	010111	011101	010001	010000
Key	101010	101010	101010	101010
	----------	-----------	-----------	----------
X-OR	111101	110111	111011	111010
1's Com- plement	000010	001000	000100	000101
Deci Equi.	2	8	4	5
Take 9's Comple.	7	1	5	4
i.e	7	15	4	
	G	O	D [Which is plaint text]	

V. CONCLUSION

This scheme is more lucid for user point of view but very difficult for attacker point of view. Here we are using 9's and 1's complement for making more complexity for attacker side , so attacker could't find as well as not guessing the plain text easily. so this scheme is more applicable for sensitive application , Again the key is used is same as well as different for all text so it is beneficial for user from both side.

VII. REFERENCES

[1] Douglas R, Stinson " CRYPTOGRPHY Theory and Practice " Second Edition .

[2] Charlie Kaufman st al. " Network Security " PRIVATE Communication in a PUBLIC World. , Prentice Hall of India Private Limited. 2003

[3] Information Technology Journal 4(3) : 204-221, 2005

[4] Claude Shannon's " Communication Theory of Secrecy Systems" .

[5] Thomas L. Floyd " Digital Fundamentals"

[6] Neal R. Wagner "The Laws of Cryptography: Perfect Cryptography: The One-Time Pad".

[7] Ritter, Terry 1991. The Efficient Generation of Cryptographic Confusion Sequences. Cryptologia "15: 81-139".

[8] Pete McCollum "Encryption Via One-Time Pads"

Sharad Patil: Computer Science from Babasahed Ambedkar Marathwada University, Aurangabad in 1990 . Presently he is working as a Head of Dept. in computer in PSGVP'S Mandal's GMC Polytechnic Shahada (MS). He is doing Ph.D. in Computer Science from Bharati University, Pune-India. He has presented and Published 9 papers in national, international conferences and journals. His area of interest is Computer Networks and Security systems.

Dr. Ajay Kumar: He has completed B.E., M.Sc.Engg. in Computer Science and Ph.D. in Computer Science. He is having 20 years of teaching experience. Presently he is working as Director, Dr. D.Y. Patil Institute, Pune , he was Professor and Head of Dept of MCA in Modern College of Engineering Pune-India, Jaywant Institute of Management Pune. He has published 4 books in Information Technology. He has also published more than 23 papers in National / International Conferences and Journals. His area of interest is Software engineering and Computer Networks .