International Journal of Information Technology and Knowledge Management
January-June 2012, Volume 5, No. 1, pp. 65-67

"IMPLEMENTED ENCRYPTION SCHEME USING EVEN(10'S AND 2'S) COMPLEMENT WITH BINARY ADDITION APPROACH"

Sharad Patil[1] Ashok Patil[2] and Ajay Kumar[3]

ABSTRACT: This paper we propose new methods for encryption by considering basic theory of unbreakable one time pad. Network security is often an unpopular subject it is unhandy, restricts what we can and cannot do, and offers no immediate payoff or reward. Its implementers may ultimately get a pat on the back, but only after disaster strikes. More frequently, security policies and the people who implement them are cursed. Nonetheless, security is absolutely essential to a network survival. It is important a company-wide security plan that takes into account the needs of every location, every department, and every machine and user within the enterprise, regardless of what type of system they may be using. In these articles we try to verify how implemented one time security encryption scheme is more lucid, effective, however it is more difficult in nature of attacker life point of view. Here in this experimental analysis, we combined different and various approaches of even complements for setting proper (one time pad) unbreakable encryption scheme for effective performance and proper security benefit.

Keywords: Security, One-time pad, encryption, Decryption, network security, computer security.

1. INTRODUCTION

The increased use of computer and communication systems by industry has increased the risk of theft of proprietary information. Although these threats may require a variety of countermeasures, encryption is a primary method of protecting valuable electronic information. In early days of computing, the greatest risk was that a clerk would get the cardboard punch cards out of order and foul up the program. Computers were huge and typically kept in specially controlled, locked rooms. Networking was minimal, and most connections to the central computer took place through dumb terminals. Computing has changed significantly, however, and connectivity has expanded far and wide. The centralized model has become less popular as distributed computing takes advantages of far-flung resources. With distributed computing, however, Vulnerability can come from many different areas. A system with multiple access points is more vulnerable[1]. Computer security becomes a matter of first importance, hence the interest of understanding what everyday practical computer security consist[2]. Firewall technology, passwords and virtual private networks are all techniques you can use to great advantages. The one-time pad encryption scheme itself is mathematically unbreakable. Therefore, the attacker will focus on breaking the key instead of the cipher text[3]. The goal of this article to show how the effective (OTP) encryption technique can be achieved including even complement with binary addition approach technique. In this paper we use novel approach of different and various complement concepts for making security stronger. Combining different complement such as 2's and 10's complement for better and concrete security and binary addition provide extra layer to security.

What is Complement Approach: A complement system or complement arithmetic is a system in which negative numbers are represented by the two's complement of the absolute value this system is the most common method of representing signed integers on computers. In such a system, a number is negated (converted from positive to negative or vice versa) by computing its two's complement. An N-bit two's-complement numeral system can represent every integer in the range -2^{N-1} to $+ 2^{N-1} - 1$.

Most computers use complement arithmetic for integer representations. The reason for this is mostly to simplify the circuitry required to perform integer arithmetic operations. We will see in that negative numbers may represented in complement form and that the operation of subtraction may be accomplished by adding the complement of a number. We will show that the complement of a number is very easy to calculate and both addition and subtraction can be accomplished by adding!

A two's-complement system, or two's-complement arithmetic, is a system in which negative numbers are represented by the two's complement of the absolute value[4]; this system is the most common method of representing signed integers on computers[5]. In such a system, a number is negated (converted from positive to negative or vice versa) by computing its two's complement. An N-bit two's-

[1] Research Student, Bharti Vidyapeeth, University., Pune(MS), India. E-mail: sd_patil057@rediffmail.com,
[2] Principal, ASC College,Shahada, Dist: Nandurbar (MS), India. E-mail: patelan71500@rediffmail.com,
[3] Director, Jawant Institute of Management Pune(MS), India. E-mail: ajay19_61@rediffmail.com

complement numeral system can represent every integer in the range -2^{N-1} to $2^{N-1}-1$. The two's-complement system has the advantage of not requiring that the addition and subtraction circuitry examine the signs of the operands to determine whether to add or subtract. This property makes the system both simpler to implement and capable of easily handling higher precision arithmetic. 10's complements also provide same advantages so, absolutely, scheme increase double layer security.

One's complement's is now days obsolete, then concept of two's complement, nine's and ten's complement provides wide applicability's in binary addition, subtraction, multiplication and division. Here in our paper work, we considered the advantages of 2's, and 10's complement into mind and applied this approach with random key generation approach. Experimentally it is tested and reveals and provides very good result,

One Time Pad Encryption: One well-Known realization of perfect secrecy is the One Time Pad, it is simple yet completely unbreakable symmetric cipher. Which was first described by Gillbert Vernam in 1917 for the 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[6], But there was no mathematical proof of this until Shannon developed the concept of perfect secrecy over 30 years later[7].

The One Time Pad has been employed in military and Diplomatic context, where unconditional security may be of great importance. (see" Claude Shannon's "Communication Theory of Secrecy Systems[3]"). In the Bell Systems Technical Journal. Here define some of the most useful criteria now. The specific characteristic offers by OTP are as follows.

- The one-time-pad is the only cryptosystem with theoretically perfect secrecy.
- The one-time-pad is one of the most practical methods of encryption where one or both parties must do all work by hand, without the aid of a computer; this made it important in the pre-computer era, and it could conceivably still be useful in situations where possession of a computer is illegal or incriminating or where trustworthy computers are not available.
- One-time pads are practical in situations where two parties in a secure environment must be able to depart from one another and communicate from two separate secure environments with perfect secrecy.
- The one-time-pad can be used in super encryption[8]
- The algorithm most commonly associated with quantum cryptography is the OTP.
- The one-time pad can be a part of an introduction to cryptography[9]

While one-time pads provide perfect secrecy if generated and used properly, small mistakes can lead to successful cryptanalysis:

2. PRESENT WORK AND METHODOLOGY

We have implemented number of encryption scheme using one's complements, 2's complements, 9's complement with binary addition subtraction with reversible approach as well as various complement approach with binary addition with Ex-OR properties 10, 11, 12. This implementation provides equal benefit with renowned algorithm. Also the algorithms is easy to handle and more sophisticated for user point of view and difficult for attacker view. In this paper we have used 10's complement as well as 2's complement [Even complement] with binary addition approach. The better understanding, the detail analysis of this method given and well explain with example in following section.

3. ALGORITHM

Here the process completed with two ends such as sender and receiver (Encryption/ Decryption) follows.

Step 1: Consider the plain text (massage), write the decimal value of plain text character from Table-1.

Table 1

Decimal No.	Alphabet	9's Complements	10's Complements	Binary 5 bit Eq. Decimal Value
1	A	8	9	01001
2	B	7	8	01000
3	C	6	7	00111
4	D	5	6	00110
5	E	4	5	00101
6	F	3	4	00100
7	G	2	3	00011
8	H	1	2	00010
9	I	0	1	00001
10	J	8,9	9,10	01001, 01100
11	K	8,8	9,9	01001, 01001
12	L	8,7	9,8	01001, 01000
13	M	8,6	9,7	01001,00111
14	N	8,5	9,6	01001,00110
15	O	8,4	9,5	01001,00101
16	p	8,3	9,4	01001,00100
17	q	8,2	9,3	01001,00011
18	r	8,1	9,2	01001,00010
19	s	8,0	9,1	01001,00001
20	t	7,9	8,10	01000,01010
21	u	7,8	8,9	01000,01001
22	v	7,7	8,8	01000,01000
23	w	7,6	8,7	01000,00111
24	x	7,5	8,6	01000,00110
25	y	7,4	8,5	01000,00101
26	z	7,3	8,4	01000,00100

Step 2: Take (write from table directly) the 10's complements of decimal equivalent.

Step 3: Convert value of 10's complements into equivalent 5 bit Binary number.

Setp 3: Generate random key not less than 5 bit

Step 4: Perform binary addition,

Step 5: Take the 2's complement of binary sum,

Step 6: Then after write the equivalent decimal value and corresponding alphabet from Table-1 as cipher text .

Step 7: end.

Here above completed the total Encryption process. Decryption process is totally reverse of encryption.

4. IMPLEMENTATION AND RESULT ANALYSIS

In this article, we consider simple example for wide and better understanding.

(A) Encrypted Process from Sender Side

Take the plain text such as GOD

G O D deci. equivalent form table G = 7, O = 15 and D = 4

Take the 10's complement 7 15 4

9 – 7 = 2 + 1 = 3, similarly for 15 is 95 and 4 is 6

Convert the 10's complement into 5 bit binary

00011 01001 00101 00110

Consider the random 5 bit key such 10101 and then perform binary addition

00011 01001 0010100110 ---- Binary Equi. Of Decimal

10101 10101 1010110101 ---- Key used

11000 11110 11010 11011

01000 00010 00110 00101

8 2 6 5

Binary Addition then after take 2's complement 2's complements then write the equi. Decimal hbfe act as a cipher text.

(B) Decrypted Process at Receiver Side

Consider the cipher text hfbe i.e. 8 2 6 5

Convert into 5 bit binary, then add key and perform binary addition.

01000 00010 00110 00101

10101 10101 10101 10101

11101 10111 11011 11010

00011 01001 00101 00110

3 9 5 6

Binary Addition Take 2's complements Convert it into equi. Decimal and take 10's complements i.e 9 – 3 = 6 + 1 = 7 similarly 15 and 4 write the equivalent alphabet which is a plain text.

7 = G , 15 = O and 4 = D So recovered plain text is GOD.

5. CONCLUSION

Computer security is very important to protect data in computer and in communication. Different algorithm modes/various encryption techniques are used to protect valuable digital assets. Our algorithm shows simplicity in implementation, more scalable, more feasible in design as part of software and hardware but hard to crack. In this method of implementation attacker come across confusion by observing decimal and binary combination with added concept of complements. In further implementation, we would like implement reversible concept of complement with binary subtraction, multiplication, division.

REFERENCES

[1] Dan Blacharski, "Network Security in Mixed Environment" IDC Books Worldwide.

[2] B. Schneier, "Applied Cryptography: Protocols, Algorithms and Source Code in C", NY. John Wiley & Sons, 1994.

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

[4] David J. Lilja and Sachin S. Sapatnekar, Designing Digital Computer Systems with Verilog, Cambridge University Press, 2005.

[5] Kunth, D.E, 1969. The Art of Computer Programming 2. Semi Numerical Algorithms Addison-Wesley, Reading, Mass.

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

[7] M. Devargas, "Network Security", Manchester, England. NCC Blackwell, 1993.

[8] http://en.wikipedia.org/wiki/#cite_note-9.

[9] http://en.wikipedia.org/wiki/#cite_note-10.

[10] Sharad Patil, Ajay Kumar "Implemented Encryption Scheme (One Time Pad) Using 9's Complement

[11] Sharad Patil, Ajay Kumar, "Modified One Time Pad Data Security Scheme: Random Key Generation Approach "International Journal of Computer and Security 3 Issue 2 March/April 2009 Malaysia.

[12] Sharad Patil, Ajay Kumar, "Effective Encryption Data Security Scheme One Time Pad: Complement Approach" International Journal of Computer Science and Communication. 1 No. I of Jan2010 Kurukshetra INDIA.