Volume 5, Issue 6, June 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A New Technique for One Time Pad Security Scheme with Complement Method

[1]Devipriya.M, [2]Sasikala.G
[1]Research Scholar, [2]Assistant Professor,
Department of Computer Science,
Adhiparasakthi College of Arts and Science,
Kalavai, India

Abstract−In Modern cryptography, a one-time pad is a system in which a private key generated randomly is used only once to encrypt a message that is then decrypted by the receiver using a matching one-time pad and key. Messages encrypted with keys based on randomness have the advantage that there is theoretically no way to "break the code" by analyzing a succession of messages. Each encryption is unique and bears no relation to the next encryption so that some pattern can be detected. With a one-time pad, however, the decrypting party must have access to the same key used to encrypt the message and this raises the problem of how to get the key to the decrypting party safely or how to keep both keys secure. One-time pads have sometimes been used when the both parties started out at the same physical location and then separated, each with knowledge of the keys in the one-time pad. In this paper, we present an implementation of one-time pad with Binary addition with 2's complements approach.

Keywords− Attacks, Cryptography, Secret, Encryption, OTP

I. INTRODUCTION

One-time pad secret writing may be a basic nonetheless solid methodology to guard short text messages. This paper explains the way to use one-time pads, the way to discovered secure one-time pad communications and the way to influence its numerous security problems. It's simple to be told to figure with one-time pads, the system is clear, and you are doing not would like special instrumentality or any data regarding scientific discipline techniques or mathematics. One-time pad secret writing is largely associate degree equation with 2 unknowns that is mathematically not possible to unravel. If properly used, the system provides actually unbreakable secret writing. While not the correct key, it'll be not possible to decipher a one-time pad encrypted message by no matter sort of scientific discipline attack, even with infinite process power and infinite time.

One-Time Pads (OTPs), I explain a practical implementation of a cryptosystem based on the one-time pad algorithm for perfectly top secret communication between two people that previously met to exchange pads. In this paper we extend one time pad through binary addition with complement approach that create cipher complicated, ultimately makes assailant life difficult.

II. RELATED WORKS

Does everybody find that there is a real thing such as a perfect encryption algorithm? In the theoretical sense, there is a solution as OTP. One-time pads are unbreakable if used properly. However, such algorithms still are rarely used in practice. In this article, we'll discuss about the one-time pad, its strengths and weaknesses, and how one time pad encryption with 2'scomplement approach makes attacker life difficult.

Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography is closely related to the disciplines of cryptology and cryptanalysis. Cryptography includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit. However, in today's computer-centric world, cryptography is most often associated with scrambling plaintext (ordinary text, sometimes referred to as clear text) into cipher text (a process called encryption), then back again (known as decryption). Individuals who practice this field are known as cryptographers.

Modern cryptography concerns itself with the following four objectives:

1) Secrecy (the information cannot be understood by anyone for whom it was unintended)
2) Reliability (the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected)
3) Non-repudiation (the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information)
4) Certification (the sender and receiver can confirm each other's identity and the origin/destination of the information)

Encryption: Encryption is the process of encoding messages or information in such a way that eavesdroppers or hackers cannot read it, but that authorized parties can. In an encryption scheme, the message or information (referred to as plaintext) is encrypted using an encryption algorithm, turning it into an unreadable cipher text. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text; encrypted data is referred to as cipher text.

To encrypt, convert the message into digits and subtract (without borrowing) the one-time pad from the text digits. Skip the first group of the one-time pad during the encryption process and use it as key indicator at the beginning of the cipher text.

Decryption: Decryption is the process of transforming data that has been rendered unreadable through encryption back to its unencrypted form. In decryption, the system extracts and converts the garbled data and transforms it to texts and Images that are easily understandable not only by the reader but also by the system. Decryption may be accomplished manually or automatically. It may also be performed with a set of keys or passwords. The process of decoding data that has been encrypted into a secret format. Decryption requires a secret key or password. Decryption is the reverse process of encryption. While encryption is coding the data into a secret format so that others cannot read or access it, decryption is decoding the data back to the original format.

III. PROPOSED METHODOLOGY

ONE TIME PAD

The One Time Pad encryption method is a binary additive stream cipher, where a stream of truly random keys is generated and then combined with the plaintext for encryption or with the cipher text for decryption by an 'exclusive OR'(XOR) addition.

It is possible to prove that a stream cipher encryption scheme is unbreakable if the following preconditions are met:

- Key must be as long as the plain text.
- The key must be truly random.
- The key must only be used once.

The One Time Pad implementation in mils electronics' products fulfills all these requirements and therefore provides absolute protection for our customer's sensitive information.

HOW IT WORKS

Typically, a one-time pad is created by generating a string of characters or numbers that will be at least as long as the longest message that may be sent. This string of values is generated in some random fashion - for example, by someone pulling numbered balls out of a lottery machine or by using a computer program with a random number generator. The values are written down on a pad (or any device that someone can read or use). The pads are given to anyone who may be likely to send or receive a message. Typically, a pad may be issued as a collection of keys, one for each day in a month, for example, with one key expiring at the end of each day or as soon as it has been used once.

When a message is to be sent, the sender uses the secret key to encrypt each character, one at a time. If a computer is used, each bit in the character (which is usually eight bits in length) is exclusively "OR'ed" with the corresponding bit in the secret key. (With a one-time pad, the encryption algorithm is simply the XOR operation. Where there is some concern about how truly random the key is, it is sometimes combined with another algorithm such as MD5.) One writer describes this kind of encryption as a "100% noise source" used to mask the message. Only the sender and receiver have the means to remove the noise. Once the one-time pad is used, it can't be reused. If it is reused, someone who intercepts multiple messages can begin to compare them for similar coding for words that may possibly occur in both messages.

The message is unbreakable anyway. Unfortunately, this ideal world hardly exists. Since it is mathematically impossible to break a one-time pad encrypted message by cryptanalysis, any eavesdropper will try to get his hands on either the original readable message or the one-time pad key, used to encrypt that message. In the real world, the eaves dropper will attempt to retrieve the identity and location of sender or receiver. Identification of the involved persons is the first step in reading their communications. The mere identification of a person who sends or receives encrypted communications, even unintelligible, might have serious consequences under an oppressive regime. Once identified, the eavesdropper can start surveillance and use technical means to retrieve information from that person's computer or perform a surreptitious search of his house to copy one-time pads that will be used in the future. The person might never know his security has been breached and his messages are read.

WHY IS OTP ENCRYPTION AND DECRYPTION IS UNBREAKABLE?

The 'brute force' attack

With One Time Pad encryption, the key used for encoding the message is completely random and is as long as the message itself. That is why the only possible attack to such a cipher is a brute force attack. Brute force attacks use exhaustive trial and error methods in order to find the key that has been used for encrypting the plain text. This means that every possible combination of key bits must be used to decrypt the cipher text. The correct key would be the one that produces a meaningful plain text.

Unlimited computing power is useless

Let's assume an eavesdropper has intercepted a One Time Pad encrypted message and that he has unlimited and time. For example, typical e-mail messages are at least 200 bytes long, requiring the testing of 1.600bits. Even if the eavesdropper is both willing and able to do this, the following paragraph will describe why unlimited computational power will not compromise the system.

Attackers must try every possible key

Since all One Time Keys are equally likely and come from a completely unpredictable noise source that is proven to be random, the attacker has to test all possible key strings.

Impossible to guess the right plain text

If he used every possible key string to decrypt the cipher text, all potential plain text strings with the same length as the original plain text would appear. As illustrated above, most of these potential plain text strings would make no sense; however, every meaningful string the same length as the original plain text would also appear as a potential plain text string. Without knowing the applied OTP, the eavesdropper has no way of finding out which meaningful string is the original plain text. Thus, trying all possible keys doesn't help the attacker at all, because all possible plain texts are equally likely decryptions of the cipher text.

IV. ALGORITHM

A. ALGORITHM FOR ENCRYPTION

Step 1: Consider the plain text (Message).Label the ASCII value of each letter from the plan.
Step 2: Convert the decimal value into eight bit binary number.
Step 3: Apply any prime number and convert into eight bit binary number as a random key.
Step 4: Perform addition for random key and plain text then we get first level result.
Step 5: Execute 2's complement for the first level result.
Step 6: Convert the 2's complement result into decimal value.
Step 7: Here we subtract decimal value from ASCII value of plain text.
Step 8: Then we get the subtracted value that is original cipher text value.

B. ALGORITHM FOR DECRYPTION

Step 1: Convert the cipher text value into eight bit binary number
Step 2: Apply any prime number and convert into eight bit binary number as a random key.
Step 3: Perform addition for random key and cipher text then we get first level result.
Step 4: Execute 2's complement for the first level result.
Step 5: Convert the 2's complement result into decimal value.
Step 6: Here we divide the decimal value by 2.we get plain text number value.
Step 7: Mark the corresponding ASCII value for the plain text number.
Step 8: At this instance we get plain text (message).

V. IMPLEMENTATION

ENCRYPTION PROCESS

TABLE 1.ENCRYPTION TABLE

ORIGINAL MESSAGE	**S**	**H**	**A**	**R**	**P**
ASCII VALUE	83	72	65	82	80
BINARY NUMBER	01010011	01001000	01000001	01010010	01010000
PRIME NUMBER	00011101	00011101	00011101	00011101	00011101
LEVEL 1 RESULT	01110000	01100101	01011110	01101111	01101101
2'S COMPLEMENT	10010000	10011011	10100010	10010001	10010011
DECIMAL VALUE	144	155	162	145	147
DECIMAL VALUE SUBTRACT FROM ASCII VALUE	144-83	155-72	162-65	145-82	147-80
CHIPER TEXT	61	83	97	63	67

DECRYPTION PROCESS

TABLE 2.DECRYPTION TABLE

CIPHER TEXT	61	83	97	63	67
BINARY NUMBER	00111101	01010011	01100001	00111111	01000011
PRIME NUMBER	00011101	00011101	00011101	00011101	00011101

LEVEL 1 RESULT	01011010	01110000	01111110	01011100	01100000
2'S COMPLEMENT	10100110	10010000	10000010	10100100	10100000
DECIMAL VALUE	166	144	130	164	160
DECIMAL VALUE DIVIDE BY 2	166/2	144/2	130/2	164/2	160/2
P(ASCII VALUE)	83	72	65	82	80
ORIGINAL MESSAGE	**S**	**H**	**A**	**R**	**P**

VI. CONCLUSION

One Time Pad (OTP) provides a novel way for two legitimate parties to establish a common secret key over a long distance. Its ultimate advantage is its unconditional security, the feat in cryptography. Combining with the one-time-pad scheme in which the private key is as long as the messages, secret messages can be communicated safely from one place to another place. This algorithm has a lot of scope to enhance the security by using combining the different approaches. We have proposed a new methodology through which one time pads can be practically used for secure communication between client and server.

REFERENCES

[1] "*Modified One Time Pad Data Security Scheme: Random Key Generation Approach "*International Journal of Computer and Security Volume 3 issue 2 March/April 2009 Malaysia (Published) by Sharad Patil, Dr. Ajay Kumar.

[2] Michael E.Gruen, *"A secure low-power approach for providing mobile encryption",* Proceedings of the Eleventh annual CCSC northeastern conference, vol -21 Issue 6,June 2006, pp288-289

[3] Ochoche Abraham, "*An improved Caesar cipher algorithm*" international journal of engineering and advanced technology , volume -2,issue -5, 1198-1202.

[4] Ch .santhosh reddy "*Poly-alphabetic symmetric key algorithm using randomized prime numbers*" international journal of scientific and research publications volume-2, issue-9, September 2012, ISSN 2250-3153.

[5] F.G. Deng and G. L. Long, "*Secure direct communication with a quantum one-time pad*," Physical Review A 69, p. 052319, 2004.

[6] Y.Dodis and J.Spencer,"*On the (non)Universality of the One-time pad*," in proceedings of the 43rd symposium on Foundations of computer science, pp376-388, 2002

