Preserving sensitive data shared through the network against security threats using cryptography

M. Janaki *[1], Dr.M.Ganaga Durga[2]

[1]*Research Scholar, Department of Computer Science, Bharathiar University,Coimbatore.*
Assistant Professor, Dr. Umayal Ramanathan College for Women, Karaikudi, Tamilnadu, India.
[2]*Assistant Professor, Government Arts College for Women, Sivaganga, Tamilnadu, India.*
[1]mjanaki81@gmail.com, [2]mgdurga@yahoo.com

Abstract

Data sharing through the networks becomes an important aspect in today's computing scenario. The main advantage of networks is fast transmission of data, at the same time the disadvantage is the security threats. This paper describes about the cryptography for ensuring data confidentiality and also discusses about substitution cipher. Cryptanalysis is done with an example data to show how the encipherment algorithms are broken which will help the researchers to develop more secured encipherment algorithms.

Keywords: Network Security, Security Threats, Cryptography, Cryptanalysis, Substitution cipher .

1. Introduction

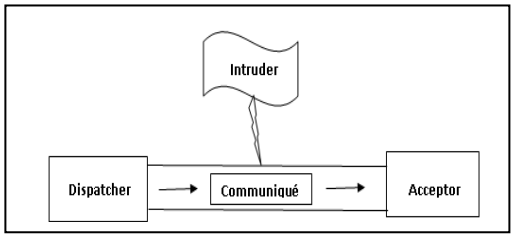
Cryptography is the strongest tool for protesting against several security threats well-organized scrambling of data, does not allow data to be read, modified or fabricated easily. Cryptography had its base in coding theory that is mathematics[1]. The computational complexity of the underlined mathematics is hidden from end user. Usually The three important aspects of a computer security is confidentiality, integrity and availability. The first aspect *confidentiality* make sure that computer-related assets are accessed only by authorized users. Confidentiality can be called as secrecy and privacy[2]. The second aspect *integrity* indicates that computer-related assets can only be modified by authorized users. The third aspect *availability* means that the computer-related assets are accessible to the legitimate users at appropriate times. Availability can also be known by its antonym denial of service.

There are many controls available to protect the computing systems from attacks. The most powerful tool in providing computer security is done with scrambling the data i.e. though the data is hacked by the cracker, it will not be in the useful form. Encryption is the term given for denoting the scrambling process[3]. The original data in the understandable format is called plain text. Using encryption the data is transformed into a scramble format called as cipher text. Security professionals nullify virtually the possibility of interception, modification and fabrication. Encryption is the best method for ensuring all aspects of computer security[4].

2. Network scenario

In a network, Dispatcher, D, is sender sending the Communiqué, C, i.e. the message, to the receiver known as Accepter, A, through the transmission medium T. If an Outsider, O, want to access the communiqué (to read, copy, modify or even destroy) then O is called as Intruder. It is not confirmed that during the transmission from D to A through T, T is a secured channel. Then the Communiqué ,C is vulnerable to attacks.

Figure 1. Network Security Threats



The Figure 1. shows the way how the Dispatcher, Acceptor, Intruder and Communiqué are related to each other. During the transmission from D to A through T,C is vulnerable to attacks and O tries to hack the communiqué by the four ways, block, intercept, modify and fabricate.

Table 1. Attacks on Network Data

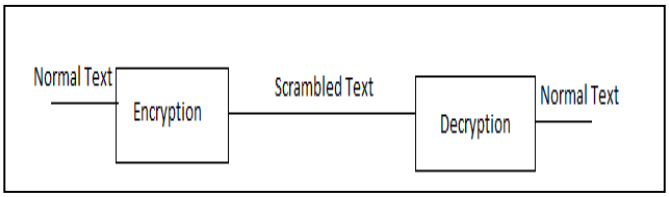
Hacking Way	Action Done	Security Breach
Block	Preventing Communiqué from reaching Acceptor	Affects the Availability of the Communiqué
Intercept	Reading the Communiqué	Affects the Confidentiality of the Communiqué
Modify	Changing the contents of the Communiqué	Affects the Communiqué's Integrity
Fabricate	Intruder sends the Communiqué to Acceptor in the name of Dispatcher	Affects the Communiqué's Integrity

Table 1. lists the ways in which the hackers affect the sensitive data shared through the network and the way in which the security goals are affected.

2.1 cryptography terminologies

There Encipherment is the process of disguising a communiqué so that it is not meaningful. Decipherment is the reverse process, transforming the disguised communiqué back to original form. A system for encipherment or decipherment is known as cryptosystem[5]. The original form of the communiqué is called normal test and the disguised form of the communiqué after encipherment is called as scrambled text. For convenience, normal text communiqué N is denoted as sequence of individual character N={n1,n2,n3,.....,nm}. Similarly scrambled text communiqué, S is written as S={s1,s2,s3...,sm}. The encipherment algorithm tells how the transformation of normal text N to scrambled text S is done. Encipherment process can be given by the notation S =E(N) and the Decipherment process can be given by the notation N=D(S) where E is called the Encipherment rule and D called the Decipherment rule. These cryptographic process were shown in the Figure 2.

Figure 2. Cryptography



Along with the set of rules for how to encipher normal text and how to decipher scrambled text often a device called Antiphon key, K is used for more security. Thus the encipherment and decipherment depends on the antiphon key. The dependence can be shown as, S=E(K,N).

3. Encipherment algorithms

The set of rules used for converting normal text to scrambled text and vice versa are called encipherment Algorithm and can be classified as keyless encipherment and keyed encipherment algorithms[6]. Keyed encipherment algorithms can be of two types: symmetric encipherment and non-symmetric encipherment. When same Antiphon key is used for encipherment and decipherment then it is known as symmetric encipherment. It is denoted as N=D(K,E,(K,N)) D and E are mirror-image processes, and hence such encipherment is known as symmetric. But sometimes, encipherment and decipherment Antiphon keys are different. Encipherment Antiphon key Ke is used for encipherment and Decipherment Antiphon key Kd is used for decipherment and denoted as N=D(Kd,E(Ke,N). This form of encipherment which uses as pair of keys is called as asymmetric encipherment.

An Antiphon key gives us flexibility in using a encipherment scheme. It is possible to create different encipherment of one Normal text message just by changing the Antiphon key. Though the encipherment algorithm is known to the intruder, one cannot access the data since the Antiphon key is unknown .Thus Antiphon key provides the additional security. In Asymmetric cryptosystem the tern cryptography, Crypt means hide, and graph means write, hence it can be meant as hidden writing[7]. It refers to the process of using encipherment to encapsulate the text to be secured. Both a cryptographer and cryptanalyst tries to recover the normal text from the scramble text. the difference is cryptographer is a person who works for a genuine dispatcher or acceptor but the cryptanalyst is a person who works for an unauthorized intruder. Cryptology is the study of encipherment and decipherment that includes cryptography and as well as cryptanalysis.

3.1 cryptanalysis methodology

A cryptanalysis aim is to be break an encipherment i.e. he attempts to recover the original meaning of scramble text[8]. A cryptanalyst can try any one among the six different ways. (i) he can break a single message by recovering the normal text from scramble text. (ii) he can break subsequent messages by recognizing the patterns in scramble text of the enciphered messages. (iii) guess some meaning by noticing some unusual frequency communication. (iv) he can detect the antiphon key to break the subsequent messages easily. (v) he can find the weak point in the encipherment algorithm (vi) he can find general weakness in the environment of use of encipherment.

An cryptanalyst works with several forms of information such as, enciphered messages, known encipherment algorithms, intercepted normal text, data items known or guessed to be in scramble text message, mathematical tools, statistical techniques, properties of languages and luck. Each piece of information can give them some clue[9]. They will assemble the clues and try to figure out the meaning of the message in the context of how the encipherment is done. An intruder need not follow any rules, their ultimate aim is to find out the meaning of the message.

Any encipherment algorithm is breakable when enough data and time are given. The two simple forms of encipherment are substitution in which one alphabet is replaced in by another alphabet and transpositions, in which the position of the alphabets are altered[10].

4. Discussion on substitution ciphers

It is the very basic form of devising "secret codes" in which a table is formed to substitute each letter in the original message. This technique is termed as mono alphabetic substitution cipher or simple substitution. Caesar cipher is the first substitution cipher used, it is a keyless cipher.

4.1. Caesar cipher

Julius Caesar has used the substitution technique which is named after him. In this technique each letter is replaced by a letter after 3 places in the alphabet list. So the normal text in was enciphered as scramble text is by applying the rule, si=E(ni)=ni+3. The full translation chart of Caesar cipher contains 26 English alphabets and its corresponding replaceable letter with a shift of 3.

Table 2. Caesar Cipher translation table

A	B	C	D	E	F	G	H	I
d	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**
J	K	L	M	N	O	P	Q	R
m	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**
S	T	U	V	W	X	Y	Z	
v	**w**	**x**	**y**	**z**	**a**	**b**	**c**	

Using this encipherment scheme given in the Table 2. the message,
MEET AT FORT BY FIVE PM
can be enciphered as
phhw dw iruw eb ilyh sp

5. Cryptanalysis of Caesar cipher

A cryptanalyst will look for the available clues in the scramble text. The following clues can be guessed by the cryptanalyst from the above Caesar cipher, (i) The break between the two words are preserved, hence the cryptanalyst can guess that the message had 6 words among that first, Third and fifth words are 4 letter words, second, fourth and sixty words are 2 letter words. (ii) The double letters are preserved EE is translated into HH. (iii) cryptanalyst made the next guess with repeated letters, when a letter is repeated, it again maps into the same scramble text always.

W & H are repeated for 3 times, P & i are repeated for 2 times. Using the above said clues the cryptanalyst can break the cipher. One way to attack this scheme is to substitute known 2 letter words at appropriate places such as am, is , to, be, he, we, at, of, by, do. Once the small words sit into its place then the analyst try to substitute matching letters for other places in the scrambled text. Then there is strong clue is the scramble text, the first word contains four letters among which middle two letters are double letters hh. Now the common guess for this pattern is week, book, root, seed, meet. Since the fourth letter is guessed as T, then the list of words becomes short.

---T AT ---T -- ---- --

By placing one by one MEET can be found.

MEET AT --- T -- ---E -M

Then the next guess can starts with four letter words ends in T such as sort, neat, part, fort, cart, suit, beat, gift. Since the first two words are MEET AT then the third word will be a place. By short listing it can be found as FORT.

MEET AT FORT -- F -- E - M

The fifty word contains 4 letters which starts with F and ends with E can have the possible guesses as fire, fine, five, After observing the previous assumptions, the valid choice will be FIVE.

MEET AT FORT -- FIVE -M

By now, it can be easily noticed that the uncovered letters are 3 positions apart from their normal text. Remaining letters can be easily found since the encipherment rule is broken.

MEET AT FORT BY FIVE PM

The Cryptanalysis described here is based on guess and assumption. But based on methodological approach such as which letters commonly start words, end words and which are common prefixed and common suffixes.

6. Conclusion

The most important challenge in the networks is protecting the sensitive data. A strong tool for protecting sensitive data is using encryption algorithms. Several encryption algorithms either symmetric or asymmetric is available today. From which algorithm can be chosen individually, two or more algorithms can be combined, a new encryption algorithm can be created, existing algorithm can be revised. Not only the encryption algorithms is important, key generation and management is also to be done efficiently for successful results. Once a better cryptography approach along with good key management concepts is created then data sharing in networks can be done effectively without any security fraught. In order to do this, the cryptanalysis is done in this paper for the Caesar cipher with an example data.

7. References

1. S.H. Weingart, S.R. White, Arnold, G.P. Double. An evaluation system for the physical security of computing systems. Computer Security Applications Conference, IEEE, 1990, 232-243.
2. Reza Amiri, Marjan kuchaki Rafsanjani, Ehsan khosravi. Black hole attacks detection by invalid IP addresses in mobile AdHoc networks. *Indian Journal of Science & Technology*. 2014; 7(4), 401-408.
3. Judith M. Myerson. Identifying enterprise network vulnerabilities. *International Journal of Network Management*. 2002; 12(3), 135-144.
4. K. Gupta, V. Gupta. Security threats in sensor network and their possible solutions. Instrumentation & Measurement, Sensor Network and Automation (IMSNA), 2012 International Symposium on, IEEE. 2012; 1, 11-13.
5. Aman kumar, Sudesh jakhar, Sunil Makkar. Distinction between secret key and public key cryptography with existing glitches. *Indian Journal of Education and Information Management*. 2012; 1(9), 392-395.
6. Marcus K. Rogersa, Kathryn Seigfriedb, Kirti Tidkea. Self-reported computer criminal behaviour: A psychological analysis. *Elsevier Ltd*. 2006; 3, 116-120.
7. Richard C. Hollinger. Hackers: Heroes of the Computer Revolution?. *Computers and Society*. 1991; 21(1), 6-17.
8. Kristopher Daley, Ryan Larson, Jerald Dawkins. A Structural Framework for Modelling Multi-Stage Network Attacks. Proceedings of the International Conference on Parallel Processing Workshops (ICPPW'02). USA. 2002, 5-10.
9. Seyedhossein Mohtasebi, Ali Dehghantanha. A Mitigation Approach to the Privacy and Malware Threats of Social Network Services. Digital Information Processing and Communications, Communications in Computer and Information Science. 2011; 189, 448-459.
10. Niv Ahituv, Yeheskel Lapid, Seev Neumann. Processing Encrypted Data, Communications of the ACM. 1987; 30(9), 777-780.

The Publication fee is defrayed by Indian Society for Education and Environment (iSee). www.iseeadyar.org

Cite this article as:

M. Janaki, Dr.M.Ganaga Durga. Preserving sensitive data shared through the network against security threats using cryptography. Indian Journal of Education and Information Management. Vol 4 (1), October 2015.