Volume 3, Issue 5, May 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Enciphering Data for Larger Files

Anju
M.Tech. CSE ,
Hindu College of Engineering,Sonepat
Haryana, India

Ms. Ayushi Aggarwal
Assistant Professor,
Hindu College of Engineering,Sonepat
Haryana, India

Abstract: This paper introduces Encryption and Decryption in terms of Cryptography Techniques. Cryptography is "The science of protecting data" & Network Security "keeping information private and Secure from unauthorized Users".This paper gives the Fundamental Requirements for the Data Transmission, the security attacks like Interruption, Interception and Modification of the data Transmission. The Cryptographic Process explaining through a generalized function is discussed through which encryption and decryption is done by the algorithm to encipher and decipher the data for a word/line[11].The computational time of the algorithm hava a major impact on the determining the efficiency of the algorithm.In this paper,a symmetric key algorithm is proposed for larger amount of data.

Keywords: Encryption,Decryption,Security,Symmetric and secret key Cryptography,Cryptanalysis,Data for encryption and decryption,caeser cipher.

I. INTRODUCTION

The Cryptanalysis is the process of attempting to discover the plain text and/ or the key.
Why & How to Provide Network Security in the Certificates issuing,The Validity & Trust for Certificate Services, Certificate Revocation in the Internet,Intranet and other Network Communications, the Applications of Network Security to the various Data Transfer techniques and protocols.[6][9] From the dawn of civilization, to the highly networked societies that we live in Today communication has always been an integral part of our existence.

- Radio communication
- Network communication
- Mobile communication
- Telephonic communication

All these methods and means of communication have played an important role in our lives, but in the past few years, network communication, especially over the Internet, has emerged as one of the most powerful Methods of communication with an overwhelming Impact on our lives. Such rapid advances in Communications technology have also given rise to Security threats to individuals and organizations. Cryptography "hidden, secret" is the study of techniques for secure communication in the presence of third parties, it is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security such asdata confidentiality, data integrity, authentication, and non-repudiation.

II. FUNDAMENTAL REQUIREMENTS

Confidential: Is the process of keeping information private and Secret so that only the intended recipient is able to understand the information.
Authentication: Is the process of providing proof of identity of the sender to the recipient, so that the recipient can be assured that the person sending the information is who and what he or she claims to be.
Integrity: Is the method to ensure that information is not tampered with during its transit or its storage on the network. Any unauthorized person should not be able to tamper with the information or change the Information during transit.
Non-repudiation: Is the method to ensure that information cannot be disowned.Once the non repudiation process is in place, the sender cannot deny being the originator of the data.

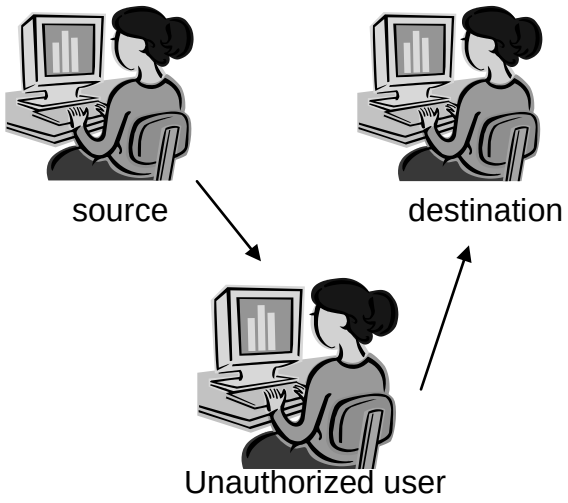


Fig. 1 (Interruption by an unauthorized user)

III. SECURITY ATTACKS

Interruption: In an attack where one or more of the systems of the organization become unusable due to attacks by unauthorized users[6][7]. This leads to systems being unavailable for use.

Interception: An unauthorized individual intercepts the message content and changes it or uses it for malicious purposes. After this type of attack[5], the message does not remain confidential.

Modification: The content of the message is modified by a third party. This attack affects the integrity of the message. So for maintaining the data secretly while communicating data between two persons or two organizations data is to be converted to other format and the data is to be transmitted[5][Fig. 1]. So now we deal with the Cryptography which is process of transmitting data securely without any interruption. Network security is the security of data transmission in the communication.

Fig. 2 (Symmetric key cryptography)

IV. WHAT IS CRYPTOGRAPHY ?

The term cryptology has its origin in Greek Kryptós lógos , which means "hidden word." Cryptography is the science of protecting data, which provides means and methods of converting data into unreadable form, so that Valid User can access Information at the Destination. Cryptography is the science of using mathematics to encrypt and decrypt data[Fig. 2]. Cryptography enables you to store sensitive information or transmit it across insecure networks(like the Internet) so that it cannot be read by anyone except the intended recipient. While cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking secure communication[1][4]. Cryptanalysts are also called attackers. Cryptology embraces both cryptography and cryptanalysis.

V. CAESER CIPHER

Caesar cipher-Replace each letter *l* with *l* +3 mod 26
Encryption formula: (x+n)mod 26
Decryption formula: (x-n)mod 26
x=text data,n=key specified;
For e.g."Attack at dawn" becomes Dwwdfn dw gdzq
It includes two components:

- Algorithm: Shift characters by a fixed amount

- Key:the fixed amount

VI. WEAKNESSES OF CAESER CIPHER

- Word structure is preserved-Break message into equal-length blocks.
  -dww dfn dwg dzq
- Letter frequency is a big clue
  -e,t,a,o most common English letters.
  -Using a single key preserves frequency.
- Solution: use multiple keys
  - E.g. shift by (3,5,7)
  - "Attack at dawn" becomes dya dhr dyk dbu

Better, but frequency information still present.An attacker that knows the block size can separate out characters encoded with different keys[3].The Caesar cipher is still useful as a way to prevent people from unintentionally reading something. **Fundamental problem**: key length is shorter than the message.

VII. CRYPTOGRAPHIC BASIC PROCESS

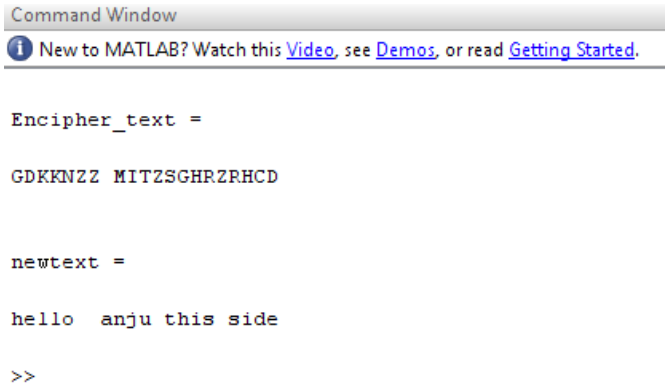
M is the original message
K enc is encryption key
M' is the scrambled message
K dec is decryption key
It is "difficult" to get M just by knowing M'
E and D are related such that
E(K enc , M) = M'
D(K dec , M') = M
D(K dec , E(K enc , M)) = M
Plaintext—M Cipher text—M' Original
Plaintext—M
Decryption function—D Encryption
function—E
So how does cryptographic process work?
The idea is rather simple. Let's say you have plaintext M. By providing the encryption key and the encryption function you get cipher text, M'. The cipher text can be decrypted using a decryption function and a decryption key and the result is the original text[2]. In cryptographic process the mathematical property is such that it is practically impossible to derive M from M' unless the key is known.

VIII. ALGORITHM FOR ENCIPHERING THE DATA FOR LARGER FILES

- Declaration of parameters i.e. size of square matrix.
- Creation of a square matrix of 27x27 with 27 shifted substitution alphabets
  1 2 3 4 5 ... 26 27
  2 3 4 5 6 ... 27 1
  3 4 5 6 7 ... 1 2
  .....
- Calling of text file from which text is to be ciphered.
- Removal of spaces from the text so as to make a string of alphabet.
- Conversion of string into lower case.
- Generation of key for suitable enciphering and deciphering.
- Conversion of text into decimal values.
- Addition and subtraction of some constant values from decimal values.
- Substitution of negative values with key in decimal vector.
- Generation of key index i.e. 1 for each element of decimal vector.
- Subtraction of a particular decimal value from each element of decimal vector according to that square matrix.
- Again addition and subtraction of some constants from last updated decimal vector.
- Getting of Enciphered text.
- Conversion of text into decimal values again.
- Addition of those constants which were subtracted from the decimal vector.
- Subtraction of those constants which were added into the decimal vector.

- Convert the decimal index back to a letter to determine the deciphered character.
- Addition of spaces at correct place.
- Conversion of alphabet into lower case.
- Getting of deciphered text.

For e.g.-If we take the text "hello anju this side" then after the execution the matlab code for the described algorithm enciphered text and deciphered text becomes:



Running implementation of the algorithm in matlab

IX. PROGRAMMING ENVIRONMENT:

MATLAB 7.6.0.324(R2008a) included in the algorithm.**MATLAB** (**mat**rix **lab**oratory)included is a numerical computing environment and fourth generation programming language developed by Mathworks,MATLAB allows matrix manipulations, plotting of functions and data, implementation of algorithms[3], creation of user interfaces, and interfacing with programs written in other languages, including C,C++,JAVA,Fortran. In 2004, MATLAB had around one million users across industry and academia.MATLAB users come from various backgrounds of engineering, science, and economics. MATLAB is widely used in academic and research institutions as well as industrial enterprises. The MATLAB application is built around the MATLAB language, and most use of MATLAB involves typing MATLAB code into the Command Window (as an interactive mathematical shell), or executing text files containing MATLAB code and functions.

X. KEY PROCESS TECHNIQUES

- **Symmetric-Key Encryption: One Key**

Symmetric-key encryption, also called shared-key encryption or **secret-key cryptography**, uses a single key that both the sender and recipient possess[2].
This key, used for both encryption and decryption, is
called a secret key (also referred to as a symmetric key or session key). Symmetric-key encryption is an efficient method for encrypting large amounts of data.But the drawback is to transfer the Key to Receiver as it is prone to security risks.

- **Public-Key Encryption: Two Keys**

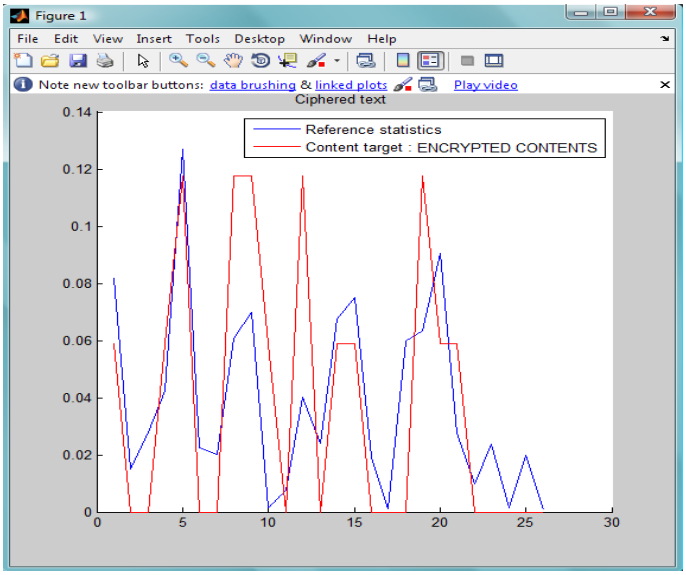
Two keys—a public key and a private key, which are mathematically related—are used in public-key encryption.To contrast it with symmetric-key encryption, public-key encryption is also sometimes
called asymmetric-key encryption. In public-key encryption, the public key can be passed openly between the parties or published in a public repository, but the related private key remains private[8].
Data encrypted with the public key can be decrypted
only using the private key. Data encrypted with the private key can be decrypted only using the public key. In Figure 1, a sender has the receiver's public key and uses it to encrypt a message, but only the receiver has the related private key used to decrypt the message.

XI. APPLICATIONS OF CRYPTOGRAPHY

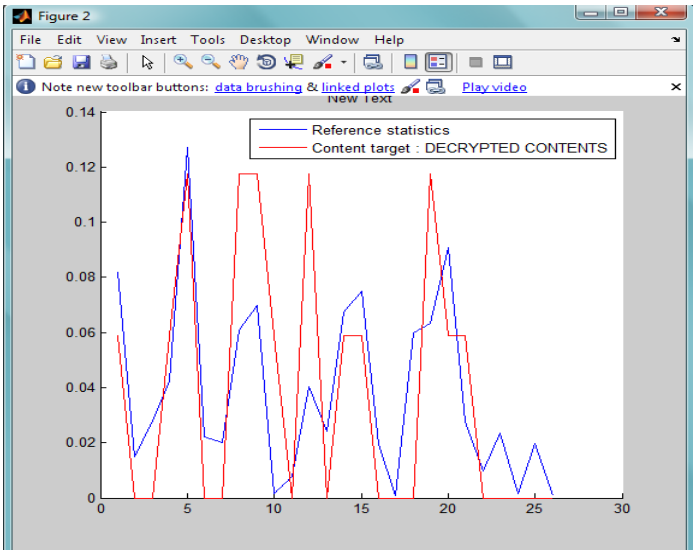
- Defense Services
- Secure Data Manipulation
- E –Commerce
- Business Transactions
- Internet Payment Systems

- Pass Phrasing
- Secure Internet Comm.
- User Identification Systems
- Access Control
- Computational Security
- Secure access to Corp Data
- Data Security.

Result performed for ENCRYPTION



Result performed for DECRYPTION



The both graphs results the non-repudiation(sending and the receiving data is same),confidentiality,security of the data by the symmetric key cryptography. Hence,curve of encrypted data and the decrypted data is same i.e. there is no lose of data in the middle and receiver found exactly the same data sent by the sender.

XII. CONCLUSION

Cryptography protects[1] users by providing functionality for the encryption of data and authentication of other users. This technology lets the receiver of an electronic message verify the sender, ensures that a message can be read only by the intended person, and assures the recipient that a message has not be altered in transit.This paper describes the cryptographic

concepts of symmetric key encryption and key exchange[10][11]. Cryptography is a particularly interesting field because of the amount of work that is, by necessity, done in secret. The irony is that today, secrecy is not the key to the goodness of a cryptographic algorithm.Regardless of the mathematical theory behind an algorithm, the best algorithms are those that are well known and well-documented because they are also well-tested and well-studied! In fact, time is the only true test of good cryptography; any cryptographic scheme that stays in use year after year is most likely a good one. The strength of cryptography lies in the choice (and management) of the keys; longer keys will resist attack better than shorter keys.

REFERENCES:

[1] Cryptography and Network Security –By William Stallings,fifth edition.
[2] Introduction to Cryptography –By Aysel Ozgur
[3] www.en.wikipedia.org.
[4] Dhanraj, C. Nandini, and Mohd. Tajuddin "An Enhanced Approach for Secret Key Algorithm based on Data Encryption Standard" International Journal of Research and Reviews in Computer Science (IJRRCS) Vol. 2, No. 4, August 2011
[5] Simmonds, A; Sandilands, P; van Ekert, L (2004) Ontology for Network Security Attacks". Lecture Notes in Computer Science. Lecture Notes in Computer Science 3285
[6] A Role-Based Trusted Network Provides Pervasive Security and Compliance - interview with Jayshree Ullal, senior VP of Cisco.
[7] YanWang, Ming Hu,Timing Evaluation of known cryptographic Algorithm,International Conference on Computational Intelligence and security, 2009.
[8] William stallings,Cryptography and Network Security:Principles & Practices‖, second edition
[9] Suyash Verma, Rajnish Choubey, Roopali soni "An Efficient Developed New Symmetric Key Cryptography Algorithm for Information Security" International Journal of Emerging Technology and Advanced Engineering Volume 2, Issue 7, July 2012
[10] AndrewS.Tanenbaum,"Computer Networks" forth edition,2004.
[11] Sarker,M.Z.H.,Parvez,and M.S., "A Cost Effective Symmetric Key Cryptographic Algorithm for Small Amount of Data" IEEE International Conference,2005,pp. 1-6

Anju received the B.Tech. degree(2007-11)from B.M.I.E.T,Sonepat affiliated by Maharishi Dayanand Univ.,Rohtak and pursuing M.Tech.(2011-13), from Hindu College of Engg.,Sonepat affiliated by Deenbandhu ChotuRam Univ. of Science and Tech.,Murthal(Sonepat).Her research interest includes security,cryptography and their applications.She is a member of IAENG(International Association of Engineers).

Ms. Ayushi Aggarwal received the B.Tech. degree(2003-07) from B.M.I.E.T,Sonepat affiliated by Maharishi Dayanand Univ.,Rohtak and M.Tech. degree(2008-11) from GuruGobind Singh Indraprastha Univ.,Delhi. Now,She is an assistant professor in the Dept. of Computer Science and Engg. at Hindu College of Engg.,Sonepat,Her research interest includes Information Security and Technologies and her research papers has been published in many free and paid international journals. She is a member of CSI(Computer Society of India).

