INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

TEXT ENCRYPTION USING CRYPTOGRAPHIC ALGORITHM

MR. PARAG S. DESHMUKH[1], Dr. H. R. DESHMUKH[2], R. G. ANANTWAR[3], R. N. GADBAIL[3]

1. M. E. First Year, Department of Computer Science & Engineering, IBSS College of Engineering, Amravati.
2. Prof and HOD, Department of Computer Science & Engineering, IBSS College of Engineering, Amravati.
3. Asst. Prof, Department of Computer Science & Engineering, IBSS College of Engineering, Amravati.

Accepted Date: 27/02/2014 ; Published Date: 01/05/2014

Abstract: This paper describes implementation of Data Encryption Standard (DES) Algorithm. The DES is Symmetric key algorithm which is the quickest and most commonly used type of encryption. Here, a single key is used for both encryption and decryption. Cryptography is a technique of encrypting and decrypting the message so as to maintain the confidentiality of the data. The usage of cryptography is not new in the digital world. Julius Caesar used Cryptography and gave the world "Caesar Cipher ".For effective, we chop – off the message into small chunks and then encrypt the messages by an encrypting algorithm and are sent via a communication medium to the receiver's side. Further, he receiver side decrypts the message by using the counterpart of the encryption algorithm and receives the message. But at times the messages get hacked by an intruder during the communication phase or by an attacker challenging the encryption algorithm. Based on attacks, the algorithms and techniques are always changed and a new and more secure and sophisticated cryptographic algorithm are sought after. It has been observed that most of the time either the adversary ruptures the connection to get message or attacks the algorithm. For secret key communication, the two users who wish to establish communication should meet to exchange key or either use a secure courier service, both of which is absolutely impractical. One essential aspect for secure communications or securing data is that of cryptography

Keywords: Authentication, Asymmetric Key, Confidentiality, Data integrity, Symmetric Key.

PAPER-QR CODE

Corresponding Author: MR. PARAG S. DESHMUKH

Access Online On:

www.ijpret.com

How to Cite This Article:

Parag Deshmukh, IJPRET, 2014; Volume 2 (9): 974-979

INTRODUCTION

Cryptography is the art of achieving security by encoding messages to make them non-readable. Cryptography is the practice and study of hiding information. In modern times cryptography is considered a branch of both mathematics and computer science and is affiliated closely with information theory, computer security and engineering. Cryptography is used in applications present in technologically advanced societies; examples include the security of ATM cards, computer passwords and electronic commerce, which all depend on cryptography. There are two basic types of cryptography: Symmetric Key and Asymmetric Key. Symmetric key algorithms are the quickest and most commonly used type of encryption. Here, a single key is used for both encryption and decryption. There are few well-known symmetric key algorithms i.e. DES, RC2, RC4, IDEA etc. Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks 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. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck. Cryptanalysts are also called attackers. Cryptology embraces both cryptography and cryptanalysis. A cryptographic algorithm, or cipher, is a mathematical function used in the encryption and decryption process. A cryptographic algorithm works in combination with a key—a word, number, or phrase—to encrypt the plaintext. The same plaintext encrypts to different cipher-text with different keys. The security of encrypted data is entirely dependent on two things: the strength of the cryptographic algorithm and the secrecy of the key. A cryptographic algorithm, plus all possible keys and all the protocols that make it work comprise a cryptosystem. "Cryptography" derives from the Greek word kruptos, meaning "hidden". The key to hiding data is to devise a hiding mechanism that is very difficult to reverse without using the decryption key [3].

CRYPTOGRAPHY

Data that can be read and understood without any special measures is called plaintext or clear text. The method of disguising plaintext in such a way as to hide its substance is called encryption. Encrypting plaintext results in unreadable gibberish called cipher text. The process of reverting cipher-text to its original plaintext is called decryption. There are many aspects to security and many applications, ranging from secure commerce and payments to private communications and protecting passwords. Cryptography is used to achieve the following goals:

Confidentiality

To ensure data remains private. Confidentiality is usually achieved using encryption. Encryption algorithms are used to convert plain text into cipher-text and the equivalent decryption algorithm is used to convert the cipher text back to plain text. Symmetric encryption algorithms use the same key for encryption and decryption, while asymmetric algorithms use a public/private key pair.

Data Integrity

To ensure data is protected from accidental or deliberate (malicious) modification. Integrity is usually provided by message authentication code or hashes. A hash value is a fixed length numeric value derived from a sequence of data. Hash values are used to verify the integrity of data sent through insecure channels. The hash value of received data is compared to the hash value of the data as it was sent to determine if the data was altered.

Authentication

To assure that data originates from a particular party digital certificates are used to provide authentication. Digital signatures are usually applied to hash values as these are significantly smaller than the source data that they represent.

TYPES OF CRYPTOGRAPHY

Cryptography is a process which is associated with scrambling plaintext into cipher-text (a process called encryption), then back again (known as decryption). There are several ways to classify the various algorithms. The most common types are Secret Key Cryptography which is also known as Symmetric Key Cryptography and Public Key Cryptography which is also known as Asymmetric Key Cryptography. In other words, if the same key is used for encryption and decryption, we call the mechanism as Symmetric key cryptography. However, if two different keys are used in a cryptographic mechanism, where one key is used for encryption, and another, different key is used for decryption; we call the mechanism as Asymmetric key cryptography. This is shown in Figure 1

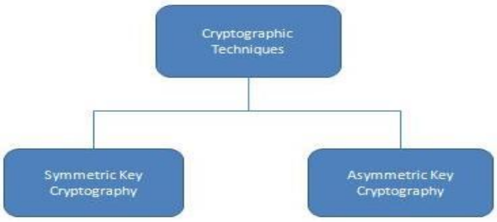


Figure 1: Cryptographic techniques

Symmetric Key Cryptography

In Symmetric key cryptography, a single key is used for both encryption and decryption. As shown in Figure 2, the sender uses the key to encrypt the plaintext and sends the cipher-text to the receiver. The receiver applies the same key to decrypt the message and recover the plaintext. Because a single key is used for both functions, secret key cryptography is also called symmetric encryption. With this form of cryptography, it is obvious that the key must be known to both the sender and the receiver; that, in fact, is the secret. The biggest difficulty with this approach, of course, is the distribution of the key [6].

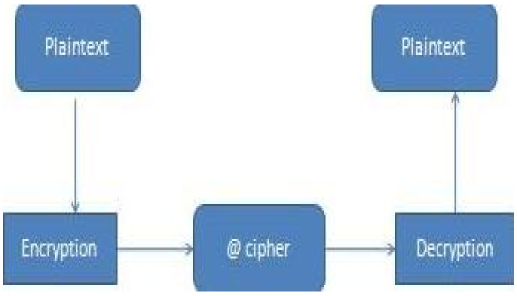


Figure 2: Symmetric Key Cryptography

Asymmetric Key Cryptography

Public or asymmetric key cryptography involves the use of key pairs: one private key and one public key. Both are required to encrypt and decrypt a message or transmission. The private key, not to be confused with the key utilized in private key cryptography, is just that, private. The owner of the key is responsible for securing it in such a manner that it will not be lost or compromised. On the other hand, the public key is just that, public. Public key cryptography intends for public keys to be accessible to all users. In fact, this is what makes the system strong. If a person can access anyone public key easily, usually via some form of directory service, then the two parties can communicate securely and with little effort. Figure 3 describes the Public Key Cryptography [4].

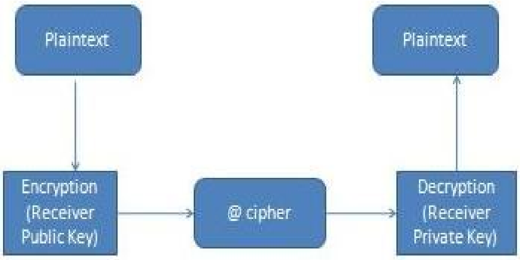

Plaintext
Plaintext
Encryption (Receiver Public Key)
@ cipher
Decryption (Receiver Private Key)

Figure 3: Asymmetric Key Cryptography

DES ALGORITHM

DES is Symmetric key encryption standard encodes plaintext in 64-bit chunks using a 64-bit key. Actually, 8-bit of these 64-bits are odd parity bits, so the DES key effectively 56-bit long.

The operations of DES are as follows:

- The DES consists of two computation steps (the first and last steps of the algorithm) in which all 64-bits are permuted and 16 identical rounds of operations in between.
- The operation of each round is identical, taking the output of previous round as output. During each round, the rightmost 32-bits of the input are moved to left 32-bits of output.
- The entire 64-bit input to the i-th round and 48-bit key for the i-th round (derived from the larger DES 56-bit long) are taken as input.
- This input is given to a function that involves expansion of four bit input chunks into six bit chunks, exclusive OR-ing with the expanded six bit chunks of the 48-bit key Ki, a substitution operation and further exclusive OR-ing with the leftmost 32-bits of the input.
- The resulting 32-bit output of the function is then used as the rightmost 32-bits of rounds 64-bit output, as shown in Figure 4.
- Decryption works by reversing the algorithm’s operations.

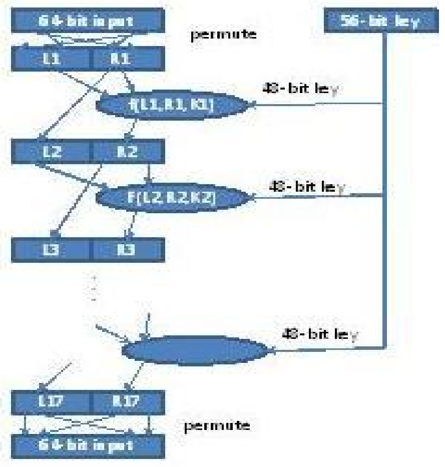
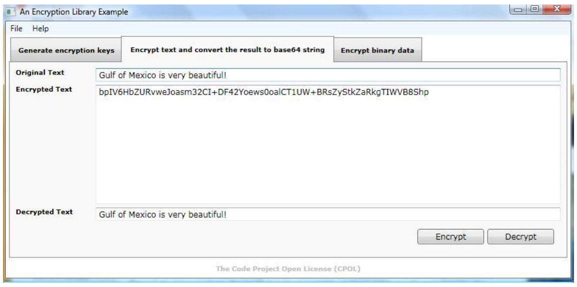


Figure 4: Basic operation of DES

RESULT

An example of encryption and decryption of data by using Data Encryption Standard (DES) Algorithm is shown in Figure 5.


An Encryption Library Example
File
Help
Generate encryption keys
Encrypt text and convert the result to base64 string
Encrypt binary data
Encrypt
Decrypt
The Code Project Open License (CPOL)

Original Text: Gulf of Mexico is very beautiful!

Encrypted Text: bpIV6HbZURvweJoasm32CI+DF42Yoews0oalCT1UW+BRsZyStkZaRkgTIWVB8Shp

Decrypted Text: Gulf of Mexico is very beautiful!

Figure 5: Example of encryption and decryption of data.

CONCLUSION

By this work we can successfully applied the security to the text data of in peer-to-peer communication or server based communication and data stored on server. During work seen that DES completely scramble the data and key so that every bit of the cipher-text depends on every bit of the data and every bit of key with good algorithm, there should no correlation between the cipher-text and either the original data or key. Finally the DES is quick and efficient symmetric key cryptographic algorithm to encrypt and decrypt data.

REFERENCES

1. A Symmetric Key Cryptographic Algorithm, Ayushi, International Journal of Computer Applications (0975 - 8887) Volume 1 – No. 15, 2010.

2. Cryptography and Network, William Stallings, Practice Hall of India.

3. S. William, Cryptography and Network Security: Principles and Practice, 2nd edition, Prentice-Hall, Inc., 1999 pp 23-50.

4. Fundamentals of Computer Security, Springer publications "Basic Cryptographic Algorithms", an article available at www.itsc.state.md.us/old site/info/InternetSecurity/Crypto/CryptoIntro.htm#Algorithms

5. S. Hebert, "A Brief History of Cryptography", an article available at http://cybercrimes.net/index .html.

6. Introduction to Public-Key Cryptography", an article available at developer. netscape.com/docs/manuals/security/pkin/contents.htm.