Secure your data

zainabmk1502@gmail.com

December 2022

1 Abstract

It provides the user a secure medium of communication over the internet, using the technique of Cryptography. The program prevents the intrusion of data from unauthorized sources, thus making it accessible only to the user and the authorized sender. AES Algorithm used in the project adds on its reliability, as it used double encryption. The program provides the user to switch between two encryption modes, 128 and 256-bits encryption.

2 Literature review

Cryptography, is the combined study of mathematical techniques linked with information security, specifically, confidentiality, data security, entity authentication, and message authentication. The roots of cryptography lie in the ancient Roman and Egyptian Civilizations. As civilizations evolved, individuals, got organized, leading to the emergence of power, supremacy, and politics. It made people realize the need for secret communication, which ensured the continuous evolution of cryptography. With the advances in secret communication, government organizations, military units, and private sectors adapted to this method of secure transmission. The arrival of the Internet helped to bring practical cryptography to the common people. It provides a pathway for secure communication that permits only the sender and receiver to access the information, which associates it with encryption. Encryption scrambles the initial text to ciphertext and then back to the primary text. With the rise in the use of ciphering, the complexity of its algorithm also increased gradually, from the very basic to the apex of secure ciphering, the Advanced Encryption Standard (AES) Algorithm. The AES Algorithm follows its particular structure for the encryption and decryption of sensitive data, making it applicable to hardware and software across the planet. There are no records of any cryptanalytic attacks against AES, proving the amount of security it provides. The protection, efficiency, and sustainability promised by AES gives it a high evaluation and make it stand out among all other ciphers

3 Introduction

3.1 Introduction to Cryptography

The Internet plays a vital role in transferring information across the world. Over the years, the fear regarding secure communication over the web has been a matter of concern, because the data can be intruded upon by some malicious user. Thus, various techniques are implemented within the public and personal sectors to guard sensitive information while conveying data from the sender to the receiver Cryptography is one of the notable techniques for the secure transfer of information over the web by using methods like encryption and decryption. It uses mathematical algorithms to design certain mechanisms capable enough to provide fundamental security services. A cipher (or cypher) is an algorithm that performs encryption and decryption in an exceedingly series of steps. Encryption: - It is the method of converting data into ciphertext to safeguard it from any intrusion from unauthorized sources. The encoded data is safe and might only be accessed through a secret key. Decryption: - It contradicts encryption and converts the ciphertext to plaintext. The encoded text is often deciphered to the initial plaintext through a secret key.

3.2 Motivation for work

Cryptography promises Confidentiality, which is the secure transfer of data. Data Integrity detects the alterations made in the original data from some unauthorized sources and authentication ensures the data being claimed by the owner. Modern Cryptography relies on the type of cryptographic key that is being employed to encrypt and decrypt the text. Cryptography is divided into two branches, Asymmetric and Symmetric based on the type of keys they use. Symmetric Cryptography uses the same key for both encryption and decryption whereas, Asymmetric cryptography requires two keys, one of which is public and the other is private, each to encrypt and decrypt the data.

3.3 About the tool and AES Algorithm

3.3.1 Secure your data: tool

This tool is a web-based encryption tool that facilitates the secure transfer of data over the internet, it used the AES method as its base to provide the security of data to the user and prevent the data being accessed by any unauthorized sources. Since, AES has not been cracked yet, it adds on to the reliability of providing a secure pathway for commuting data.

3.3.2 AES Algorithm

Advanced Encryption Algorithm (AES), is a standard algorithm which is a widely accepted symmetric encryption algorithm. AES follows a symmetrical block cipher algorithm that accepts plain text in blocks of 128 bits (as 16 bytes) and converts them to ciphertext using keys of sizes 128, 192, and 256 bits. In the 1990s DES was rendered insecure because of its comparatively small key size of 56-bits. The 3DES/TDES also known as Triple Data Encryption Algorithm was also ineffective against brute force attacks and slowed down the process substantially. The National Institute of Standards and Technology (NIST) demanded an algorithm efficient in both software in hardware implementations, contradictory to this DES was only practical in hardware implementation which led to the replacement of DES with AES. AES data encryption is a cryptographic algorithm with mathematical efficiency and exponentially stronger key lengths than that of DES. It is based on the Substitution Permutation network (SP Network), consisting of a list of linked operations that involve the substitution of certain inputs with specific outputs and bit shuffling (permutation) as well.

3.4 Problem Statement

Our aim is to protect the data by encrypting it in either 128 or 256 bit by using AES algorithm on a web server.

3.5 Objective of the work

Our aim is to protect the data by encrypting it in either 128 or 256 bit by using AES algorithm on a web server.

3.6 Organization of the thesis

AES is a symmetric block cipher algorithm with a block/chunk size of 128 bits. It converts these individual blocks using keys of 128, 192, and 256 bits. Once it encrypts these blocks, it joins them together to form the ciphertext. We have made a website consisting of both AES Encryption and Decryption tool with a simple design so that the user finds no difficulty in using it. In our website, firstly there are two options: (i) the user is first asked to enter the text that he or she wants to encrypt or (ii) upload a text file which has the message to be encrypted. After that, the user will be asked to enter the key size, i.e., 128 bit or 256 bits. According to the key size entered it will be decided by the program to run ten or fourteen rounds of encryption to encrypt the text entered by the user. After this the user is asked to enter a secret key which is known only to the user on the receiver's end to decrypt the data as AES algorithm follows an symmetric form of encryption and decryption and uses a common secret key on both ends. Now the final step is to click on the encrypt button and the encrypted text will be generated and shown on the webpage. Now, for the decryption process, the user on the receivers' side will be asked to enter some inputs. Firstly, the user will be asked to enter the encrypted text that was generated by the sender. After that, the user shall be asked to enter the key size of data and it should match to the value which was entered by the sender. Like if the sender entered 128 bit key size for encryption, then the key size should also be 128 bit for decryption else there would be an internal server error and the data will not be decrypted. After entering the key size, the user has to enter the same secret key that was entered by the sender. Here also, if the secret key does not match, there would be an internal server error and the data will not be decrypted. After entering all these inputs, clicking on the decrypt button will decode the encrypted text given by the user and the decrypted message will be shown on the webpage.

4 Related works

Modern-day Cryptography has wide applications, based on the secure communication standards it offers. Some of which are Authentication/ Digital Signatures: - Cryptography is used in authentication and digital signatures for verification of certain information, identity, the origin of the document, or any such information. The use of a hash function and a private signing function provides for this method. Time Stamping: - It clarifies if a certain document or communication existed or checks if it was delivered on time. It is based on the encryption model of the blind signature scheme, to allow the sender to get messages receipted by another party confidentially. Electronic Money: - Blind Signature Scheme of cryptography allows money transactions without revealing the identity of the customer. Encryption is used in electronic money transfer schemes to guard conventional data. End-to-End Encryption: - It employs public key encryption, to truly secure messaging systems. In emails, the public key is stored in the key server tied to our name and the email address can be associated with anyone. OpenPGP and S/MIME are the two kinds of email encryption available. In WhatsApp, the symmetric key cryptographic algorithms and Curve25519-based algorithms are used to ensure integrity and confidentiality.