

SECURE DATA ENCRYPTION

USING CRYPTOGRAPHY

GROUP DETAILS

Department : Computer Science & Engineering

Semester : VII

- 1) KOMOLIKA AGARWAL (18ETCCCS053)
- 2) PIHU JAIN (18ETCCCS071)
- 3) ISHIKA JAIN (18ETCCCS046)

ACKNOWLEDGEMENT

We are very grateful to our teachers and professors who give us a chance to work on this project. We would like to thank him for giving us valuable suggestions and ideas.

We would like to thank our college for providing us all the necessary resources for the project .

ABOUT PROJECT

Digital communication witnesses a noticeable and continuous development in many applications in the Internet. Hence, secure communication sessions must be provided. The security of data transmitted across a global network has turned into a key factor on the network performance measures. So, the confidentiality and the integrity of data are needed to prevent eavesdroppers from accessing and using transmitted data.

So ,We are creating a windows application that is used for converting the plaintext into ciphertext . Application uses the powerful techniques of cryptography.

CRYPTOGRAPHY

Cryptography is a method of protecting information and communication through the use of code , so that only those for whom the information is intended can read and process it.

It secures information & communication from algorithms that are derived from mathematical concepts and set of rule based calculations to transform messages in ways that are harder to decipher. These algorithms are used for cryptographic key generation , confidential communication such as credit card transaction & emails , web browsing on internet , etc.

TYPES OF CRYPTOGRAPHY

- SINGEL KEY OR SYMMETRIC KEY ENCRYPTION
- PUBLIC KEY OR ASYMMETRIC KEY ENCRYPTION

SINGEL KEY OR SYMMETRIC KEY ENCRYPTION

It creates a fixed length of bits known as a block cipher with a secret key that the creator/sender uses to encipher data (encryption) and the receiver uses to decipher it. Examples of this type :

Advanced Encryption Standard (AES) it is successor to the DES and DES3 . It uses longer key length 128 bits, 192 bits , 256 bits to prevent brute force and other attacks. It is established in November 2001 by the National Institute of Standards and Technology(NIST) as a Federal Information Processing Standard(FIPS 197) to protect sensitive information.

PUBLIC KEY OR ASYMMETRIC KEY ENCRYPTION

It uses a pair of keys, a public key associated with the creator/sender for encrypting messages and a private key that only the originator knows (unless it is exposed or they decide to share it) for decrypting that information. Example of this type :

RSA used widely on the internet. The RSA algorithm is named after those who invented it in 1978: Ron Rivest, Adi Shamir, and Leonard Adleman. The RSA algorithm ensures that the keys, are as secure as much possible as can . For this it takes two large prime numbers x and y and multiply them. The two integers are co-prime if the only positive integer that divides them is 1.

OBJECTIVE OF PROJECT

- The purpose of this project is to provide the correct data with security to the users.
- Only the Authorized persons i.e., who are using our application will be there in the Network who can access the data and decrypt the data for their use.
- In Asymmetric algorithm an encryption technique is employed for encrypting a secret message into a Cipher text using the Senders Private Key and receiver public key. The Cipher Text is finally embedded in a suitable cover image and transferred securely to deliver the secret information.

METHODOLOGY OF PROJECT

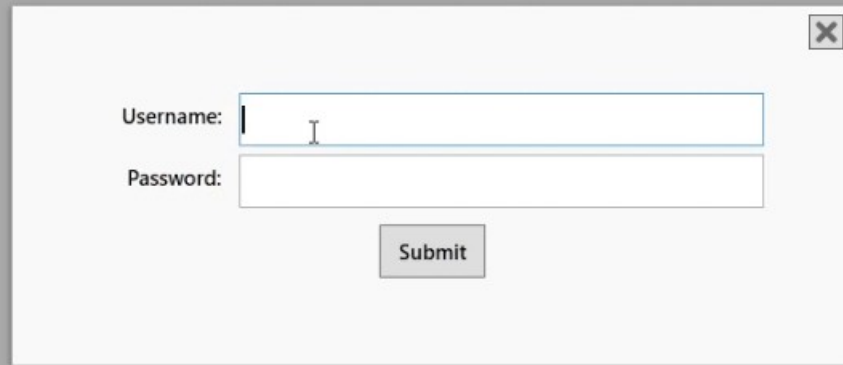
- First the user will register or login on the application.
- On start, the user will be required to choose the method i.e. encryption or decryption
- If the user chooses the method encryption then further the encryption technique option will be given to import the private key and then further select file or folder for AES Encryption..
- If user selects On submit the uploaded file will be encrypted with key and the encryption key will be stored in the database.

METHODOLOGY OF PROJECT

- The encrypted data will be stored in new file created by user and will be saved in user defined location
- If the user chooses decryption the user will be required to provide the key details of the encrypted file.
- Basis of the details the decryption will be performed.
- The decrypted data will be stored in new file created and will be saved in user defined location.

APPLICATION

- It is used for decrypting the logs that are created by various application at runtime .
- It is used to transfer various confidential application data to clients.



A login form is centered on a gray background. The form has a white background and a thin gray border. In the top right corner of the form is a small square button with a black 'X' icon. Below this, the text 'Username:' is followed by a text input field. The cursor is at the end of the field. Below the username field is the text 'Password:' followed by another text input field. At the bottom center of the form is a rectangular button labeled 'Submit'.

Username:

Password:

Submit

Certificate: C:\Users\A [path] \certs\c Choose

Logging in ...



Encryption Flow



Private Key:

Choose

Key Password:

Enter



File:

Choose

Algorithm:

AES-256



Hash:

SHA256



Mode:

OFB

☐

Delete original file

Import



File name: my_text

This is my secret text.

Algorithm: AES-256

Mode: OFB

Hash: SHA256

Save

Cancel

Decryption Flow

Certificate:

Choose

Login

First the user will need
to select the certificate
for the authentication



Folder name:

ne

Enter

PROJECT DEPENDENCIES

- C#
- .NET
- Microsoft Visual Studio
- SQL Server

PROJECT CONCLUSION

- In this project, we deal with the concepts of security of digital data communication across the network.
- By the development of the windows application we got a clear understanding of the various cryptographic techniques used by our network security department.
- We also learned Team Work and Team Management to take our project at an level to succeed.

THANK YOU
