

Data And Application Security

Project Report

Secure File Sharing With Dropbox

Team:

Bhanu Arora	bxa151730
Emy Emmanuel	exe150030

Introduction

Dropbox - Security Concerns

While there are different tools and extensions for securing Dropbox, it doesn't cater to most of the areas of security.

Dropbox encrypts data before uploading it to the cloud or syncing it across devices. But Dropbox owns the keys to unlock this encrypted information. With data and keys in Dropbox's hands, the cloud service could, in theory, read your information, as could successful hackers. This illustrates why data and key separation are an essential element for ensuring robust security.

Dropbox does have encryption on its servers. But as soon as you download a file, it's no longer protected. Dropbox offers server-side encryption, which means data is secure at rest on its servers. But its protection doesn't extend to devices. So if a file is downloaded to a device that doesn't have Dropbox installed, the security protection will break. This means that mobile devices and other access points introduce significant risks.

Although Dropbox's access controls prevent other users from seeing files unless they've been explicitly shared, mistakes are still possible. In this regard, Dropbox's convenience is double-edged. With sharing possible with the click of a button, it's all too easy to make costly mistakes. Users might share sensitive information with the wrong people, a mistake that isn't easy to correct.

Security Problems Addressed

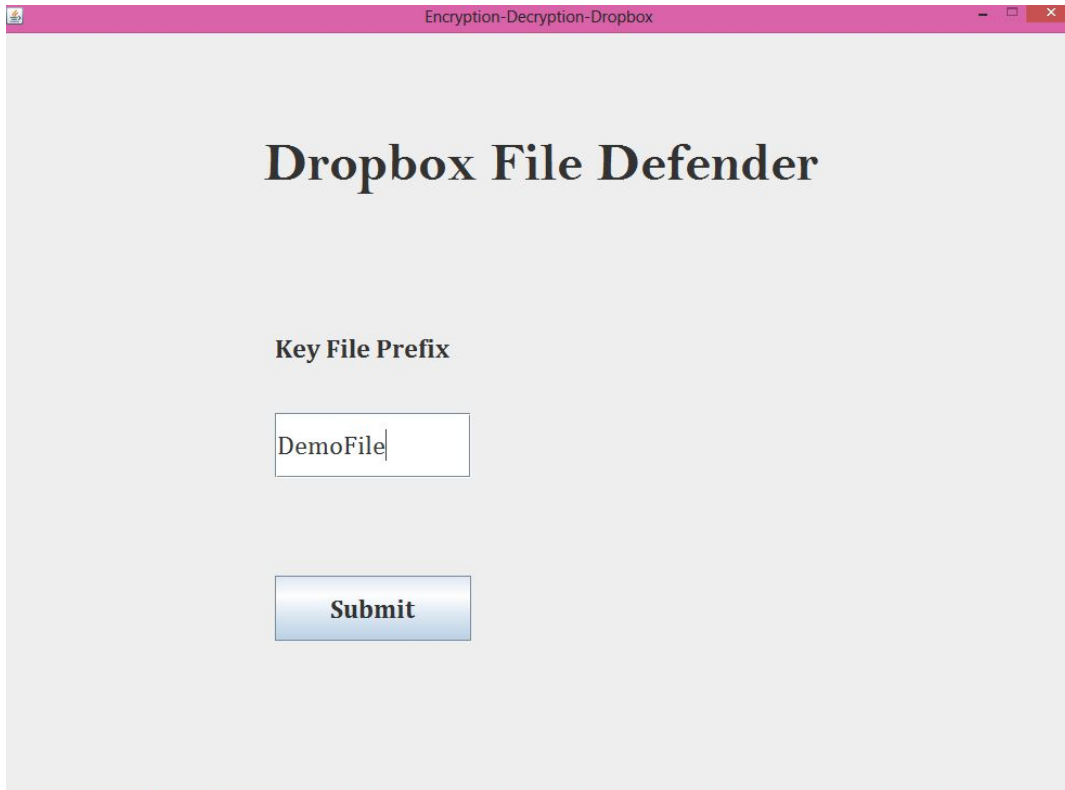
In this application we encrypt files before giving them to Dropbox. This way, even if Dropbox were hacked or your file were leaked, no one except you and your authorized viewers could access it.

Secured sharing of files between two clients using pre shared key and public cryptography is implemented in the project for file sharing among multiple users.

There are two set of keys used in this project. One is a *Master key* which is pre-shared among users who will be sharing files. The second is the *Public and Private Key pair* used to encrypt files before sharing them on dropbox. The encrypted file uploaded using the public key can be decrypted using the private key of the receiver.

Step 1:

Alice enters a unique prefix

The image shows a web application window titled "Encryption-Decryption-Dropbox". The main heading is "Dropbox File Defender". Below this, there is a label "Key File Prefix" followed by a text input field containing the text "DemoFile". Below the input field is a blue "Submit" button.

Encryption-Decryption-Dropbox

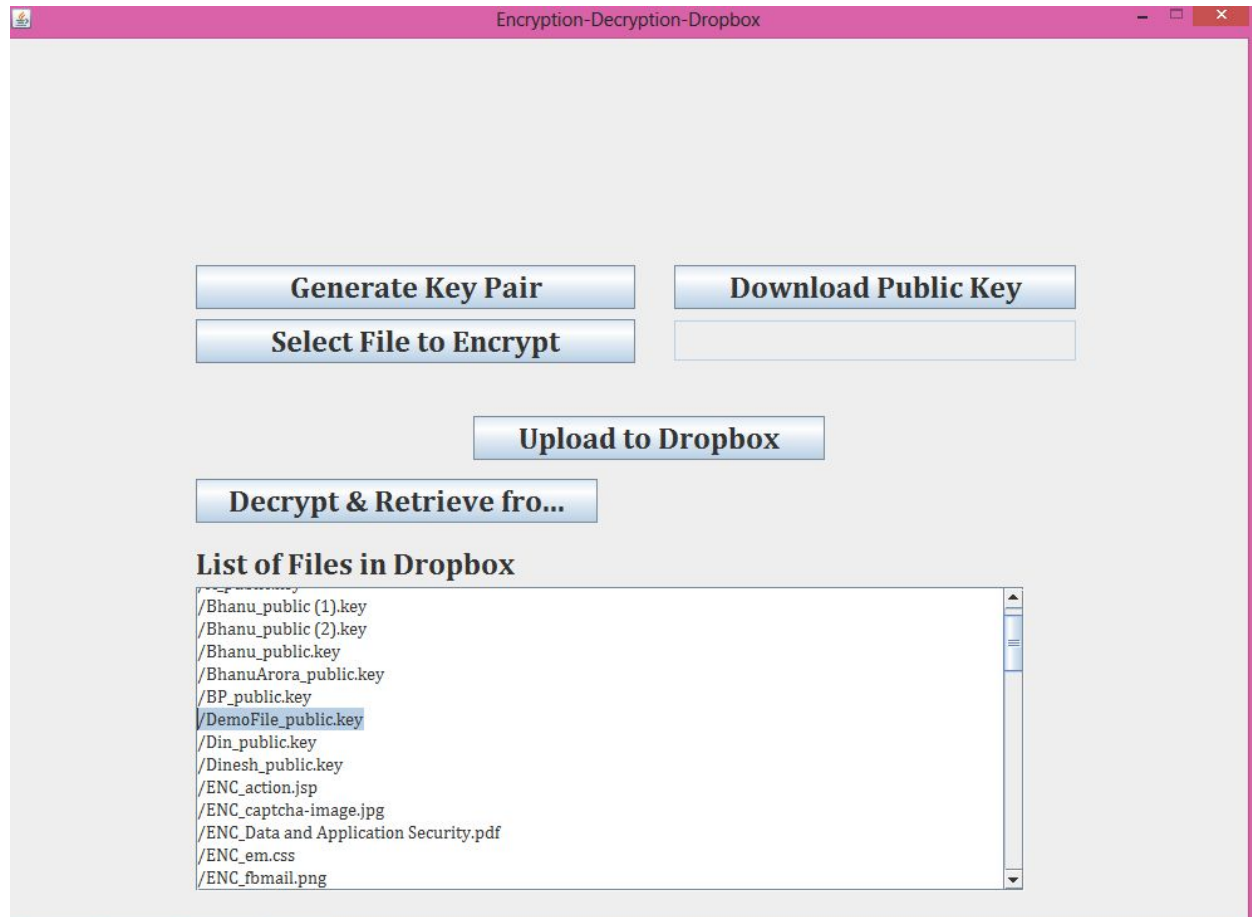
Dropbox File Defender

Key File Prefix

Submit

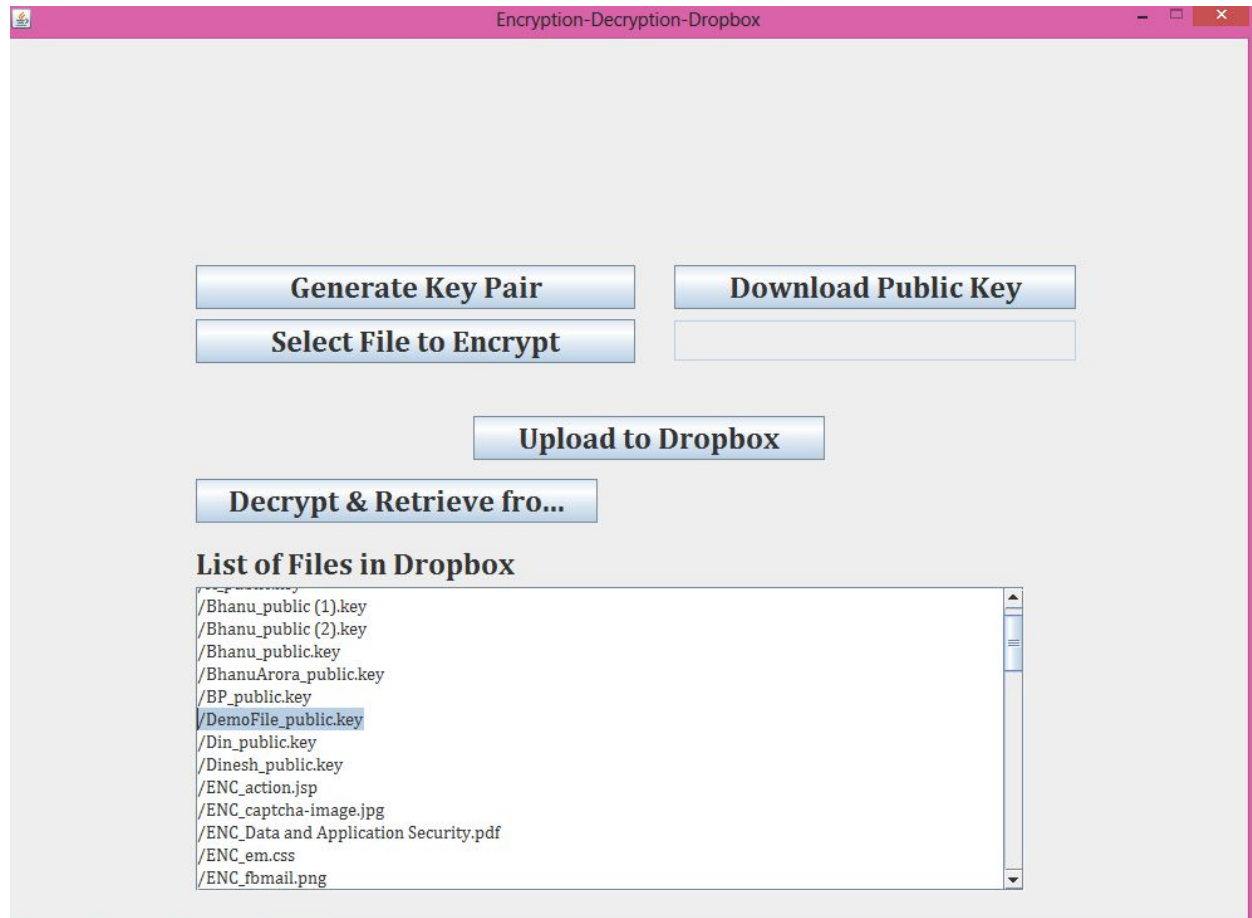
Step 2:

Generate key pair



Step 3:

Two keys generated with file names containing prefix



And public key uploaded on Dropbox which we can see in the above image in the list of files in DropBox.

Step 4:

Alice open the software with same prefix

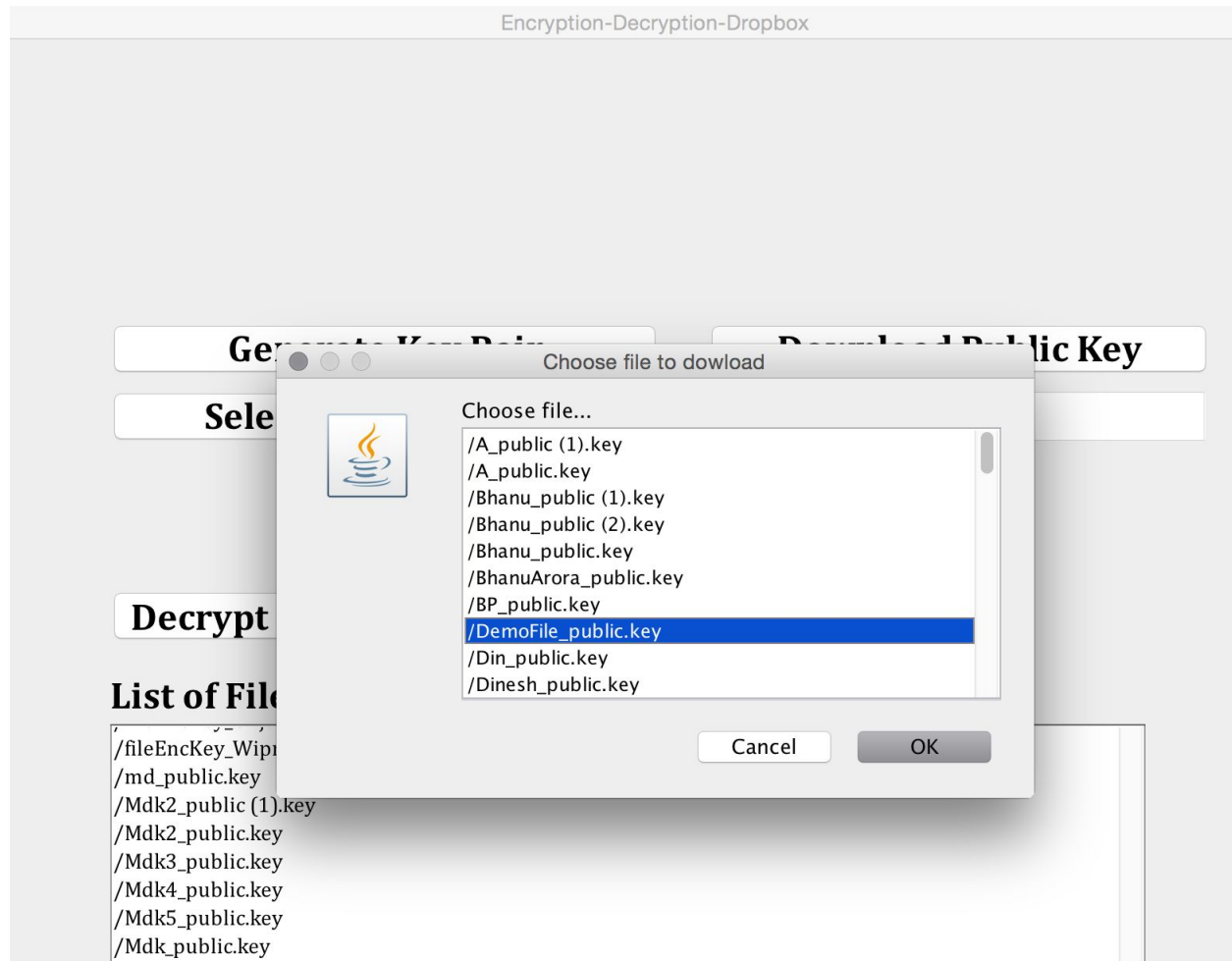
Encryption-Decryption-Dropbox

Dropbox File Defender

Key File Prefix

Step 5:

Click on download public key



Step 6:

Select the public key file from available options

Browse file to send

Click upload

Encryption-Decryption-Dropbox

Generate Key Pair

Download Public Key

Select File to Encrypt

DAS Test.docx

Upload to Dropbox

Decrypt & Retrieve from ...

List of Files in Dropbox

/fileEncKey_Wipro Experience.docx.keycipher

/md_public.key

/Mdk2_public (1).key

/Mdk2_public.key

/Mdk3_public.key

/Mdk4_public.key

/Mdk5_public.key

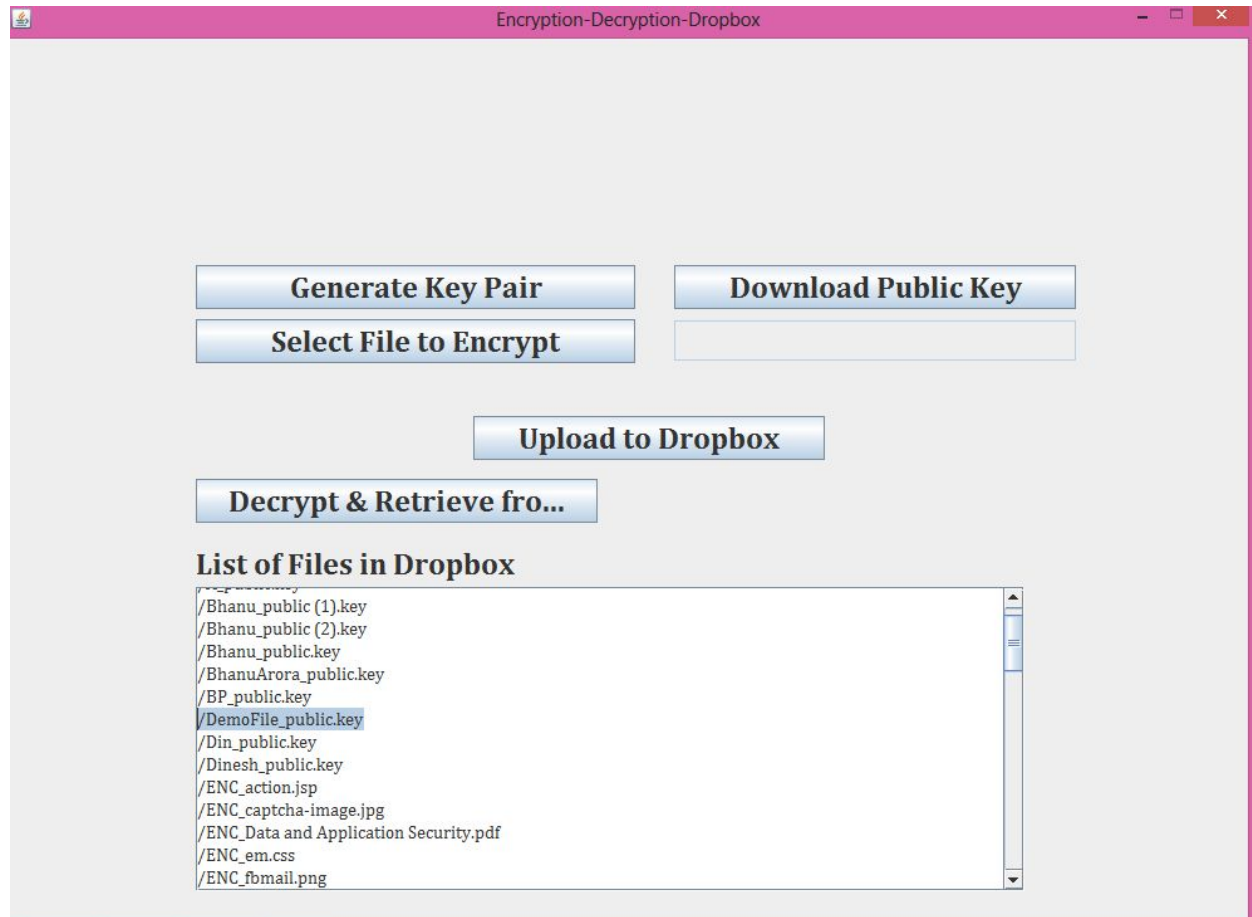
Step 7:

Encrypted file uploaded



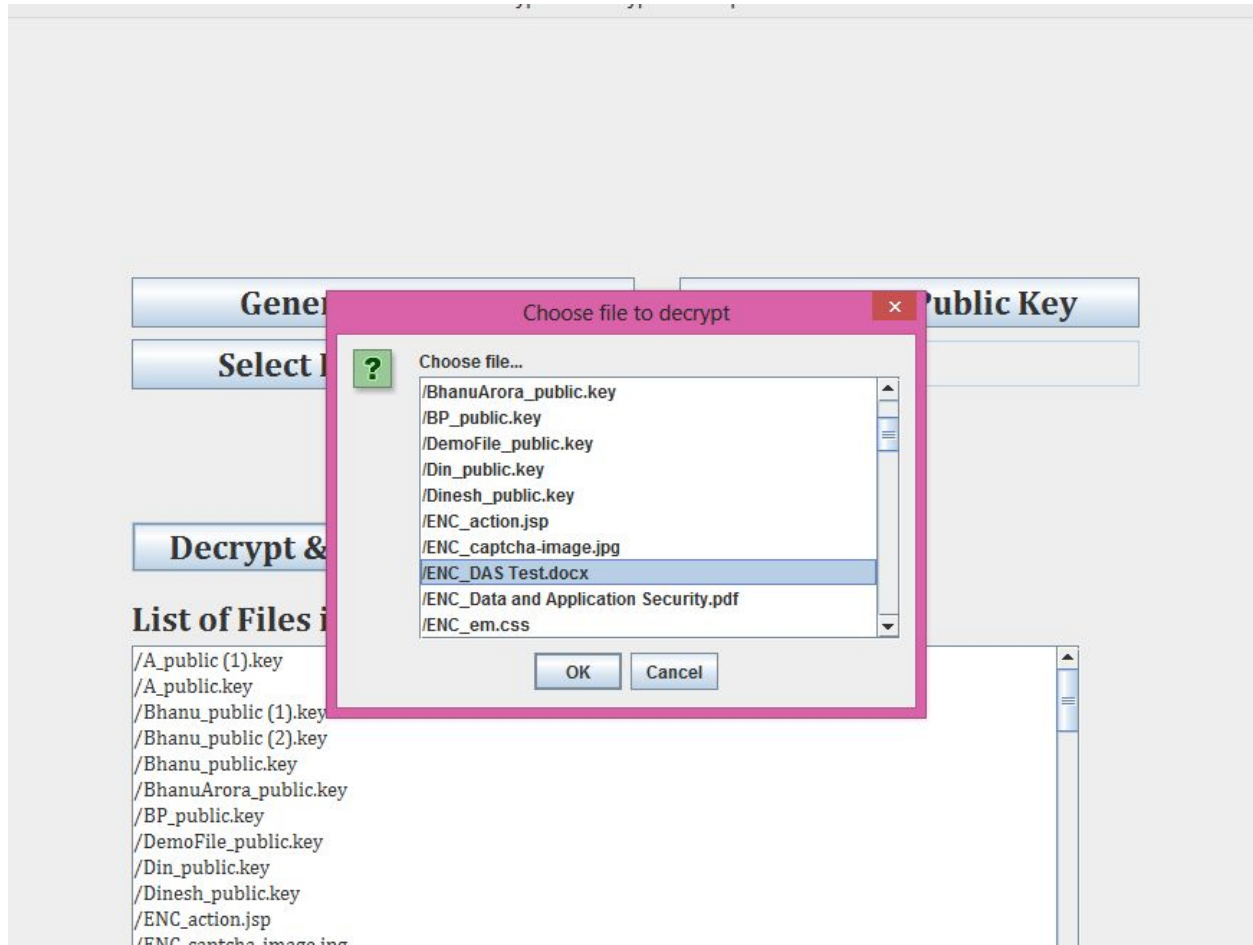
Step 8:

Bob click on decrypt and download



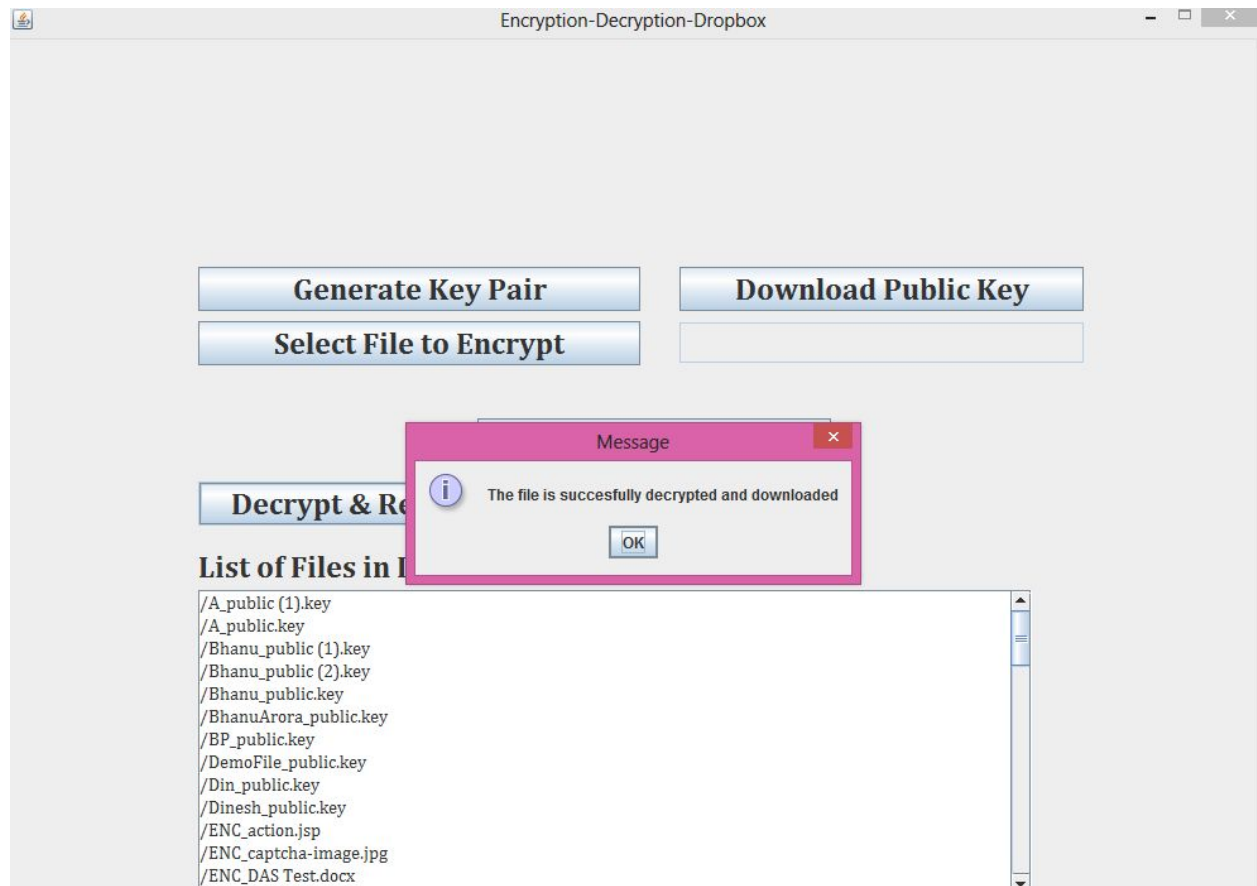
Step 9:

And select The file uploaded by Alice



Step 10:

Decrypted file downloaded



Step 11:

All keys and files will be stored in temp folder that will be created in the directory from where the application is running.

