Batch: B1, B3

Roll No.: 1611083, 1611106, 1611114

Experiment No. DCC IA 2

Grade: AA / AB / BB / BC / CC / CD /DD

Title: Develop secure data storage and privacy protection on any cloud for dropbox like clients

Objective: To develop secure data storage and privacy protection on any cloud for dropbox like clients

Group Members:
- **Vridhi Patel - 1611106**
- **Pankti Thakkar - 1611114**
- **Sanjana Joshi – 1611083**

Problem Statement:
Topic 6: Develop secure data storage and privacy protection on any cloud for dropbox like clients
- Cloud security is a major concern for large business users and consumers with sensitive data or intellectual property
- This project will require that you study effective techniques for security and privacy on cloud storage services
- You will understand the use of certificates, encryption and authentication mechanisms
- You are expected to develop desktop clients that use the service to host and exchange data in the Cloud similar to applications like 'dropbox' etc.

Abstract:
Dropbox
Dropbox is a place where all your team's content comes together. Where you can use the tools you love. Where we help you cut through the clutter and surface what matters most. It's the world's first smart workspace. Dropbox brings files together in one central place by creating a special folder on the user's computer. The contents of these folders are synchronized to Dropbox's servers and to other computers and devices where the user has installed Dropbox, keeping the same files up-to-date on all devices. Dropbox uses a freemium business model, where users are offered a free account with a

set storage size, with paid subscriptions available that offer more capacity and additional features. Dropbox Basic users are given two gigabytes of free storage space. Dropbox Plus users are given two terabytes of storage space, as well as additional features, including advanced sharing controls, remote wipe, and an optional Extended Version History add-on. Dropbox offers computer apps for Microsoft Windows, Apple macOS, and Linux computers, and mobile apps for iOS, Android, and Windows Phone smartphones and tablets.

Features:

- **Focus on the work that matters:** Scattered content, constant interruptions, difficulty coordinating—there's a smarter way to work. Dropbox helps people be organized, stay focused, and get in sync with their teams.
- **Be organized:** Bring traditional files, cloud content, Dropbox Paper docs, and web shortcuts together in one place, so you can organize and tackle your work efficiently.
- **Store and access files from anywhere:** Store your files in one safe place, and access your files from your computer, phone, or tablet. Any changes you make will sync across your account.
- **Bring all your content together:** Create and edit your work—including cloud content and Microsoft Office files—directly in Dropbox, so you spend less time switching between apps or searching for files.
- **Give context to your meetings:** Plan meetings like a boss with a calendar integration that intelligently suggests content for your upcoming meeting, note taking templates to use, and relevant files related to your event.
- **Easy access to what's important:** Starred folders help you quickly find the folders you use the most and access them from your desktop, mobile device, or dropbox.com.
- **Cloud storage:** Keep all your files safe with powerful online cloud storage
- **File sharing:** Share any file or folder easily with anyone, hassle free
- **Team management made simple:** With new Dropbox admin features, you can simplify team management, support data security and compliance, and gain actionable insights into team activity.
- **Connect your tools to Dropbox:** Stop searching and switching between apps when you connect your content to the tools you use, Slack, Zoom, HelloSign, and other Dropbox integrations.

Related Theory:
Cloud Storage Security: How secure is your data in the cloud

Data is moving to the cloud at a record pace. Cloud-based solutions are increasingly in demand around the world. These solutions include everything from secure data storage to entire business processes.

Cloud-based internet security is an outsourced solution for storing data. Instead of saving data onto local hard drives, users store data on Internet-connected servers. Data Centers manage these servers to keep the data safe and secure to access.

Enterprises turn to cloud storage solutions to solve a variety of problems. Small businesses use the cloud to cut costs. IT specialists turn to the cloud as the best way to store sensitive data.

All files stored on secure cloud servers benefit from an enhanced level of security. The security credential most users are familiar with is the password. Cloud storage security vendors secure data using other means as well.

Some of these include:

- **Advanced Firewalls:** Firewalls inspect traveling data packets. Simple ones only examine the source and destination data. Advanced ones verify packet content integrity. These programs then map packet contents to known security threats.

- **Intrusion Detection:** Online secure storage can serve many users at the same time. Successful cloud security systems rely on identifying when someone tries to break into the system. Multiple levels of detection ensure cloud vendors can even stop intruders who break past the network's initial defenses.

- **Event Logging:** Event logs help security analysts understand threats. These logs record network actions. Analysts use this data to build a narrative concerning network events. This helps them predict and prevent security breaches.

- **Internal Firewalls:** Not all accounts should have complete access to data stored in the cloud. Limiting secure cloud access through internal firewalls boosts security. This ensures that even a compromised account cannot gain full access.

- **Encryption:** Encryption keeps data safe from unauthorized users. If an attacker steals an encrypted file, access is denied without finding a secret key. The data is worthless to anyone who does not have the key.

- **Physical Security:** Cloud data centers are highly secure. Certified data centers have 24-hour monitoring, fingerprint locks, and armed guards. These places are more secure than almost all on-site data centers. Different cloud vendors use different approaches for each of these factors. For instance, some cloud storage systems keep user encryption keys from their users. Others give the encryption keys to their users.

Implementation Details:

AssureCloud: Privacy Enhanced Cloud Storage for Dropbox

We have implemented a software utility that enhances a user's privacy when storing data files in cloud storage, specifically DropBox. The software accomplishes the following goals:

- Encrypting a file, prior to being uploaded to the cloud storage
- Decrypting the encrypted file upon downloading
- Sharing the file with other users in a secure manner.

Convergent Encryption:

Convergent encryption is a self-encryption technique that encrypts a file with a key derived from the file itself. The key is obtained by applying a one-way hash to the file. What follows is an outline of steps for convergent encryption by a cloud storage user Alice:

1. We first generate RSA key pair for Alice.
2. Given a file F, Alice derives an encryption key K from the file by applying SHA-256 to F.
3. She then encrypts the file F into a ciphertext C with AES in Counter mode (AES-CTR) under the key K.
4. She protects the key K by encrypting it into W using her own RSA public key.
5. She then uploads both C and W to the cloud storage service which will ensure that C and W are stored together.

At a later stage, Alice can decrypt the encrypted file C into the original file F by

1. Downloading both C and W from the cloud storage server.
2. Extracting the key K from W by the use of her RSA private key.
3. Decrypting the ciphertext C with AES-CTR under the key K to recover the original file F.

Programming Language and Software Tools:

The above cryptographic programming is done in Python (www.python.org), by utilizing the PyCrypto cryptographic package (www.pycrypto.org, or www.dlitz.net/software/pycrypto).

Also, we use the Dropbox API for storing and retrieving the encrypted files from Dropbox.

Steps for implementation:

1. Generate public and private key pairs
2. All users have their own public-private key pairs.
3. Perform convergent encryption of a file prior to uploading.
4. Decrypt a file upon downloading.
5. Sharing
   a. Generate a re-sealed key for sharing a file with a friend (assuming the friend's public key is already known)
   b. Upon receiving a sealed key, do all the required decryption operations to obtain the original file.
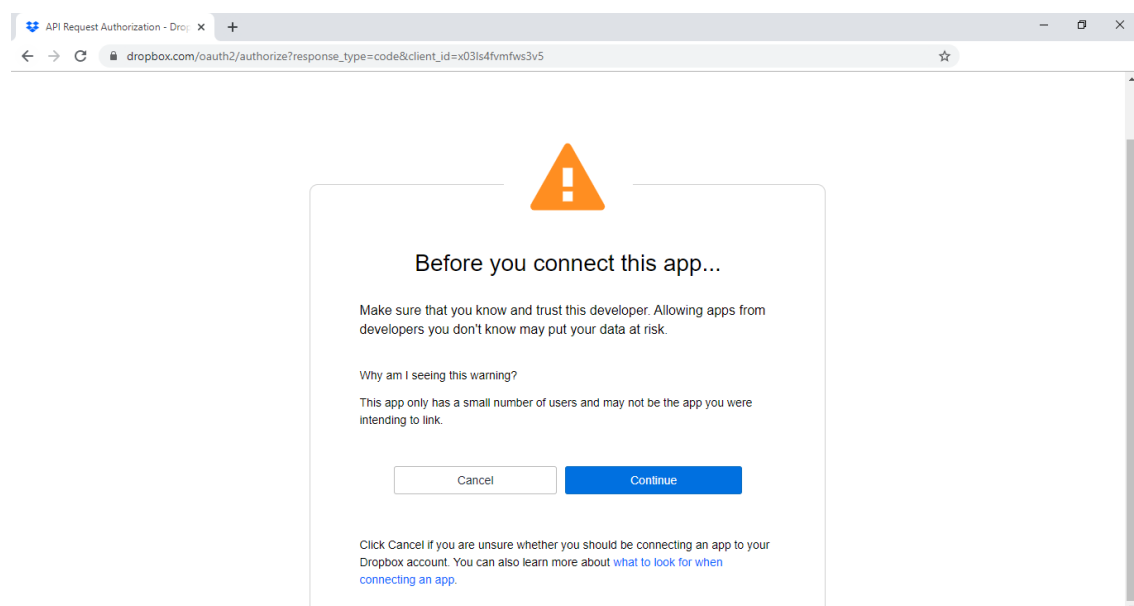
Output:

Running the main file:

Authorizing the App:

AssureCloud would like access to its own folder,
Apps › AssureCloud, inside your Dropbox. Learn more

Cancel   Allow

Enter this code into AssureCloud to finish the process.

slqE7e0uG5AAAAAAAAABEGyJhHcYCawBwEAU8la7xTs

Entering the authorization code and user is authenticated successfully

```
Enter the authorization code here: sIqE7e0uG5AAAAAAAAABEGyJhHcYCawBwEAU8la7xTs
Authentication successful!

Generating RSA key pair for Pankti

Hello, Pankti!

 What do you want to do next . . .
 1. Upload a file
 2. Download a file
 3. Share the file with friend
 4. Exit
```

RSA Key Pair generated for the user:

Feature 1: Encryption of the file and uploading it to dropbox

Before uploading:

File upload:

```
Enter your choice here : 1


 UPLOAD FILE FEATURE

Enter file name: sample.html
File encryption in progress . . .
Pankti, your file is encrypted successfully!

Creating new encrypted secret key

File upload in progress . . .
Pankti, your encrypted file has been successfully uploaded!
```

After uploading:

Dropbox > Apps > AssureCloud > data

Overview

Click here to describe this folder and turn it into a Space   Show examples

Create new file ▾

Name ↑	Modified ▾
{} sample.html	24 secs ago

File uploaded in an encrypted form:
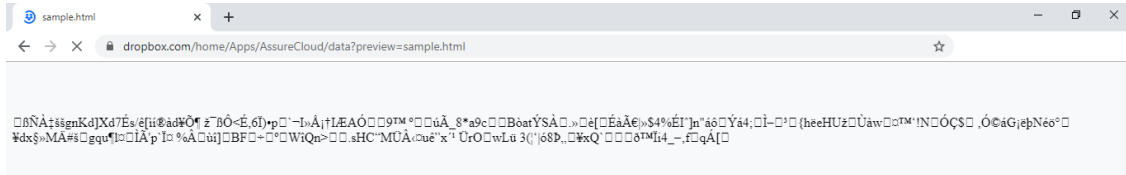
Encrypted secretKey for the file stored on dropbox:

Feature 2: Downloading the file and decrypting it to view it locally

Before downloading:
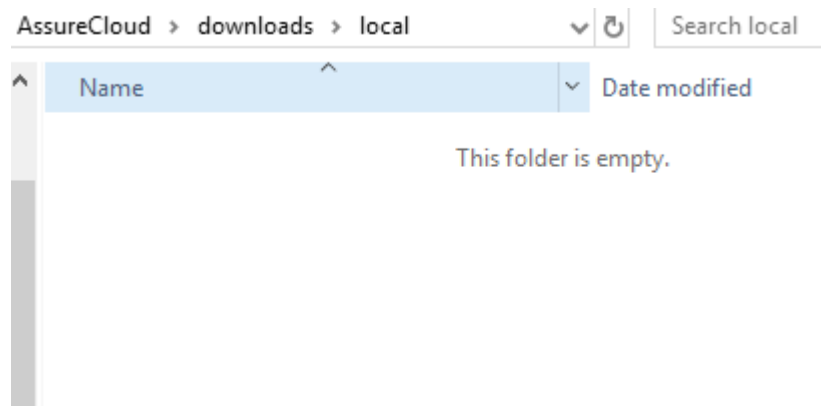
File download:

```
Enter your choice here : 2


 DOWNLOAD FILE FEATURE

Enter file name: sample.html
Downloading the file - sample.html
 Download location - ../downloads/local
Download successfully complete!
```

After download:
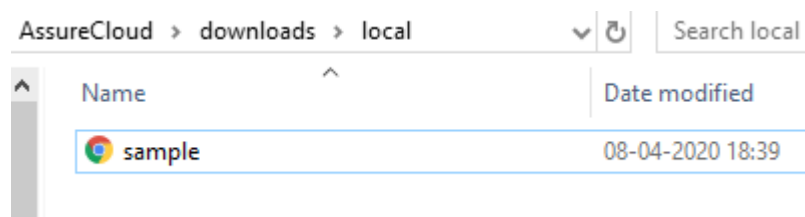
Decrypted File:

DCC IA-2

Vridhi Patel - 1611106

Pankti Thakkar - 1611114

Sanjana Joshi - 1611083

Feature 3: Sharing the file with a friend

Shared folder before sharing:

```
AssureCloud  >  downloads  >  shared        ∨  ↻     Search shared

  ^   Name                    ^                  Date modified

                        This folder is empty.
```
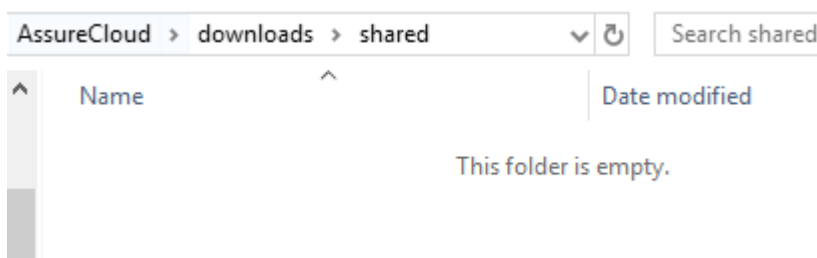
Sharing the file with a friend:

```
Enter your choice here : 3


 SHARE FILE FEATURE

Enter file name: sample.html
Enter the name of person to share file with: Vridhi
Hi, I am Pankti!
I am re-sealing this key with Vridhi's public key

 Let us assume: Pankti notifies Vridhi with key and cipher text!

Done! Let me share this cryptic file and key with Vridhi


Pankti, your encrypted file has been successfully uploaded!

Hi, I am Vridhi!
Oh I received something from Pankti!
 Downloading the file - sample.html
 Download location - ../downloads/shared/Vridhi
Download successfully complete!  Lets check!
```

RSA Key Pair generated for the friend:

Secret key encrypted using friend's RSA public key stored on dropbox, to allow him/her to access the file:

Shared folder after sharing shows the decrypted file:

Decrypted File:

DCC IA-2

Vridhi Patel - 1611106

Pankti Thakkar - 1611114

Sanjana Joshi - 1611083

Conclusion:

From this IA, we understand the importance of security of our data in cloud. We study effective techniques for security and privacy on cloud storage services and thus we develop secure data storage and privacy protection application for dropbox users through which they encrypt the files before uploading them to dropbox, download and decrypt to view them, and securely share them with other desktop clients.