Cryptography Project - 2
CS 6903

Encrypting files before storing in a cloud storage

- Ketan Ghotekar
Puru Pathak

Guide: Giovanni Di Crescenzo

Introduction:

- Cryptography is a science that applies complex mathematics and logic to design strong encryption methods, thus allowing people to keep confidence in the electronic world.
- It thus plays an important role in accordance to the wide range of cyber attacks.
- However, post the 'HeartBleed' bug in the OpenSSL cryptographic software library, there is a dire need for encrypting files before storing them in the cloud storage.
- This was the main motivation behind implementation of this project.

Environment and Primitives:

- Operating System: Ubuntu 12.04+
- System configurations:

  - 1 GB RAM

  - 64 - bit or 32 - bit system (for cloud upload and download module)

  - Intel Processor

  - 100 MB storage
- Libraries used:

  - OpenSSL

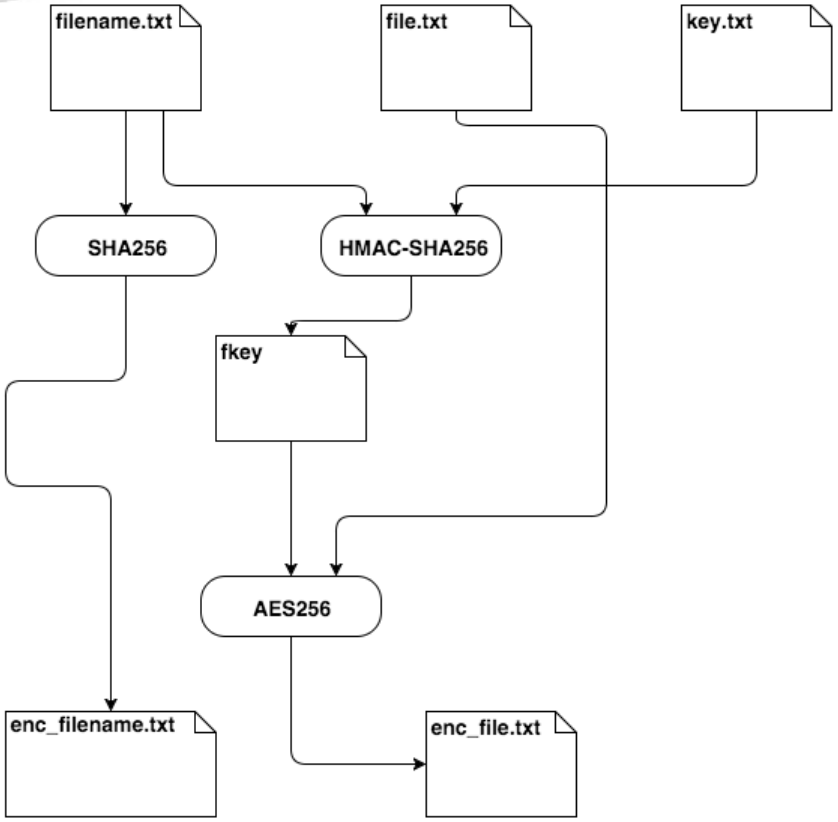
  - libSSL

Project Task allocation:

Task:	Performed by:
Created the workflow and researched on the algorithms, environments and libraries.	Ketan and Puru
Tested and finalized AES, SHA, HMAC, OpenSSL.	Ketan and Puru
Implementation of Amazon S3 file upload and download.	Ketan and Puru
Unit, functional and system testing for the application.	Ketan and Puru

Application Workflow: 1. Processing and Encryption

- Processing takes as input: key.txt, filename.txt and file.txt
- It outputs: enc_file.txt and enc_filename.txt
- The IV is randomly and dynamically generated using the OpenSSL library.
- The filename is SHA256 hashed to generate enc_filename.txt
- HMAC-SHA256 of key and filename is generated to obtain fkey.
- The fkey is used to encrypt enc_file.txt in AES256 OFB mode.
- HMAC of file.txt and fkey is generated for testing integrity.



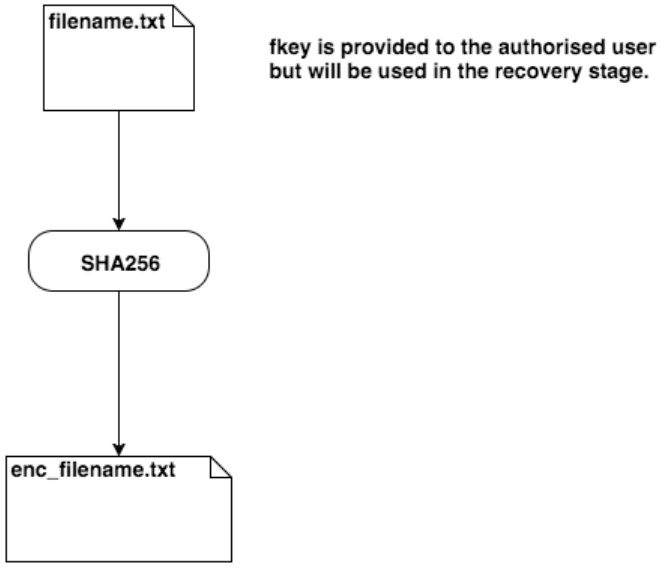
Extra Credit – Application Workflow: 2. Amazon S3 File upload

- Provide a filname to be uploaded to the Amazon S3 bucket.
- Please ensure that the file path is correct.
- The Amazon S3 file upload module will thus upload the desired file to the bucket.

```
kghoteka@ubuntu:~/ghotekar-pathak-cs6903f15project$ ./ghotekar-pathak-aws-s3-cloud-upload aadf327c8267c09d6fffd87a1a80ad3c798469ff332b7a57b9e8c045d46b2af7
File aadf327c8267c09d6fffd87a1a80ad3c798469ff332b7a57b9e8c045d46b2af7 has been uploaded to Amazon S3 bucket ketan-cloudcomputing
kghoteka@ubuntu:~/ghotekar-pathak-cs6903f15project$
```

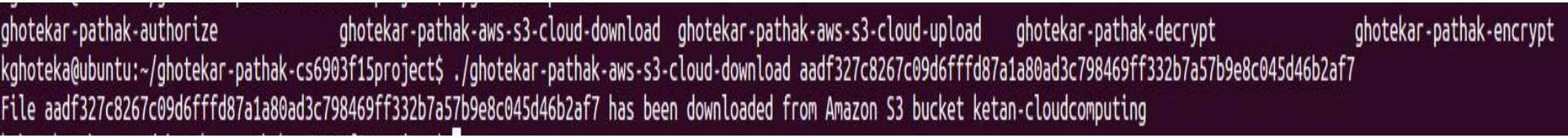
Application Workflow: 3. User Authorization

- Authorization takes as input: filename.txt
- It outputs: enc_filename.txt
- The enc_filename.txt is generated by SHA256 hash of the filename.txt



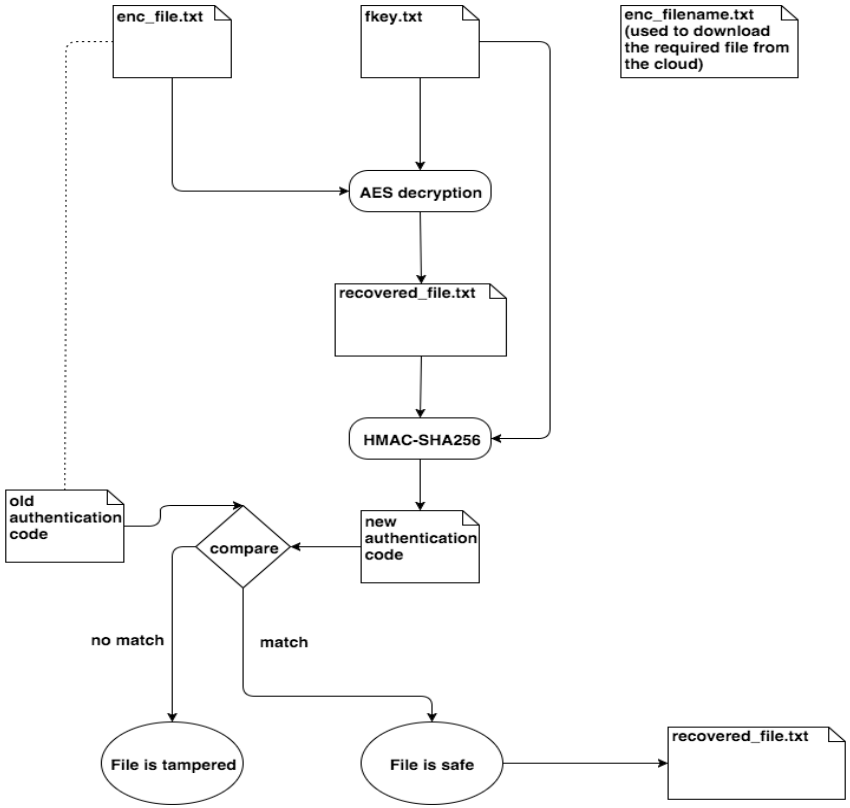
Extra Credit – Application Workflow: 4. Amazon S3 File download

- Provide a filename to be downloaded as the parameter.
- Make sure that the file is present in the S3 bucket.
- Desired file will be downloaded.



Application Workflow: 5. File Recovery

- Recovery takes as input: enc_file.txt, enc_filename.txt and fkey.txt
- It outputs: recovered_file.txt
- enc_file.txt is decrypted using the fkey by AES256 decryption.
- enc_file.txt is used to extract the old authentication code
- The new message authentication code is calculated using HMAC-SHA256 on fkey and recovered_file.txt and is compared with the old authentication code.
- If matched, the recovered_file outputted to the user is correct



Project Criteria satisfaction:

1. Data Processing Functionality: The application functionality is preserved without any side effects.
2. Confidentiality: The data content (AES encrypted) and filename (hashed) cannot be revealed.
3. Authentication and Integrity check: Message authentication code is generated using HMAC-SHA256 and a key a required to recover the data.
4. Attack sustainability: Data replay, data eavesdropping and data modification can be sustained due to the algorithms and techniques used.
5. Efficiency: The application performs efficiently in accordance to varying input sizes.

Additional Benefits!

- Our application uploads and downloads the processed file from the Amazon S3 cloud, thus making use of the services provided by Amazon AWS.
- The S3 adds an additional layer of security to our data processing application.
- The Amazon inspector is an automated security assessment service which minimizes the likelihood of security and compliance issues.
- AWS WAF prevents SQL injection or cross-site scripting and custom rules specific to the application.

Extra credit: Google Cloud Platform

- The Google cloud platform is based on the Google Security Model which is an end to end process.
- The data for each cloud storage object and it's metadata is encrypted under the 256-bit AES.
- Each encryption key is itself encrypted with a regularly rotated set of master keys.
- Cloud interconnect and managed VPN create encrypted channels between the private IP and Google network.

Extra credit: Microsoft Azure

- The Azure is compliant with ISO 270001 in connection with physical security measures taken.
- Enhanced TLS/SSL cypher suits enabling Perfect Forward Secrecy(PFS).
- PFS uses different encryption key for every connection, making it more difficult for attackers to decrypt connections.
- Azure thus integrates Microsoft's security development lifecycle (SDL) guidelines.

Extra credit:
AWS - Amazon web services

- The Amazon EBS encryption uses AWS key management service (AWS KMS) customer master keys (CMK) when creating encrypted volumes.
- Each newly created volume is encrypted with a unique 256-bit key protected with the key management infrastructure.
- The infrastructure uses Federal Information Processing Standards (FIPS) 140-2 approved cryptographic algorithms.

Extra credit: Dropbox

- Dropbox files at rest are encrypted using 256-bit Advanced Encryption Standard (AES).
- It uses SSL/TLS to protect data in transit between Dropbox apps and servers.
- Two step verification is used as an extra layer of security at login.

References:

- wiki.openssl.org
- www.security.stackexchange.com
- www.linuxcareer.com
- www.stackoverflow.com
- www.chilkatsoft.com
- www.randomkeygen.com