VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

EMAIL ENCRYPTION, AUDITING AND ANALYSIS

FALL SEMESTER 2020-21

INFORMATION SECURITY AND AUDIT ANALYSIS (CSE 3501)

PROJECT COMPONENT

SUBMITTED BY

ADTIYA SINGH DHULL (18BCB0144)
MOHD UMAR (18BCE0196)

SUBMITTED TO

PROF.VIMALA DEVI K.
SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

OCTOBER 2020

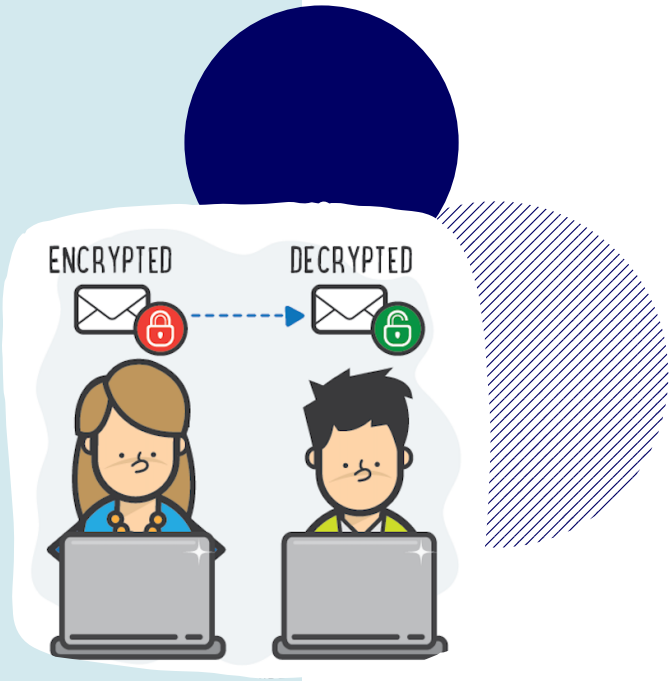


Table of Contents

ABSTRACT

E-mail is one of the most frequently used means of communication. Confidentiality, integrity and authenticity are often indispensable in e-mail communication, especially in business use. However, these security objectives can only be guaranteed with the help of additional encryption solutions.

Today, there are a variety of client, gateway and software-as-a-service solutions for e-mail encryption. Companies are faced with the challenge of finding the most suitable solution for them. Our research work presents findings from a utility value analysis which provides a comprehensive process for selecting an appropriate solution for securing e-mail traffic. We present the basic principles behind the utility value analysis and how it is used for the evaluation and selection process of e-mail encryption solutions.

Current e-mail security systems base their security on the secrecy of the long-term private key. If this private key is ever compromised, an attacker can decrypt any messages— past, present, or future—encrypted with the corresponding public key.

INTRODUCTION

E-mail travels on the web so they are exposed to the intruders. So, privacy of emails may be compromised b/w sender's and receiver's side without giving any warning. In today's electronic world, e-mail becomes the backbone of the most organizations' daily activity.

As we know email becomes most frequent in the world so e-mail security becomes more important. For the security, organizations must control the situations by taking any approach or invest wisely including all the solutions.

Let consider the services provided by e-mail to the business, email storage and management can be broken down into a number of components like flow of the mail, storage of the mails, how do we exchange public keys, how do we assign trust and how user access the emails. These issues are the part of total security agenda.

In order to secure e-mail there are some steps :

☒ Generate an Identity
☒ Configure secure e-mail software
☒ Get public keys for software
☒ Get public keys for recipients
☒ Start sending secured messages

LITERATURE SURVEY

1. Effectiveness comparison of the AES and 3DES cryptography methods on email text messages

By - Indrayani; Rini; Dhimas Adi; Ferdiansyah; Pramudita; Satria

Electronic mail or email is among the most popular data or message carrier. One of its powerful features is the sent message history records which have a long lifetime without big memory devices. However, with those technology advancements, the security aspects have become a serious concern. The ease of access to the networks has made an exposed leakage for some irresponsible parties who have the competencies to steal the information while the delivery streams take place. The email user is advised to add another security act such as encrypting toward the email contents before it being sent using ESP service. In this paper AES and 3DES cryptography method successfully implemented to securing email text messages. Email message being encrypted first using both algorithms, and then being evaluated and analyzed from various aspects. Evaluation's results shows that AES is better in terms of compile time, while 3DES is better in terms of increasing message's size after the encryption process, but the change in the addition of bytes is not significant. So based on the results of tests, email users are recommended to use AES encryption.

2. Secure e-mail communication — Comparison and selection of encryption solutions using an utility value analysis approach

By - D. Fischer; B. Markscheffel; K. Scherr

In this paper, the utility value analysis (UVA) is applied as a decision support concept to the selection process of encryption solutions for e-mail communication. In our practice-oriented project, Z1 SecureMail Gateway from Zertificon is the solution with the greatest total benefit. We were able to show that the selection process is made much more transparent by the UVA in particular because the individual requirements of users can be taken into account directly in the selection process by weighting the target criteria.

3. Cryptography and Network Security 2017 Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data

By - Ako Muhamad Abdullah

Advanced Encryption Standard (AES) algorithm is one on the most common and widely symmetric block cipher algorithm used in worldwide. This algorithm has an own particular structure to encrypt and decrypt sensitive data and is applied in hardware and software all over the world. It is extremely difficult to hackers to get the real data when encrypting by AES algorithm. Till date is not any evidence to crake this algorithm. AES has the ability to deal with three different key sizes such as AES 128, 192 and 256 bit and each of this ciphers has 128 bit block size. This paper will provide an overview of AES algorithm and explain several crucial features of this algorithm in details and demonstration some previous researches that have done on it with comparing to other algorithms such as DES, 3DES, Blowfish etc.

3. A simple construction of encryption for a tiny domain message

By - Rashed Mazumder; Atsuko Miyaji; Chunhua Su

In modern cryptography, message encryption is an important tool for providing data-privacy and authenticity. In many applications, it is used such as password storage, data integrity check, wireless network, automated teller machine card, and credit card. Usually, the size of a message is arbitrary. In addition, many techniques and constructions are available for the variable and fixed size of message encryption. Interestingly, we address the issue of small domain message encryption (SDE). Generally, the existing constructions are based on blockcipher such as AES/DES and scratch function. Hence, these solutions are reasonable for the bigger size of data. However, these are heavy and expensive for the small size of message encryption under the platform of Internet of Technology-end device (IoT), and resource constrained devices. In addition, the size of plaintext and ciphertext should be equal for satisfying the property of small domain encryption. Actually, J.Black and P.Rogaway formally addressed the above issues for the first time. Following that certain schemes have been launched under the SDE such as Mix-and-Cut shuffle, Swap-or-Not, Thorp-Shuffle, and FNR.

Moreover, Sometimes-Recursive shuffle (SRS) is the pioneer construction yet in respect of low encryption time. However, it needs to execute 1000 calls of AES for achieving full security. Therefore, the construction of SRS is also heavy and expensive for the IoT environment and resource constrained devices. Under these circumstances, we propose a simple scheme that follows by Fiestel structure. The internal format is based on small keyed-function. Our construction can encrypt small size of a message. Furthermore, the size of plaintext and ciphertext are equal.

5. E-Mail Security Framework Through Various Virus Encryption Techniques

By - Ashutosh Prasad Bhatt; Monika Sharma

On Internet, securing mail has always been an important issue. Various standards and products have been created. Virus is the program which harms our files and makes them infected and performs abnormal actions. And because of not proper knowledge or lack of knowledge, the users do not know how to keep their system secure and deal with the problems. There are various techniques proposed by the researchers through which user can encrypt the virus on mails and provide a healthy platform for operations. In this research paper, we have done analysis of encryption techniques and proposed a new framework to improve the email security.

6. Performance study of enhanced SHA-256 algorithm

By - A. Gowthaman, Sumathi Manickam

The prolong growth of wired and wireless communication has spark off the revolution for the generation of new cryptographic algorithms. Hash functions are similar and important cryptographic fields, which are very complicate for data integrity assurance and data security services. This paper looks into optimization technique in new VLSI architecture for the SHA-256 hash functions are presented. This paper combines different techniques namely rescheduling of Carry Select Adder and Non linear Pseudo code random generator for improving the functions in an inner loop of hashing algorithm. The new system can minimize the critical path by rescheduling of inner part of the SHA architecture.

PROBLEM STATEMENT

It is widely believed that security and usability are two antagonistic goals in system design. E-mail encryption algorithms and software have been in the market for about two decades. Yet, they have not been implemented strictly in any protocol.To encrypt or not to encrypt is the question that today's email clients present their users. Given this choice, most users chose the "zero-click" alternative—not to encrypt. The perceived risks that encryption protects against presumably pale when compared to the difficulty of encrypting.

OBJECTIVES

- **Studying multi-factor authentication :** To understand how easy it is to hack into e-mail accounts and find confidential mails.

- **Encrypting and testing mails in real time :**

    1. We aim at developing a small web server that shall serve as a means of sending and receiving mail.
    2. We will imitate a simple S/MIME digital signature protocol, a standard end-to-end mail encryption protocol.
    3. Also, as a part of our project, we will generate a protocol to encrypt the message with a:
    4. Standard SHA-256 encryption method;
    5. Standard DH algorithm (on the message header);
    6. A dual layer encryption using AES and DH encryption methods; finally

PROPOSED WORK

As we are trying to create a mail server and receiver module to demonstrate our encryption method, we'll create our own server in Python. Every step in the encryption can be viewed for experimental purposes. We will further try to model the time complexity of the framework so as to compare it with the present-day framework of mails. We will be doing all this with the help of AES Encryption Algorithm and SHA-256 Function.

The following are the steps that will happen :

1. Enter your message in the text area provided
2. Click on Encrypt and enter a secret password when prompted for
3. It will encrypt the text and redirect you to the Gmail
4. Send it to desired receiver and on receiver side, person will have to copy the link and paste it to browser
5. He will be redirected to our web app and will be prompted for the password (currently, assumed that somehow it is shared securely between two parties)
6. When he enters password decryption is done successfully and corresponding plaintext is displayed in the box.

FIG 1. Block Diagram of SHA-256

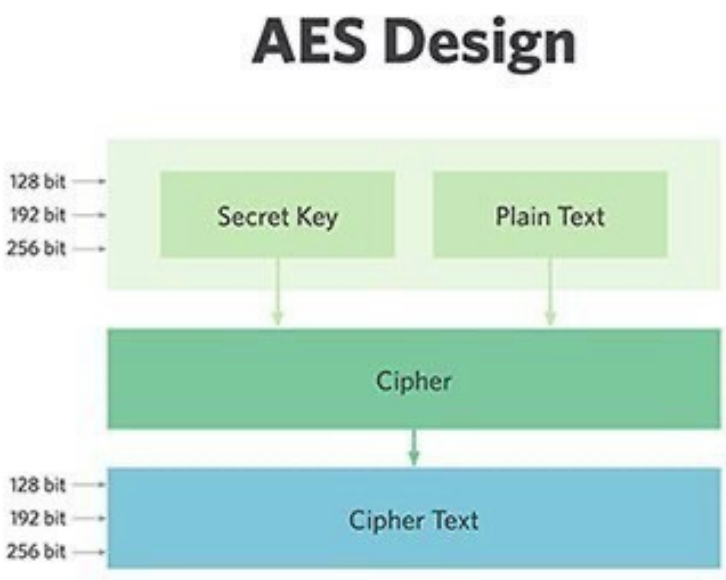


FIG 2. Block Diagram of AES

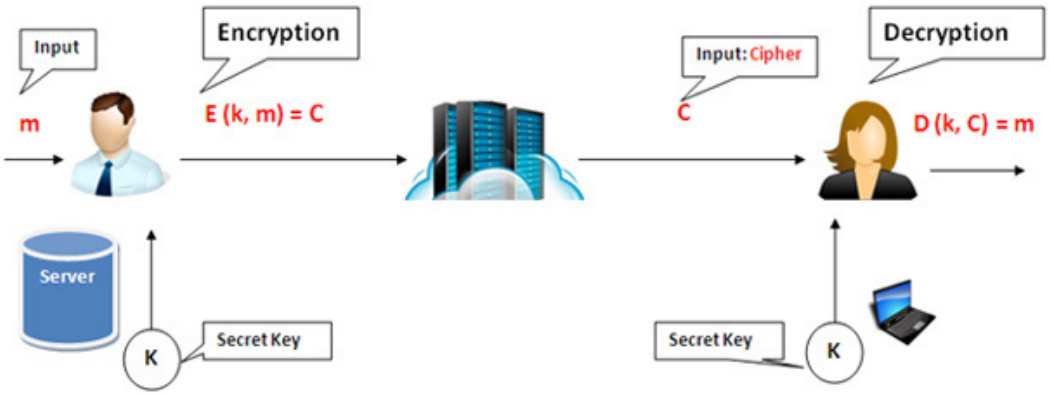
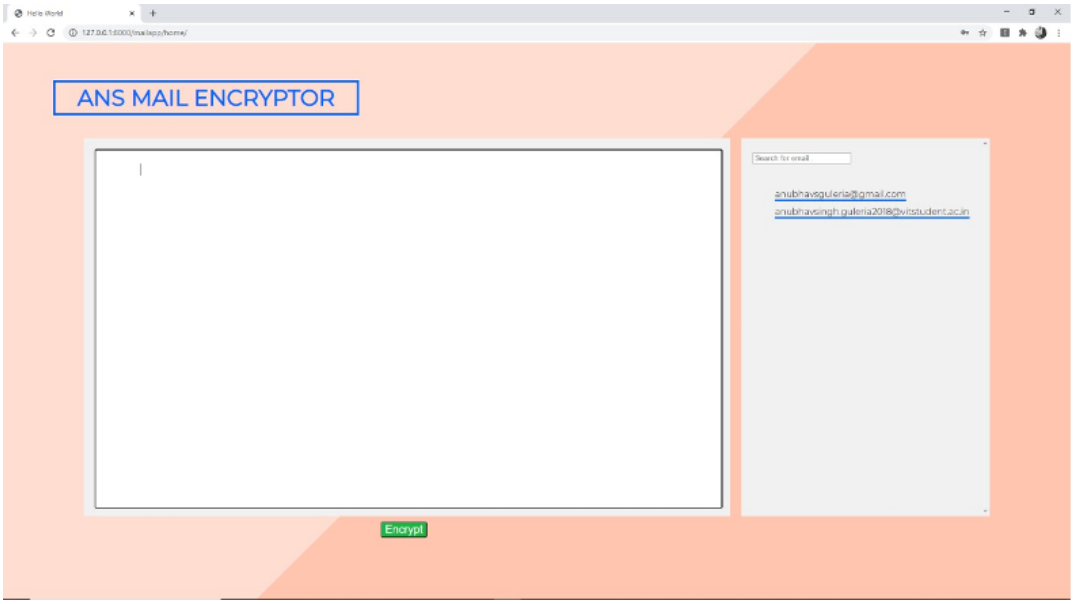


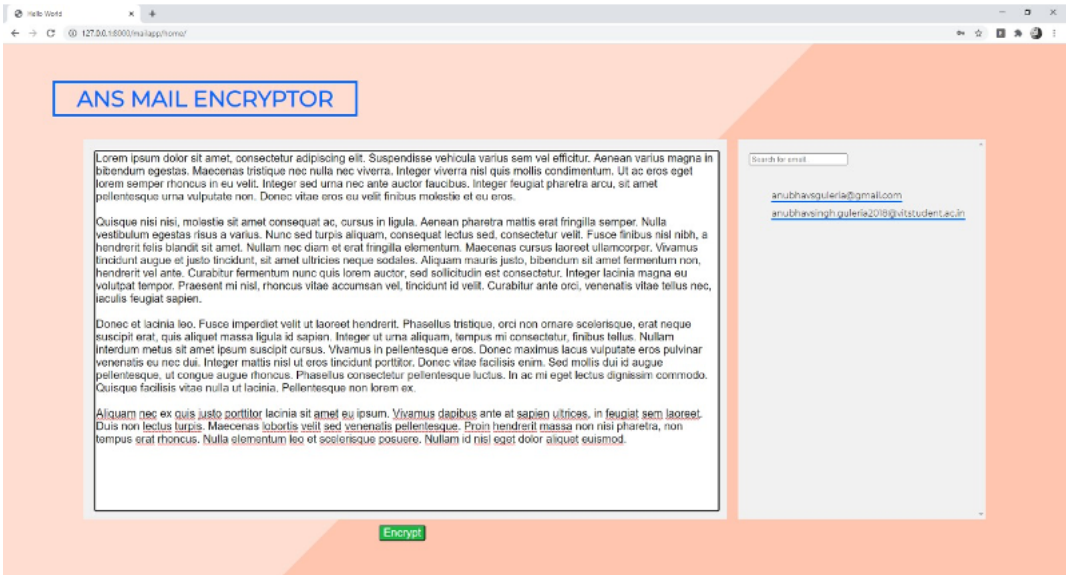
FIG 3. Data Flow Diagram

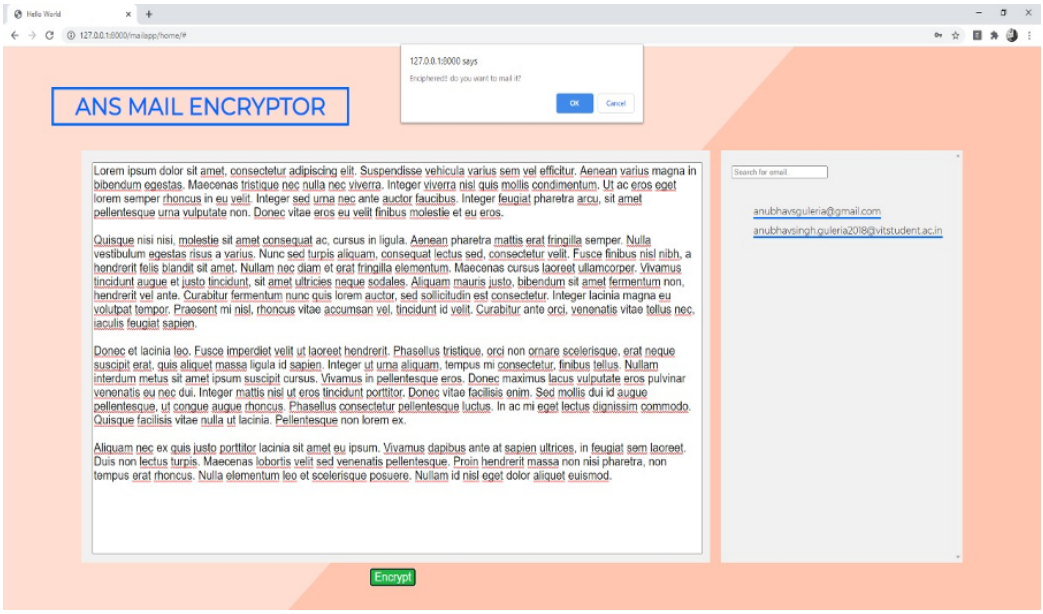
CODE

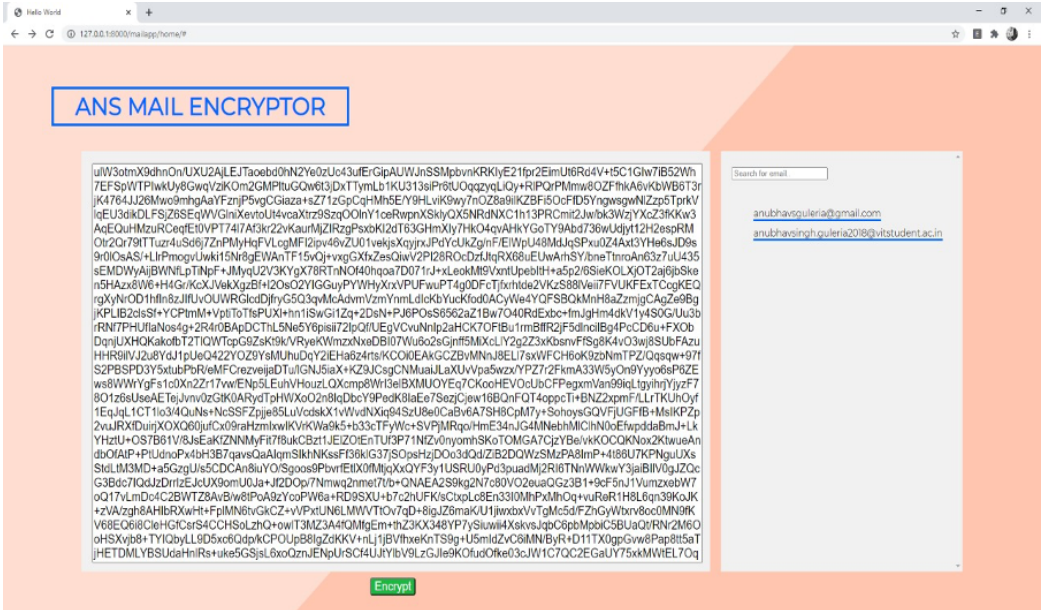
Google Drive : https://drive.google.com/drive/folders/1UH-5BNUtasBIq_73VTW4EoqxIGpB_NDy?usp=sharing

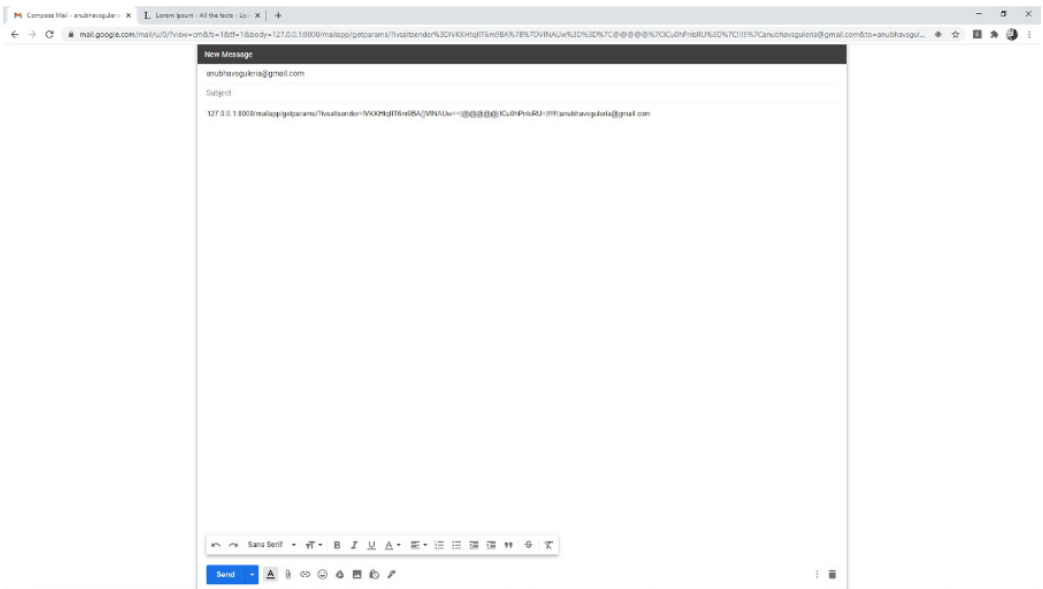
SCREENSHOTS

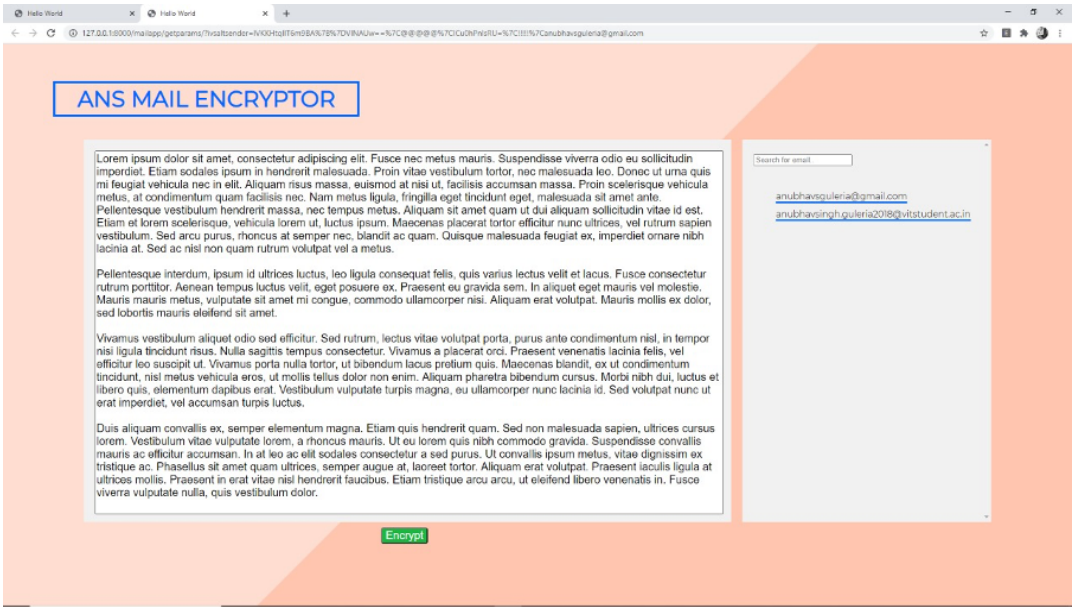





ANS MAIL ENCRYPTOR
127.0.0.1:8000 says
Encipherect! do you want to mail it?
OK
Cancel
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Suspendisse vehicula varius sem vel efficitur. Aenean varius magna in bibendum egestas. Maecenas tristique nec nulla nec viverra. Integer viverra nisl quis mollis condimentum. Ut ac eros eget lorem semper rhoncus in eu velit. Integer sed urna nec ante auctor faucibus. Integer feugiat pharetra arcu, sit amet pellentesque urna vulputate non. Donec vitae eros eu velit finibus molestie et eu eros.
Quisque nisi nisi, molestie sit amet consequat ac, cursus in ligula. Aenean pharetra mattis erat fringilla semper. Nulla vestibulum egestas risus a varius. Nunc sed turpis aliquam, consequat lectus sed, consectetur velit. Fusce finibus nisl nibh, a hendrerit felis blandit sit amet. Nullam nec diam et erat fringilla elementum. Maecenas cursus laoreet ullamcorper. Vivamus tincidunt augue et justo tincidunt, sit amet ultricies neque sodales. Aliquam mauris justo, bibendum sit amet fermentum non, hendrerit vel ante. Curabitur fermentum nunc quis lorem auctor, sed sollicitudin est consectetur. Integer lacinia magna eu volutpat tempor. Praesent mi nisl, rhoncus vitae accumsan vel, tincidunt id velit. Curabitur ante orci, venenatis vitae tellus nec, iaculis feugiat sapien.
Donec et lacinia leo. Fusce imperdiet velit ut laoreet hendrerit. Phasellus tristique, orci non ornare scelerisque, erat neque suscipit erat, quis aliquet massa ligula id sapien. Integer ut urna aliquam, tempus mi consectetur, finibus tellus. Nullam interdum metus sit amet ipsum suscipit cursus. Vivamus in pellentesque eros. Donec maximus lacus vulputate eros pulvinar venenatis eu nec dui. Integer mattis nisl ut eros tincidunt porttitor. Donec vitae facilisis enim. Sed mollis dui id augue pellentesque, ut congue augue rhoncus. Phasellus consectetur pellentesque luctus. In ac mi eget lectus dignissim commodo. Quisque facilisis vitae nulla ut lacinia. Pellentesque non lorem ex.
Aliquam nec ex quis justo porttitor lacinia sit amet eu ipsum. Vivamus dapibus ante at sapien ultrices, in feugiat sem laoreet. Duis non lectus turpis. Maecenas lobortis velit sed venenatis pellentesque. Proin hendrerit massa non nisi pharetra, non tempus erat rhoncus. Nulla elementum leo et scelerisque posuere. Nullam id nisl eget dolor aliquet euismod.
Search for email
anubhavsguleria@gmail.com
anubhavsingh.guleria2018@vitstudent.ac.in
Encrypt


ANS MAIL ENCRYPTOR
Search for email
anubhavsguleria@gmail.com
anubhavsingh.guleria2018@vitstudent.ac.in
Encrypt


New Message
anubhavsguleria@gmail.com
Subject
Send



ANALYSIS

For analysing for threats from emails we need to look at :

security/deliverability
Do you have

- Bounce-removal process?
- Privacy policies in place?
- Easy (and easily visibly) unsubscribe/opt-out instructions

Format

- If you haven't given recipients the opportunity to select their preferred format, use a "sniffer."subject line
- No cutting and pasting
- Special characters kept to a minimum (or eliminated completely
- Free of spam-like words
- Action-oriented

Header

- Name of newsletter/organization
- Company URL

- Tagline
- Date

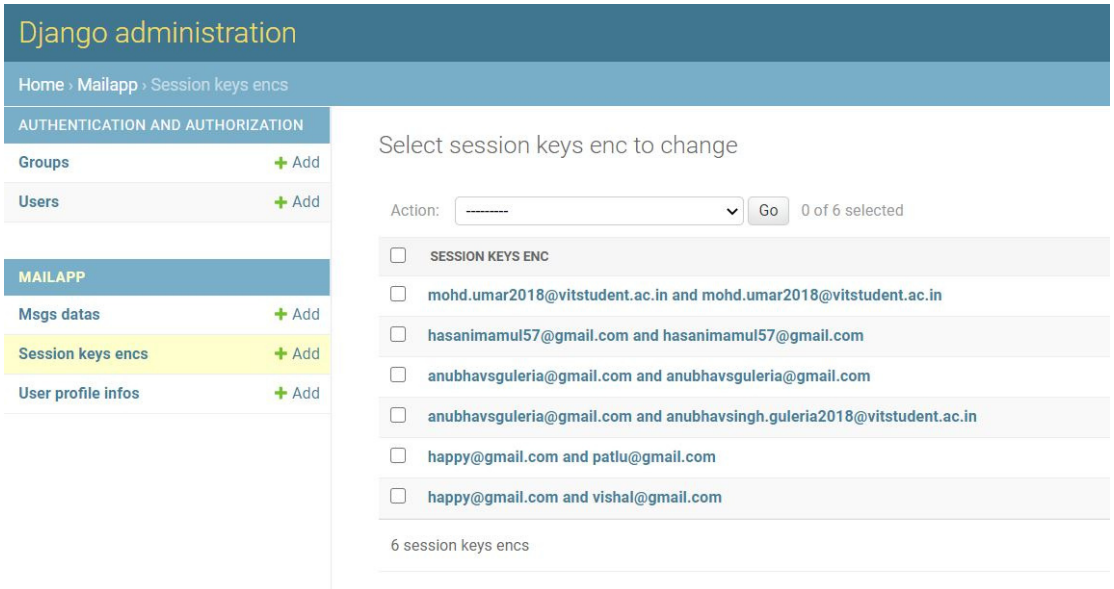
Content

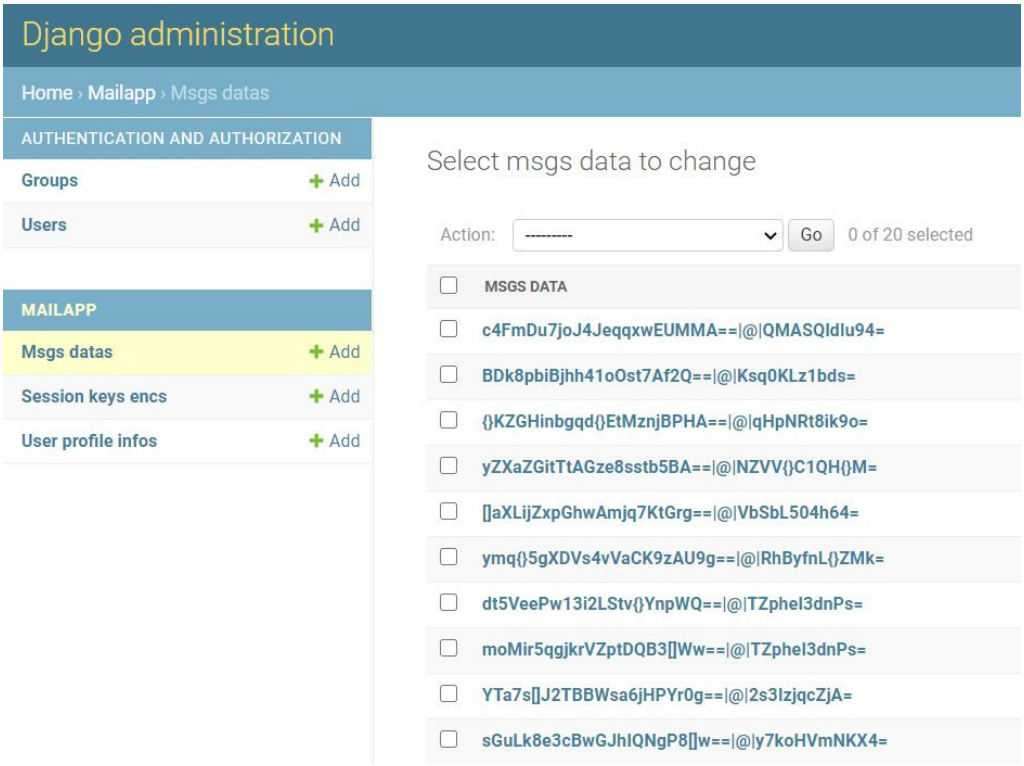
- No boring articles (be creative!)
- Art/images
- Personalized
- Calls to action

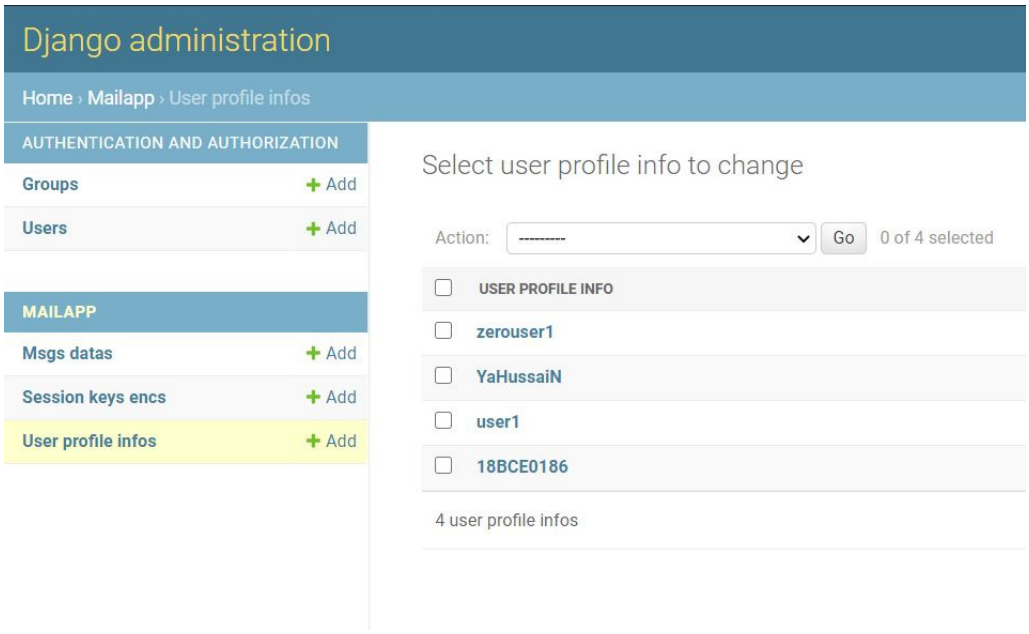
Footer

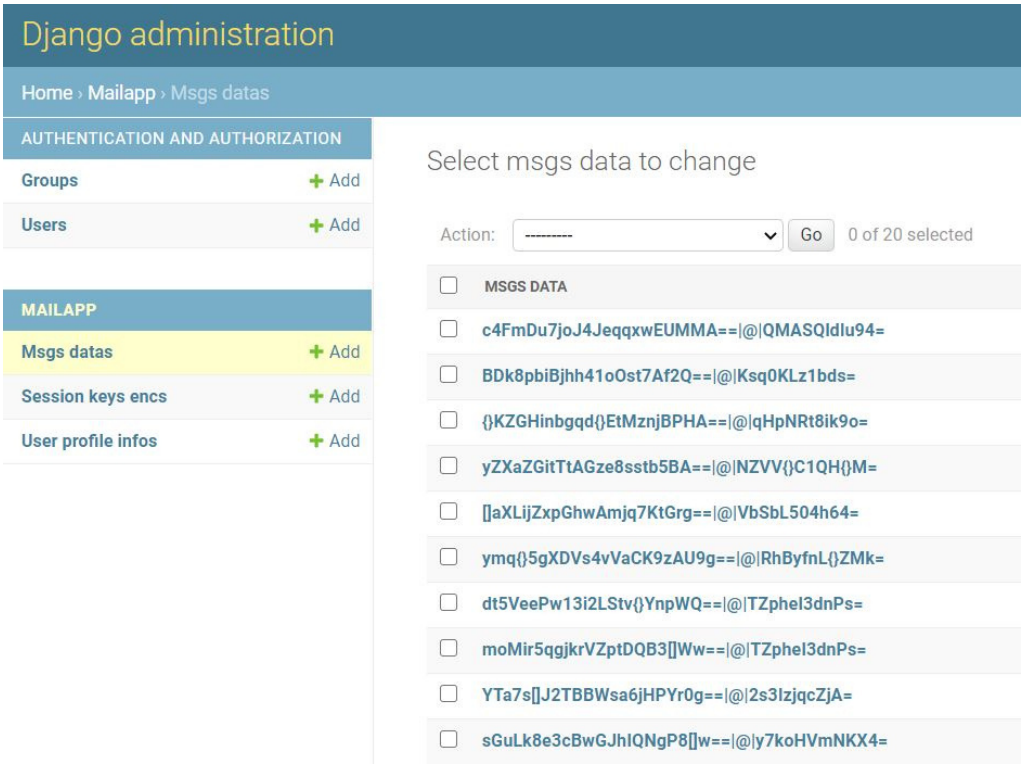
- Key contacts
- Unsubscribe information
- Encourage recipient to forward message

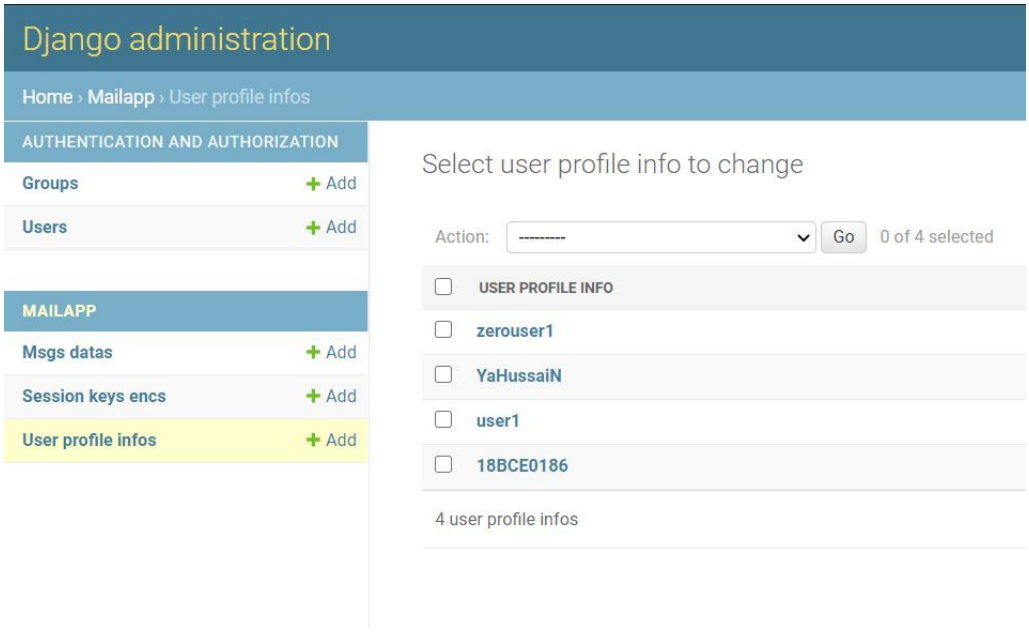
In this project, since we are the admin we can find out what the secure key, users logged in and to whom is the email sent. The following are screenshots showing analysis of the project :




Django administration
Home › Mailapp › Msgs datas
AUTHENTICATION AND AUTHORIZATION
Groups + Add
Users + Add
MAILAPP
Msgs datas + Add
Session keys encs + Add
User profile infos + Add
Select msgs data to change
Action: --------- Go 0 of 20 selected
MSGS DATA
c4FmDu7joJ4JeqqxwEUMMA==|@|QMASQIdlu94=
BDk8pbiBjhh41oOst7Af2Q==|@|Ksq0KLz1bds=
{}KZGHinbgqd{}EtMznjBPHA==|@|qHpNRt8ik9o=
yZXaZGitTtAGze8sstb5BA==|@|NZVV{}C1QH{}M=
[]aXLijZxpGhwAmjq7KtGrg==|@|VbSbL504h64=
ymq{}5gXDVs4vVaCK9zAU9g==|@|RhByfnL{}ZMk=
dt5VeePw13i2LStv{}YnpWQ==|@|TZphel3dnPs=
moMir5qgjkrVZptDQB3[]Ww==|@|TZphel3dnPs=
YTa7s[]J2TBBWsa6jHPYr0g==|@|2s3IzjqcZjA=
sGuLk8e3cBwGJhIQNgP8[]w==|@|y7koHVmNKX4=

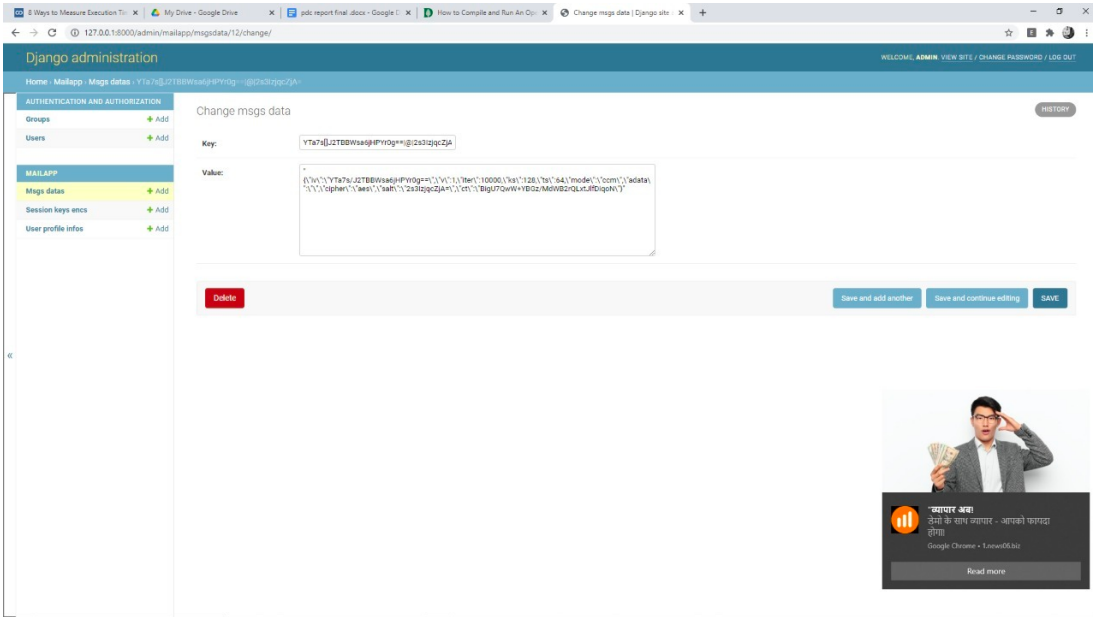

Django administration
Home › Mailapp › User profile infos
AUTHENTICATION AND AUTHORIZATION
Groups + Add
Users + Add
MAILAPP
Msgs datas + Add
Session keys encs + Add
User profile infos + Add
Select user profile info to change
Action: --------- Go 0 of 4 selected
USER PROFILE INFO
zerouser1
YaHussaiN
user1
18BCE0186
4 user profile infos

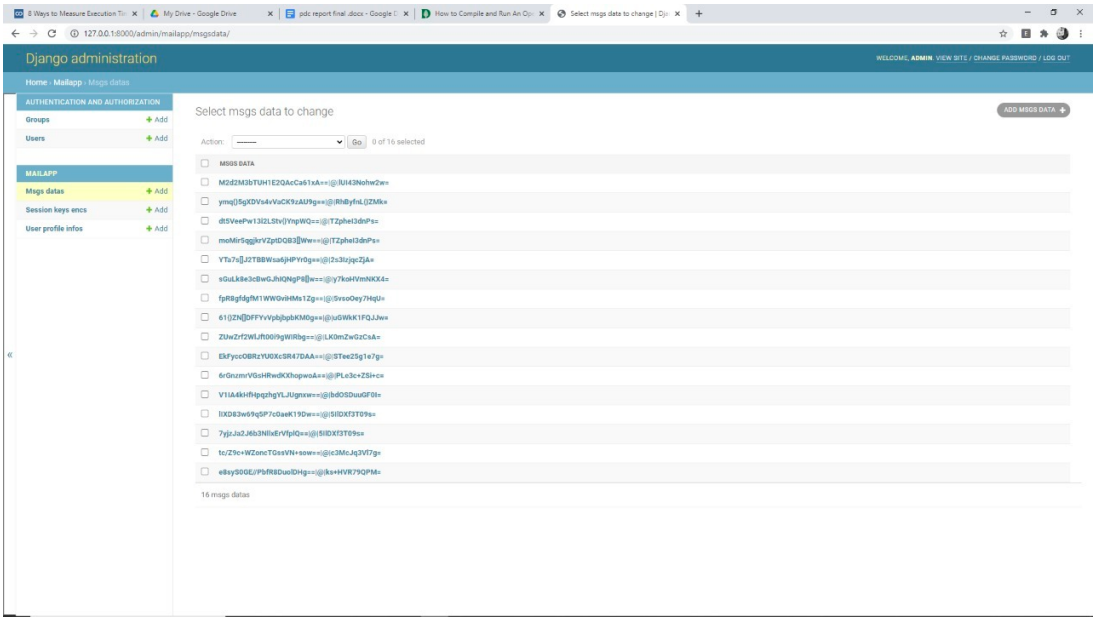

Django administration
Home › Mailapp › Msgs datas
AUTHENTICATION AND AUTHORIZATION
Groups + Add
Users + Add
MAILAPP
Msgs datas + Add
Session keys encs + Add
User profile infos + Add
Select msgs data to change
Action: --------- Go 0 of 20 selected
MSGS DATA
c4FmDu7joJ4JeqqxwEUMMA==|@|QMASQldlu94=
BDk8pbiBjhh41oOst7Af2Q==|@|Ksq0KLz1bds=
{}KZGHinbgqd{}EtMznjBPHA==|@|qHpNRt8ik9o=
yZXaZGitTtAGze8sstb5BA==|@|NZVV{}C1QH{}M=
[]aXLijZxpGhwAmjq7KtGrg==|@|VbSbL504h64=
ymq{}5gXDVs4vVaCK9zAU9g==|@|RhByfnL{}ZMk=
dt5VeePw13i2LStv{}YnpWQ==|@|TZphel3dnPs=
moMir5qgjkrVZptDQB3[]Ww==|@|TZphel3dnPs=
YTa7s[]J2TBBWsa6jHPYr0g==|@|2s3IzjqcZjA=
sGuLk8e3cBwGJhIQNgP8[]w==|@|y7koHVmNKX4=

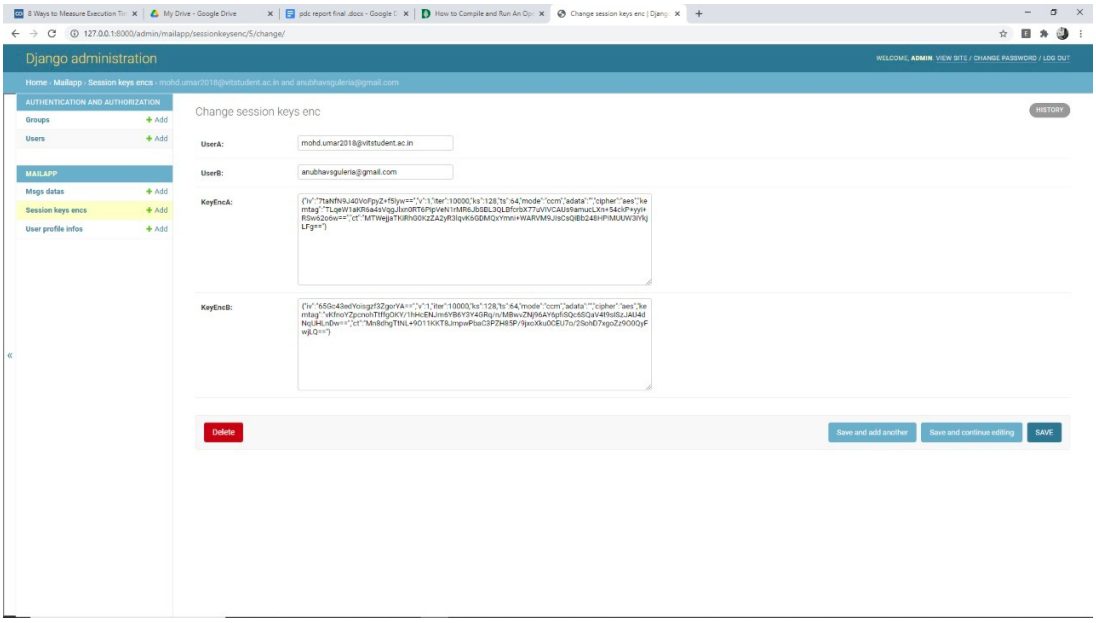

Django administration
Home › Mailapp › User profile infos
AUTHENTICATION AND AUTHORIZATION
Groups + Add
Users + Add
MAILAPP
Msgs datas + Add
Session keys encs + Add
User profile infos + Add
Select user profile info to change
Action: --------- Go 0 of 4 selected
USER PROFILE INFO
zerouser1
YaHussaiN
user1
18BCE0186
4 user profile infos

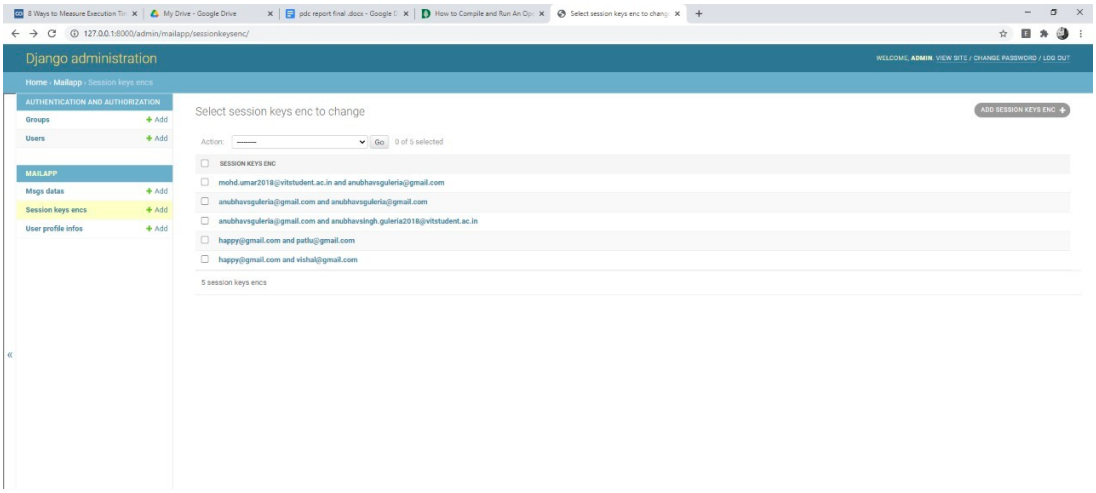
AUDITING

We perform auditing by finding out what is the content of the emails and we also can find out what are the users upto. In order to reduce threats.









CONCLUSION

After performing various email encryption, decryption, auditing and analysis techniques, we have understood the how the Information Security Analysis and Audit works. Now a day's data secrecy and protection are the most important thing, so as per analysis, we found out that detection of known and unknown threats provides a secure platform.

As e-mail threats are powerful in present scenario and will become more powerful in future and e-mail system is the best and favorite platform for the attackers to spread these threats. So, there is lots of scope for the researchers for further improvement.

REFERENCES

[1] https://ieeexplore.ieee.org/document/8938579/

[2] https://www.researchgate.net/publication/311435679_E-mail_Security_Issues_and_Solutions

[3] https://ieeexplore.ieee.org/document/8356439

[4] https://ieeexplore.ieee.org/document/7926080

[5] https://www.researchgate.net/publication/283517888_Performance_study_of_enhanced_SHA-256_algorithm

[6] https://www.researchgate.net/publication/317615794_Advanced_Encryption_Standard_AES_Algorithm_to_Encrypt_and_Decrypt_Data

[7] https://ieeexplore.ieee.org/document/9065809

[8] https://digitalguardian.com/blog/what-email-encryption

[9] https://www.pandasecurity.com/en/mediacenter/panda-security/how-to-encrypt-email/

[10] https://www.reallysimplesystems.com/blog/email-security-protocols/