ID Based Encryption and Decryption using Python

DEPARTMENT OF

ELECTRONICS AND COMMUNICATION & ENGINEERING

MLDS PROJECT REPORT

Author:

1. P.V.V.S. ADITYA
2. K. MOURYA

PROJECTMENTOR:

Dr. K. Nagaraju

November 2021

Certificate

Department of Electronics and communication Engineering

INDIAN INSTITUTE OF INFORMATION TECHNOLOGY
DESIGN AND MANUFACTURING, KURNOOL

This is to certify that this is a bonafide record of the project presented by the students whose names are given below during Monsoon and Year 2021 in partial fulfilment of the requirements of the degree of Bachelor of Technology in Electronics and communication Engineering.

ROLL NO	Name of Students
120EC0012	P.V.V.S. ADITYA
120EC0023	K. MOURYA

Dr. K. Nagaraju,
(Project Mentor)

Dr. Mohamed Asan Basiri,
(Head of Department)

November 2021

Acknowledgements

We would like to express our sincere thanks to **Dr. K. Nagaraju** for his valuable guidance and support in completing my project. We would also like to express our gratitude towards our Hon'ble Director **Prof. D.V.L.N. Somayajulu** and Head of the department **Dr. Mohamed Asan Basiri**, for giving us this great opportunity to do a project on. Without their support and suggestions, this project would not have been completed.

Abstract

Swap messages with your friends using the art of cryptography changing the text of a message so that people who do not know your secret methods cannot understand it!

Cryptography The word cryptography comes from the ancient Greek words for “hidden” and “writing.” People have been using this technique to send secret messages for nearly 4,000 years.

Here are some special terms used in cryptography

Cipher: a set of instructions for altering a message to hide its meaning.

Encrypt: to hide the secret message.

Decrypt: to reveal the secret message.

Ciphertext: the message after it has been encrypted. Plaintext: the message before it has been encrypted.

The program will ask you if you want to create a secret message or reveal what a secret message says. It will then ask you to type in the message. If you choose to make a secret message, your message will be turned into what looks like total gibberish. But if you choose to reveal a message, nonsense will be turned into text you can read!

So, we will use some encryption techniques to turn the original message into secret message so that message cannot be understand everybody until he/she know the techniques and the member how have the same software can decrypt that confidential information.

Table Of Contents

1. Introduction

A huge amount of private data is sent around the Internet every day like mails, messages, photos, documents, and a lot more.

The Internet protocols send private data in packets on the same routes as everyone else's data, and unfortunately, attackers have figured out ways to look at the data whizzing around the Internet.

The internet is a dangerous place – as unfortunate as it is to have to say that – there are hackers and cybercriminals looking to take advantage of people at every turn.

Now, it should be pretty obvious why you need security & encryption if you have been following along up until this point. If you are running a website that is collecting personal information, financial information, even login information and passwords—you need to keep that information safe for your users. As we mentioned, the default communication protocol, HTTP, is not secure. Anyone who knows how can readily see all the communication taking place across an HTTP connection That alone should be enough to convince you. But if it is not, here's a couple of other things to consider. First, if you are running a business, you may think that only the biggest companies must worry about cybercrime. That is false. According to Symantec, 74% of small and medium-sized businesses have been targeted by a cyber-attack in just the last 12 months. And even more terrifying, 60% of the small businesses that fall victim to a cyber-attack go out of business within six months.

Second, even if you are not a business or you are not collecting what you consider to be vital information from visitors—if your users can login you absolutely need encryption. It does not matter if you are not selling anything, if users can login—you must encrypt. The internet is unique in that users can only do so much to protect themselves, a lot of the onus for protecting people falls on the websites they visit. You do not want to gain a reputation as a site that doesn't protect its visitors. And beyond that, people's password hygiene, in general, is atrocious. Meaning, people reuse that same password across multiple accounts and

seldom change them. A breach on your site might seem innocuous, but if cybercriminals can use those stolen passwords to access other, more important accounts—your users are going to blame you.

So, there you have it. Encryption is a practice wherein information is encoded in such a way that only an authorized party can read it. It's really an integral part of any web security strategy. And now, it's also a basic requirement on the internet.

2. Encryption, Decryption & User Uniqueness

2.1. Encryption

In cryptography, encryption is the process of encoding information. This process converts the original representation of the information, known as plaintext, into an alternative form known as ciphertext. The problem with HTTP is it's not secure, which means that anyone who knows what they're doing can essentially see – for lack of a better term all the communication between your computer and the server. That means that any information that is exchanged can be intercepted and either stolen or manipulated by a third party.

Encryption prevents that from happening by securing your connection via the SSL/TLS protocol. When encryption is active, it basically scrambles the communication between your computer and the server so that only the other party can unscramble it and read it. To any third party that's listening in on the connection, the communication is complete unintelligible.

2.2. Decryption

The conversion of encrypted data into its original form is called Decryption. It is generally a reverse process of encryption. It decodes the encrypted information so that an authorized user can only decrypt the data because decryption requires a secret key or password. One of the reasons for

implementing an encryption-decryption system is privacy. As information travels over the Internet, it is necessary to scrutinise the access from unauthorized organisations or individuals. Due to this, the data is encrypted to reduce data loss and theft. Few common items that are encrypted include text files, images, e-mail messages, user data and directories. The recipient of decryption receives a prompt or window in which a password can be entered to access the encrypted data. For decryption, the system extracts and converts the garbled data and transforms it into words and images that are easily understandable not only by a reader but also by a system. Decryption can be done manually or automatically. It may also be performed with a set of keys or passwords.

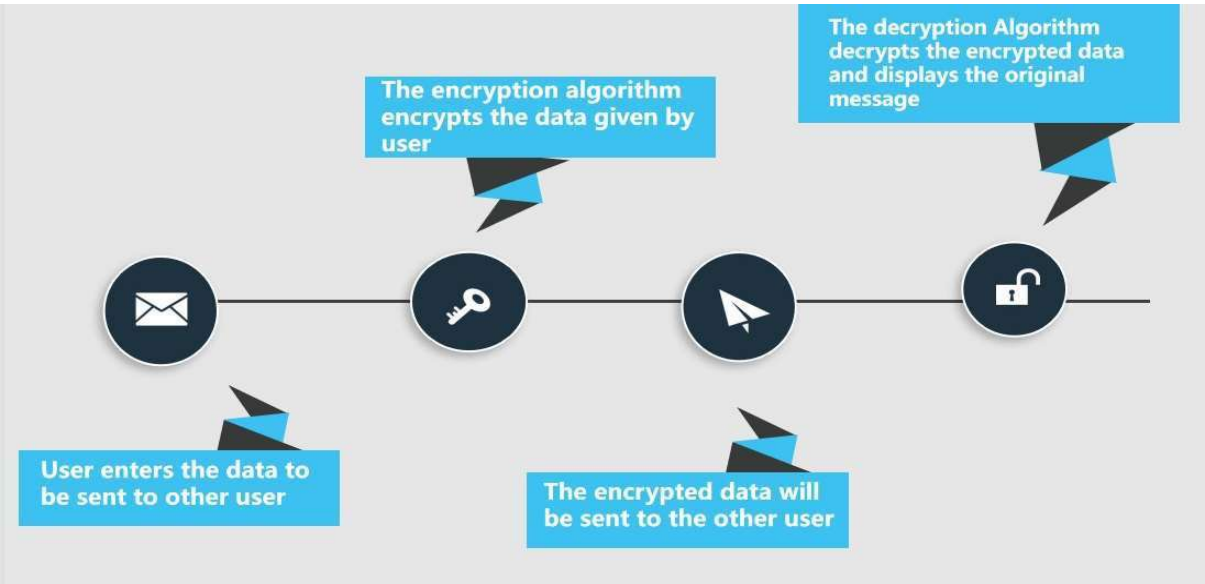
There are many methods of conventional cryptography, one of the most important and popular method is Hill cipher Encryption and Decryption, which generates the random

Matrix and is essentially the power of security. Decryption requires inverse of the matrix in Hill cipher. Hence while decryption one problem arises that the Inverse of the matrix does not always exist. If the matrix is not invertible then the encrypted content cannot be decrypted. This drawback is completely eliminated in the modified Hill cipher algorithm. Also, this method requires the cracker to find the inverse of many square matrices which is not computationally easy. So, the modified Hill-Cipher method is both easy to implement and difficult to crack.

2.3. User Uniqueness

User uniqueness refers to the distinct identification of an individual based on specific associated data. In the context of messaging, only a singular user possessing certain distinct statistics will receive the message. This ensures that the communication is targeted to a specific and recognizable recipient, enhancing personalized engagement and effective communication.

3. Process Flow



4. Dive into algorithms

Encryption:

The algorithm uses the unique user ID of the receiver and encrypts the data based on the ID of the receiver in order to maintain the user uniqueness

```
def encrypt(rec_ID,Message):
    L_enc = list(rec_ID.split("-"))
    for i in L_enc:
        if i == "0":
            Message= "$%^&*(^$~`" + Message
        elif i == "1":
            Message=Message*2
        elif i == "2":
            Message=Message[:1]+"#%🐱🚲"+Message[1:]
        elif i == "3":
            Message=Message[:5]+"😁#!😡"+Message[5:]
        elif i == "4":
            Message=Message + "😋%^~"
        elif i == "5":
            Message=Message[:8]+"*$!😤~`"+Message[8:]
        elif i == "6":
            for j in range(0,len(Message),15):
```

```
                Message=Message[:15] + "+=_🏠" +Message[15:]
        elif i == "7":
            for j in range(0,len(Message),2):
                Message=Message[:2] + "$@`1~😂" +Message[2:]
        elif i == "8":
            d=int(len(Message)/6)
            Message=Message[:d]+"10021"+Message[d:]
        elif i == "9":
            q=int(len(Message)-4)
            Message=Message[:q] + "👼"+Message[q:]
        else:
            print('Please Enter a Valid Receiver ID')
    print("\n\n           ****Receiver's Console***\n")
    print("Encrypted message: ",Message)
    return(Message)
```

Decryption:

As the encryption process takes place based on the Receiver's ID so this user will only be able to decrypt the encrypted message.

```
def decrypt(rec_ID,mess_dec):
    L_dec = list(reversed(rec_ID))
    for i in range(0,len(L_dec),2):
        if L_dec[i] == '0':
            mess_dec=mess_dec.replace("$%^&*(^$~`",'')
        elif L_dec[i] == '1':
            mess_dec=mess_dec[slice(0,len(mess_dec)//2)]
        elif L_dec[i] == '2':
            mess_dec=mess_dec.replace("#%😸🚓",'')
        elif L_dec[i] == '3':
            mess_dec=mess_dec.replace("😁#!😵",'')
        elif L_dec[i] == '4':
            mess_dec=mess_dec.replace("😊%^~",'')
        elif L_dec[i] == '5':
            mess_dec=mess_dec.replace("*$!🤧~`",'')
        elif L_dec[i] == '6':
            mess_dec=mess_dec.replace("+=_🏠",'')
        elif L_dec[i] == '7':
            mess_dec=mess_dec.replace("$@`1~😂",'')
        elif L_dec[i] == '8':
            mess_dec=mess_dec.replace("10021",'')
        elif L_dec[i] == '9':
```

```
            mess_dec=mess_dec.replace("🍲",'')
        else:
            break
    print("Decrypted message:",mess_dec)
```

Message:

Message sent by the sender will be encrypted based on the receiver's ID and will be sent to him due to uniqueness and this encrypted message can be decrypted by the receiver only.

User uniqueness:

The message will be sent only to the user whose ID has been used by the sender and will be sent in encrypted form.

5. Future Work

- OPEN SOURCE
- Developing better encryption & decryption algorithms
- Improve user uniqueness algorithm

6. Applications

- Used in sending confidential information
- Making internet a safer place to surf on
- Secure important data and files from hackers.