



**VIT<sup>®</sup>**  
**Vellore Institute of Technology**  
(Deemed to be University under section 3 of UGC Act, 1956)

**School of Computer Science and Engineering**  
**Residential Complex Visitor Authentication System**  
**REVIEW-3 REPORT(Documentation)**

SUBMITTED BY

**C Harshith Suraag (19BCI0138)**

**Vishal Haswani (19BCI0181)**

**Rahul Gupta (19BCI0225)**

**Sarthak Sharma (19BCI0226)**

PREPARED FOR

**Cryptography Fundamentals**

**CSE 1011**

**PROJECT COMPONENT**

SUBMITTED TO

**Dr. Madhu Viswanathan**

## **Abstract**

The project deals with the creation of a visitor Authentication System for a Residential Complex. It deals with Managing the details of all the residents of the complex in an Encrypted Database and maintaining communication between Admin of the server and residents to Send Private keys and public keys to all residents for encryption of OTP Authentication. The data of all residents are stored in a Database and is Encrypted using the DSA algorithm.

The purpose of our project is to provide Visitor Authentication and remove any kind of vulnerabilities from the system and to help reduce criminal activities such as Theft, Robbery, Kidnapping etc.

## **Introduction**

### **Theory**

Database: Collection of Resident Data

Use of SQL Database. Use of Python for Backend and HTML, CSS, JS for Front End.

Use of DES and RSA Algorithms for encryption of data and OTP respectively.

### **Aim**

Our goal in this project is to make a Simple and Secure Authentication System for visitors, visiting a huge apartment complex. We focus on providing Visitor Authentication and removing any kind of vulnerabilities from the system and Maintain Authentication and Confidentiality

### **Objective**

Provide Encryption to Resident Data By encrypting It.

Encrypted OTP for sending it even over unsafe networks

Asymmetric Encryption so that only Resident Knows Private key

Maintaining Authentication of Visitors

### **Motivation**

I was once at bangalore and was visiting my relatives' home. It was the first time I saw this system in action. It was simple and a vulnerable system. Once I reached at the entrance of the apartment complex the guard inquired about the Flat Number I was visiting, then he took a picture of me and told me to call the owner of the apartment to ask and tell him the OTP, received by the owner. I called my relative and asked him the OTP. The loopholes in this system proved to be vulnerable like what if my relative's phone was stolen or what if a third-party tries to tap the SMS containing OTP (Since OTP is directly sent as plaintext) and Hence Decided to develop a system to provide better Security and maintain authenticity for verification of Visitors.

## **Features**

Visitor tells the security guard the details of the Apartment Owner and sends him an SMS with a Number and a Link.

Residents visit the Link and Enter the Number, Private Key, Password. This Generates a Second Number. (Decrypted OTP)

The Owner Calls the visitor and tells him the Second Number, which is verified by the Security Guard.

## **Literature Survey**

1. Visitor Pass - Abhay Gaidhani, Suraj Sahijwani, Parag Jain, Shantanu Jadhav, Ankush Jain(2015)

A system for Visitor Pass was discussed in the paper by Prof. Abhay Gaidhani, Suraj Sahijwani, Parag Jain, Shantanu Jadhav, Ankush Jain in year 2015. This paper aims to develop a system for Gate pass using Raspberry Pi. The main aim was to save paper with the help of Internet Connectivity to send SMS and Email for verification of user.

2. UTAUT - Norizan Anwar, Mohamad Noorman Masrek(2012)

There are varieties of similar systems available in the market when you search the visitor management system in any of the search engines available. Those systems come with various features to offer to their customers with different price ranges. This visitor application system is called Visitor Management System (VMS) and with the motto "Handling Your Visitor at Your Fingertips". Visitor Management System (VMS) was designed and developed in order to monitor visitor movement in an organization. The application can be viewed from local LAN (Intranet) with a standard web browser such as Microsoft Internet Explorer with no additional software or plugin to load. VMS will be placed at the main guardhouse and will be handled by the corporate security section. Each of the departments will be located with at least one front desk officer to monitor the current visitor to visit their department.

One of the gaps identified is the physical aspect of using a mobile phone in case of a theft or network snooping analysis, hence we use Encrypt the OTP and also use Asymmetric Encryption so that only the resident knows the key.

## **Concepts Used**

RDBMS - Stands for "Relational Database Management System." An RDBMS is a DBMS designed specifically for relational databases. Therefore, RDBMSes are a subset of DBMSes.

A relational database refers to a database that stores data in a structured format, using rows and columns. This makes it easy to locate and access specific values within the database. It is "relational" because the values within each table are related to each other. Tables may also be related to other tables. The relational structure makes it possible to run queries across multiple tables at once.

**DES Algorithm** -The DES (Data Encryption Standard) algorithm is a symmetric-key block cipher created in the early 1970s by an IBM team and adopted by the National Institute of Standards and Technology (NIST). The algorithm takes plain text in 64-bit blocks and converts them into ciphertext using 48-bit keys.

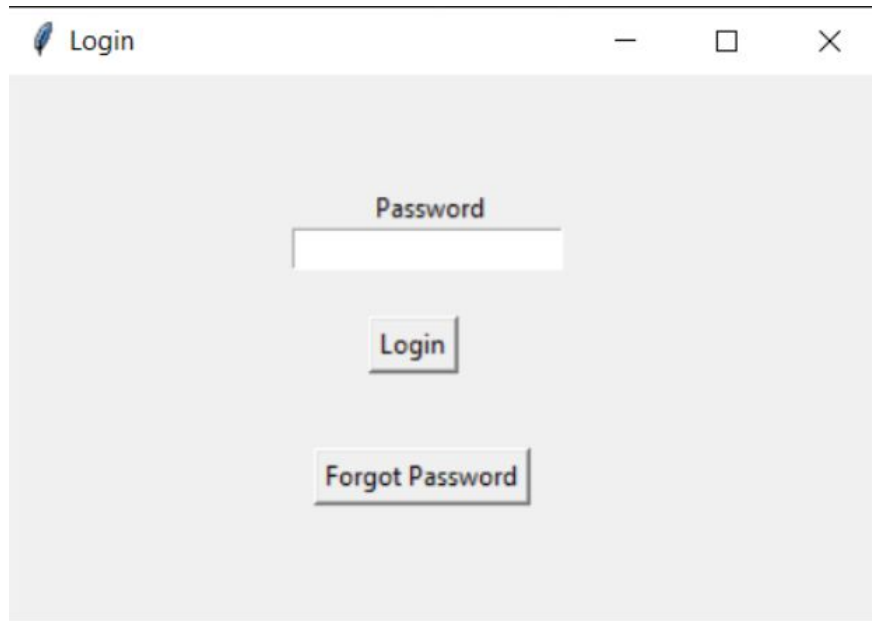
**RSA Algorithm** - RSA (Rivest–Shamir–Adleman) is a public-key cryptosystem that is widely used for secure data transmission. It is also one of the oldest. The acronym RSA comes from the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman, who publicly described the algorithm in 1977.

In a public-key cryptosystem, the encryption key is public and distinct from the decryption key, which is kept secret (private). An RSA user creates and publishes a public key based on two large prime numbers, along with an auxiliary value. The prime numbers are kept secret. Messages can be encrypted by anyone, via the public key, but can only be decoded by someone who knows the prime numbers.

## **Working(Architecture)**

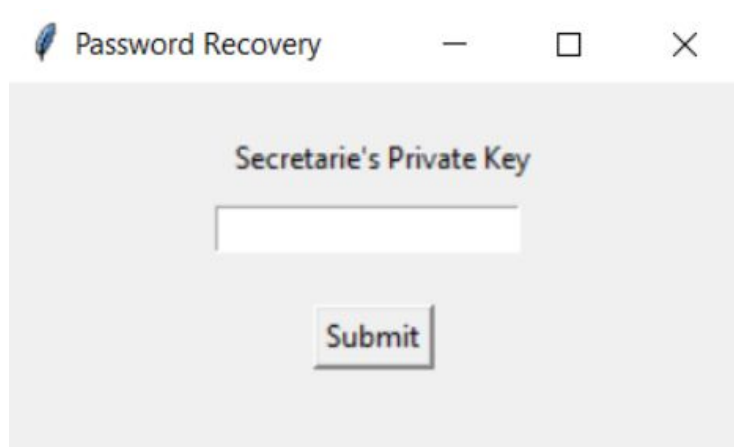
### **Admin/Guard Side Working**

1. Login Page -

A screenshot of a web browser window titled "Login". The window has a light gray background. In the center, there is a text input field labeled "Password". Below the input field, there are two buttons: "Login" and "Forgot Password". The window has standard minimize, maximize, and close buttons in the title bar.

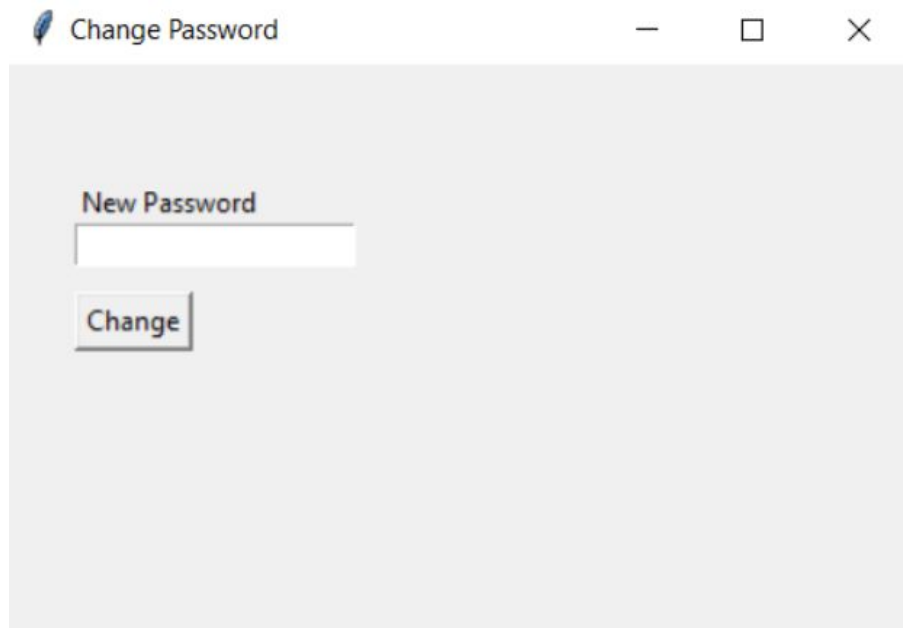
This is the login Page that the security guard uses to login with his password every morning and also to do a monthly routine by the ADMIN.

## 2. Login Forget Password -

A screenshot of a web browser window titled "Password Recovery". The window has a light gray background. In the center, there is a text input field labeled "Secretarie's Private Key". Below the input field, there is a button labeled "Submit". The window has standard minimize, maximize, and close buttons in the title bar.

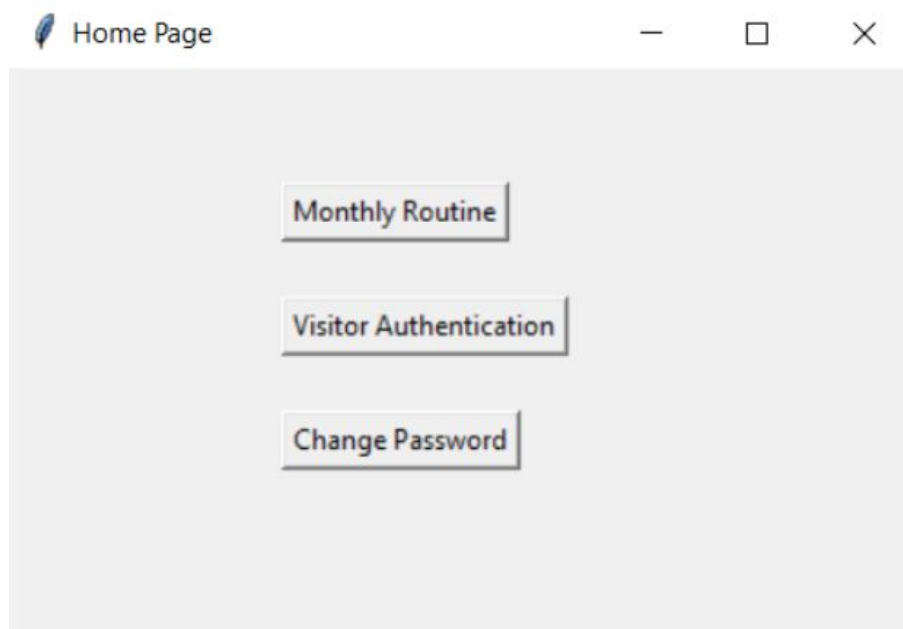
This is the Forget Password page is used to reset if the guard forgets password the admin private key is used to Reset it.

## 3. Password Reset Page



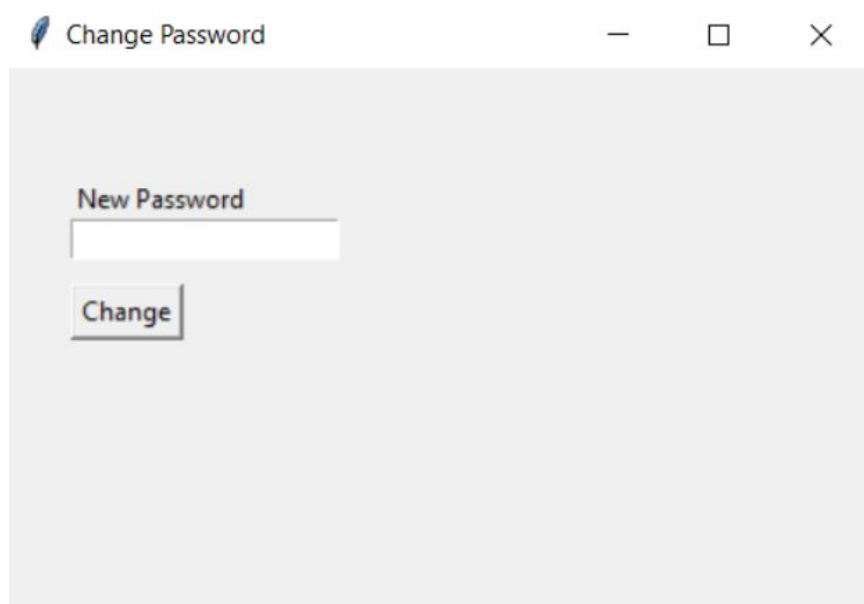
New Password will be entered here either by the admin or the Security Guard.

#### 4. Home Page



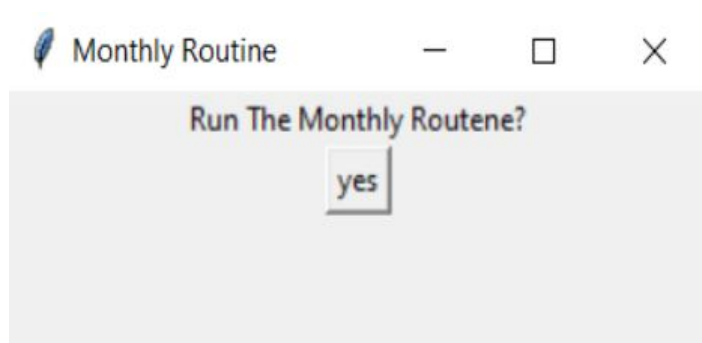
This is the main homepage that the security guard will see after logging in, it has three buttons namely - Monthly routine, visitor authentication and change Password.

#### 5. Change Password



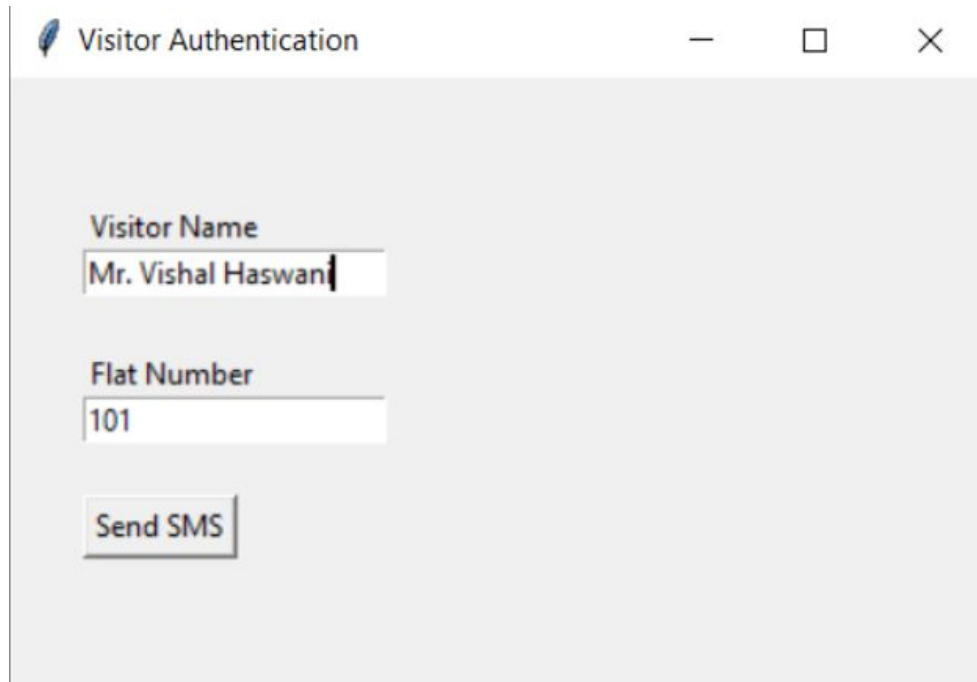
This is for changing the login Credentials.

#### 6. Monthly Routine



This is used to run the Monthly routine where All the residents receive Their RSA private key for decrypting RSA encrypted OTP whenever they get a visitor

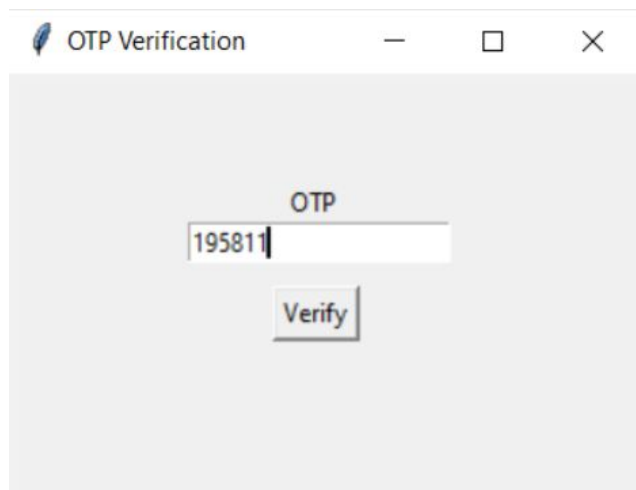
#### 7. Visitor Authentication



The screenshot shows a window titled "Visitor Authentication" with a feather icon on the left and standard window controls (minimize, maximize, close) on the right. The window has a light gray background. Inside, there are two text input fields. The first field is labeled "Visitor Name" and contains the text "Mr. Vishal Haswan". The second field is labeled "Flat Number" and contains the text "101". Below these fields is a button labeled "Send SMS".

The Visitor Authentication Page is opened when a visitor arrives and used to give details of visitors and the apartment they visit and send the Encrypted SMS.

#### 8. OTP Authentication



The screenshot shows a window titled "OTP Verification" with a feather icon on the left and standard window controls (minimize, maximize, close) on the right. The window has a light gray background. Inside, there is a text input field labeled "OTP" containing the text "195811". Below the field is a button labeled "Verify".

Decrypted OTP Entered by Security Guard for visitor verification

#### 9. Verified Page





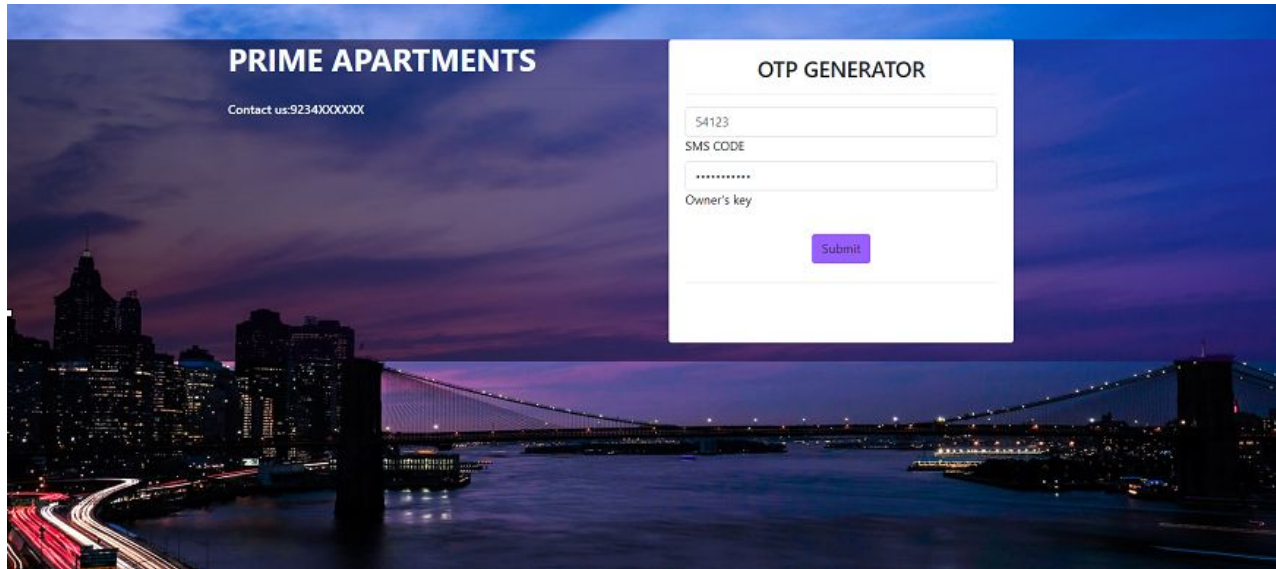
10. SMS Received by Resident.

Sent from your Twilio trial  
account - Mr. Vishal Haswani  
is here to visit kindly copy the  
Code  
61981366  
and Visit The website:  
[www.google.com](http://www.google.com)

\

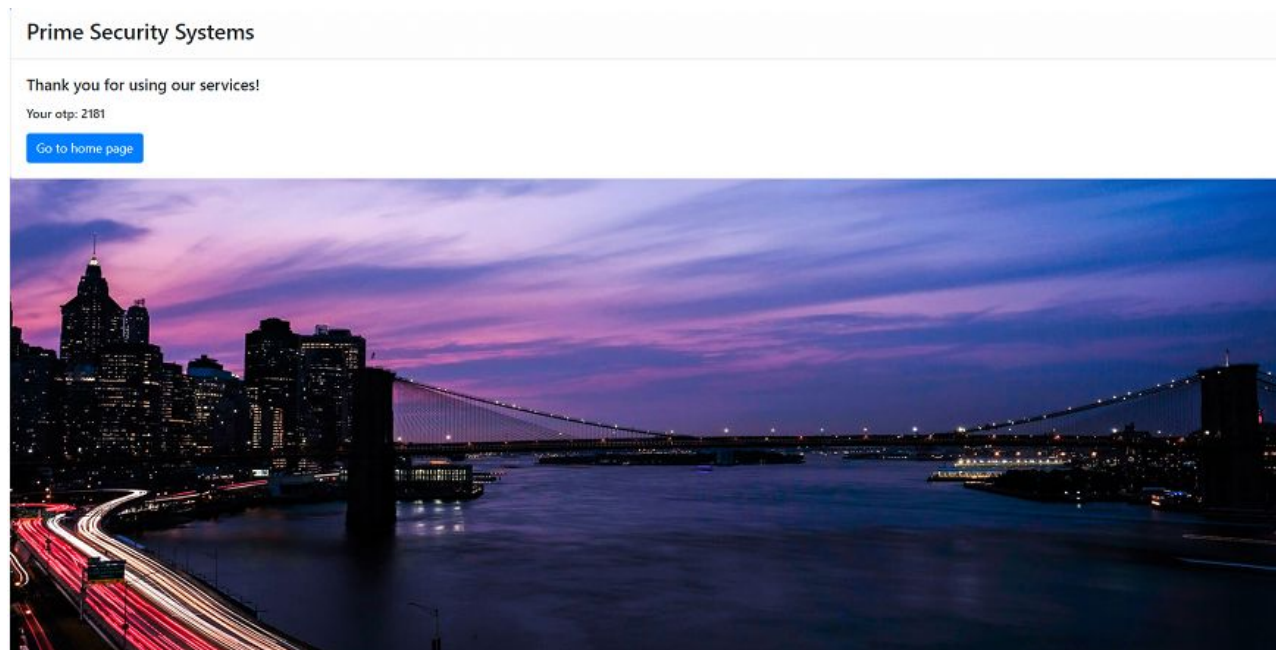
**Resident Application Working**

## 1. Home Page



In this PageThe president enters their private key and the received encrypted OTP from SMS In order to Decrypt it.

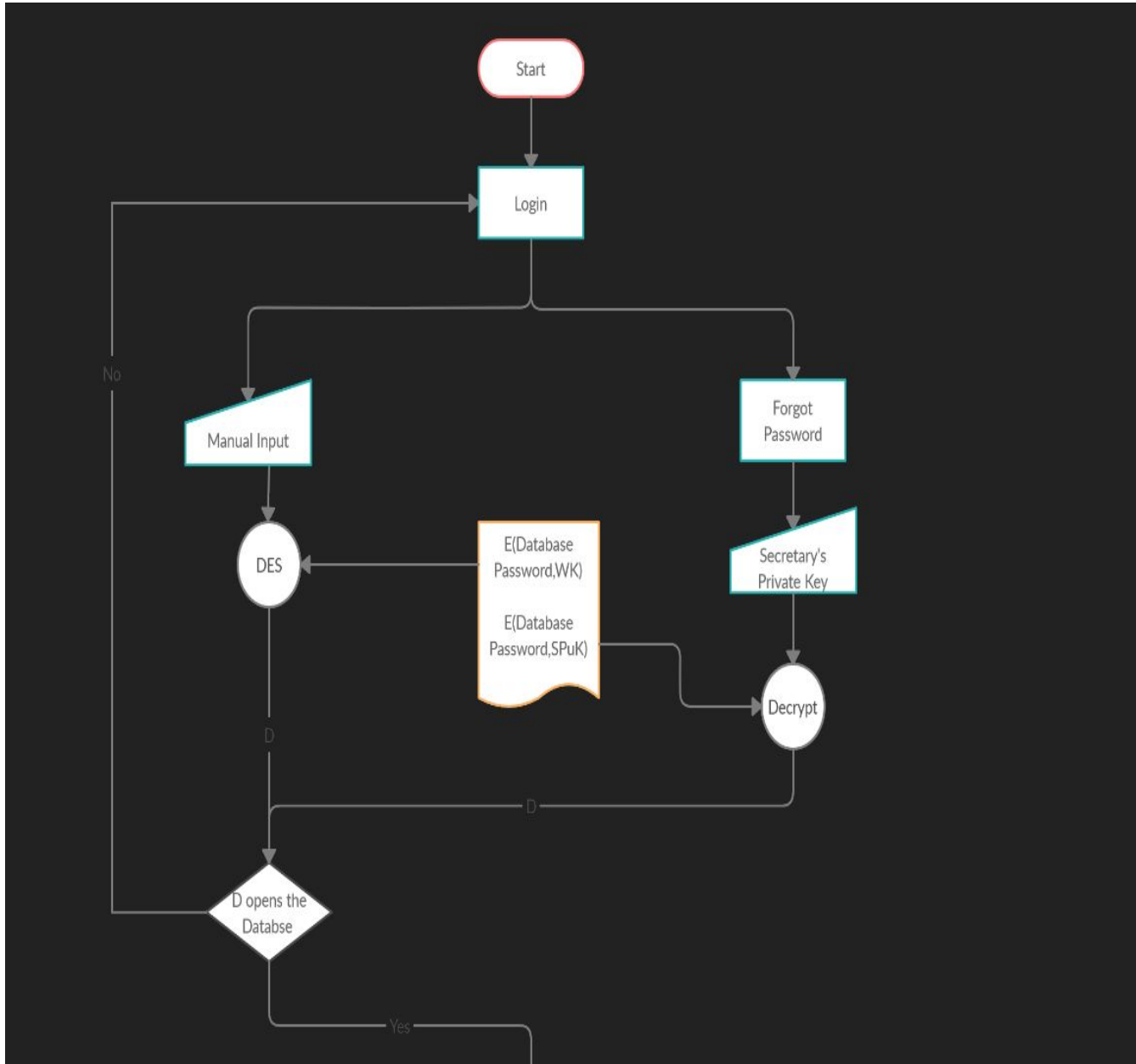
## 2.Decrypted OTP Page

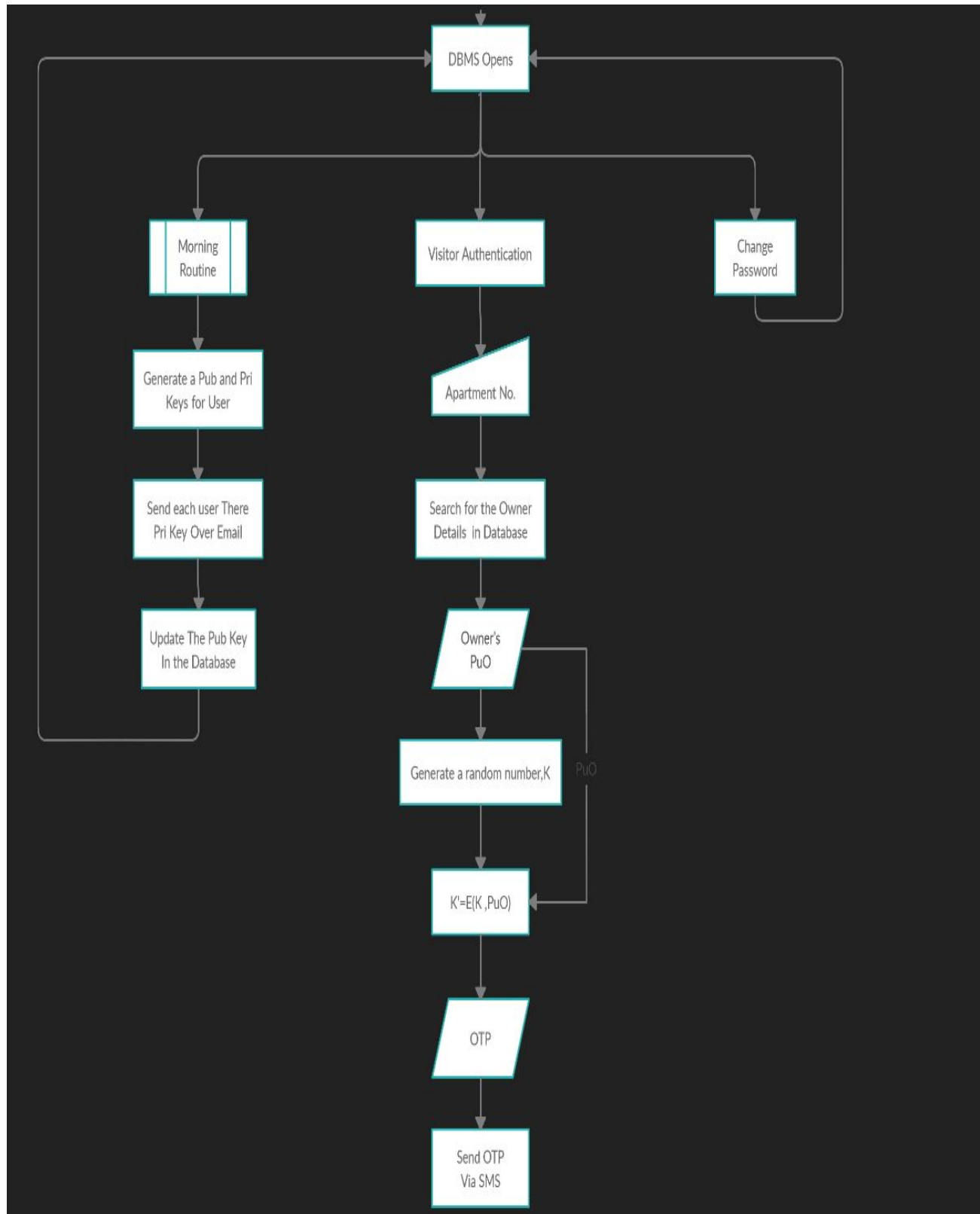


In this Page We get the Decrypted Plain Text OTP and tell this to the security guard in order to verify the Visitor

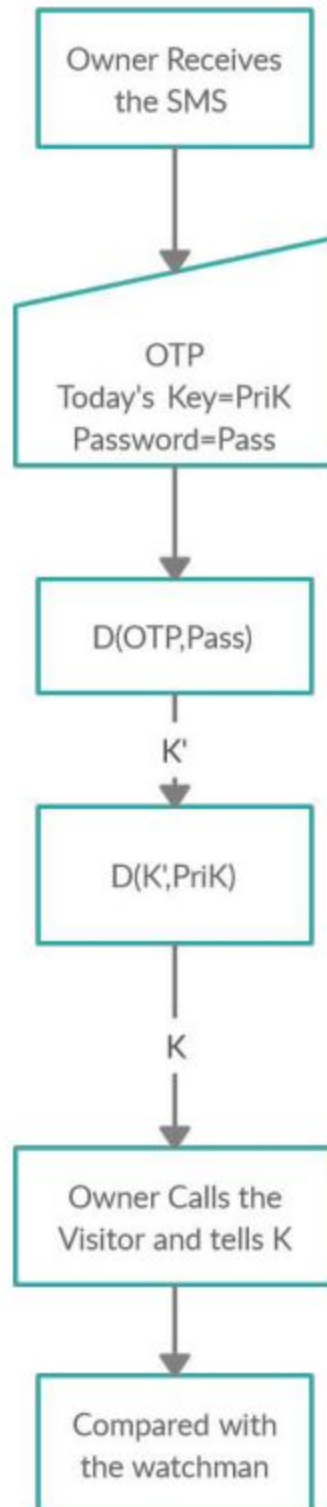
## Design and ER Diagram

Server Side Working





## Client Side Working -



Encrypted Data generated by the setup -








---

d80a33399bdea091  
c42092f993dcbda8  
88549d241226970c  
b447483801a0959c  
c08afc14afde30d3  
396ec530e186c814  
98766dee7a868900  
3570704a730a3cf4  
0eaec2bf988d3188  
65fbdb1986beafd8  
9f1916a1c6439309  
535402d89f914fa2  
1fb459c8477c97d9  
d4b9d59d2df4ec38  
870e76840362eb19  
b66c6a7e4396bff8

28399559 42292496 17203410 2156900 85830471 1771814 468

---

## Codes Used -

	__pycache__	02-11-2020 23:25	File folder	
	Application	02-11-2020 23:25	Python File (no co...	10 KB
	DATABASE	02-11-2020 23:25	SQL File	1 KB
	DES	02-11-2020 23:25	Python File	5 KB
	hexAndString	02-11-2020 23:25	Python File	2 KB
	Info File Generator	02-11-2020 23:25	Python File	1 KB
	RSA	02-11-2020 23:25	Python File	2 KB

Application.py - Contains the files for main working of the server end GUI Handled by the Security Guard and Admin to conduct Monthly routines and verify Visitors.

DATABASE Contains the queries used to make the SQL Database.

DES.py Consists of the DES encryption Algorithm Used to Encrypt the Database

jexAndString.py is used for hex to string and string to hex conversions for DES algorithm

InfoFileGenerator.py is run to initially setup a database to the server and encrypt all the data in it.

RSA.py Consists of The RSA Algorithm used to Encrypt the OTP using SHared public Key.

## Conclusion -

By using Our System Residents have an option in increasing the level of security enforced in their premises. It enables free, secured, fast and easy visitor registration.

1. Computerized records give better management and manipulation of data, through searching and report generation.
2. Its installation is easy and hence does not require professionals for the same. The system is easy to maintain and use.
3. It gives reliable and efficient security protection on which one can rely.
4. Unauthenticated and unwanted users cannot enter the Residential space.
5. Biometric functions can be coupled with the existing system to gain extra security

#### References -

- 1] Norizan Anwar, Mohamad Noorman Masrek, Yanty Rahayu Rambli, (2012), Visitor Management system by applying the model of UTAUT, Faculty of Information Management, Universiti teknologi MARA (UiTM) Selengor, Malaysia (IEEE).
- [2] Prof. Abhay Gaidhani 1 , Suraj Sahijwani 2 , Parag Jain 3 , Shantanu Jadhav 4, Ankush Jain 5, (2015), System for Visitor Pass. Department of Computer Engineering, Sandip, Institute of Engineering Management, Nashik.
- [3] M.N. Noorhuzaimi@Karimah, S. Junaida , A. Noraziah, K. Huei Chen Fakulti Sistem Komputer Kejuruteraan Perisian.(2009), Digital Visitor Information Management Systems (VIMS) Application and Design. Universiti Malaysia Pahang Karung Berkunci 12, 25000 Kuantan, Pahang.
- [4] Srinivas Nidhra, Likith Poovanna, Vinay Sudha Eithiraj, (2012), Visitor Management Schedule System- An Intelligent Decision Support System, School of Computing, Blekinge Tekniska Högskola, Karlskrona, Sweden