

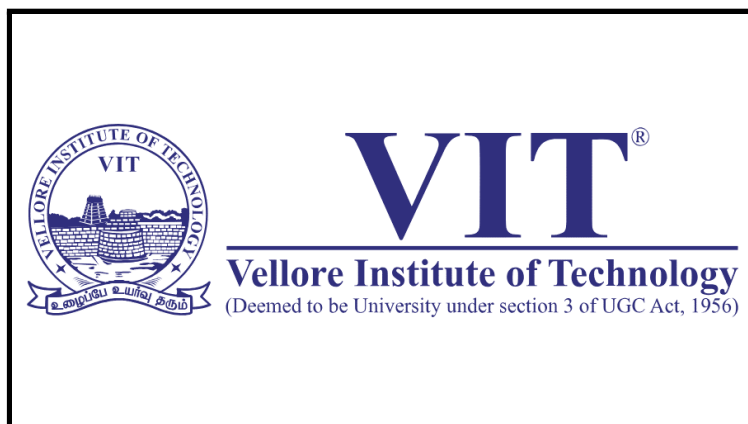
A Project Report on
Secure Data Encryption using Hash And RSA
Algorithms

Submitted in partial fulfilment for the award of the degree of
B.Tech (Computer Science and Engineering)
By

Raghav Jindal - 18BCE2080
Nimish Batra - 18BCE2087

Prepared For
CSE3502 - Information Security Management

Under the guidance of
Dr. Anil Kumar K
Associate Professor



SCHOOL OF COMPUTER SCIENCE & ENGINEERING
2021 - 2022

ABSTRACT

In the current scenario, Data Security is required to transfer confidential information over the network. In an inclusive range of applications, Security is also challenging. For data security Cryptographic algorithms play a vital role against spiteful attacks. In the popular performances of Public Key Infrastructures, **RSA** algorithm is extensively used and hashing technique. The core theme of the project focuses on the development of Security in ATM Transaction System in **Python using Hash and RSA algorithms**. The report contains the strategy used in making ATM Transactions, Comparison with different kinds of algorithm, advantages of Hash algorithm.

INTRODUCTION

The growth in electronic transactions has resulted in a greater demand for fast and accurate user identification and authentication .Over the past three decades, consumers have been largely depending on and trusting the Automatic Teller Machine (ATM) to conveniently meet their banking needs. However, despite the numerous advantages of the ATM system, ATM fraud has recently become more widespread. So it becomes a necessity to secure the confidential data of the user like personal identification numbers(PIN) and all the transactions . ATM card that is assigned a Personal ID Number (PIN). Hashing technique creates a unique encrypted result from a data set. The encrypted result is called a hash, a signature, or a digest, all of which mean the same thing. It is a one way hash, which means that the hash resulting from the algorithm is not meant to be unencrypted. For this reason we use it in ATM security. You have an ATM card that is assigned a Personal ID Number (PIN). The card provider used a hash algorithm to create a hash from your PIN which is stored on the card on a magnetic stripe. When the card is used, it is inserted into a slot on a machine, and the machine asks for the PIN. The user is expected to enter the PIN, which the machine uses to create a hash, which is then compared to the hash stored on the card. The user is not allowed to use the card if the two hashes do not match.

OVERVIEW

In ATM Transactions we only focus on ATM features and mainly on security. The feature transactions is a topic of deep interest in the Finance domain. The system should be good enough to represent the ATM in feature form. Features of an ATM are in two modules – admin and user. Admin module features include creation of new accounts, pin creation and updating them in the database. Admin module feature category includes taking the input profile information.

This method uses RSA and Hash function algorithms to implement this feature. This method is often termed as One way encryption method. Both these

methods fall under the admin module feature category. Then this data is decrypted to an information set that represents the user's bank information to the server. Encryption is a multistage technique. Encryption uses all the relevant information from the ATM output information that is given by a user that is to be sent to the server. It forms an encrypted text of the account number, where the output of others is sent to the server using RSA. User module features include pin updating, withdrawal, balance enquiry etc. The method used to encrypt this user information is RSA and hash function algorithm. We have implemented this system user friendly and totally secure to protect user information.

In the ATM transactions method, we can also implement SHA(Secure Hash Algorithm), MD5(Message Digest). ATMs are the most important part to maintain a user's financial life.

Attacks on various points

Digital banking faces many robbery cases which are divided into the following main categories: 1. Attack on the digital infrastructure for accessing information about different funds transfers. 2. Digital Infrastructure attack on ATM management 3. Clients Side attacks while performing e-banking

Attacks related to ATM

1. Fraud - Fraud is done by the usage of fake cards. Skimming is one of the method by which fraud is performed. The attackers install the skimmers in the ATM's card reading slots. These skimmers are not visible to the users of the ATM. The person coming for service of the machine checks these skimmers manually.
2. Physical -As the name suggests the attackers physically try to loot the cash out from the ATM. This is the most common attack. These are prevented from deploying security personnel for the ATM.
3. Logic -These attacks mainly include use of malware. Skimmer is one of the examples of the logic attack. The attacker tries to get the knowledge about the algorithm from which the bank is performing the transactions.

LITERATURE REVIEW

Studies on the topic state that [1] In the modern years the need for security has amplified many folds. It explains that the need to secure data is not new and goes way back to the time of 1st world war and even further back to the time of Julius Caesar. This paper provides a history of the data encryption techniques used in history and how they have developed from Caesar cipher to DES and from DES to Triple-DES, AES and recent algorithms. This study explained the pros and cons of earlier algorithms and why they aren't used today. The main focus of this paper is

initially general data hiding methods and then cryptographic algorithms. A brief study of a paper [2] presented a new Hybrid security algorithm for RSA cryptography named Hybrid RSA (HRSA). Here calculation of “public key” (P) plus “private key” (Q) depends on the value of M, i.e. the product of 4 prime numbers. So the difficulty involved in factoring the M increases. Another appealing feature about this algorithm is the fact that the computation of P and Q involves the calculation of some more midway factors which makes the calculation more complex. This approach eradicates the transfer of variable x and M, where x is the multiplication of 2 prime numbers a and b. Thus the proposed approach gives a more safe path for encryption and decryption procedure. To substantiate this statement, the “key generation time”, “encryption speed” and “decryption speed” of the proposed algorithm HRSA are compared with conventional RSA and ERSA techniques. Another research was referred to because of the use of a wireless medium in the project whose problem statement was [3], Security over Vehicular ad hoc network by means of Wi-Fi IEEE 802.11p standard and recognizing accurate attacker vehicles is a main challenge over VANET. Reducing costs of computation, effective expenditure of limited resources and giving uncompromised security was always a challenge over VANET. In this study, RSA algorithm based encryption and decryption techniques and implementation of limit with double RSU has been replicated using MATLAB software. Such background can be used while designing better MAC protocols, transmitting schemes, security features in VANETs. Providing confidentiality, message integrity, detecting and removing nasty and misbehaving nodes from VANET is the focus of this study.

The literature of behavioural studies on ATMs has mainly focused on adoption and diffusion of technology, impact of technology adoption from customers perspective, suppliers perspective, and bankers perspective [1].

Major Technology Adoption Models as per the study of Norris and Yin (2008), Technology Adoption Research is almost twenty-five years old and there are around eight important theories of adoption. All these eight theories are derived from the foundation of innovation diffusion and Technology acceptance model. The exception among eight models is the Social Cognitive Theory. Technology acceptance model is quite individual focused among eight adoption models. However, other models focus on how diffusion of innovation takes place within the firm. Oliveira and Maria (2011) have explored that there is a dearth of academic literature on reviews of adoption models at firm level used in Information Technology literature[1]. Author discussed Diffusion of Innovation Theory and Technology, Organization, and Environment (TOE)[7]. For more complex new technology adoption, it is important to integrate more than one theoretical model to achieve a better understanding of the adoption phenomenon. But in many cases, technology adoption research is a replication without substantive theoretical advances. However, there are sample opportunities to make theoretical advances using our current knowledge as the starting point[5]. These are the conclusions of the authors based on their review and comparison of major milestones of technology adoption research, Job Satisfaction

research and Theory of Planned behaviour. Most of the theories have emphasized on the factor influencing adoption behaviour and the process of diffusion of technology. These models also reveal the individual difference and cultural difference in technology adoption.

The first developed algorithm for the ATM transactions used to extract features of the bank, for e.g. Cash withdrawal, deposit or balance enquiry. These features were selected in a region form to perform transaction[4]. There was only simple encryption techniques used like for example play fair cipher technique. This method was good but didn't show great results because of less amount of cryptography used.

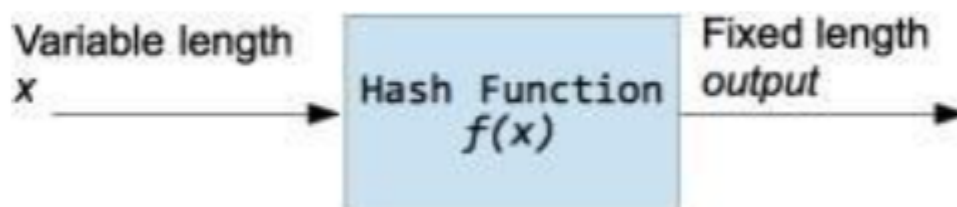
ALGORITHM USED IN OUR PROJECT

In the ATM Transactions system, we need to secure sensitive data of user like PIN, etc.

To maintain this security, we implemented this system cryptography using hash function and RSA algorithm.

HASH FUNCTION ALGORITHM

A hash function is a function that takes input of a variable length sequence of bytes and converts it to a fixed length sequence. It is a one-way function. This means if f is the hashing function, calculating $f(x)$ is pretty fast and simple, but trying to obtain x again will take years. The value returned by a hash function is often called a hash, message digest, hash value, or checksum. Most of the time a hash function will produce unique output for a given input. However, depending on the algorithm, there is a possibility to find a collision due to the mathematical theory behind these functions.



Hash functions are used inside some cryptographic algorithms, in digital signatures, message authentication codes, manipulation detection, fingerprints, checksums (message integrity check), hash tables, password storage and much more.

Some of the Hash function algorithm examples are : • MD5 SHA (SHA1,SHA224, SHA256,SHA384,SHA512)

RSA ALGORITHM

RSA algorithm is an asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. Public Key and Private Key. As the name describes, the Public Key is given to everyone and the Private key is kept private .

Key Generation: - 1. Generate two large prime numbers, suppose p & q . 2. $n = p * q$
3. $m = \Phi(n) = (p-1) * (q-1)$ 4. Choose a small number e , co-prime to m and $\text{GCD}(m, e) = 1$ such that $1 < e < \Phi(n)$ 5. Find d such that $(d * e) \bmod \Phi(n) = 1$

• Cipher text = (plain text) ^{e} mod n • Plain text = (Cipher text) ^{d} mod n

The ATM sends the pin using RSA encryption to the server. The Server decrypts that and uses a hash function for further processing.

PROPOSED METHODOLOGY

To implement ATM transactions we have divided our project into two parts. One module comprises the Administrator and the other one is the ATM.

The Admin module is responsible for creation of the database, and handling the customers. Admin module just assigns the card no to the individuals that come to open a new bank account. The bank balance is updated and stored in the database. There is no pre-assigned pin for the users; the user sets his pin on his own when he goes to the ATM for the first time.

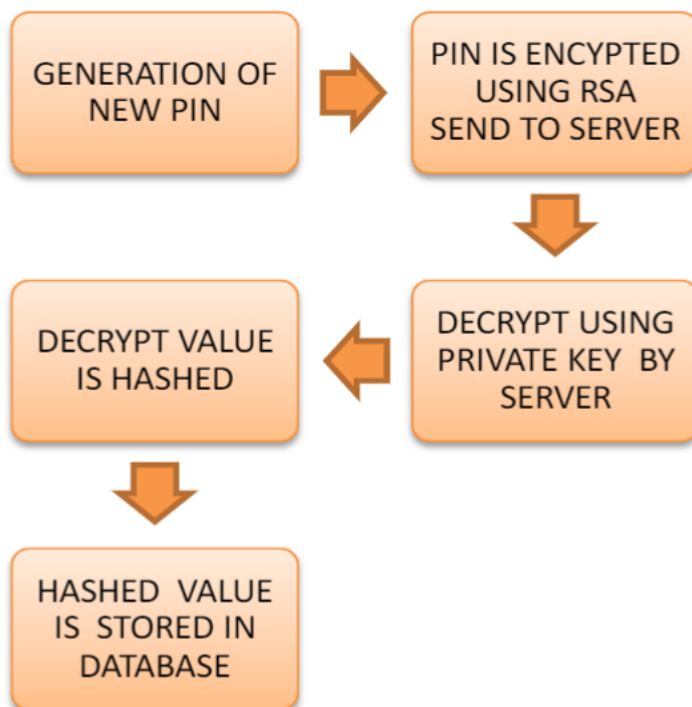
In the ATM when the user starts his transaction, the ATM sends the data to the server. The server then checks and compares them in the database. If the card number is wrong then it asks to enter the correct card else it asks for the pin.

If coming for the first time then it asks for the new pin generation else for his transaction code. The pin is encrypted by the RSA algorithm and sent to the Server, the server firstly decrypts the pin and then hashes the pin.

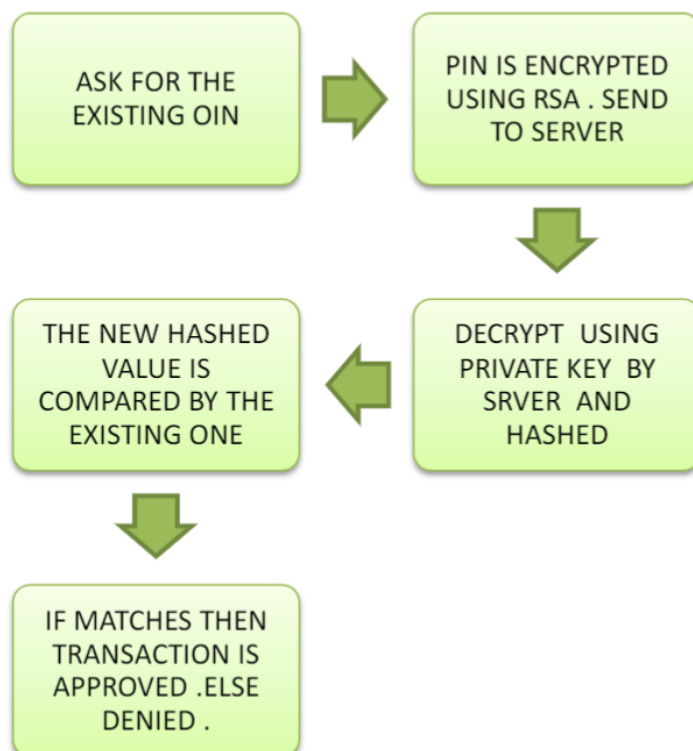
Hashing is used because it is one-way profile and no Man in the middle (MIM) attack can take place over it. If user comes for the first time, hashed pin is stored in the database. Else the hashed pin is then compared to the stored hashed pin. If the pin matches, it transacts the amount and the same is updated in the database.

If pin doesn't matches it asks for correct pin and aborts the transaction.

USER COMING FOR THE FIRST TIME



USER WANTS TO MAKE TRANSACTION IN THE EXISTING ACCOUNT



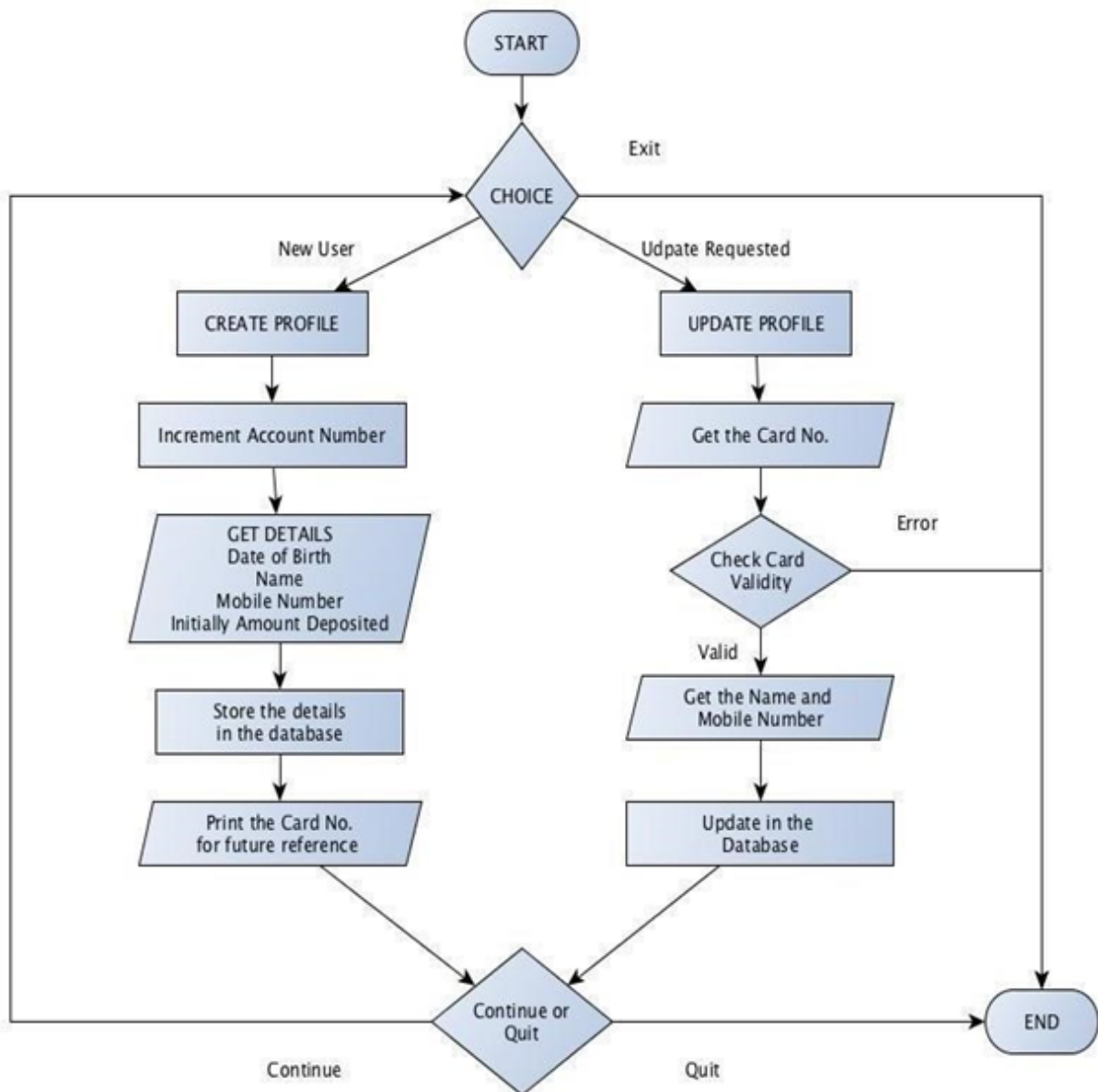
MODULE COMPONENTS:

In this Project, we will be using two modules : • Admin • ATM (user)

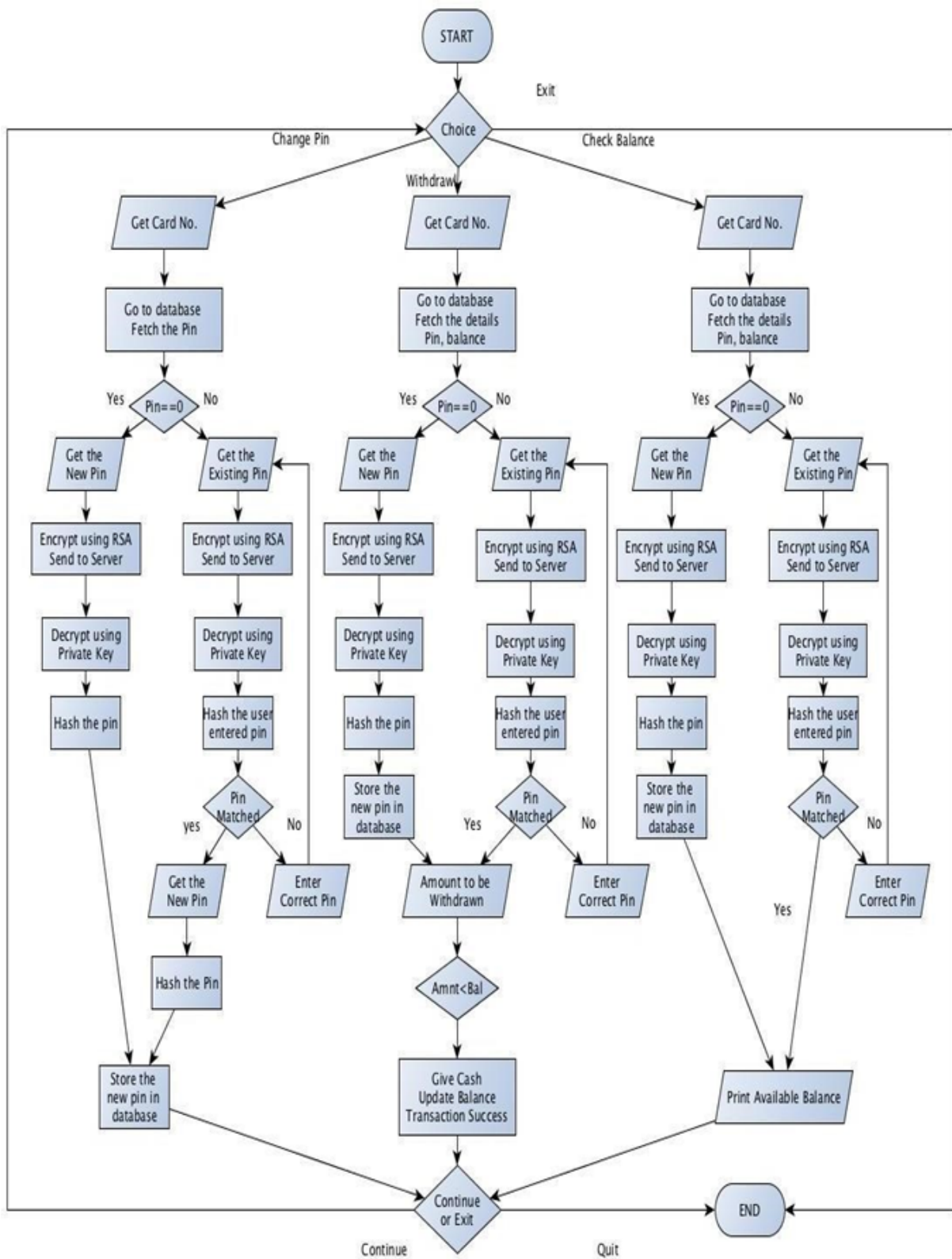
Admin

If there comes a new user, he needs to create a new account/profile where the account number will be given serial wise and the user needs to enter his/her personal details. The given details by user are stored in encrypted form in database. After creating new account, the new user is provided with the card number for using ATM service.

After creating and giving his/her details to the server, if he/she needs to update his/her details, he/she should enter card number to login and to check validity. He/she enter the updated details and the same details is updated in the database.



ATM (user)



ATM Services:

1. Update PIN
2. Withdrawal and update balance
3. Print Available balance

CODE :-

ATM.py

The image shows a Visual Studio Code editor with a Python file named `finalATM.py` open. The file contains a simple ATM system implementation. The code includes functions for encryption, decryption, and updating card details. The terminal output shows the program running and displaying a menu of options: 1. Withdrawal, 2. Check Balance, 3. Create or Charge Pin, 4. Exit. The user has chosen option 1, entered card number 632008 and pin 1234, and the program has successfully created a new pin 2345.

```

17 # AccountInfo.db
18 # PINA REPORT.pdf
19 # finalAdmin.py
20 # finalATM.py
21
22 def encrypt(p):
23     q=7
24     n=p*q
25     phi=(p-1)*(q-1)
26     for e in range(2,phi):
27         if gcd(e,phi)== 1:
28             break
29     f=2**e+1
30     g=n-1
31     for i in range(1,10):
32         x = 1 + 1*phi
33         if x % e == 0:
34             d = int(x/e)
35             break
36
37 def encrypt(msg):
38     c=(msg**e)%n
39     return c
40
41 def decrypt(c):
42     y=(c**d)%n
43     return y
44
45 def update(cardNo,pin):
46     conn=sqlitedb.connect("AccountInfo.db")
47     cmd="select * from details where Card_No='"+str(cardNo)+"'"
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100

```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL

2: python

Please choose among the following options:

1. Withdrawal
2. Check Balance
3. Create or Charge Pin
4. Exit

Enter your choice: 1

Enter the Card No.: 632008

Enter the pin: 1234

Enter amt to be removed: 20000

Enter a new pin: 2345

Pin Created Successfully

Do you want to continue:

1. Yes
- 2.No

Enter your Choice: []

Python 3.8.8 64-bit

meet.google.com is sharing your screen. Stop sharing Hide

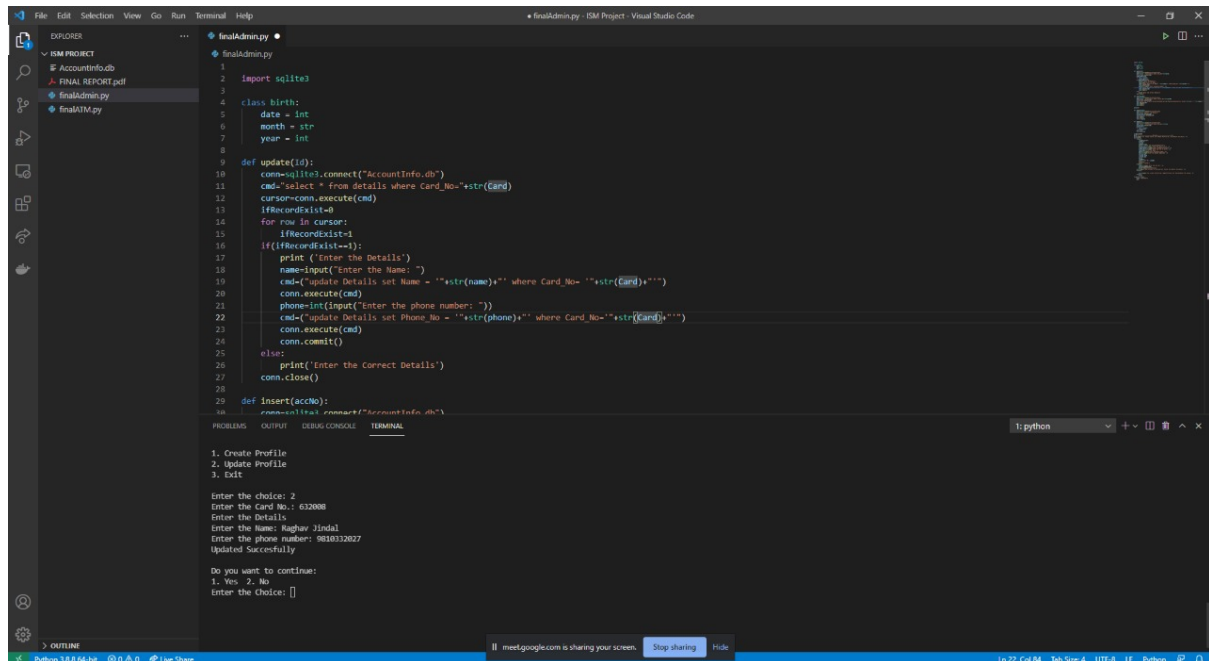
Ln 38, Col 20 Sources 1 UTF-8 Python

ADMIN.py

The screenshot shows a Visual Studio Code editor with a Python file named `finalAdmin.py`. The code is a simple web application for managing account information. It uses a SQLite database and a command-line interface. The terminal output shows the command `python .\finalAdmin.py` being executed, and the program prompts the user to enter details for a new profile. The details entered are: Day of birth: 12, Month of birth: october, Year of birth: 2000, Name: Raghuw Lalini, Phone number: 9686822004, Amount deposited: 1000000, Card No: 612008. The output ends with 'Created'.

OUTPUT :-

ADMIN.py



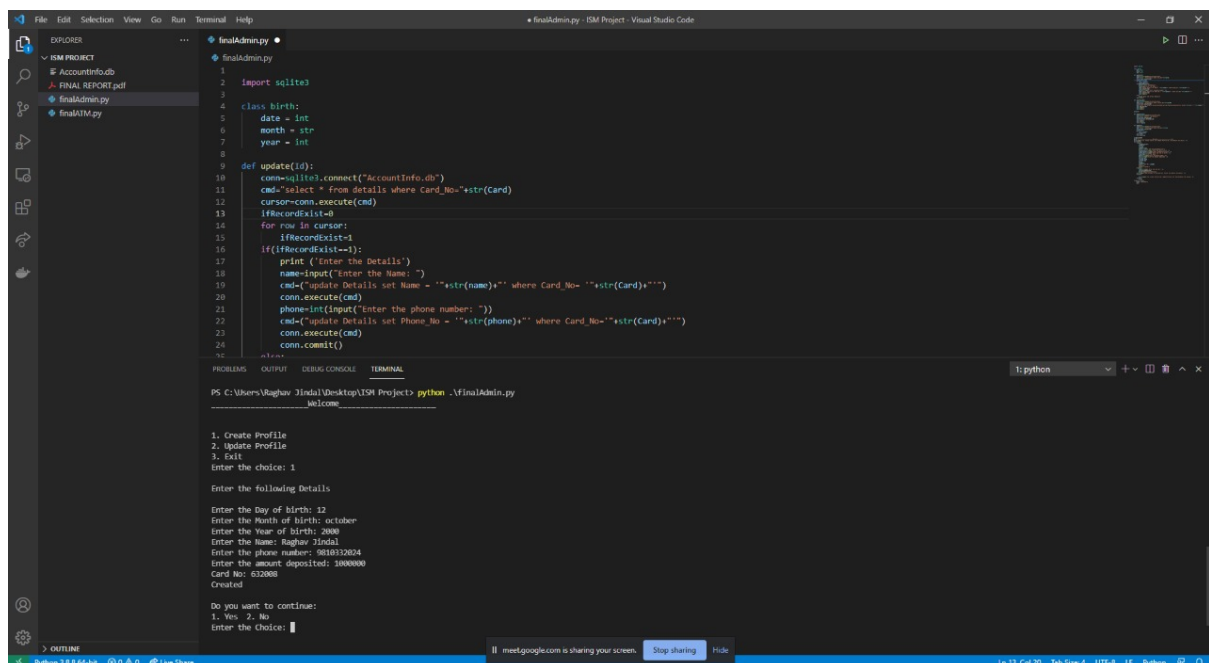
The screenshot shows the Visual Studio Code editor with the file `finalAdmin.py` open. The code defines a `birth` class with attributes `date`, `month`, and `year`. It includes an `update(id)` function that connects to a database, checks for record existence, and updates details if provided. The terminal output shows the program running and successfully updating a record.

```
1 import sqlite3
2
3 class birth:
4     date = int
5     month = str
6     year = int
7
8 def update(id):
9     conn=sqlite3.connect("AccountInfo.db")
10    cmd="select * from details where Card_No='"+str(Card)+"'"
11    cursor=conn.execute(cmd)
12    if RecordExist==0:
13        for row in cursor:
14            if RecordExist==1:
15                print('Enter the Details')
16                name=input("Enter the Name: ")
17                cmd=("update Details set Name = '"+str(name)+"' where Card_No='"+str(Card)+"'")
18                conn.execute(cmd)
19                phone=int(input("Enter the phone number: "))
20                cmd=("update Details set Phone_No = '"+str(phone)+"' where Card_No='"+str(Card)+"'")
21                conn.execute(cmd)
22                conn.commit()
23            else:
24                print('Enter the Correct Details')
25                conn.close()
26
27 def insert(accNo):
28     conn=sqlite3.connect("AccountInfo.db")
```

Terminal Output:

```
1. Create Profile
2. Update Profile
3. Exit
Enter the choice: 2
Enter the Card No.: 632008
Enter the Details
Enter the Name: Raghar Jindal
Enter the phone number: 9818332027
Updated Successfully
Do you want to continue:
1. Yes 2. No
Enter the Choice: []
```

ATM.py



The screenshot shows the Visual Studio Code editor with the file `finalATM.py` open. The code defines a `birth` class with attributes `date`, `month`, and `year`. It includes an `update(id)` function that connects to a database, checks for record existence, and updates details if provided. The terminal output shows the program running and successfully creating a new profile.

```
1 import sqlite3
2
3 class birth:
4     date = int
5     month = str
6     year = int
7
8 def update(id):
9     conn=sqlite3.connect("AccountInfo.db")
10    cmd="select * from details where Card_No='"+str(Card)+"'"
11    cursor=conn.execute(cmd)
12    if RecordExist==0:
13        for row in cursor:
14            if RecordExist==1:
15                print('Enter the Details')
16                name=input("Enter the Name: ")
17                cmd=("update Details set Name = '"+str(name)+"' where Card_No='"+str(Card)+"'")
18                conn.execute(cmd)
19                phone=int(input("Enter the phone number: "))
20                cmd=("update Details set Phone_No = '"+str(phone)+"' where Card_No='"+str(Card)+"'")
21                conn.execute(cmd)
22                conn.commit()
23            else:
24                print('Enter the Correct Details')
25                conn.close()
26
27 def insert(accNo):
28     conn=sqlite3.connect("AccountInfo.db")
```

Terminal Output:

```
PS C:\Users\Raghar Jindal\Desktop\ISM Project> python .\finalAdmin.py
Welcome
1. Create Profile
2. Update Profile
3. Exit
Enter the choice: 1
Enter the following Details
Enter the Day of birth: 12
Enter the Month of birth: october
Enter the Year of birth: 2000
Enter the Name: Raghar Jindal
Enter the phone number: 9818332024
Enter the amount deposited: 1000000
Card No: 632008
Created
Do you want to continue:
1. Yes 2. No
Enter the Choice: []
```

Account_No	Name	Card_No	Phone_No	Balance	Pin
1	1 Archit Goyal	632001	8708170952	11000	4814036714628610464
2	2 Sahil	632002	9478915417	20000	659473584131336959
3	3 Ayush	632003	9087612345	17000	4814037714606610416
4	4 Sanjana	632004	6379455237	56000	-4537751433782229301
5	5 Sneha	632009	9195527301	77440	4836789986166528717
6	6 ritika	632006	6379455237	23000	-7579529882229579058
7	7 Damodar sharma	632007	6767565657	2340000	0
8	8 Raghav Jindal	632008	9810332027	1000000	-6672160824449135408

Database updated after the user has set a PIN which is stored in the form of a hash value.

CONCLUSION:

We have made a Secured Data Encryption System using Python language and it is storing details in encrypted form of user ensuring security to user. The RSA technique used helps to prevent the third party from knowing the keys of the user. The Hash function prevents the Man in Middle attack. It can be implemented in the real world for personal uses.

REFERENCES

- [1] Jyotiranjana Hota, "Automated Teller Machines in India", Proceedings of GLOGIFT 13, Dec-2013
- [2] Oliveira, T. and Martins, M, F. (2011) Literature Review of Information Technology Adoption Models at Firm Level, The Electronic Journal Information Systems Evaluation, 14(1): 110-121.
- [3] Hota, J.R. (2013) Growth of ATM Industry in India, CSI Communications, 36(11): 23-25.

- [4] Agarwal, R. and Prasad, J. (1998) A Conceptual and Operational Definition of Personal Innovativeness in the Domain of Information Technology, *Information Systems Research*, 9(2): 204-215.
- [5] Identifiers for Digital Identity Management.
- [6] Laplante, P. A. (1977). *Real-time systems design and analysis* (2nd ed.). Washington, DC: IEEE Press.
- [7] Devinaga, R. (2010). ATM risk management and controls. *European journal of economic, finance and administrative sciences*. ISSN 1450-2275 issue 21.
- [8] Heather Crawford (2011). *Applying Usable Security Principles to Authentication*.
