

**SECURING ATM TRANSACTIONS
(CYBER SECURITY FOR CYBER PHYSICAL
SYSTEMS)**

CSE3502

Information Security Management

F1-TF1

J – Component Project

by

**CHIRAG JAIN 18BIT0008
MAHAK GUPTA 18BIT0041
MUSKAN SAHNI 18BIT0382**

under

Prof. PRIYA V.



VIT[®]
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

ABSTRACT :

ATMs allow to make deposits and withdraw money and even you can print a statement, view your account balance and even transfer money between your accounts. ATMs, if properly secured, are safe and most convenient way to manage our money. To protect our money and transaction we need to safeguard them from different type of attacks. Nowadays due to development in technology, new ATM machines are being built up with more and more security. But to destroy this security level, threats are being imposed. Regardless of enhancement in the automation, still ATM are prone to thefts and frauds.

TABLE OF CONTENTS :

S.No.	CONTENTS	PAGE No.
1.	Problem Statement	4
2.	Literature Review	5-17
3.	Case Study of Canara Bank	18-19
4.	Techniques Used	19
5.	Expected Outcome	19
6.	Proposed Model	20
7.	Man In The Middle Attack	21-26
8.	Elgamal Encryption	27-36
9.	Conclusion	36
19.	Result	36-38

PROBLEM DEFINITION:

Cryptography has become the most widely used network security technique due to its incomparable efficiency and applications in the field of network security. The applications of cryptography not only includes confidentiality but also user authentication, integrity and much more. Applications of cryptography is everywhere whether it be a WhatsApp text message or a banking transaction. In our project : We have discussed about the security measures that takes place when a client makes a transaction in the ATM machine. So, what happens behind the scenes is when the customer inserts the card, the machine reads the card details present in the magnetic tape of the card which travels to banks server in encrypted format to preserve confidentiality, then the user is prompted for the PIN which is stored in the banks database but in the encrypted format, to be more precise hashed format. The need for storing the PIN in the hashed format which is irreversibly encrypted is because in case of some unfortunate data leak even if the PIN gets in the wrong hands the money in the bank remains safe, and the same we have implemented in this project by integrating the concept of Elgamal encryption with the SHA-512 authentication to provide additional security to the PIN generated for the ATM users.

OBJECTIVES:

- ❖ To review the literature on the impact of adoption of ATM technology from the perspective of customers, banks and suppliers.
- ❖ To provide additional security to the PIN generated for the ATM.
- ❖ Implement Man in the Middle Attack
- ❖ Protect from Man in the Middle attack.
- ❖ Comparison of different kinds of algorithm and the advantages of Hash algorithm to find the better of three.

LITERATURE SURVEY

1. Karovaliya et al,2015

The purpose of this paper is to reinforce security of the conventional ATM model. New concept that enhances the overall experience, usability and convenience of the transaction at the ATM. To completely eliminates the chances of fraud due to theft and duplicity of the ATM cards Techniques Used: Features like face recognition and One-Time Password (OTP) are used for the enhancement of security of accounts and privacy of users. Face recognition technology helps the machine to identify each and every user uniquely thus making face as a key. Moreover, the randomly generated OTP frees the user from remembering PINs as it itself acts as a PIN.

How model works:

First, the user will swipe the ATM card. A live image is captured automatically through a webcam installed on the ATM, which is compared with the images stored in the database. If it matches, an OTP will be sent to the corresponding registered mobile number. This randomly generated code has to be entered by the user in the text box. If the user correctly enters the OTP, the transaction can proceed. Therefore, the combination of face recognition algorithm and an OTP drastically reduces the chances of fraud plus frees a user from an extra burden of remembering complex passwords. **Cryptographic hash functions:**

Various Cryptographic hash functions are used to improve the security level. MD5 also known as Message Digest because it is widely used hash function. Since, it is the fastest cryptographic hash function, it is convenient to use MD5 and is mostly accepted by a wide variety of platforms.

Comparison:

The existing ATM model uses a card and a PIN which gives rise to increase in attacks in the form of stolen cards, or due to statically assigned PINs, duplicity of cards and various other threats. To overcome, hybrid model which consists of conventional features along with additional features like face recognition and one-time password (OTP) is used. Database holds information about a user's account details, images of his/ her face and a mobile number which will improve security to a large extent.

Future Scope:

Facial recognition technique seems more challenging as compared to other

biometrics, thus more efficient algorithm can be developed. The flaws in face recognition technique like the inability to detect face when beard, aging, glasses and caps can be rectified and eliminated or reduced. If the cost of retina or iris recognition reduces, it can be used instead of face recognition.

2. A Review on Secure ATM by Image Processing ,2016

Every biometric system has its limitation. Therefore, identification based on multiple biometrics is an emerging trend as multimodal biometrics provides a more balanced solution to the security multimodal systems involve the use of many biometric systems.

Concepts used in Paper:

This paper proposes an ATM security model that would combine a physical access card, a pin and electronic facial recognition. It encloses the information regarding the 'image processing'. And discussed one of the major application of image processing 'biometrics'. Biometrics technology turns your body in to your password. It discussed various biometric techniques like finger scan, retina scan, facial scan, hand scan etc

Algorithm:

Algorithm takes customer's picture(s) when account is opened and allow user to set nonverified transaction limits At ATM, use access card and PIN to pre-verify user Take user's picture, attempt to match it to database image(s) If match is successful, allow transaction If match is unsuccessful, limit available transactions.

With new improved techniques like Artificial Intelligence security margin can be increased from simple 60-75% to 80-100%. Thus an ATM model can be developed that is more reliable in providing security by using facial recognition software. This type of security model can be used to minimise ATM frauds.

3. Mahajan et al,2016

The gains of technology brought about by the advent of Automated Teller Machines (ATMs) cannot be over-emphasized. Whatever benefits accruable to parties are almost lost through frauds perpetrated through card-related transactions on ATMs. This paper presents a solution of still enjoying the dividends of ATM through combined biometric features at the expense of cards and its attendant vulnerabilities.

Techniques Used:

Automated Teller Machine by the use of biometrics is proposed in this paper.

How the model works:

The combined biometric features approach is to serve the purpose both the identification and authentication that card and PIN do. While iris replaces the card, fingers are used to do the authentication. Thus, the existing card present transactions can be reliably carried out at the ATM site only by the authentic owner.

Comparison between old techniques and the proposed way:

To use an ATM presently, demands having a card that has to be authenticated by PIN as a second factor authentication. To aid memory, some users write their PINs in diaries or store them on some other unprotected devices. The moment the card is accessible, PIN is guessed or obtained through other means such as social engineering, shoulder surfing or outright collection under duress.

Recently, Biometric ATMs are introduced to be used along with card. When, in place of cards, some biometric features such as iris, retina scans or face are captured and further authentication is done by palm or finger print, then ATM transactions cannot be done except by the authentic owner of the account.

4. Jacobs et al, 2011**Techniques Used:****SmartCards:-**

A smartcard is a tiny computer, contained on a single chip. Traditionally these chips were embedded in a piece of plastic the size of a credit card, but over the years variations in form and appearance have been introduced. Smartcards are the natural choice for secure storage of biometric information. The card can protect the information, it cannot easily be cloned, and even if a card is lost or stolen, the protection it provides remains in place.

Performance and Quality:

Biometric systems are not perfect. When trying to match a stored biometric with one freshly obtained, there is always the chance of false matches and false non-matches. A false match occurs when the system reports a match when in fact the stored biometric comes from someone else. A false non-match occurs when the system reports that the two don't match, even though both are from the same person. False

matches are often called false accepts, and false nonmatches false rejects, but beware that this terminology can be confusing: if a database of biometrics is used to check that known terrorists do not enter the country, then a false nonmatch leads to a false accept (into the country), not a false reject.

5. Practical Attacks on Proximity Identification Systems,2006

The number of RFID devices used in everyday life has increased, along with concerns about their security and user privacy. This paper describes initial findings on practical attacks that are implemented against 'proximity' (ISO 14443A) type RFID tokens. Focusing mainly on the RF communication interface paper discuss the results and implementation of eavesdropping, unauthorized scanning and relay attacks.

Techniques:

RFID is a collective term for near field communication devices and in reality refers to devices adhering to a number of different standards. In the HF band interfaces have been standardized for "proximity" (ISO 14443 [12]), "vicinity" (ISO 15693 [13]) and "near field" (NFCIP1/ECMA340, ISO 18092 [15]) devices, with maximum operating ranges in the order of 10 cm to 1 m.

Relay Attacks:

Relay attacks cannot easily be prevented by cryptographic protocols that operate at the application layer of an RFID protocol stack. An attacker executing a relay attack cannot avoid causing a delay in the system.

6. COMPARISON OF VARIOUS BIOMETRIC METHODS,2014

This paper presents comparison concerning various biometric systems simply by defining their advantages and disadvantages. A brief introduction is usually offered regarding commonly used biometrics, including, Face, Iris, Fingerprint, Finger Vein, Lips, Voice. The comparison criteria list introduced is restricted to accuracy, size of template, cost, security level, and long term stability. **Techniques Used:**

1) Facial recognition involves an evaluation of facial features. It is a computer system application for automatically determining or verifying an individual from a digital image or a video framework from a video source. One of the techniques to do this is simply by evaluating selected facial features from the image as well as from facial database.

2) Iris recognition offers one of the most secure strategies of authentication and recognition. Once the impression of an iris has been taken using a standard digicam, the authentication process involves, evaluating the present subject's iris with stored version. It is one of the most accurate technique with very low false acceptance as well as rejection rates. This is how the technology becomes very useful

3) Voice recognition is a technology through which sounds, phrases and words voiced by human beings are transformed into electrical signals, and then these signals are converted into code design.

7. Frimpong et al,2016

A huge number and type of systems need reliable personalized recognition system to either authorize or determine the identity of an individual demanding their services. The motive of using a system like this is to warrant that the left out services are accessed only by an authentic user and no other person is able to access it. In the absence of robust personal recognition schemes, these systems are vulnerable to the deceptions of an imposter. The proposed system demonstrates a three tier design structure. The first level is the verification unit, which focuses on the enrollment phase, enhancement phase, feature extraction and matching of the fingerprints. The second tier is the database end which acts as a storehouse for storing the fingerprints of all ATM users' preregistered as templates and PIN as text. The last tier showcases a system platform to relate banking transactions such as balance inquiries, mini statements and withdrawal.

The basic idea of this paper is to introduce multiple authentication levels in order to increase the security and make the system more immune to attacks.

The metrics used for its effectivity are:

- ❖ False Accept Rate (FAR)
- ❖ False Rejection Rate (FRR)
- ❖ Equal error rate (EER)

The algorithm is of the flow: pin verification followed by a fingerprint verification while keeping in track of the total number of attempts (here 3). If both levels are passed the access is granted.

The results depicted in this paper are:

The proposed fingerprint and PIN system has an overall efficiency of 94%, FAR 4%, FRR 2%, TER 6% and GAR 98%. The results are promising but the FAR values is a concern .Though 4% might seem a small number but for a big enough sample space since the ATMs are used 24*7*365 in multiple regions a failure rate of 4 % can result in about thousands of failed authentic transactions in a day. Hence scalability is a major issue. Moreover addition of fingerprint might seem a good idea, but it is an expensive process to implement from scratch and there are multiple methods to forge a fingerprint.

8. Onyesolu et al,2012

The authors here have conducted a survey on the usage margins of various biometrics which can be used for a single level authentication. The increase in ATM transactions lead to increase in demand for efficient and accurate user identification and authentication. One time passwords and access codes for buildings, banks accounts and computer systems often use personal identification numbers (PIN's) in order to get security clearance from the authority. Conventional method of identification based on possession of ID cards or exclusive knowledge like a social security number or a password are not all together reliable.

An embedded fingerprint biometric authentication scheme for automated teller machine (ATM) banking systems is proposed in this paper. In this scheme, a fingerprint biometric technique is fused with the ATM for person authentication to ameliorate the security level. Popular methods of authentication based on possession of ID cards or exclusive knowledge like a social security number or a password are not all together reliable. If one's ID is stolen or one forgets the PIN then it is a tough process to recover it back but the biometric identity is more or less unique and always remain with the person, this fact forms the basis for this paper.

9. De Luca et al,2010

The various methods discussed in the above two papers are usually on efficiency, security, and memorability in comparison with traditional PIN entry systems. It remains unclear, however, what appropriate values for PIN-based ATM authentication actually are. We conducted a field study and two smaller follow- up studies on real-

world ATM use, in order to provide both a better understanding of PIN-based ATM authentication, and on how alternative authentication methods can be compared and evaluated. The results of this paper point that there is a huge effect of contextual factors on security and performance in PIN based ATM use. Some factors are dependent upon human nature and his physical. The data for the primary field observation is collected over a period of two months. Each ATM was at least visited four times, with at least one observation session on a Sunday and at least one session during "rush hour" (i.e., mid- mornings, noon, or early evenings). This was to ensure that the data collected was as broad as possible and did not, e.g., only include off- peak times, which could have biased the results. Rush hours and off-peak times were identified in pre- observations. Depending on the location (e.g. close to a supermarket) these times differed not only between cities, but also between locations within the cities.

For instance, the rush hour close to a supermarket was between 5pm to 7pm while the rush hour at an ATM in a pedestrian area with shops and restaurants was during lunch time (around 1pm).

The limitation of the survey are that to get the info the users have to be disturbed from general course as it is not collected from a specific focus group and hence dependent upon many human factors.

10. Porretti et al,2016

The authors of this paper have described a new vision for ATM Security Management that is proposed by the GAMMA project, and implemented by its "core" prototype called Security Management Platform. The GAMMA method can be shortly described as a network of distributed nodes built within the ATM system and providing interfaces to (ATM) internal and external as well as internal users.

GAMMA establishes **three different levels for managing security**:

- ❖ the European level represented by the European GAMMA Coordination Centre (EGCC)
- ❖ the National level represented by the National GAMMA Security Management Platform (NGSMP)
- ❖ the Local level represented by local security systems as well as Local GAMMA

11. Hota et al,2013

The articles were categorized under two main themes- Adoption of ATM Technology and Impact of Adoption of ATM Technology. Impact of ATM Technology is further categorized into three sub themes- Customer's Perspectives, Bank's Perspectives and Supplier's Perspectives. This study reveals that there is a dearth of academic literature on Multi-Vendor ATM Technology in developing countries .The ATM Software is to be customized with the help of personalized Technology option so as to fulfil the needs of multiple cultures in countries like India. Popularizations of biometric and multilingual ATMs are also required in Rural Areas

The purpose of this paper is to review literature on the impact of adoption of ATM technology from the perspective of customers, banks and suppliers. As per the changing demand of the customers, innovative software solutions are regularly released. Similarly, banks are deploying CRM technology to facilitate personalized needs of customers on one to one basis. Suppliers of ATMs are also under pressure to provide ATMs to banks which can meet the latest customer needs. 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.

12. Isaac kofi et al,2016

In this paper, the authors have proposed a multifactor (PIN and Fingerprint) based authentication security arrangement to enhance the security and safety of the ATM and its users. The proposed system demonstrates a three-tier design structure. The first tier is the verification module, which concentrates on the enrolment phase, enhancement phase, feature extraction and matching of the fingerprints. The second tier is the database end which acts as a storehouse for storing the fingerprints of all ATM users preregistered as templates and PIN as text. The last tier presents system platform to relate banking transactions such as balance inquiries, mini statements and withdrawal.

13. Madhuri More et al,2018

In this research paper, the authors have proposed an enhanced feature to improve the service of ATM cash withdrawal in less time with more level of security. It proposes to combine the ATM & Mobile banking to reduce the time of withdrawal, increasing the level of security by adding a new feature in the Mobile banking.

14. Kavita Hooda et al ,2016

In this paper, the author has followed an intuitive approach to introduce biometric authentication technique in ATM systems, i.e., face recognition technique from 3 different angles using high resolution camera. Although various biometric techniques like fingerprint, eye recognition, retina and iris recognition have been devised as an authentication method for ATM machines, there is still a need to enhance the security in ATM systems to overcome various challenges. She has focused on designing a module of an ATM simulator based on face recognition from 3 different angles in order to minimise frauds associated with the use of ATM systems.

Prachi More et al, 2016[15]

In this paper, the author has presented a survey of different technologies for ATM security. However, in these technologies, there are some limitations. By comparing various technologies which are used for ATM security, the author has observed that fingerprint technology appears to be better and more secure than the other technologies.

Serial No	Title of Paper	Author Name	Year of Publishing	Journal	Merits
1	Enhanced Security for ATM Machine with OTP and Facial Recognition Features	1. Karvaliya 2. Mohsin 3. Karedia	2015	W7 gives better encryption results in terms of security against statistical analysis attacks	Enhances the overall experience, usability and convenience of the transaction at the ATM

2	A Review on Secure ATM by Image Processing	1. Shiven dra Dwivedi 2. Ranjana Sharma	2016	International Conference on Advanced Computing	ATM model can be developed that is more reliable in providing security by using facial recognition software. This type of security model can be used to minimise ATM frauds.
3	New Approach in Biometrics to Combat the Automated Teller Machine Frauds: Facial Recognition	1. Mahajna 2. Priyanka	2016	International Journal Of Engineering And Computer Science.	The existing card present transactions can be reliably carried out at the ATM site only by the authentic owner.
4	Biometrics and Smart Cards in Identity Management	1. Bart Jacobs 2. Erik Poll	2011	Computer Security Journal	The card can protect the information, it cannot easily be cloned, and even if a card is lost or stolen, the protection it provides remains in place.
5	Practical Attacks on Proximity Identification Systems	1. Yicon g Zhou 2. Karen Panetta	2009	Proceedings of the 2006 IEEE Symposium on Security and Privacy	An attacker executing a relay attack cannot avoid causing a delay in the system.
6.	COMPARISON OF VARIOUS BIOMETRIC METHODS	1. N. Ranjana 2. R. Sai ni	2014	International Journal of Advances in Science and Technology (IJAST)	we can easily identify a person in a crowd and by so we can verify their identity

7	Improving Security Levels In Automatic Teller Machines (ATM) Using Multifactor Authentication	1. Twum, Frimpong 2. Isaac kofi 3. Asante Michael	2016	International Journal of Science and Engineering Applications	They increase the security and also system more immune to attacks
8	Secret data communication system using Steganography, AES and RSA	1. Onyesolu Moses 3. Ezeani, Ignatius	2012	International Journal of Advanced Computer Science and Applications.	fingerprint biometric technique is fused with the ATM for person authentication to ameliorate the security level.
9	Towards understanding ATM security - A field study of real world ATM use	1. De Luca 2. Alexander 3. Langheinrich 4. Hussmann, Heinrich	2010	ACM International Conference Proceeding Series.	Enhanced the security features which are "built in" into the authentication mechanism. That is, the security of a system should not rely on active secure behavior of a user.
10	A New Vision for ATM Security Management: The Security Management Platform	1. C. Porretti 2. R. Lahaije 3. D. Kolev	2016	International Conference on Availability, Reliability and Security	They described a new vision for ATM Security Management is gamma project that implemented by the federated architecture of the Security Management Platforms

11	Steganography using RSA Algorithm	1. Hota, J.R	2013	Growth of ATM Industry in India, CSI Communication	1.Its easiness and portability make it different from other available tools.
12	Improving Security Levels In Automatic Teller Machines (ATM) Using Multifactor Authentication.	1. Twum 2. Frimpong 3. Isaac 4. Asantefi 5. Michael	2016	International Journal of Science and Engineering Applications	proposed a multifactor (PIN and Fingerprint) based authentication security arrangement to enhance the security and safety of the ATM and its users.
13	Cardless Automatic Teller Machine (ATM) Biometric Security System Design Using Human Fingerprints .	1. Madhuri More 2. Sudarshan Kankal 3. Akshay Kumar 4. Rupali Adhau	2018	International Journal of Advance Engineering and Research Development	proposed an enhanced feature to improve the service of ATM cash withdrawal in less time with more level of security.
14	ATM Security	1. Kavita Hooda	2016	International Journal of Scientific and Research Publications	Author has focused on designing a module of an ATM simulator based on face recognition from 3 different angles in order to minimise frauds associated with the use of ATM systems.

15	Survey of Security of ATM Machine	1. Prac hi More 2. Dr. S.D. Markand e	2016	International Journal of Advanced Research in Computer and Communication Engineering	According to authors observation fingerprint technology appears to be better and more secure than the other technologies.
-----------	---	--	------	---	--

ENCRYPTION USED IN CANARA BANK :

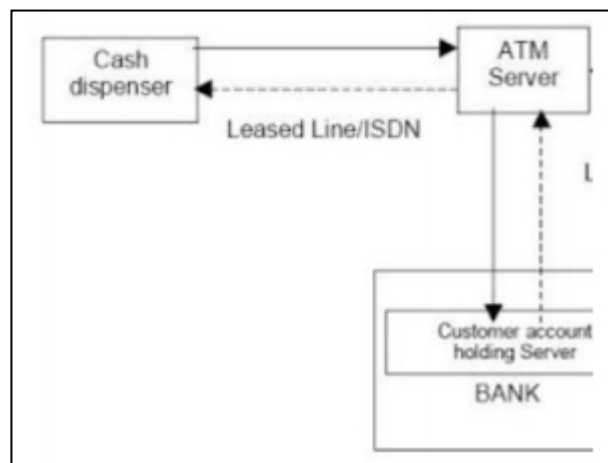
Canara bank encryption methodology used is 256 bit AES technology. Mostly bank's do not share technique of encryption because attacker can directly use that technique to hack the bank system.

So according to our research :

ATM PIN VALIDATION :

The following components are involved in an ATM transaction:

- ❖ The ATM machine cash dispenser. This is the machine where you plonk your card, punch your pin and pluck out the cash.
- ❖ The ATM server. This is the server that the ATM machine connects to behind the scenes. The ATM card number and the pin are sent to this server encrypted using 256 bit AES and shared secret key between the ATM machine and the ATM server. The ATM server verifies the PIN by decrypting it and verifying it from database and does the transaction by sending the request to your bank.



AES stands for Advanced Encryption Standard and is a majorly used symmetric encryption algorithm. It is mainly used for encryption and protection of electronic data.

Is AES 256 crackable?

AES 256 is virtually impenetrable using brute-force methods, AES would take billions of years to break using current computing technology. Hackers would be foolish to even attempt this type of attack. Nevertheless, no encryption system is entirely secure. Researchers who have probed AES have found a few potential ways in. In 2009, they discovered a possible related-key attack. This type of cryptanalysis

attempts to crack a cipher by observing how it operates using different keys. Fortunately, the related-key attack is only a threat to AES systems that are incorrectly configured.

Since the AES cipher itself is so secure, the main risk comes from side-channel attacks. These don't attempt a brute-force assault, but rather try to pick up information the system is leaking. Hackers can listen in to sounds, electromagnetic signals, timing information, or power consumption to try to discover how the security algorithms work. Through cache side-channel attack attacker is able to recover the encryption key. Side-channel attacks can be prevented by removing information leaks or masking the leaked data so it doesn't yield any useful information. A careful implementation of AES will guard against these side-channel risks. AES256 is a symmetric key algorithm, meaning each recipient must receive the key through a different channel than the message where there are chances of attack.

How our model is addressing these attacks on 256 bit AES :

- ❖ AES is a symmetric algorithm hence single encryption key has to be passed from sender to receiver ,which is not a case in asymmetric algorithm(Elgamal).
- ❖ We have integrated the concept of Elgamal encryption with the SHA-512 authentication to provide additional security to the PIN generated for the ATM users. The user enters the 4-digit PIN which is then encrypted using the Elgamal encryption technique following which it is converted into its corresponding hash value using the SHA-512 algorithm. This message digest is then finally sent to the server, where it is then compared with the existing hash values in the directory. So even if the attack happens during transmission through channel , attacker will get hashed values and as we know SHA is irreversible hence attacker cannot retrieve the original message(useful information) from these hashed values.

TECHNIQUES TO BE USED & EXPERIMENTAL SETUP:

- ❖ EterCap
- ❖ Elgamal Encryption SHA – 512

Basically we have integrated both the concepts.

Language Used :

Python Platform Used: Python Idle

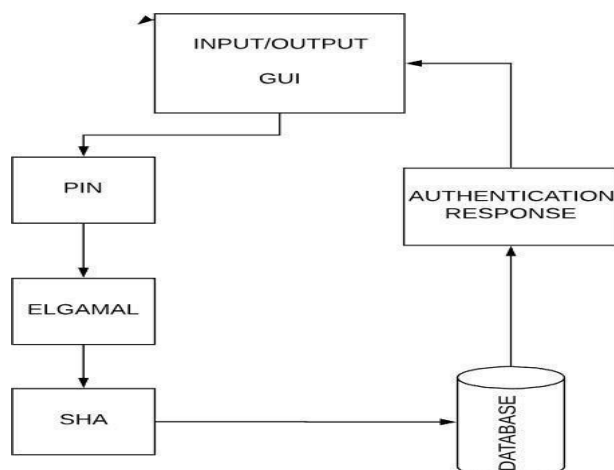
EXPECTED OUTCOME:

- ❖ We will successfully implement Man In The Middle Attack.
- ❖ We will integrate the concept of Elgamal encryption with the SHA-512 authentication to provide additional security to the PIN generated for the ATM users. This is a secure way of transmission as it protects from man in the middle attack because if the attackers tries to decode, he will get only the hash value and will not be able to get the actual pin.

PROPOSED MODEL:

In our project, we have integrated the concept of Elgamal encryption with the SHA-512 authentication to provide additional security to the PIN generated for the ATM users. The user enters the 4-digit PIN which is then encrypted using the Elgamal encryption technique following which it is converted into its corresponding hash value using the SHA-512 algorithm. This message digest is then finally sent to the server, where it is then compared with the existing hash values in the directory. If a match is found, the corresponding user details are then fetched and the same is then reflected on the client- side output.

ARCHITECTURE DESIGN:



MAN IN THE MIDDLE ATTACK :

EtterCap

Ettercap is an open-sourced network security tool kit for man-in-the-middle type attacks. In the early days of its development, Ettercap was developed as a sniffer for LAN use only. As the software gained traction in the network security community, Ettercap gained more features that support both active and passive dissection of many protocols as well as extension features for network and host analysis.



How Ettercap Works:

Ettercap has two main sniffing options, passive and active sniffing.

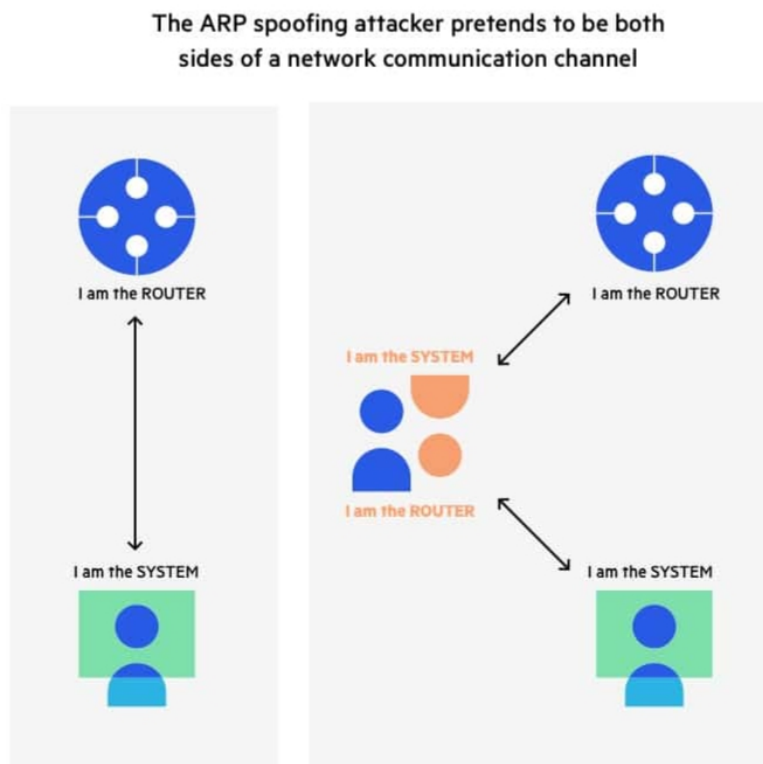
UNIFIED:

This method works essentially the same as Wireshark. It sniffs all the packets that pass on the cable. We can choose to put the interface in promisc mode. The packet not directed to the host running ettercap will be forwarded automatically using layer 3 routing. So we can use a mitm attack launched from a different tool and let ettercap modify the packets and forward them for us.

BRIDGED:

This mode forwards the traffic from one to the other using two network interfaces. While forwarding traffic, it also performs sniffing and packet filtering to the traffic. This sniffing method is stealthy since there is no way to find that someone is in the middle on the cable. We can look at this method as a mitm attack at layer 1. We will be in the middle of the cable between two entities.

APR poisoning- Get into a man-in-the-middle position



To do that, we need to trick the victim's computer into thinking I am the router so the victim's computer can send me packets. At the same time, I also need to trick the router to think I am the victim computer so the router can forward me packets I am not supposed to see. To achieve this, we use ARP poisoning.

APR, address resolution protocol, is a protocol that allows Internet communication to reach a specific device on the network. Essentially, ARP translates Internet protocol addresses to Media Access Control (Mac) addresses, and vice versa.

Hosts (victim computers) maintain an ARP cache that maps between IP

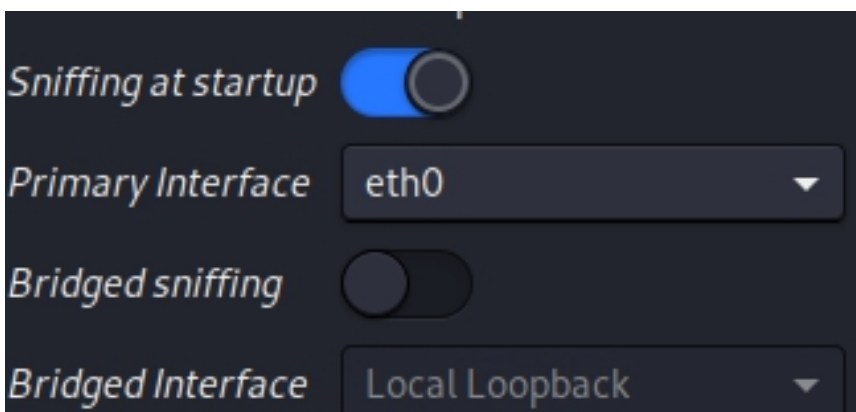
address and Mac address. If the host doesn't know the Mac address for an IP address, the host will send out an ARP request packet and ask for the matching MAC address.

Snapshots

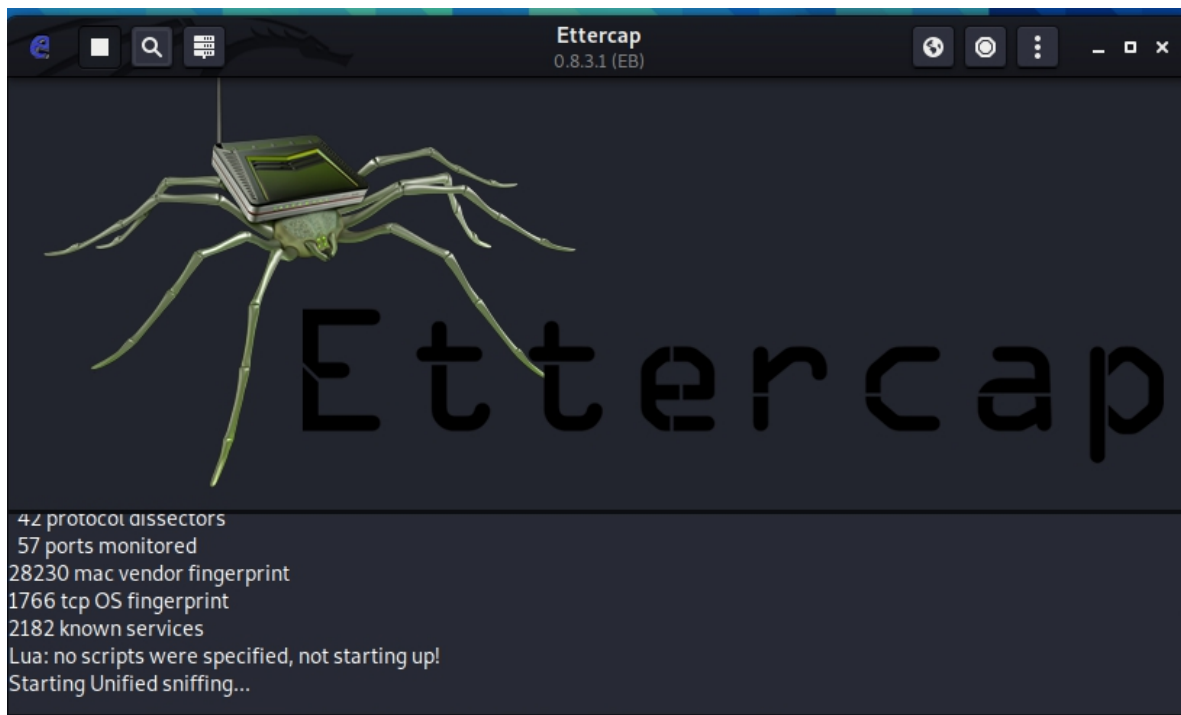
-Start Ettercap



-Select network interface to sniff on



-Identify host on a network

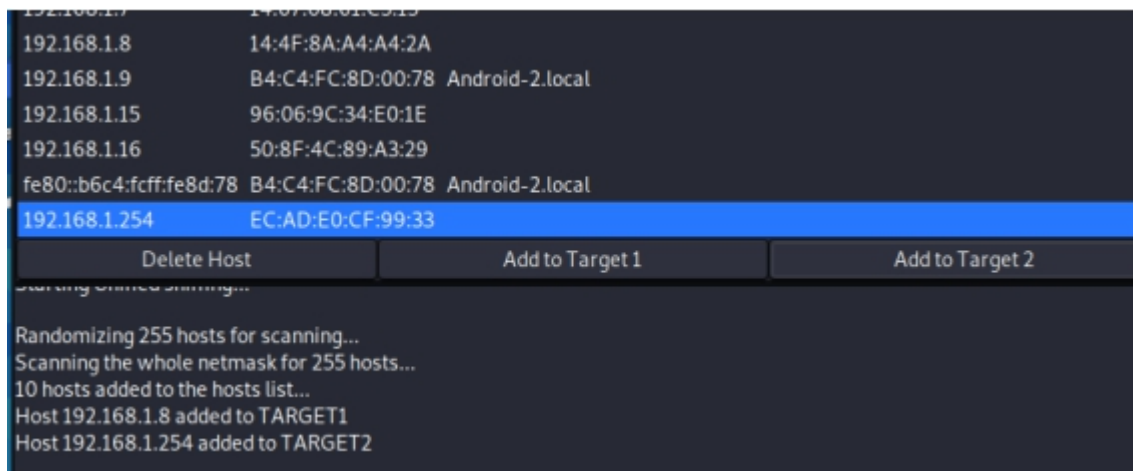


The image shows the "Host List" window in Ettercap 0.8.3.1 (EB). The window contains a table with the following data:

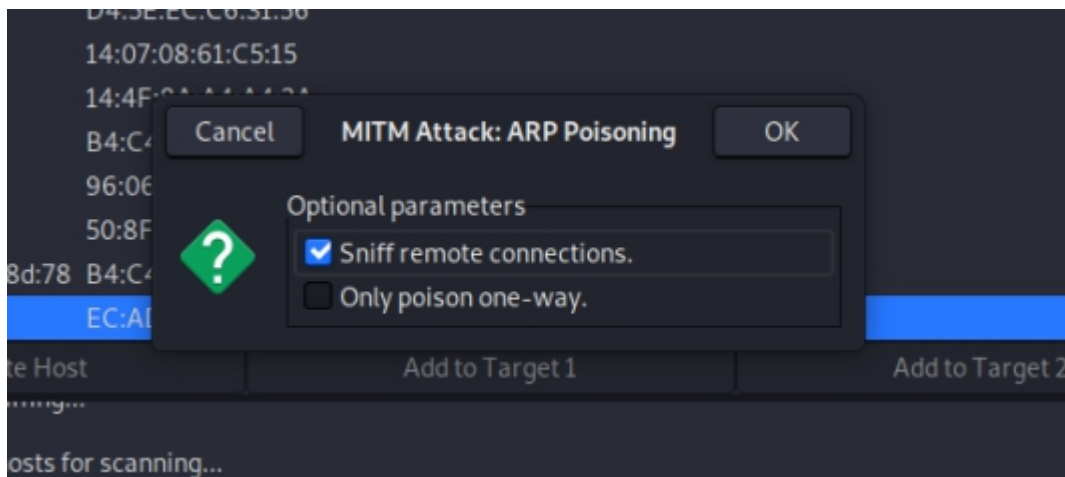
IP Address	MAC Address	Description
192.168.1.1	00:6D:61:D8:F2:D9	
192.168.1.2	66:8D:C9:35:4B:6E	
192.168.1.4	E2:4D:D7:0C:06:C2	
192.168.1.6	D4:5E:EC:C6:31:56	
192.168.1.7	14:07:08:61:C5:15	
192.168.1.8	14:4F:8A:A4:A4:2A	
192.168.1.9	B4:C4:FC:8D:00:78	Android-2.local
192.168.1.15	96:06:9C:34:E0:1E	
192.168.1.16	50:8F:4C:89:A3:29	
fe80::b6c4:fcff:fe8d:78	B4:C4:FC:8D:00:78	Android-2.local
192.168.1.254	EC:AD:E0:CF:99:33	

-Select Host to Target with

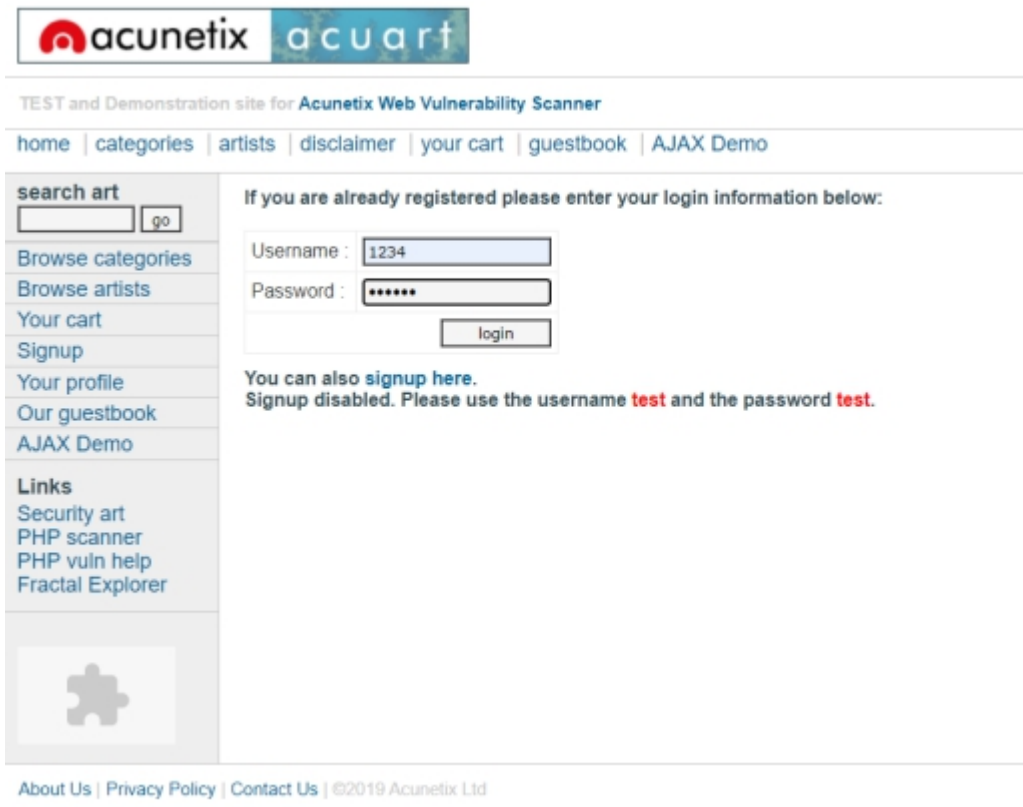
ARP Spoofing



-Launch Attacks on Targets



-intercepting the password



The screenshot shows the Acunetix acuart website. The header includes the Acunetix logo and the text "TEST and Demonstration site for Acunetix Web Vulnerability Scanner". Below the header is a navigation bar with links: home, categories, artists, disclaimer, your cart, guestbook, and AJAX Demo. The main content area is divided into two columns. The left column contains a search bar, a list of links (Browse categories, Browse artists, Your cart, Signup, Your profile, Our guestbook, AJAX Demo), and a section titled "Links" with sub-links (Security art, PHP scanner, PHP vuln help, Fractal Explorer). The right column contains a login form with the heading "If you are already registered please enter your login information below:". The form has fields for Username (containing "1234") and Password (containing "*****"), and a "login" button. Below the form, there is a message: "You can also [signup here](#). Signup disabled. Please use the username **test** and the password **test**." The footer contains links: About Us, Privacy Policy, Contact Us, and ©2019 Acunetix Ltd.

```
GROUP 1 : 192.168.1.8 14:4F:8A:A4:A4:2A
GROUP 2 : 192.168.1.254 EC:AD:E0:CF:99:33
HTTP : 18.192.172.30:80 -> USER: 1234 PASS: aaaddd INFO: http://testphp.vulnweb.com/login.php
CONTENT: uname=1234&pass=aaaddd
```

RESULT :

We can see that Ettercap successfully ARP poisoned the target and intercepted an HTTP login request the target was sending to an insecure website.

ELGAMAL ENCRYPTION:

ALGORITHM:

Elgamal Encryption Elgamal encryption, in cryptography, is an asymmetric (public) encryption technique. As the name suggests, it uses asymmetric key encryption wherein there exists two separate keys, a combination of public and private keys each for the both the parties involved in the communication.

This technique is based on the complexity of calculating discrete logarithm in a cyclic group, i.e., it prevents us from computing the value of g^ak , even if know the values of g^a and g^k .

In a given communication using Elgamal technique, if we assume A to be the sender and B, the receiver, the following steps could be listed out that shall be executed:

1. Generation of public and private key

- ❖ The user selects a very large number ' q ' and a cyclic group F_q .
- ❖ An element ' g ' is selected from the cyclic group F_q and an element a such that $\text{GCD}(a, q) = 1$.
- ❖ $h = g^a$ is then computed.
- ❖ The values ' F_q ', ' h ', ' q ' and ' g ' becomes the public key and the value ' a ' is retained as the private key.

2. Encryption at the sender site

- ❖ The sender selects a random integer ' k ' from the cyclic group F_q such that $\text{GCD}(k, q) = 1$.
- ❖ Following this, the values $p = g^k$ and $s = h^k = g^{ak}$ are computed
- ❖ The values ' s ' and ' M ' are then multiplied together where ' M ' is the message.
- ❖ Finally, the tuple $(p, M \times s) = (g^k, M \times s)$ is sent as the encrypted message to the receiver.

3. Decryption at the receiver site

- ❖ The receiver calculates the value $s = p_a = g_a k$
- ❖ Following this the value $M \times s$ is divided by 's' to obtain 'M'.

SHA ENCRYPTION

SHA (Secure Hash Algorithms) are a family of cryptographic algorithms to ensure the authentication of data. It functions by converting a given message into a hash value or a message digest of a definite size (a fixed size string generated from the message). The algorithm that does the same comprises of functions including bitwise operations, modular addition and compression functions. The algorithms work on the principle of a one-way function, i.e., once the messages are transformed into their respective hash values, they cannot be converted back to the original form. Encrypting passwords or PINs is one of the common applications of the SHA algorithms. This comes as an immediate effect of the fact that the server side has to actually only keep track of the specific hash values corresponding to the entered passwords/PINs of a particular user instead of the actual password/PIN. The benefit that it provides is that if the database, by any chance gets hacked, the attacker would only get to get their hands on the hash values and not the actual PINs.

In addition to that, SHAs exhibit the avalanche effect wherein modifying even a single character in the message leads to a drastic alteration in the hash value. This prevents the attacker from even finding out the length of the original message, let alone the message itself.

Integration of the Elgamal Encryption with SHA Authentication

In our project, we have integrated the concept of Elgamal encryption with the SHA-512 authentication to provide additional security to the PIN generated for the ATM users. The user enters the 4-digit PIN which is then encrypted using the Elgamal encryption technique following which it is converted into its corresponding hash value using the SHA-512 algorithm.

This message digest is then finally sent to the server, where it is then compared with the existing hash values in the directory. If a match is found, the corresponding user details are then fetched and the same is then reflected on the clientside output.

CODE :

Main.py

```
C:\Users\chira\Desktop\final\main.py - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help

main.py
1 from Tkinter import *
2 from auth import *
3 from math import pow
4 window = Tk()
5 window.attributes("-fullscreen",True)
6 w = window.winfo_screenwidth()
7 h = window.winfo_screenheight()
8
9 window.title("Welcome to CANARA BANK ")
10 window.configure(background = "LightSeaGreen")
11 hashDir = {'efe9adc30b262cc6ef6e4da7b9a97bdfb7c89e6fa313b17d1c86624bd615dddaae1fbc3975211339857ecfccd8399869e3f22433de34dc2993dce348acd': 'CHIRAG JAIN-1881T0008', #7828
12 'dd809f2083b0ircab1654fac601bb3568f2110f6db007c8633c9f974dc126f17fc3a76a7841b5fa393ec7879ec39c8548b1ee68940888c1cd45c58ab2ff590f': 'MUSKAN SAHNI-1881T0392', #6774
13 '6f826cf5a8359854258e184537b978c39cf497bcd66118bd2d25072e537034fa6360d5e066296660f84b5b816847266b81455cb0723fffe7025804002e301': 'MAHAK GUPTA-1881T0041', #8367
14 }
15 hashDirLen = len(hashDir)
16 hashList = list(hashDir.keys())
17
18 def authenticate():
19     newWin = Toplevel(window)
20     newWin.attributes("-fullscreen",True)
21     newWin.title("Authentication")
22     newWin.configure(background = "LightSeaGreen" )
23     Label(
24         newWin,
25         text = "Welcome to CANARA BANK ",
26         bg = "LightSeaGreen",
27         fg = "DarkCyan",
28         font = "Consolas 72"
29     ).place(
30         x = 90,
31         y = 50
32     )
33     p = PINEntry.get()
34     PINEntry.delete(0,END)
35     if len(p) == 4 and p.isdigit():
36         q = 12345678901234567890 #random.randint(pow(10,20),pow(10,50))
37         g = 23931164504956447807213117212663825326210289577470
38         key = gen_key(q) #Receiver_Private_key
39         h = power(g,key,q)
40         out = encrypt(p,q,h,g)
41         flag = 0
42         for i in range(len(hashList)):
43             if out == hashList[i]:
44                 flag = 1
45                 pos = i
46                 break
47         if flag == 1:
48             Label(
49                 newWin,
50                 text = "PIN Matched. Hello, " + hashDir[hashList[pos]] + "!",
```

```
main.py - C:\Users\chira\Desktop\NIS PROJECT\main.py
File Edit Format Run Options Windows Help

if len(p) == 1:
    p = hashlib.sha256(p).hexdigest()
    q = 12345678987654321234567898 #random.randint(pow(10, 20), pow(10, 50))
    q = 23931164504956447807213117212663825326210289577470
    key = gen_key(q) #Receiver Private key
    h = power(g, key, q)
    out = encrypt(p, q, h, q)
    flag = 0
    for i in range(len(hashList)):
        if out == hashList[i]:
            flag = 1
            pos = i
            break
    if flag == 1:
        Label(
            newWin,
            text = "PIN Matched. Hello, " + hashDir[hashList[pos]] + "!",
            bg = "LightSeaGreen",
            fg = "Navy",
            font = "Consolas 20"
        ).place(
            x = 430,
            y = 300
        )
        Button(
            newWin,
            text = "Back",
            width = 20,
            font = "Calibri 15",
            bg = "LightSeaGreen",
            fg = "White",
            command = newWin.destroy
        ).place(
            x = 550,
            y = 425
        )
    else:
        Label(
            newWin,
            text = "No match found. Please try again.",
            bg = "LightSeaGreen",
            fg = "Maroon",
            font = "Consolas 20"
        ).place(
            x = 430,
            y = 300
        )
        Button(
            newWin,
```

Auth.py

```
auth.py - C:\Users\chira\Desktop\NIS PROJECT\auth.py
File Edit Format Run Options Windows Help

import random
from math import pow
import hashlib
import time
start = time.time()
a = 7
def gcd(a, b):
    if a < b:
        return gcd(b, a)
    elif a % b == 0:
        return b
    else:
        return gcd(b, a % b)
# Generating large random numbers
def gen_key(q):
    key = 1234567898765432123456789 #random.randint(pow(10, 20), q)
    while gcd(q, key) != 1:
        key = random.randint(pow(10, 20), q)
    return key
# Modular exponentiation
def power(a, b, c):
    x = 1
    y = a
    while b > 0:
        if b % 2 == 0:
            x = (x * y) % c
            y = (y * y) % c
            b = int(b / 2)
        return x % c
# Asymmetric encryption
def encrypt(msg, q, h, g):
    en_msg = []
    k = 19 #gen_key(q) # Private key for sender
    s = power(h, k, q)
    p = power(g, k, q)
    for i in range(0, len(msg)):
        en_msg.append(msg[i])
    print("g^k used : ", p)
    print("g^ak used : ", s)
    for i in range(0, len(en_msg)):
        en_msg[i] = s * ord(en_msg[i])
    print ("encrypted pin", en_msg)
    output = hashlib.sha512(str(en_msg[1])).hexdigest()
    print ('hash generated', output)
    return output
# Driver code
def main():
```

```
auth.py - C:\Users\chira\Desktop\NIS PROJECT\auth.py
File Edit Format Run Options Windows Help

key = 1234567898765432123456789 #random.randint(pow(10, 20), q)
while gcd(q, key) != 1:
    key = random.randint(pow(10, 20), q)
return key

# Modular exponentiation
def power(a, b, c):
    x = 1
    y = a
    while b > 0:
        if b % 2 == 0:
            x = (x * y) % c
            y = (y * y) % c
            b = int(b / 2)
        return x % c

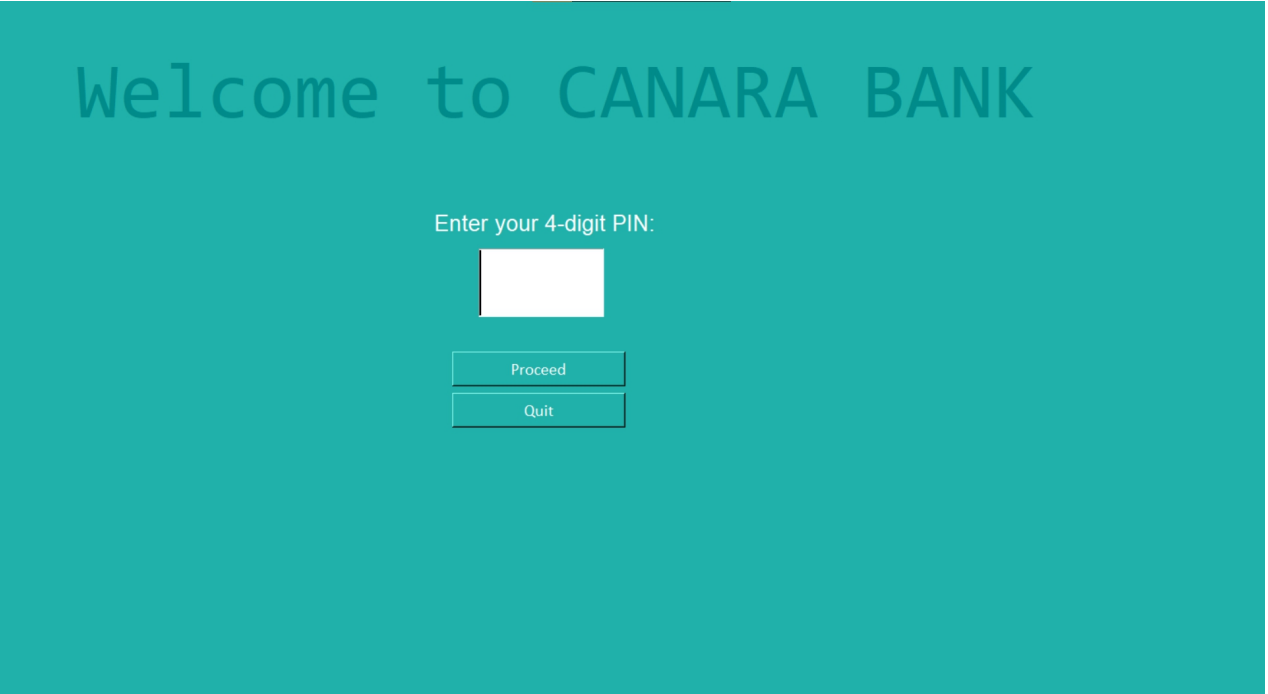
# Asymmetric encryption
def encrypt(msg, q, h, g):
    en_msg = []
    k = gen_key(q) # Private key for sender
    s = power(h, k, q)
    p = power(g, k, q)
    for i in range(0, len(msg)):
        en_msg.append(msg[i])
    print("g^k used : ", p)
    print("h^k used : ", s)
    for i in range(0, len(en_msg)):
        en_msg[i] = s * ord(en_msg[i])
    print ('encrypted pin', en_msg)
    output = hashlib.sha512(str(en_msg[1])).hexdigest()
    print ('hash generated', output)
    return output

# Driver code
def main():
    msg = raw_input('Enter 4 digit pin: ')
    end = time.time()
    print("Original Message :", msg)
    q = 12345678987654321234567898 #random.randint(pow(10, 20), pow(10, 50))
    g = 2398114856956447807213117212663825326210289577470
    key = gen_key(q) # Private key for receiver
    h = power(q, key, q)
    print("g used : ", g)
    print("h used : ", h)
    en_msg = encrypt(msg, q, h, g)

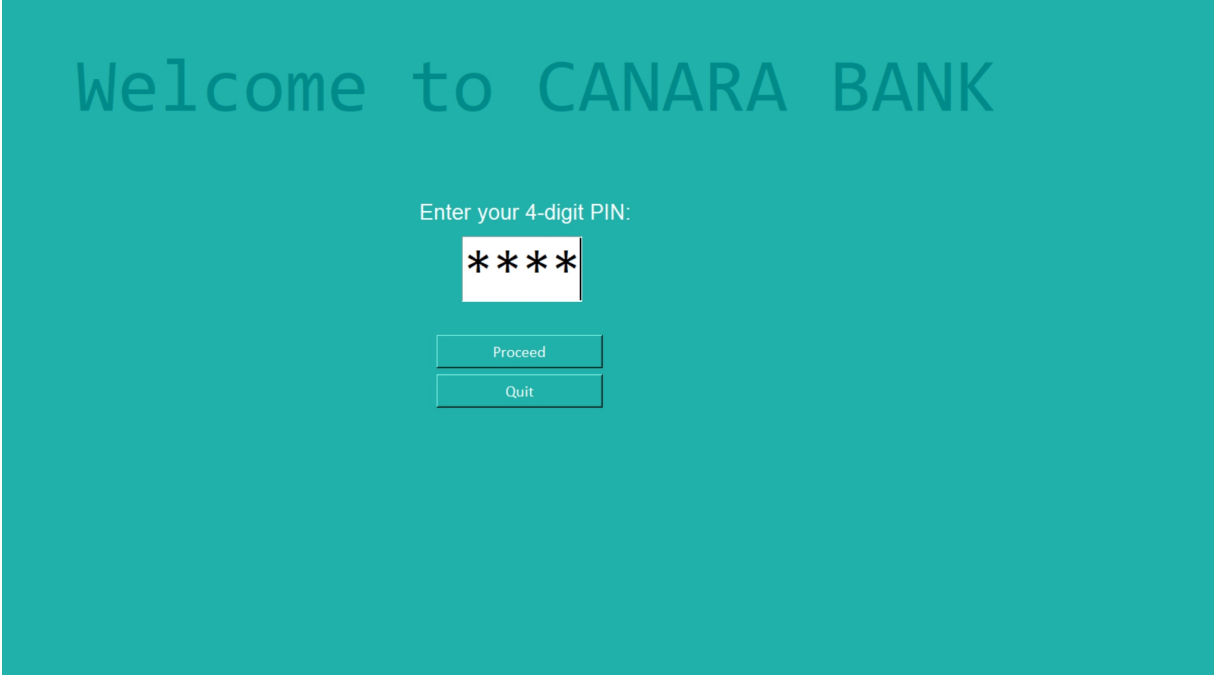
    print(end-start)
if __name__ == '__main__':
    main()
```

RESULT :

Welcome Screen



Entering a valid input but incorrect PIN



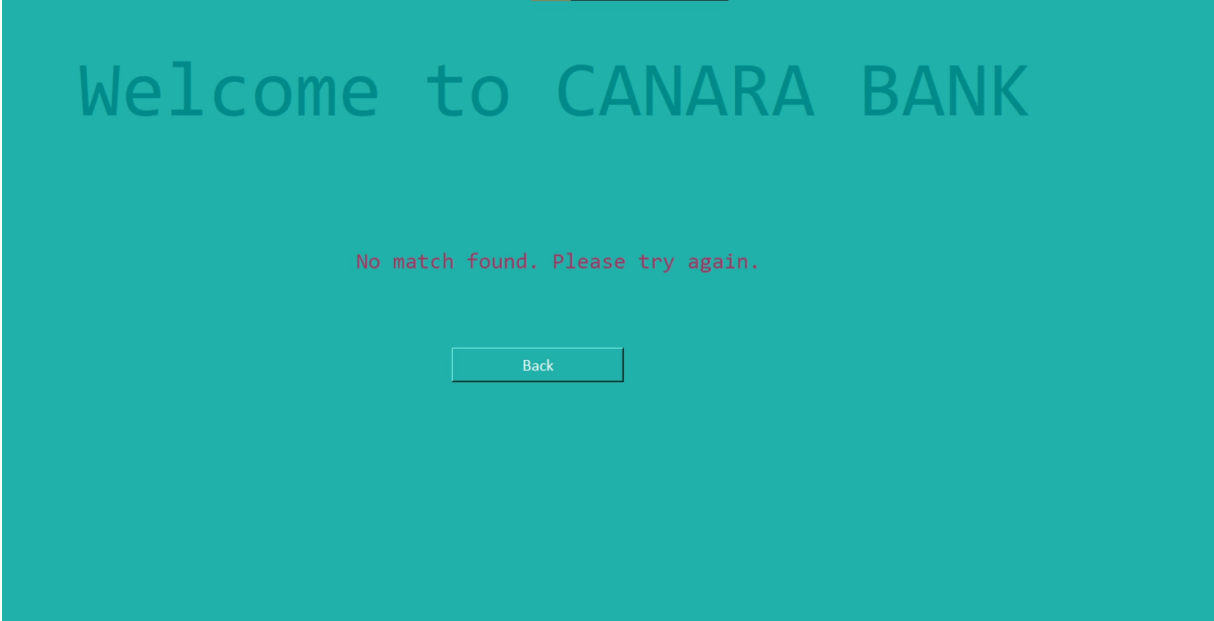
Welcome to CANARA BANK

Enter your 4-digit PIN:

Proceed

Quit

Showing error message for a valid but incorrect PIN



Welcome to CANARA BANK

No match found. Please try again.

Back

Entering a valid and a correct PIN

Welcome to CANARA BANK

PIN Matched. Hello, CHIRAG JAIN-18BIT0008!

Back

Welcome to CANARA BANK

PIN Matched. Hello, MUSKAN SAHNI-18BIT0382!

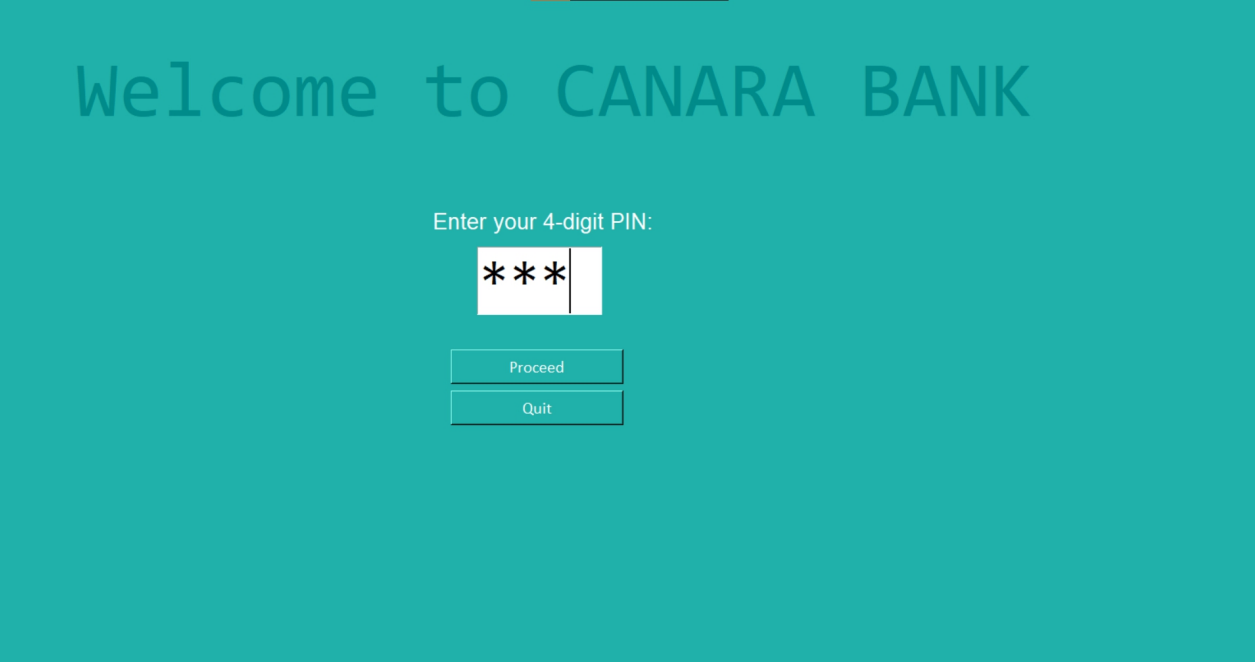
Back

Welcome to CANARA BANK

PIN Matched. Hello, MAHAK GUPTA-18BIT0041!

Back

Entering an invalid PIN



Welcome to CANARA BANK

Enter your 4-digit PIN:

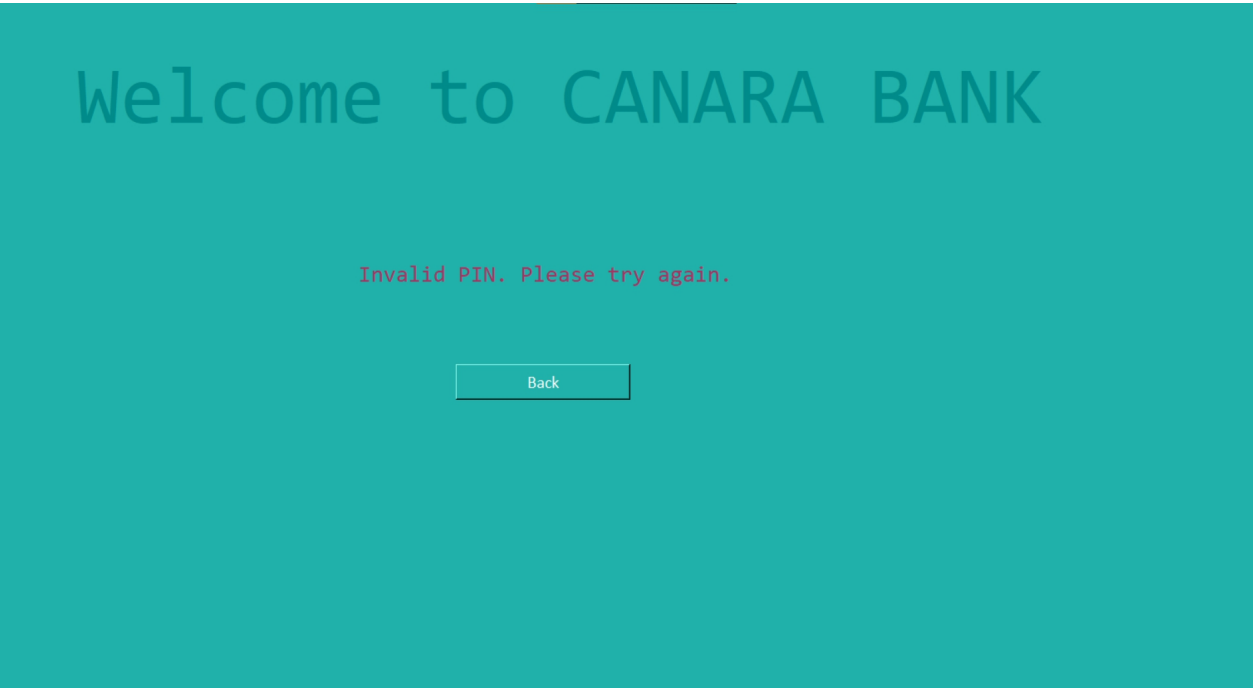
***|

Proceed

Quit

This screenshot shows the Canara Bank login interface. At the top, the text 'Welcome to CANARA BANK' is displayed in a large, light blue font. Below this, the instruction 'Enter your 4-digit PIN:' is shown. A PIN input field contains three asterisks followed by a vertical cursor line. At the bottom of the input area, there are two buttons: 'Proceed' and 'Quit'.

Displaying error message for an invalid message



Welcome to CANARA BANK

Invalid PIN. Please try again.

Back

This screenshot shows the Canara Bank login interface after an invalid PIN entry. The 'Welcome to CANARA BANK' text remains at the top. Below it, an error message 'Invalid PIN. Please try again.' is displayed in a red font. At the bottom, there is a single 'Back' button.

Equivalent results for CLI (Server-side)

Entering a valid but incorrect PIN

```
>>>
Enter 4 digit pin: 1234
('Original Message :', '1234')
('g used : ', 23931164504956447807213117212663825326210289577470L)
('g^a used : ', 14504671374771338041634698L)
('g^k used : ', 34215135440877585739649990L)
('g^ak used : ', 115663736140444448214089630L)
('encrypted pin', [5667523070881777962490391870L, 578318680702222410704481500L,
5898850543162666858918571130L, 6014514279303111307132660760L])
('hash generated', 'b7860b463279fa09a55f8fd4e00f0e0f2a29517bfc9bbab1b3efbeebddc0
5023562cc6d301395632fcf59ea4da205c320c34745c89eld3f58f925a1094bf2109')
2.91700005531
>>>
```

Entering a valid and correct PIN

```
>>>
Enter 4 digit pin: 7828
('Original Message :', '7828')
('g used : ', 23931164504956447807213117212663825326210289577470L)
('g^a used : ', 14504671374771338041634698L)
('g^k used : ', 34215135440877585739649990L)
('g^ak used : ', 115663736140444448214089630L)
('encrypted pin', [6361505487724444651774929650L, 6477169223864889099989019280L,
578318680702222410704481500L, 6477169223864889099989019280L])
('hash generated', 'efe9a4c30b262cc66f6be40afb9a97bdfbb7c89e66a313b17d16c86624bd
615dddaaelfb6c3975211339057ec6cca0309069e3f22433de34d62993de6e340acd')
3.7539999485
>>> |
```

Entering an invalid PIN

```
>>>
Enter 4 digit pin: 123
('Original Message :', '123')
('g used : ', 23931164504956447807213117212663825326210289577470L)
('g^a used : ', 14504671374771338041634698L)
('g^k used : ', 34215135440877585739649990L)
('g^ak used : ', 115663736140444448214089630L)
('encrypted pin', [5667523070881777962490391870L, 578318680702222410704481500L,
5898850543162666858918571130L])
('hash generated', 'b7860b463279fa09a55f8fd4e00f0e0f2a29517bfc9bbab1b3efbeebddc0
5023562cc6d301395632fcf59ea4da205c320c34745c89eld3f58f925a1094bf2109')
2.38999986649
```

Some stored PIN-Hash values for different customers

7828	efe9a4c30b262cc66f6be40afb9a97bdfbb7c89e66a313b17d16c86624bd615dddaae1fb6c3975211339057ec6cca0309069e3f22433de34d62993de6e340acd	CHIRAG JAIN- 18BIT0008
6774	ddb09f20b3b0fcab1654fac601b83568f2110f6db007c8633c9f974dc126f2f75c3e76a7841b5fa393ec7879ec39c8548b16e689f09888c1cd45c58eb2ff590f	MUSKAN SAHNI- 18BIT0382
8367	6f826cf5a8359854258e184537b978c39cff97bcde6118bd2df25072e537034fa66360d5e066296660f84b5be8168472b6b81455cb0723fffe7025804002e301	MAHAK GUPTA- 18BIT0041

CONCLUSION

It is hence seen that using elgamal with hashing proves helpful as it reduces man in the middle attacks to a great extent owing to the fact that hash are irreversible. The 4 digit pin is converted to a fixed 256 bit hash value based upon which the pin is verified. Since strong and weak collision resistance follows hence it is highly improbable to find another pin with the same hash value. Even if the attacker gets a hold of the hash value he cannot find the original pin, hence keeping the identity of the user intact. The only shortcoming with this technique is that it is not permanent and while the system becomes scalable then the chances of collision becomes higher. Elgamal with hash gave the best time values for run time hence is used for the model here. As far as future work is concerned, using biometric identities is becoming the need of the hour but the obvious shortcomings were mentioned in the literature survey. To overcome this a hybrid biometric authentication system could be made for future which cannot be forged and is hundred percent immune to external attacks.

REFERENCES

- [1] Karovaliya, Mohsin & Karedia, Saifali & Oza, Sharad & Kalbande, Dhananjay. (2015). Enhanced Security for ATM Machine with OTP and Facial Recognition Features. Procedia Computer Science. 45. 10.1016/j.procs.2015.03.166.
- [2] A Review on Secure ATM by Image Processing
- [3] [3] Mahajan, Priyanka. (2016). New Approach in Biometrics to Combat the Automated Teller Machine Frauds: Facial Recognition. International Journal Of

Engineering And Computer Science. 10.18535/ijecs/v5i5.22.

[4] Jacobs, Bart & Poll, Erik. (2011). Biometrics and Smart Cards in Identity Management. 10.1007/978-90-6704-731-9_23.

[5] Practical Attacks on Proximity Identification Systems (Short Paper) Proceedings of the 2006 IEEE Symposium on Security and Privacy (S&P'06)

[6] COMPARISON OF VARIOUS BIOMETRIC METHODS, International Journal of Advances in Science and Technology (IJAST) Vol 2 Issue I (March 2014)

[7] Twum, Frimpong & Nti, Isaac kofi & Asante, Michael. (2016) Improving Security Levels In Automatic Teller Machines (ATM) Using Multifactor Authentication. International Journal of Science and Engineering Applications. 5. 126-134. 10.7753/IJSEA0503.1003

[8] Onyesolu, Moses & Ezeani, Ignatius. (2012). ATM Security Using Fingerprint Biometric Identifier: An Investigative Study. International Journal of Advanced Computer Science and Applications. 3. 10.14569/ IJACSA.2012.030412

[9] De Luca, Alexander & Langheinrich, Marc & Hussmann, Heinrich. (2010). Towards understanding ATM security - A field study of real world ATM use. ACM International Conference Proceeding Series. 10.1145/1837110.1837131.

[10] C. Porretti, R. Lahaije and D. Kolev, "A New Vision for ATM Security Management: The Security Management Platform," 2016 11th International Conference on Availability, Reliability and Security (ARES), Salzburg, 2016, pp. 493-498. doi: 10.1109/ARES.2016.50

[11] Automated Teller Machines in India: A Literature Review from Key Stakeholders Perspectives Hota, J.R. (2013) Growth of ATM Industry in India, CSI Communications, 36(11): 23-25.

[12] Twum, Frimpong & Nti, Isaac kofi & Asante, Michael. (2016). Improving Security Levels In Automatic Teller Machines (ATM) Using Multifactor Authentication. International Journal of Science and Engineering Applications. 5. 126-134. 10.7753/IJSEA0503.1003

[13] [13] Cardless Automatic Teller Machine (Atm) Biometric Security System Design Using Human Fingerprints – Madhuri More, Sudarshan Kankal, Akshay Kumar Kharat, Rupali Adhau – International Journal of Advance Engineering and Research Development, Volume 5, Issue 05, May -2018

- [14] ATM Security – Kavita Hooda – International Journal of Scientific and Research Publications, Volume 6, Issue 4, April 2016
- [15] Survey of Security of ATM Machine - Prachi More, Dr. S.D. Markande – International Journal of Advanced Research in Computer and Communication Engineering, Vol. 5, Issue 4.