

IRREVERSIBLE ENCRYPTION FOR SECURING ATM TRANSACTIONS

A PROJECT REPORT

for

NETWORK AND INFORMATION SECURITY (ITE4001)

in

B.Tech – Information Technology and Engineering

by

NITIN VANKADARI (18BIT0227)

KUSHAGRA AGARWAL (18BIT0231)

PRIYAL BHARDWAJ (18BIT0272)

ROHAN JAIN (18BIT0429)

Under the Guidance of

Dr. SHANTHARAJAH S P

Professor Grade 1, SITE



VIT[®]

Vellore Institute of Technology

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

School of Information Technology and Engineering

June, 2021

I. ABSTRACT

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.

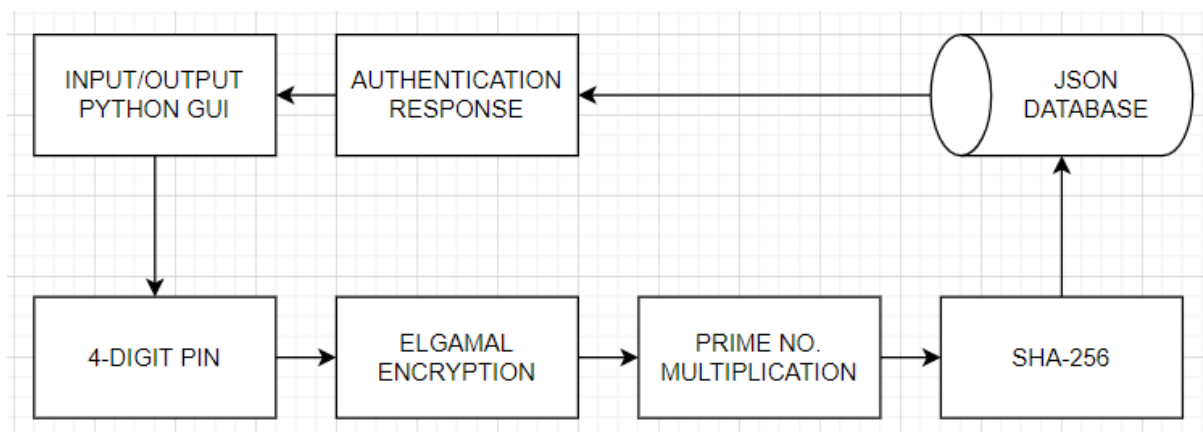
II. PROBLEM STATEMENT

The present ATM model uses a card and a PIN. This is a very simple ATM model and can easily be attacked. The attacks can in form of stolen cards, duplicity of cards or due to statically given PINS. To improve the security of ATM, biometric technique was also introduced in which user has to give biometric first and then after verifying he has to enter the PIN. This improved security but later it failed as there were different errors found in this technique.

III. PROPOSAL

We propose a different and much more secure way of protecting ATM machine. In our proposed model, first user enters the pin, this pin is encrypted using elgamal cryptographic algorithm and then the resulted output is given as input to SHA-256 Hash. This is a secure way of transmission as it protects from man in the middle attack because if the attackers try to decode, he will get only the hash value and will not be able to get the actual pin.

IV. ARCHITECTURE



V. WORKING

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

- a. The user selects a very large number 'q' and a cyclic group F_q .
- b. An element 'g' is selected from the cyclic group F_q & element a such that $\text{GCD}(a, q) = 1$.
- c. $h = g^a$ is then computed.
- d. 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

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

- a. The receiver calculates the value $s = p^a = g^{ak}$.
- b. Following this the value $M \times s$ is divided by ' s ' to obtain ' M '.

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 keeps 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.

VI. PSEUDOCODE

Idea of ElGamal cryptosystem

Suppose Alice wants to communicate to Bob.

1. Bob generates public and private key:
 - Bob chooses a very large number q and a cyclic group F_q .
 - From the cyclic group F_q , he chooses any element g and an element a such that $\gcd(a, q) = 1$.
 - Then he computes $h = ga$.
 - Bob publishes F , $h = ga$, q and g as his public key and retains a as private key.
2. Alice encrypts data using Bob's public key:
 - Alice selects an element k from cyclic group F such that $\gcd(k, q) = 1$.
 - Then she computes $p = gk$ and $s = hk = gak$.
 - She multiplies s with M .
 - Then she sends $(p, M*s) = (gk, M*s)$.
3. Bob decrypts the message:
 - Bob calculates $s' = pa = gak$.
 - He divides $M*s$ by s' to obtain M as $s = s'$.

. SHA-256 Integration

- Each digit of our 4-digit pin is encrypted using elgamal and stored in list.
- Next, we multiply each encrypted item in the list with different prime numbers and add them.
- Now we pass this value to SHA-256 hash function and generate the hash of our pin.
- This value is stored in our JSON file to be matched with while logging in.

VII. CONCLUSION

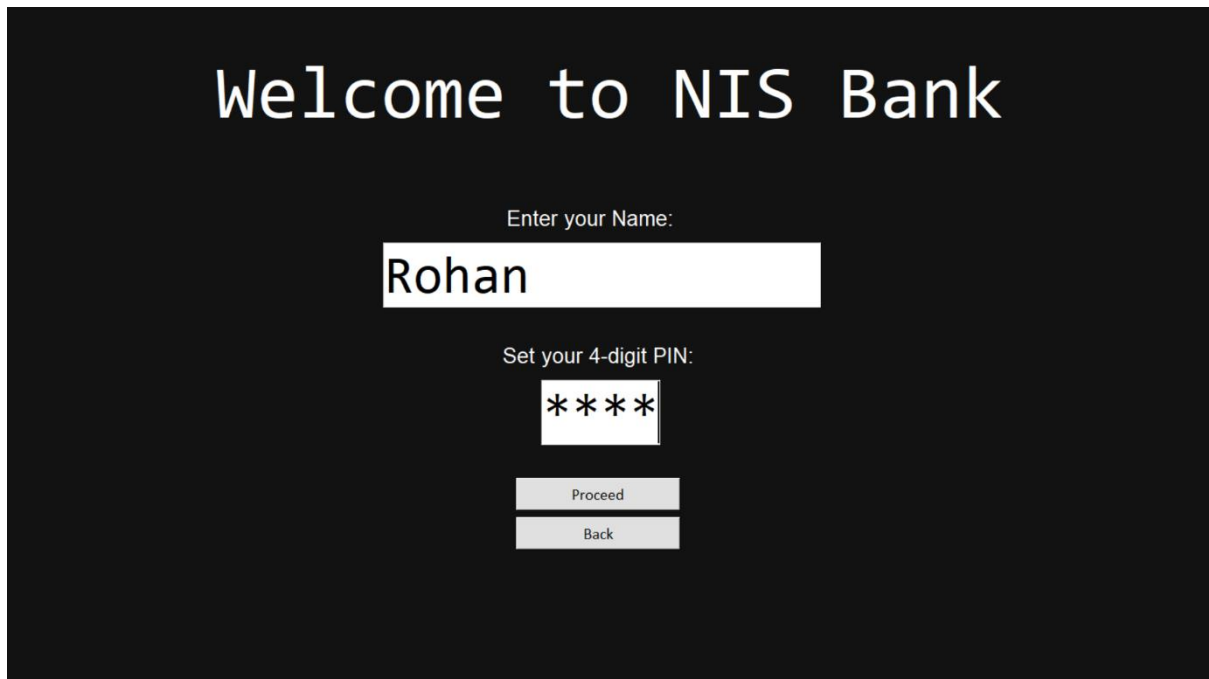
It is hence seen that using elgamal with hashing proves helpful as it reduces man in the middle attacks to a great extent owing to the fact that hash are irreversible. The 4 digit pin is converted to a fixed 256 bit hash value based upon which the pin is verified. Since strong and weak collision resistance 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.

VIII. DEMO SNAPSHOTS

Home page:



New User Registration:



A registration form for NIS Bank with a dark background and white text. The title 'Welcome to NIS Bank' is at the top. Below it, the prompt 'Enter your Name:' is followed by a text input field containing 'Rohan'. The next prompt is 'Set your 4-digit PIN:', followed by a PIN input field showing four asterisks. At the bottom are two buttons: 'Proceed' and 'Back'.

Welcome to NIS Bank

Enter your Name:

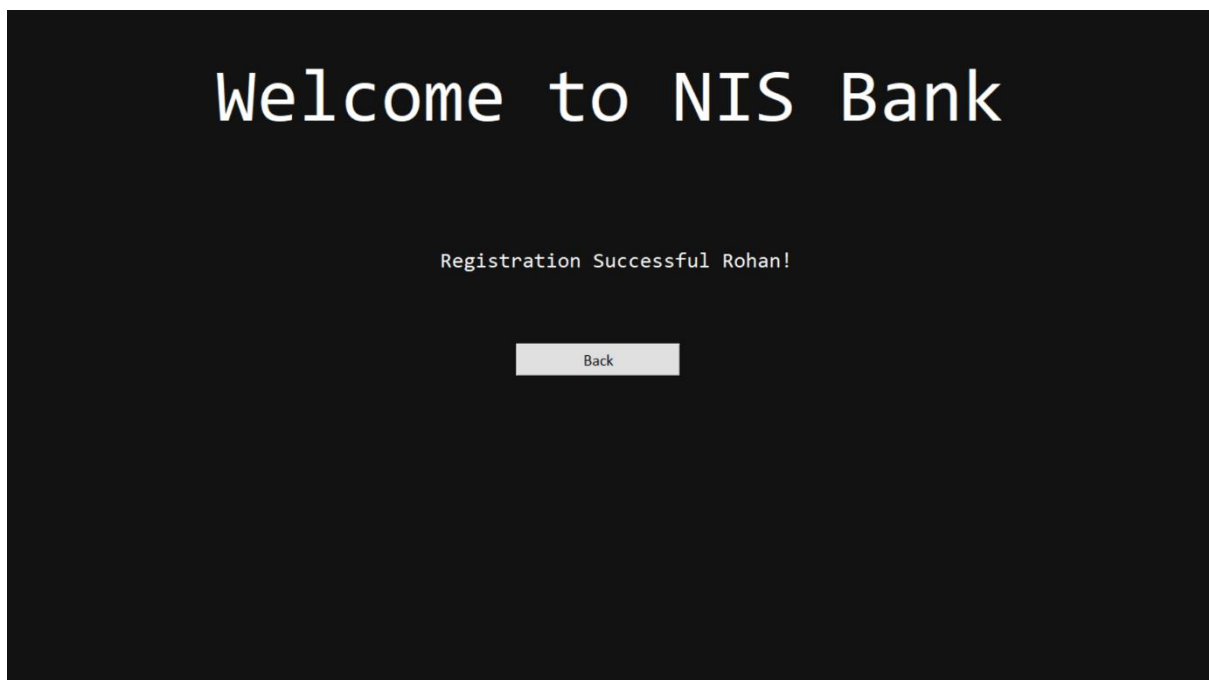
Rohan

Set your 4-digit PIN:

Proceed

Back

Successful Registration:



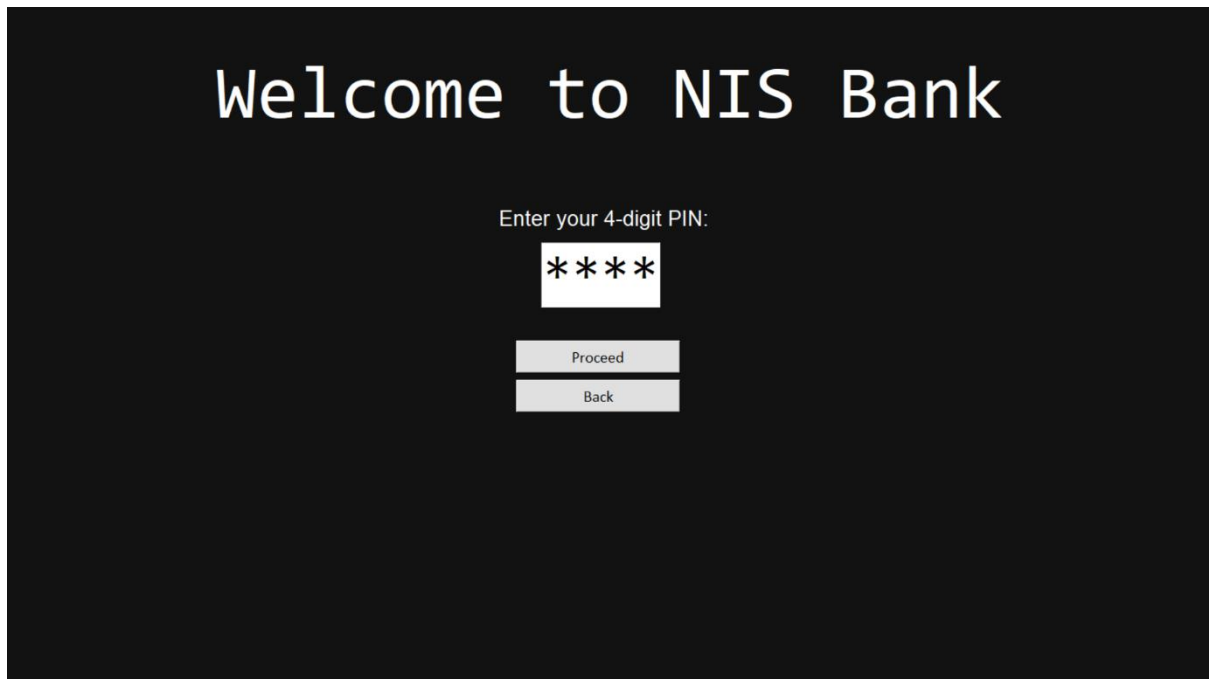
A confirmation screen for NIS Bank with a dark background and white text. The title 'Welcome to NIS Bank' is at the top. Below it, the message 'Registration Successful Rohan!' is displayed. At the bottom is a single 'Back' button.

Welcome to NIS Bank

Registration Successful Rohan!

Back

Existing User Login:

A dark-themed login screen for NIS Bank. At the top, the text "Welcome to NIS Bank" is displayed in a large, white, monospace-style font. Below this, the prompt "Enter your 4-digit PIN:" is shown in a smaller white font. Underneath the prompt is a white rectangular input field containing four asterisks "****". At the bottom of the screen, there are two white rectangular buttons: "Proceed" on top and "Back" on the bottom, both in a small, dark font.

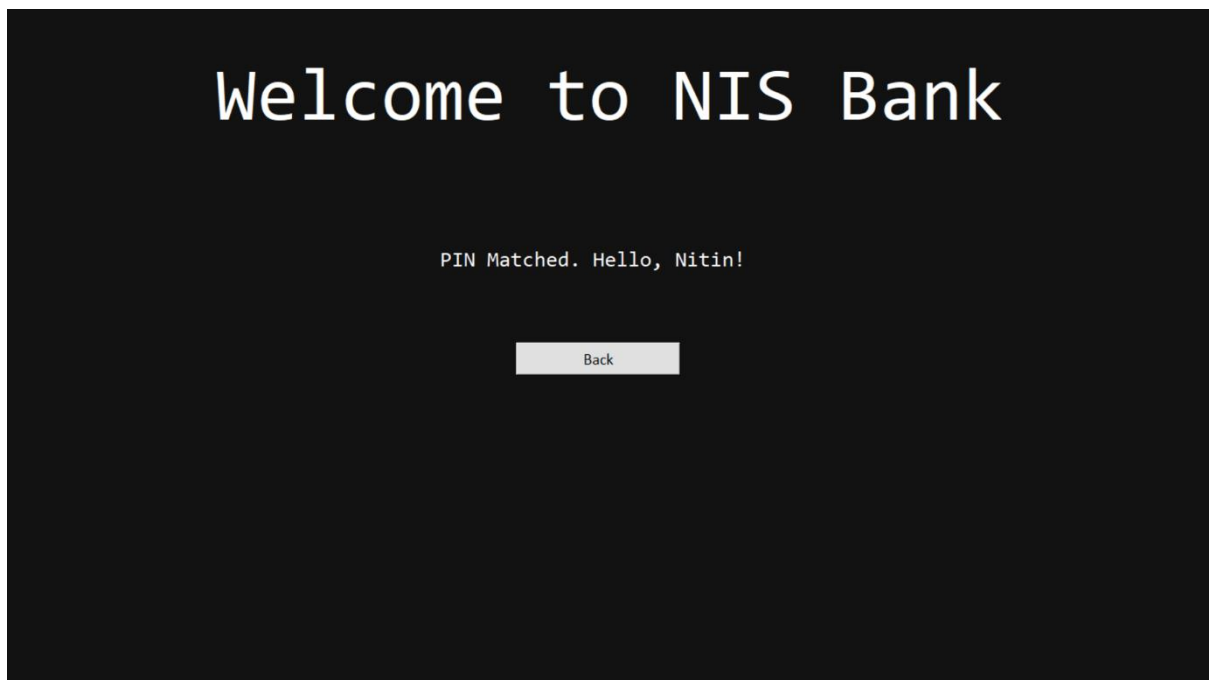
Welcome to NIS Bank

Enter your 4-digit PIN:

Proceed

Back

Successful Login:

A dark-themed screen showing a successful login for NIS Bank. At the top, the text "Welcome to NIS Bank" is displayed in a large, white, monospace-style font. Below this, the message "PIN Matched. Hello, Nitin!" is shown in a smaller white font. At the bottom of the screen, there is a single white rectangular button labeled "Back" in a small, dark font.

Welcome to NIS Bank

PIN Matched. Hello, Nitin!

Back

Appendix

GitHub Link for Code: [Click Here](#)