VIT®

Vellore Institute of Technology

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

NETWORK INFORMATION AND SECURITY

ONLINE CARD PAYMENT SECURITY USING ENHANCED RSA

KUNJ PATEL 19BIT0256

ISHITA JOHRI 19BIT0284

SEJAL BHARTI 19BIT0286

ABSTRACT

RSA (Rivest, Shamir, Adleman) algorithm is an asymmetric cryptography algorithm. Asymmetric refers to the fact that it works on two different keys i.e., Public Key and Private Key. It means an unpredictable (typically large and random) number is used to begin generation of an acceptable pair of keys suitable for use by the algorithm. As the name describes, the Public Key is given to everyone, and the Private key is kept private. This project proposes the creation of a complete and realistic RSA encrypt solution for CARD PAYMENT SECURITY, as well as an upgraded RSA encrypt solution. CVV is among the most significant participants within the online card payment process, so it's critical to protect this delicate entity. Thus, adopting an enhanced RSA approach, our suggested algorithm encrypts the CVV number, which may then be applied further so that the user only has to enter the encrypted number to complete successful transactions. When compared to the old RSA technique, the usage of enhanced RSA has strengthened security even further.

INTRODUCTION

Because of the rise in e-commerce, there is a clear need for some type of encryption technology to assure security and a feasible means to ensure that the user's data is securely maintained in the database. As a result, our system employs RSA for this purpose. Asymmetric encryption algorithms, such as the RSA algorithm, are a subset of symmetric encryption algorithms. The algorithm is known as a public key encryption algorithm, and it is widely used and recognised. The usage of RSA, particularly in this card-related system, increases the security of the process. Because the data is encrypted, financial transactions can now be conducted safely without fear of an intruder gaining access to the database. RSA was one of the first big developments in public key cryptography, and it was the first algorithm that was ideally suited for both signing and encryption. Ronald Rivest, Adi Shamir, and Leonard Adleman are the three MIT mathematicians who created this algorithm. In today's world, RSA is widely used for secure Internet communication (browsers, S/MIME, SSL), operating systems (Sun, Microsoft, Apple, Novell), and hardware (Sun, Microsoft, Apple, Novell) (cell phones, ATM machines).

The design of the RSA security software evolved a bit from the need for an all acceptance information security system and partly from the need for a user friendly package that can fulfil any large ecommerce organization’s information security needs. Enhanced RSA is based on the Existence of four Prime Numbers that will give the ability to the enhanced encryption method to increase the difficulty of factoring of the variable (n), Its speed which is a crucial factor increases the process of encryption and decryption. While generating the variable (n) by original RSA algorithm, this helps to generate the public and private key which includes the

number of 500 digits by using two primes number with 200 digits each. Multiplication process will take much longer time than the time to generating the same variable (n) by using four prime numbers where each number with 200 digits. The time it takes to multiply four prime integers with 200 digits takes substantially longer than the time it takes to generate the same variable (n).

LITERATURE REVIEW

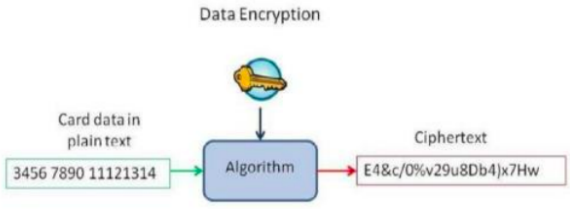
1. This work uses a modified technique of RSA that incorporates an exponential variant of RSA with four prime numbers and multiple public keys using the k neighbor algorithm. Using the k-nearest neighbor technique, my modified approach adds an extra layer of security. It makes the determined value in cipher text more random. Because it eliminates the hassle of redundancy in both cypher and plain text. There is no repeat of encrypted text in the modified technique, which is the same as plain text. Any intruder will find it tough to hack the information being delivered if you use this method. It assists in improving the approach's efficiency and security. The modified strategy employs two public keys that are supplied independently, preventing the attacker from gaining extensive knowledge of the keys and thereby decrypting the communication.
2. This paper offers an RSA-based E-cash network and examines the system's operations in detail by constructing a simplified system. The results of the experiments reveal that the system has a number of advantages, including a modest range of public keys provided by the bank, as well as being convenient and secure. The client might control the random number in the card to conduct procedures such as blind signature using an intellectual card embedded with the application. Furthermore, this random variable could be used as the intelligent card's identifying password. Naturally, this technique has several flaws, such as the excessively long key length. It's possible that the maximum length is more than four times the length of N. This study presents a revolutionary E-cash payment mechanism that is both secure and convenient. Based on the feature of the modulus operation, this technique may meet the demand for E-cash with only a few public keys and solve the

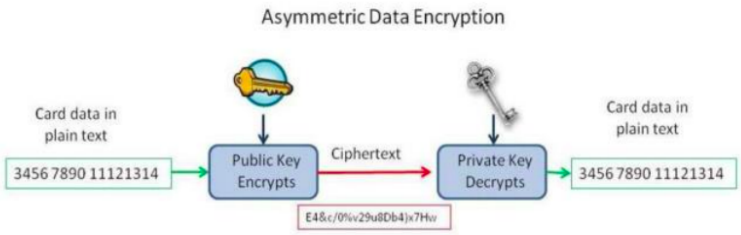
problem of payment modification by employing blind signature and direct signing. As a result, the proposed technique might be employed for online ecommerce transactions.

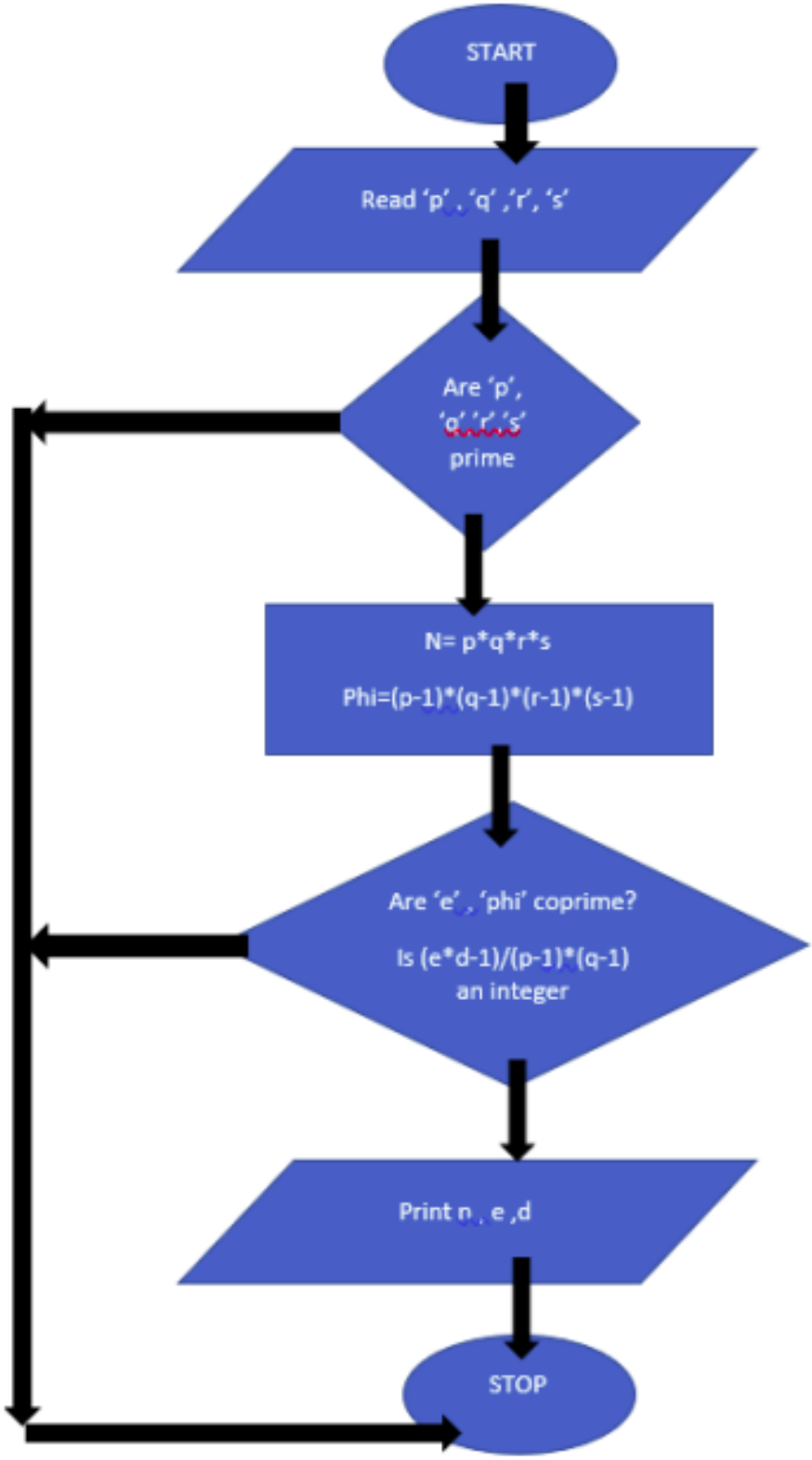
3. A model of two untraceable BS systems is presented in this study. The computation time requirements of the cryptographic operations involved in various steps of the schemes have been evaluated using Hwang's and Lee's schemes. The literature analysis reveals that both Hwang's and Lee's schemes are untraceable, even though untrace ability is a critical but difficult criterion for any BS scheme. Furthermore, each of them meets the other criteria for a great BS scheme, and compromising their security is difficult. However, a comparison of calculation time requirements reveals that Hwang's approach takes significantly longer than Lee's to complete the simulation. Hwang et Al approaches on the other hand, are based on the RSA cryptosystem, which is by far the easiest to grasp and apply. The simulation model's output is a comparison of the computing time requirements of the chosen BS schemes' blinding, singing, unblinding, and verification phases.

PROPOSED NETWORK SECURITY MODEL

The public key can be supplied to a merchant or to the end POS device in the online payment environment, and that device will hold the key in hardware or software. Even if the key is obtained by someone who shouldn't have access to it, the person can only use it to encrypt data; he won't be able to decrypt anything. On the other hand, the associated private key, which is used for decryption, must be treated with extreme caution. The CVV number is encrypted in our system using the ERSA complicated algorithm. Only the encrypted CVV number will be utilized for online payments. Even if a hacker obtains a person's credit card information, he will be unable to use the right CVV number. In asymmetric cryptography, the RSA algorithm is the most widely used public key encryption algorithm. There are two types of keys: public and private. A Modular is a system component that assists other components in providing services but is not generally considered a separate system. A detachable component is one that may be swapped out for others to create units of varying size, complexity, or function, as in. As a result, the RSA cryptosystem is built using modular techniques.






START
Read 'p', 'q', 'r', 's'
Are 'p', 'q', 'r', 's' prime
N= p*q*r*s
Phi=(p-1)*(q-1)*(r-1)*(s-1)
Are 'e', 'phi' coprime?
Is (e*d-1)/(p-1)*(q-1) an integer
Print n, e ,d
STOP

KEY GENERATION

Enhanced RSA involves a public key and a private key. The public key is known by everyone and is used for encrypting the messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key. The keys for the RSA algorithm are generated the following way: Choose four distinct prime number p,q,r,s. Compute n = p*q*r*s. n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length. Computeφ(n)=φ(p)φ(q)φ(r)φ(s)=(p−1)*(q−1)*(r−1)*(s−1)== n -(p+ q+r+s1),where φ is the Euler's totient function. Choose an integer e such that $1 < e <$φ(n) and gcd(e, φ(n)) = 1; i.e., e and φ(n) are coprime. e is released as the public key exponent. e having a short bit-length and small Hamming weight results in more efficient encryption – most commonly 216 + 1 = 65,537. However, much smaller values of e (such as 3) have been shown to be less secure in some settings. Determine d as $d \equiv e-1 \pmod{\varphi(n)}$; i.e., d is the multiplicative inverse of e (modulo φ(n)). This is more clearly stated as: solve for d given $d \cdot e \equiv 1 \pmod{\varphi(n)}$ This is often computed using the extended Euclidean algorithm. Using the pseudocode in the Modular integers section, inputs a and n correspond to e and φ(n), respectively. d is kept as the private key exponent. The public key consists of the modulus n and the public (or encryption) exponent e. The private key consists of the modulus n and the private (or decryption) exponent d, which must be kept secret. p, q,r ,s and φ(n) must also be kept secret because they can be used to calculate d as in Units.

ENCRYPTION - CLIENT SIDE

Suppose a person A transmits his public key (n, e) to a person. B then wishes to send message M to A. Since we are encrypting the CVV no the user has to enter the required RSA details for only once. The ciphertext will be generated when the user mentions the CVV no.

DECRYPTION - SERVER SIDE

Service side here is the bank which has got the value of d. Since they are decrypting the CVV they already have the d value The plain will be generated when the bank server side uses the default CVV no.

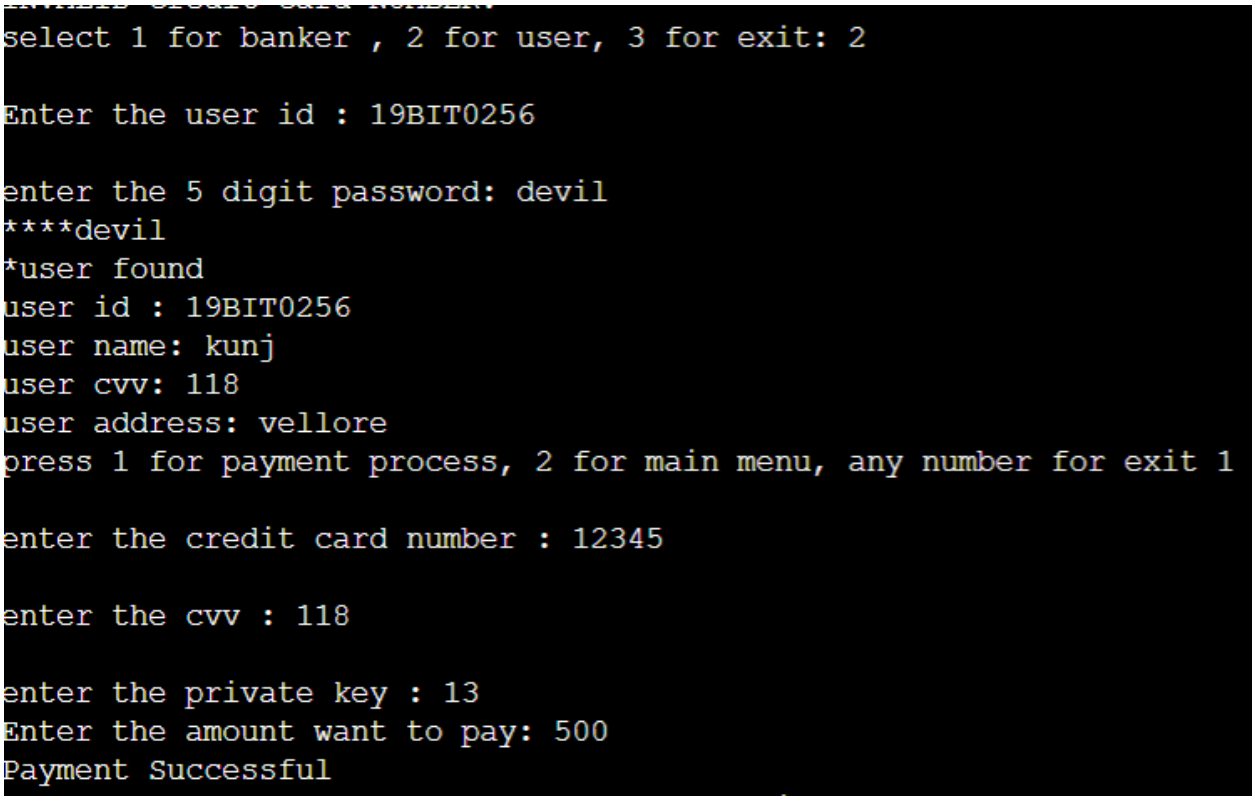
MODULES

1) Register: Users will have to register in order to get access to the system.
2) Login: User will have to provide his username and password in order to login to the system.
3) Records: Here all the products can be viewed by the user along with its other details like short description,
4) Payment: In order to perform any transaction here the user needs to provide his bank information like his Card no, CVV no to make the payment.
5) Encryption: The CVV no using encrypted using Enhanced RSA

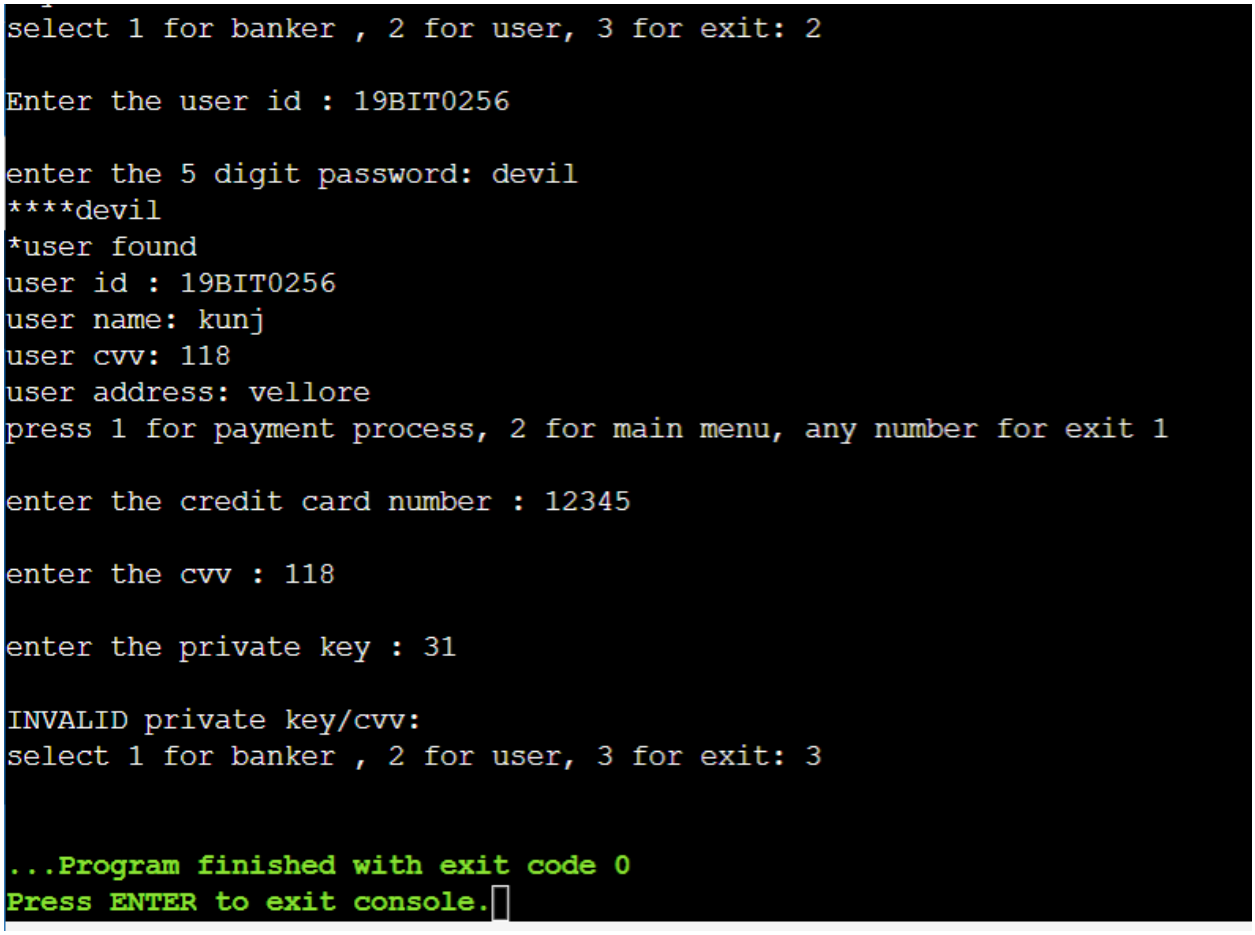
IMPLEMENTATION

```
    7 | # include <fstream> # include <string.h> # include <iostream> # include
      |                     ^

select 1 for banker , 2 for user, 3 for exit: 1
ENTER BANKER ID: 2345
Enter 10 digit password: incredible
*********sh: 1: cls: not found
*                      .       ADMINISTRATOR PAGE


Choose from the following option:
1. add user
2.view user details
3. Main Page

ENTER THE OPTION: 1
enter four large prime numbers(p, q, r and s): 2 3 5 7
select the value of e: 5 7 11 13 17 19 23 25 29 31 35 37 41 43 47  31
sh: 1: cls: not found
        ADD USERS
Enter the following details
User Name: kunj
User id: 019BIT0256
Enter credit card number 12345
Enter cvv: 118
Enter Address: vellore
Create new password(5): devil
enter the initial balance: 5000

Original cvv: 118
encrypted cvv is : 30
Private Key: 13
```

Encrypting cvv, using the prime numbers given by the user, and providing the private key to the user for future transactions.



Entering the correct CVV and private key so as to decrypt the encrypted value of CVV stored in the bank's server.



When an incorrect private key is entered, the transaction won't happen and will display the message Invalid private key/cvv.

CONCLUSION

We can raise the complexity of the encryption of the CVV number, which is a very crucial aspect in online Card Payment activity, by using Enhanced RSA, which takes into account four parameters rather than the original RSA approach, which only employed two. The proposed system's use of prime numbers enhances encryption and decryption time. The use of the ERSA method makes computation more difficult and contributes to the level of security while using a credit card.

The brute force attack which is generally employed by the attackers to exploit and get knowledge about keys. Brute force can work to an extent on traditional RSA, but with Enhanced RSA the computational complexity is far too much for an attacker to deploy brute force attacks. Hence, this new Enhanced RSA also addresses the defense from the attackers on how to make them ineffective.

REFERENCES

[1] Yun Ling, Yiming Xiang and Xun Wang, "RSA-based secure electronic cash payment system," IEEE International Conference on Industrial Engineering and Engineering Management, Singapore, 2017, pp. 1898-1902. (2017)

[2] K. Alam, K. Md Rokibul Alam, O. Faruq and Y. Morimoto, "A comparison between RSA and ElGamal based untraceable blind signature schemes," 2016 International Conference on Networking Systems and Security (NSysS), Dhaka, pp, 1-4.(2016)

[3] M. Savari, M. Montazerolzohour and Y. E. Thiam, "Comparison of ECC and RSA algorithm in multipurpose smart card application," Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), Kuala Lumpur, 2012, pp. 49-53.(2012)