

PAPER • OPEN ACCESS

## Enhanced rearrangement technique for secure data transmission: case study credit card process

To cite this article: Tushar Vyavahare *et al* 2017 *IOP Conf. Ser.: Mater. Sci. Eng.* **263** 042102

View the [article online](#) for updates and enhancements.

### Related content

- [Modified Multi Prime RSA Cryptosystem](#)  
M Ghazali Kamardan, N Aminudin, Norziha Che-Him et al.
- [High capacity optical encryption system using ferro-electric spatial light modulators](#)  
Paul C Mogensen, René L Eriksen and Jesper Glückstad
- [An analysis of environmental data transmission](#)  
Lina Yuan, Huajun Chen and Jing Gong

# Enhanced rearrangement technique for secure data transmission: case study credit card process

**Tushar Vyavahare, Darshana Tekade, Saurabh Nayak, N Suresh kumar and S S Blessy Trencia Lincy**

School of Computer Engineering, VIT University, Vellore-632014, Tamil Nadu, India

E-mail: sureshkumar.n@vit.ac.in

**Abstract.** Encryption of data is very important in order to keep the data secure and make secure transactions and transmission of data. Such as online shopping, whenever we give our card details there is possibility of data being hacked or intruded. So to secure that we need to encrypt the data and decryption strategy should be known only to that particular bank. Therefore to achieve this objective RSA algorithm can be used. Where only intended sender and receiver can know about the encryption and decryption of data. To make the RSA technique more secure in this paper we propose the technique we call it Modified RSA, for which a transposition module is designed which uses Row Transposition method to encrypt the data. Before giving the card details to RSA the input will be given to this transposition module which will scramble the data and rearranges it. Output of transposition will be then provided to the modified RSA which produces the cipher text to send over the network. Use of RSA and the transposition module will provide the dual security to whole system.

## 1. Introduction

Internet has become the most important thing for day to day to transmission in today's era. Tremendous amount of data is transfer over the network even at every second. Therefore we should make sure that this data is secure enough to provide the reliability of communication and also preserve the data integrity. Also to ensure that the data is protected from illegal user and unauthorized access. To achieve the same we need some cryptography techniques. To establish the secure connection between client and server for data transmission, such as browser and mail client like Gmail. It allows confidential information of a user like credit card numbers, cvv, expiry date and password and other login credentials to be sent and receive in secure manner.

But to accomplish this goal we need a strong encryption technique. It is really important to make sure that how data is encrypted so that no one can crack it. Asymmetric encryption is also known as public key cryptography. For encoding and decoding public key cryptography uses a separate key. For encryption purpose any user can use the public key of a certain user to encrypt a message. But on the other hand private keys are secret. This also provides the secure way of decryption on receiver side. RSA is the very common asymmetric encryption algorithm for secure data transmission.

To send the data sender can make use of the public of a particular receiver and encrypts the data with the help of its own private key. To double the level of security we have implemented a module called transposition module which will help to keep data more secure from intruder. When the encrypted data is sent over the network in the form of cipher text, on the receiver side decryption is performed by giving the data as input to the Modified RSA on the receiver side and further its output



will be given to the Row transposition module on the receiver side which will decrypts the data and fetches the original details encrypted by the sender.

## 2. Related work

Aayush Chhabra et al. [1] proposed an technique to improve a security provided by RSA. In this technique main focus is on to reduce the need of transferring  $n$  and multiplication of two larger numbers .reduces the necessity to transfer  $n$ , the multiplication of two random large prime numbers. Due to large numbers it's become really difficult to crack message. Wang Rui et al. [2] developed a RSA algorithm which is known as K-RSA. Main Advantage of this approach is that it uses multiple parameters. However it provides faster speed as compared to other modified RSA algorithms. These algorithms work on decryption process of message in very well manner and try to reduce the comparisons. Pranesh et al. [3] proposed a technique is that original message is divided into two arrays. After rearranging their positions, those Arrays are combined. The modified message data is given as an input to the proposed RSA encryption technique. Hemalatha et al. [4] proposed an Attribute- Based Encryption technique, It is a asymmetric key encryption scheme. It mainly focused on scalability and flexibility. Arockiam et al.[5] introduces an approach that combines two algorithms algorithms RSA and Diffie-Hellman technique. Here the main idea is to provide a security for communication path between sender and receiver. The RSA algorithm can be used for Public key cryptography and digital signature. Diffie Hallman algorithm mainly used as key exchange technique. In this approach output of RSA given as input to Diffie Hellman. RSA algorithm used for key generation. Mohammad et al. [6] proposed the Diffie Hallman technique is used for producing a cipher message for given plain message.

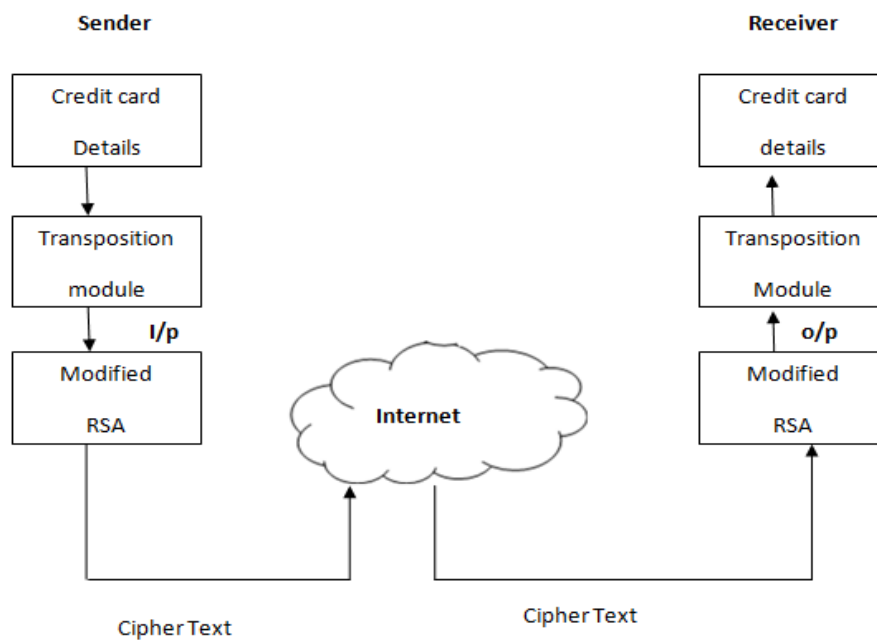
## 3. Proposed work

The proposed method here focuses on the providing the dual security to the data which is getting transferred over a network. The original input data bits will be scrambled and rearranged in certain way and this rearranged data will again be modified in order to encrypt it in a more protective way. The normal or traditional RSA technique is

### 3.1. Architecture of system

To give the overall idea about the proposed model and flow of the project see Figure 1 (Architecture of the system). This diagram basically gives the overall idea about how the each model and component of project works. In credit card system for processing any transaction the user(Sender) gives the required and necessary information about the card details which includes Unique credit card number , password ,CVV and expiry date . All this information is in numerical format. These numerical values are consolidated as one string and it is given as input to the transposition Model. Transposition module is not actually involved in encryption process. But to accomplish the motive of dual security approach transposition module rearranges data in particular manner as explained in transposition section 3.3.

The output of the transposition module will be the scrambled data which will be given input to the Modified RSA algorithm. By using Chinese Remainder Theorem the data will be encrypted as described in section 3.2 and this entire process will generate the cipher text. Now the data is ready to send over the network. This information will be received at the intended receiver and the decryption process will be carried out. Output of transposition module while decryption is treated as the plain text and this will be displayed to the receiver.



**Figure 1 Architecture of the system**

### 3.2 RSA with CRT

Here say  $D_i$  is decoding coefficient which refers to the number of multiplication which are required to perform in order to calculate  $N_i$  which identifies the range of the result which are obtained as intermediate results. From the observations we can say that complexity of decryption module  $M_i$  of RSA depends on the parameters  $D_i$  and  $N_i$  as mentioned above CRT and RSA plays the important role to decide the scale of  $D_i$  and  $N_i$ . The final equation includes,  $M_i = C_i^{D_i}$ .

#### 3.2.1 Key generation for the algorithm

1. consider the two prime numbers (say  $pr_1$  and  $pr_2$ ) nearly of same size. Take the gcd of  $pr_1$  and  $pr_2$  which should be equal to 2
2. Now Calculate  $N_i$ .  $pr_1 * pr_2$  therefore,  $N_i = pr_1 * pr_2$
3. Choose any two numbers (say  $Rn_1$ ,  $Rn_2$ ). Take the gcd of  $(Rn_1, pr_1-1) = 1$  Also take the gcd of  $(Rn_2, pr_2-1) = 1$  and take  $Rn_1 \equiv Rn_2 \pmod{2}$
4. In order to choose  $d_i$ , make sure that  $d_i \equiv Rn_1 \pmod{pr_1-1}$  and  $d_i \equiv Rn_2 \pmod{pr_2-1}$ .
5.  $X = d_i - 1$
6.  $Y = X \pmod{N_i}$ . This gives  $N_i$

From key generation algorithm we get public key and private key. Public key here is  $pk = (N_i, e_i)$  and the private key here is  $(pr_1, pr_2, Rn_1, Rn_2)$ . By step 5 and 6 we can calculate  $e_i$  for that take the gcd of  $(d_i, pr_2-1) = 1$ . Also take gcd of  $(d_i, N_i) = 1$ .

Now in step 4 apply the Chinese Remainder Theorem. Here the different mod operations have to be comparatively prime pairs to obtain the correct answer. Here as you can observe that  $(pr_1-1)$  and  $(pr_2-1)$  both are even therefore we cannot CRT (Chinese Remainder Theorem). On the other hand if you see the gcd of  $[(pr_1-1)/2, (pr_2-1)/2] = 1$ . Also we know that gcd of  $(Rn_1, pr_1-1) = 1$  and gcd of  $(Rn_2, pr_2-1) = 1$ . Here  $Rn_1, Rn_2$  are odd numbers and  $Rn_1-1, Rn_2-1$  are even numbers. At last we have gcd of  $(d_i, pr_1-1) = 1$  which indicates that  $d_i$  is odd number and on the other hand  $(d_i-1)$  is even number.

To find  $d_i = R_{n1} \bmod p_{r1}-1$ ,  $d_i = R_{n2} \bmod p_{r2} -1$

First find a solution to:

$$d_i-1 = (R_{n1}-1) \bmod (p_{r1}-1)$$

$$d_i-1 = (R_{n2}-1) \bmod (p_{r2}-1).$$

Simplify the equation ,

$$x_i = d_i = (d_i-1)/2 = (R_{n1}-1)/2 \bmod (p_{r1}-1)/2$$

and

$$x_i = d_i = (d_i-1)/2 = (R_{n2}-1)/2 \bmod (p_{r2}-1)/2,$$

Now by applying Chinese Remainder Theorem we can calculate  $d_i$  as follows:

$$d = (2 * d_i) + 1$$

### 3.2.2 Decryption Algorithm for RSA + CRT

Consider message  $P_m$  be the plaintext and  $C_m$  as cipher text. If  $C_m$  is not divisible by  $p_{r1}$  and  $R_{n2} = d_i \bmod p_{r1}-1$ , then  $M_{cp} = C_j \bmod p$ .

For decryption purpose follow the steps as below:

1.  $mP = M_{cp} \bmod p_{r1} = C_j \bmod p_{r1}$  and

$$mQ = M_{cq} \bmod p_{r2} = C_j \bmod p_{r2}.$$

2. Now apply chinese remainder theorem

$$J = mP \bmod p_{r1} = C_j \bmod p_{r2},$$

$$J = mQ = R_{n2} \bmod p_{r2} = R_{n2} \bmod p_{r2}.$$

### 3.2.3 Transposition Module

In the proposed method the role of transposition module is significantly important. When data for credit card such as Pin , card number and password is given as input to the system. This data needs to rearrange before it is given to the modified RSA for further encryption process. Earlier many data arrangement techniques have been used such as based on even numbers rearrangements, Odd number rearrangements, Prime Numbers rearrangement of data etc . But if we think of it in the intruder's point of view we will observe that these techniques are likely to be predicted by intruder and therefore extract the information. This puts the whole system in unsecure environment. To avoid it we came up with another approach which fill out these loop holes and also it is less likely to be predicted by the network intruder. The technique is called as Row Transposition Module. In Row Transposition module, numbers are first arranged in matrix form and then transpose of matrix is taken. Transposed matrix will put the original matrix row elements as column elements and vice-versa [See the Figure 2].

**Original Data:** 1 2 3 4 5 6 7 8 9

$$A = \begin{bmatrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 9 \end{bmatrix} \longrightarrow A^T = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix}$$

**Original Matrix    Transpose Matrix**

**Rearranged Data:** 1 4 7 2 5 8 3 6 9

**Figure 2 Row Transposition Module Technique**

#### 3.2.4. Algorithm for transposition Model

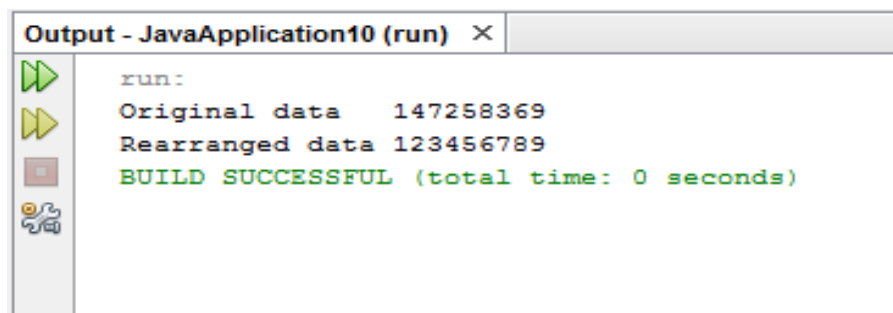
Step 1 Input the numeric data N

Step 2 arrange the data in matrix form (Matrix90 [A])

Step 3 Take the transpose of the original matrix. i.e. [A] T

Step 4 Extract elements from matrix in Column wise format which gives rearranged data R

#### 4. Results

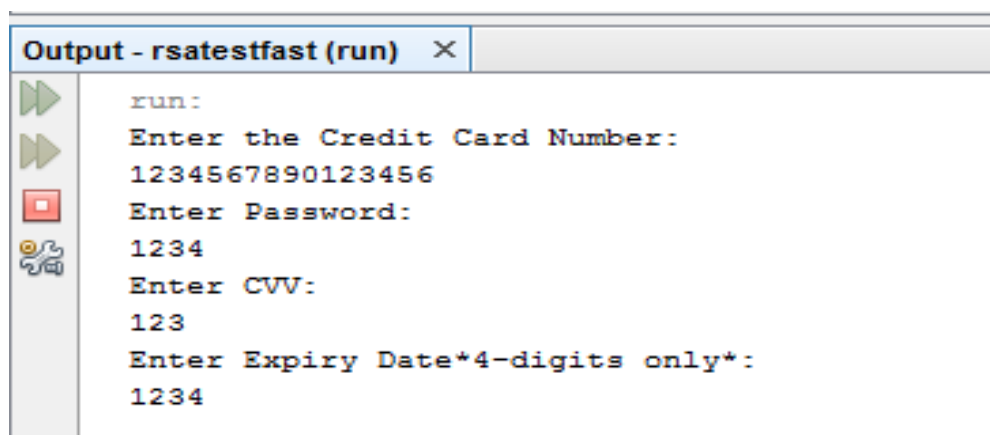


```

Output - JavaApplication10 (run) ×
run:
Original data 147258369
Rearranged data 123456789
BUILD SUCCESSFUL (total time: 0 seconds)

```

**Figure 3 Output of Transposition Module**



```

Output - rsatestfast (run) ×
run:
Enter the Credit Card Number:
1234567890123456
Enter Password:
1234
Enter CVV:
123
Enter Expiry Date*4-digits only*:
1234

```

**Figure 4 Credit card details for encryption process**

```

final string is:123456789012345612341231234
Cipher Text: 147036322258141433369252114
Message m:
147036322258141433369252114

```

**Figure 5 Input data to M-RSA**

```

ALICE ENCRYPTS m FOR BOB; BOB DECRYPTS IT:
Message encrypted with Bob's public key:
3178878244890593383361357228736526086289333801625612219002855767166718766457544

Original message back, decrypted:
147036322258141433369252114

ALICE SIGNS m FOR BOB; BOB VERIFIES SIGNATURE:
Message signed with Alice's private key:
175315591799153373471705108885434637740048899515576983152474945398741134609859290834884108571

Original message back, verified:
147036322258141433369252114

```

**Figure 6 Encryption by sender**

```

BOB SIGNS AND ENCRYPTS m FOR ALICE;
ALICE VERIFIES SIGNATURE AND DECRYPTS:
Message signed and encrypted,
using Bob's secret key and Alice's public key:
147036322258141433369252114

Original message back, verified and decrypted,
using Alice's secret key and Bob's public key:
147036322258141433369252114

```

**Figure 7 Decryption by receiver**

```
Original message back, verified and decrypted,  
  using Alice's secret key and Bob's public key:  
147036322258141433369252114  
Credit Card Number:1234567890123456  
Password:1234  
CVV:123  
Expiry Date:1234
```

**Figure 8 Output data at receiver side**

## 5. Conclusion

In this paper we have proposed technique for secure transaction and transmission of data using credit card case study .We can conclude from the above result that with this technique data can be transmitted more securely over the network. We have combined RSA and Transposition module to enhance the security. The novelty of our technique is that the data is first rearranged with transposition module, we have used row transposition method to encrypt the data and then the input is fed to RSA thus making the transmission more secure.

## References

- [1] Chhabra A and Mathur S (2011) Modified RSA Algorithm: A Secure Approach. In Computational Intelligence and Communication Networks (CICN), 2011 International Conference on 545-548
- [2] Wang Rui; Chen Ju and Duan Guangwen (2011) Ak-RSA algorithm *Communication Software and Networks (ICCSN)* **21** 27-29
- [3] Pranesh R, Harish V, Vigneshwaran M and Manikandan G A New Approach for Secure Data Transmission
- [4] Hemalatha S and Manickachezian R Security Strength of RSA and Attribute Based Encryption for Data Security in Cloud Computing
- [5] Arockiam L and Monikandan S (2013) Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm *International Journal of Advanced Research in Computer and Engineering* **2**
- [6] Mohammad, Malakooti V and Nilofar Mansourzadeh A Robust Information Security Model for Cloud Computing Based on the Scrambling Algorithm and Multi Level Encryption