Volume 1, No. 1, August 2010

Journal of Global Research in Computer Science

RESEARCH PAPER

Available Online at www.jgrcs.info

Secure Transmission of Data Using CRT-RSA

V.Senthil Balaji*[1] and R.Rengaraj alias Muralidharan*[2]

*Assistant Professor, Dept. of Computer Applications,
Saranathan College of Engineering, Tiruchirapalli, Tamil Nadu, India
v_senthilbalaji@yahoo.co.in, rengaraj_ramanujam@yahoo.co.in

***Abstract*:** A new scheme for transmitting encrypted data across networks from sender to receiver through multiple channels. The CRT-RSA algorithm is used for generating cipher text from original message blocks of data. The inverse transformation of the algorithm is applied at the receiver end for decryption of cipher text into original message. The theory implementation of this scheme is described in this paper.

Keywords: Cryptography, Secure transmission, CRT, RSA, Multiple Channels, Block cipher.

INTRODUCTION

The transfer of confidential or proprietary information requires secure channel. Many secure transmission methods require a type of encryption. To open an encrypted file the exchange of keys is done through other transmission methods. Encryption is the cryptographic primitive method mostly used in protecting the secrecy of the data. The Chinese remainder theorem CRT [1] states that if q0, q1...qk -1 are k pair wise relatively prime positive integers and a0, a1...ak -1 are positive integers then there exists exactly one integer *a* where $0 \leq a < q$ for $q=\prod_{i=0}^{k-1} qi$ such that a = ai mod qi for $0 \leq i < k$. The integers q0, q1...qk -1 are called the moduli while the integers a0, a1...ak -1 are called the residues. The CRT has well known applications in both secret sharing and error correcting codes [2]. In this work, RSA encryption with Chinese remainder theorem will be combined to produce a scheme for transmitting sensitive data over multiple channels.

In digital communications, parallel transmission is the simultaneous transmission of related signal elements over two or more separate paths. Multiple cables are used which can transmit multiple bits simultaneously, which allows for higher data transfer rates than can be achieved with serial transmission. RSA (which stands for Rivest, Shamir and Adleman who first publicly described it) is an algorithm for asymentric public key cryptography.

PROPOSED MODEL

Using *R* number of multiple transmission channels between the sender and the receiver from which *S* Channels are chosen using some selection criteria. The original message or plain text is divided into N bits of cipher blocks. These blocks are encrypted using an RSA-CRT module. The encrypted data is transmitted over a set of *S*-selected channels. The remaining *R-S* channels are used to transmit irrelevant data in order to decrease the ability of the intruders from hacking.

At the receiver side, the inverse of the RSA-CRT is applied to the original N-bit cipher block which where received through S-channels, and then decrypt module is used to get the original message or plain text. Prior to transmission of cipher data the selected S-channels are informed at the receiver side. The data received through R-S channels at the received end are discarded.

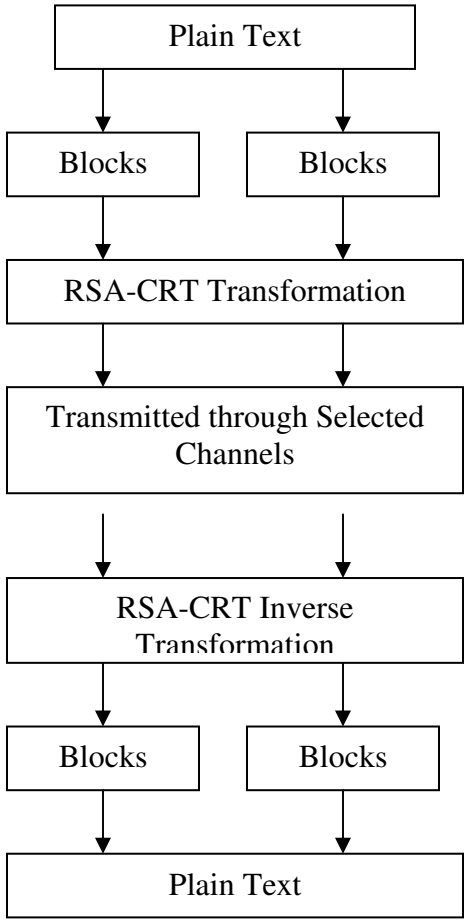

Figure 1: Data Blocks

The plain text is being spitted into equal size of blocks. These blocks of data are being sent to the intended receiver through multiple selected channels, after applying RSA-CRT transformations.

Session Phase

There is two different sessions executed during transmission. The first sessions is initiated before the transmission while the second session initiated at the end of the transmission. The first session is termed as sender session, while the second session is receiver session.

Sender Session

The sender process executes the following steps:
1.On data arrival for transmission, the data or message *M* is partitioned into blocks.
2.The partitioned block is transmitted after applying RSA-CRT transformation.
3. Transmit the transformed data into *S* selected channels.
4. The sender process waits for more input until data available for sending. This sender side is a blocked phase.

Receiver Session
The receiver process executes the following steps:
1.Select the channels step.
2. In this step, the receiver process waits for input from different channels. This operation is blocking.
3. The received data on each channel is maintained as separate blocks.
4. These blocks are decrypted using inverse module of RSA-CRT transformation.

Channel Selection

The transmission channels *S* a subset from *R* is chosen on accounting of various constraints such as, network traffic, congestion occurrence, and previous network failures. On the *R-S* transmission channels irrelevant data is sent. For identifying irrelevant data a stream of pre-determined bits are being added to blocks of data before transmission on *R-S* channels.

Number of Channels

The maximum number of channels *max(S)* used for transmission is based on the number of blocks to be transmitted with an *max_constraint* on the *max(S)*.

Chinese Reminder Theorem in RSA

The usage of Chinese Reminder Theorem (CRT) during decryption results much faster. The RSA-CRT differs from the standard RSA in key generation and decryption.

RSA-CRT key generation

1. Let p and q be very be two very large primes of nearly the same size such that gcd (p-1, q-1) = 2.

2. Compute $N = p*q$.

3. Pick two random integers dp and dq such that gcd (dp, p-1)=1,
   gcd (dq, q-1)=1 and dp=dq mod 2.

4. Find d such that d=dp mod p-1 and d=dq mod q-1.

5. Compute e=d-1 (mod ((p-1)*(q-1)).

The public key is <N, e> and the private key is <p, q, dp, dq>. Since, gcd (dp, p-1)=1 and d=dp mod p-1, we have gcd (d, p-1)=1. Similarly, gcd (d, q-1)=1. Hence gcd (d, ((p-1)*(q-1)))=1 and by step 5, e can be computed.

In step 4, the values of p-1 and q-1 are even. so Chinese reminder theorem cannot be directly applied. Hence, gcd((p-1)/2,(q-1)/2)=1. Since gcd(dp, p-1)=1 and gcd (dq, q-1)=1, (as per step 3) essentially dp, dq are odd integers and dp-1, dq-1 are even integers. We have gcd (d, p-1)=1, which implies that d is odd and d-1 is even.

To find solution to
d=dp mod p-1,
d=dq mod q-1.
We find d-1=dp –1 mod p-1,
d-1=dq –1 mod q-1.

By applying the cancellation law and taking the common factor 2 out, we have
x=d'= (d-1)/2=(dp –1)/2 mod(p-1)/2,
x=d'=(d-1)/2=(dq –1)/2 mod(q-1)/2.

Using Chinese Remainder Theorem we find d such that d = (2*d') +1.

RSA-CRT Decryption

The cipher text C is retrieved from the encryption algorithm.

For decryption we find
1. Mp=Cdp(mod p)= Cd(mod p) and Mq=Cdq(mod q)= Cd(mod q).

2. Then using Chinese Remainder Theorem, we find a solution for
M=Mp(mod p)= Cd(mod p),
M=Mq=Cdq(mod q)= Cd(mod q).

In this particular technique of transferring data using multiple channel and RSA-CRT, we can justify that the security is maintained because there may be a chance for the intruders to break the encrypted method by using long permutation method. So, we can surely justify that data will be more

secured by using multiple channels compared to data using single channels. In serial transmission even though the data's security can be maintained but the chance for maintaining the reliability is very less. That is, there are some types of users who aim only in affecting the reliability of the transmission but not about breaking the secrecy of the data. In our paper since we are dealing with multiple channels, the rate of reliability will be high compared with single channel.

Loss Mechanism	**Number of Packets**	**Loss Rate**
Node Reset	265	$2x10^{-4}$
Unknown	71	$6x10^{-5}$
Congestion	26	$2x10^{-5}$
CRC Failure	5	$4x10^{-6}$
Failed Device	0	0
Accounting	0	0

Table 1: Total number of lost packets due to factors of reliability

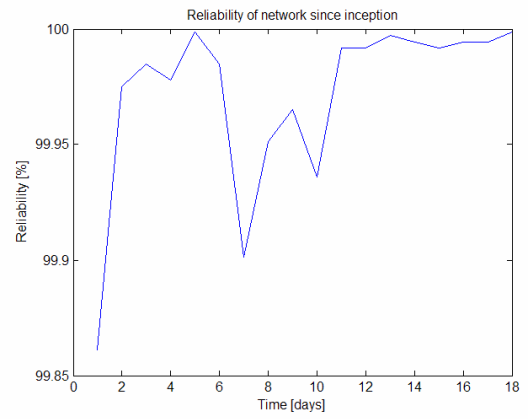

Figure 2

CONCLUSION

In this paper new technique for transmitting data is introduced. The proposed scheme is found to be more secure by transmitting data through different channels for the same receiver in various blocks

REFERENCES

[1] Aho A., Hopcroft J., and Ullman J. The Design and Analysis of Computer Algorithms. Addison-Wesley, Reading, Mass., 1974.

[2] Goldreich Oded, Ron Dana, Sudan Madhu, Chinese Remaindering with errors. Proceedings of the Thirty- First annual ACM Symposium on Theory of Computing 1998.

[3] Ahmed A. Belal, Alexandria, Secure Transmission of sensitive data using multiple channels.

[4] Dan Boneh and Hovav Shacham, Winter/Spring 2002. Fast Variants of RSA. CryptoBytes-Volume 5, No. 1, Winter/Spring 2002, pg 1-9. Available:http://www.rsasecurity.com/rsalabs/cryptobytes/CryptoBytes_January_2002_final.pdf

[5] Hung-Min Sun and Mu-En Wu, 2005, February. An Approach Towards Rebalanced RSA-CRT with Short Public Exponent. Cryptology ePrint Archive: Report 2005/053, Available: http://eprint.iacr.org/2005/053