International Journal of Advance Research in Science and Engineering
Volume No.06, Special Issue No.(01), December 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

AN IMPLEMENTATION OF ALGORITHM FOR SECURITY IN WIRELESS COMMUNICATION NETWORK MODELS

[1]Dave Malay Bharat Kumar , [2]Dr. Jitendra Seethlani

[1,2] Research Scholar, Sri Satya Sai University of Technology and Medical Sciences, India)

ABSTRACT

Communication or computer networks areundergoing a fast development in various fields of applications like Information technology, business, e-commerce, medical applications etc. Even more, wireless sensor networks targets the applications like temperature sensing, destruction estimation, military and many others where human support is required only at remote console. Whatever is the communication scenario, wired locally or wireless geographically, or sensor nodes at remote location, it involves the source, receiver and a channel. Therefore, the channel is vulnerable for attack by an imposter which could challenge the authenticity and confidentiality of the communication data. In this paper, we constructed a reliable cryptography tool model by utilizing the properties of RSAalgorithm in the Matlab programming environment. This algorithm can be efficiently used for communication networks for creating an authentic layer for secure data transfer. We take ATM Banking transaction as an illustrative communication network between ATM machine client and Banking server and implementing the algorithm usage that utilizes public cryptography, RSA algorithm encryption and decryption method.

I INTRODUCTION

Information security is the protection of information and its critical elements, including the system and the hardware that process, store, and transmit that information. Cryptography plays an important role in today's digital world. Many cryptographic techniques have been developed to meet the various requirements arising from applications. Cryptographic algorithm, which is also called a cipher, is the mathematical function used for encryption and decryption. Generally, there are two related functions: one for encryption and the other for decryption. Encryption/decryption protects information from being used by the attacker. Encryption/decryption is a security mechanism where cipher algorithms are applied together with a secret key to encrypt data so that they are unreadable if they are intercepted.

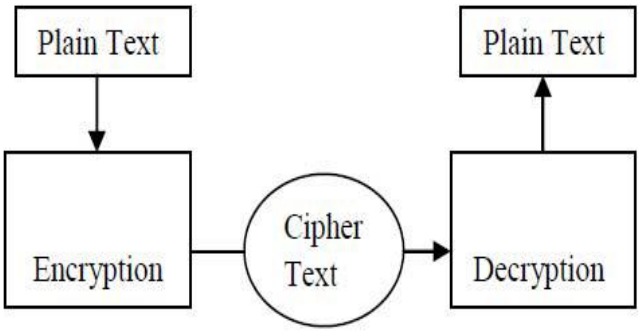
Hence, a communication or computernetwork that involves the infrastructure behind any applicationinvolves great deal of information transmission, storage in the real time. This can also increase the risk of data attack by an intruder or an imposter that can hamper the communication between client and the server. The attacks can be of passive,

where the intruders listen the communication and can be otherwise an active attack, where the intruder modifies the communication data. Both these types of attacks involve serious havoc to the communication privacy. Take an example of online net banking transaction between the customer machines to the bank server. Any attack on this confidential data can go for complete destruction of the banking concept. In order to prevent these attacks, data encryption at the source anddecryption at thereceiver can be made into existent so that nofraudulent activity will be possible if waiting in thecommunication channel. Even if the imposter made a passive attack on the encrypted data recovery in the channel, the data is of not in use. Cryptography, a science, involves an encryption and decryption pair that can be of one of the major technique in practice to prevent unauthorized access into the network. This paper, we utilize the properties of RSA algorithm and also made the encryption and decryption algorithm more robust by providing alternate password settings by taking the example of ATM banking transaction involves ATM machine, channel, bank server and in addition, we use customer's mobile to set the secondary password settings. The algorithm is constructed using Matlab programming environment, constructed reliable cryptographic model through GUI, and tested this communication model using the mobile settings inbuilt on the Matlab GUI model.

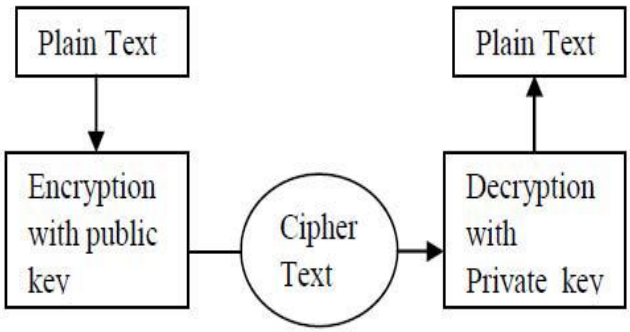
II METHODOLOGY

Cryptography is a process which is associated withscrambling plaintext (ordinary text, or clear text) into cipher text (process called encryption), then back again to plain text (known as decryption). Symmetric cryptography shares the same key for encryption and decryption process. Asymmetric cryptography uses two different keys – public and private keys. Private Key is derived from public key. Symmetric cryptography is easy to implement, fast in computation and easy to construct as it involves simple substitution and permutation method. This techniques used in applications where lot of data transfer involved but not taken care security issues to the extend. Asymmetric or public key cryptography method involves mathematical concepts that made thistechnique used for highly secure data transfer applications like military, banking and internet transactions, email, e-commerce, business and many others where private and confidential data transfer need to be made highly secure and authenticity.Symmetric cryptography algorithms include DES (Data standard Encryption), triple or 3 DES, AES (Advanced Encryption Method) and Asymmetric or public key cryptography algorithms include RSA (Rivest ShamirAdleman), ECC (Elliptic Curve Cryptosystem), Diffie-Hellman protocol etc.

International Journal of Advance Research in Science and Engineering
Volume No.06, Special Issue No.(01), December 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354



Symmetric Cryptography



Asymmetric Cryptography

III RSA ALGORITHM

This paper utilizes the underlying mathematical foundations of RSA Algorithm. RSA Algorithm is a public key cryptography method invented in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman. RSA works on the mathematical functions of selecting prime numbers, modular exponentiation, Euler totient function to select the field. Algorithm also requires the two keys involved, one published key or public key, some part of the public and private key, and the private key is computed from the public key. The steps ofRSA algorithm as follows:

1. Select two different prime numbers p and q.
2. Calculate n = p*q. n will be used as modulo for public and private key.
3. Calculate f(n)=(p-1)*(q-1), where f(n) is Euler totientfunction.
4. Select an integer e such that 1<e<f(n) and GCD (e,f(n))=1; e and f(n) are co-prime.
5. Determine d, multiplicative inverse of e mod f (n). And, d is the private key.

International Journal of Advance Research in Science and Engineering
Volume No.06, Special Issue No.(01), December 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

Encryption:

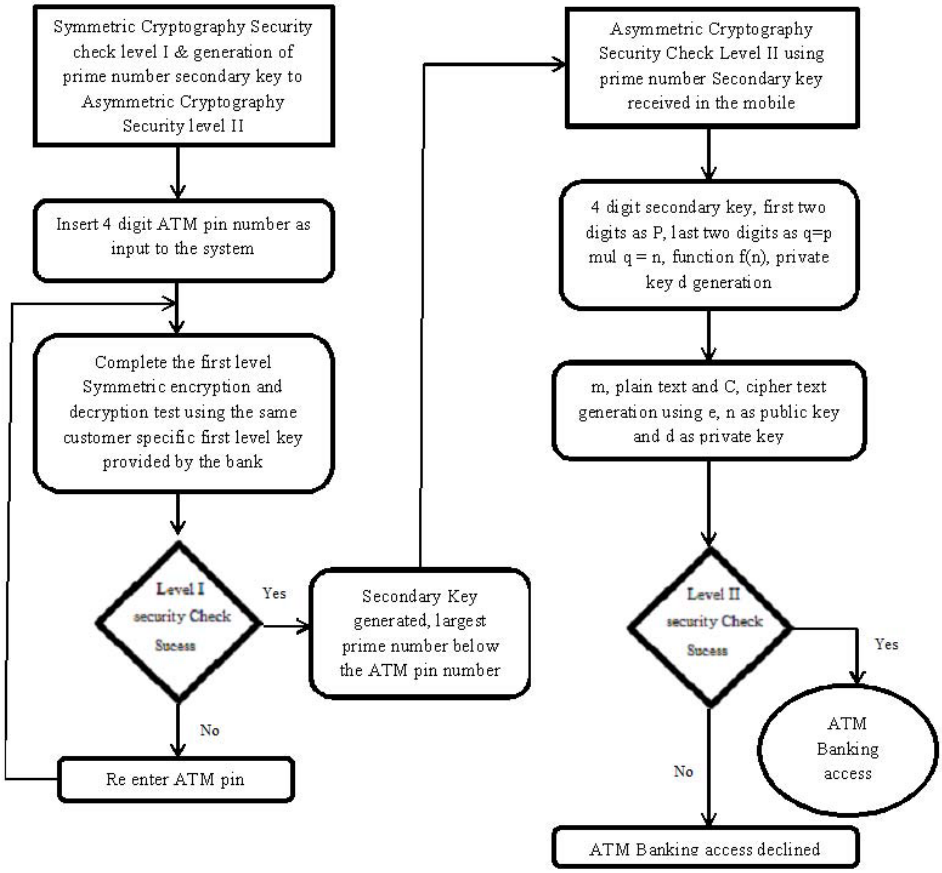
'A' (Source) transfer the data 'm' with the public key (e,n) to 'B' (Receiver) receives the data m with the private key (d,n) such that 0 < m < n and the Cipher text obtained by the relation: c = me mod n.

Decryption:

B use private key, d to get the original plain text or message, m by the relation: m = cd mod n.

IV IMPLEMENTATION

We propose a combine approach by using the symmetricand asymmetric cryptography algorithms and generate two security keys which make the system more robust against the intruder attack. The block diagram of the proposed algorithm design is given in the below Figure:



Proposed work block diagram

International Journal of Advance Research in Science and Engineering
Volume No.06, Special Issue No.(01), December 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

Algorithm design steps

The detailed steps of the proposed algorithm design are given below:

1. Symmetric level security check level I – Here, the customer after swiping the ATM card, will ask to input secure PIN number.

2. After entering the PIN number, first security check need to complete by entering customer specific primary security key provided by the bank completing the symmetric encryption and decryption process. Encryption is a simple addition of each digit of PIN number with primary key. Decryption is the reverse process of encryption by each encrypted digits of PIN number subtract with the same primary key to get the original PIN number.

3. The symmetric security check if completed successfully will receive a pop up message in the banking ATM terminal and also the secondary key generated which sends to the customer mobile. This secondary key utilized for the Asymmetric or public key cryptography algorithm level II step.

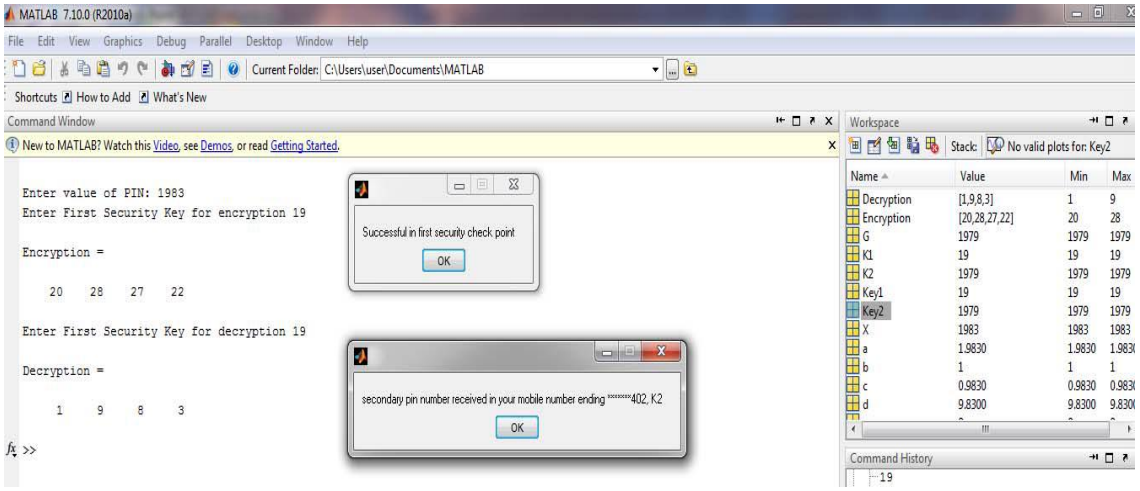
4. In the asymmetric or RSA algorithm, 4 digit secondary key generated from Level I security step will be utilized. This secondary key is the largest prime number just below the ATM pin number. This is designed because RSA algorithm works with two prime numbers, p and, q which forms the modulo n = p*q. The first two digits of secondary key will be taken as ‘p’ and last two digits taken as ‘q’. Then, completes the RSA algorithm as described in section III. After successful completion of the RSA security check level II, customer or user will get access into the ATM Banking network for necessary transactions.

V RESULTS

GUI provides provision two test two security levels. The GUI for the proposed algorithm design is shown below:

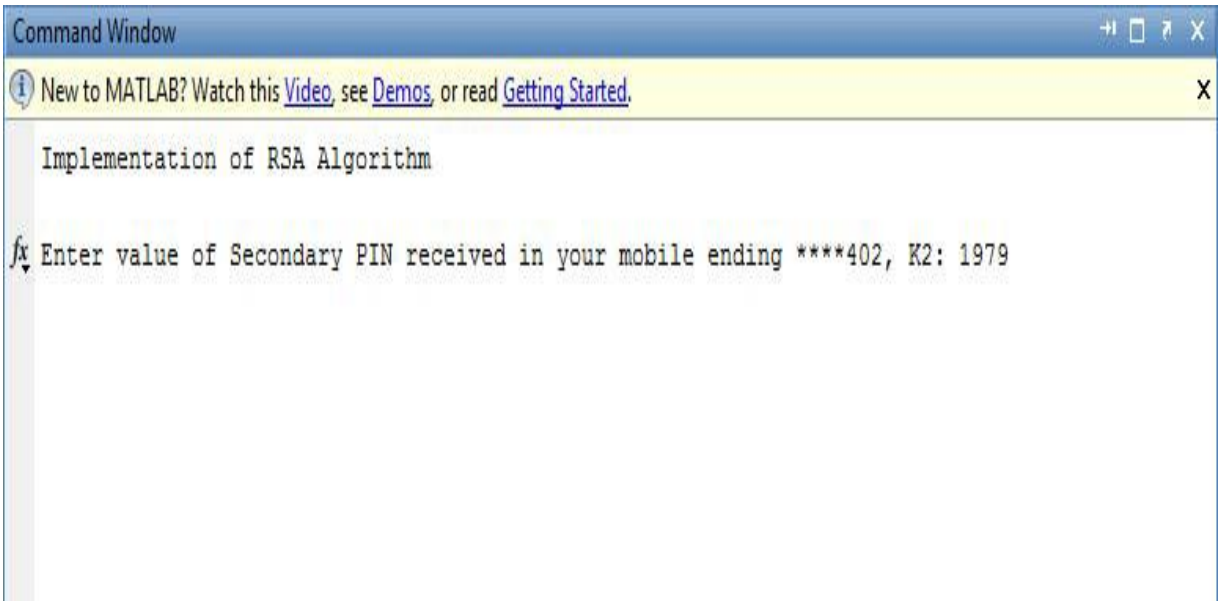
a) ATM reliable communication network security model GUI

International Journal of Advance Research in Science and Engineering
Volume No.06, Special Issue No.(01), December 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354



b) Command window options to enter ATM pin number, primary encryption and decryption key and verifying stage of First level of security check and generation of secondary key received at customer mobile.

For illustration purpose, we provide ATM pin number as 1983. Encryption and decryption key as 19. This receives the pop up message showing successful in first security check as well assecondary key generation re eived at the customer mobile as Key = K2 = 1979. This secondary key is the maximum value of prime number just below the ATM pin number.



c) Matlab command window option to enter the secondary PIN received in the mobile,

International Journal of Advance Research in Science and Engineering
Volume No.06, Special Issue No.(01), December 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

In this window, we enter the secondary PIN number, K2 =1979. This is the RSA security check level II. This secondary key is a prime number as it need for the RSA algorithm to proceed.

d) Option to enter a text message

After inputting the 4 digit secondary PIN, the first two digits is taken as p and the last two digits taken as q and completes the RSA algorithm and receives the corresponding values for N, Public key, e, Function f(n) or phi and the generation of private key, d.

e) Completion of encryption and decryption steps of RSA and generation of the final security code received in the mobile.

The step above completes the RSA algorithm encryption and decryption step and the generation of the final security code Z to receive in the mobile. For illustration, we chose the prime number minus 1. In this example, Z = 1978. Once this security code is entered correctly, then the access granted for banking transactions otherwise declined.

VI CONCLUSION

The proposed work ensures high security level of ATM banking transaction. We choose ATM network as an example of communication networks as this involves the ATM banking machine as client which communicates to the banking server through high optic communication link. RSA algorithm involves mathematical function which adds on the security access in the process. Symmetric cryptography technique is easy to implement, less computation steps involved, mathematical complexity is less and is a fast in processing. For applications where not a high security measure is involved, we can select symmetric cryptography method of encryption and decryption. But, this method involves simple mathematical operation, same key is used at both encryption and decryptionprocess. So there is every chance for a brute force or trial out attack to receive the key and thereby the encryption and decryption step. This makes the security of the communication network in threat of fraudulent attack. In asymmetric or public key cryptography, such as RSA algorithm, there is a high security check mechanism involved as it involves mathematical foundations and number theory and field facto to decide the corresponding encryption and decryption process. It involvestwo keys, both public and private key to get the plaintext or message from source to receiver. Even though an intruder tried for a brute force or other cryptanalysis method, it is very difficult to receive the public and private keys and also secondary keys generated which send to the customer mobile phone to complete the transactions.

In this work, we combine both symmetric and asymmetric methods. It is not just two security level checks. It involves secondary key generations at each level. When, ATM card inserted, ATM Pin number entered and that follows a first level security check by entering the customer specific pin provided by the bank to the customer. After successful first level, generation of secondary pin number to mobile. Then, proceed to the second level RSA security check using secondary pin. Again, final security code generated and sends to the mobile after successful completion of RSA algorithm security level check point. If all the three steps completed successfully then only the user will get an access into the ATM communication network transactions. The communication network security method developed in this paper aims to include the strengths of symmetry and asymmetry cryptography techniques and generation of necessary secondary keys to the client mobile phone as to complete each security check measures to grant access into the network.

REFERENCES

[1] B. Persis Urbana Ivy, PurushothamanMandiwa, Mukesh Kumar, ‘A Modified RSA cryptosystem based on ‘n’ prime numbers’, International Journal of Engineering and Computer Science, ISSN:2319-7242 Vol 1 Issue 2, Nov 2012 page no. 63-66.

[2] Rajan S Jamgekar, GeetaShantanu Joshi, ‘File Encryption and Decryption Using Secure RSA’, International Journal of Emerging Science and Engineering, ISSN:2319-6378 Vol 1 Issue 4, Feb 2013

[3] James L Massey, Fellow, IEEE, 'An Introduction to ContemperoryCryptology', Invited paper, Proceedings of the IEEE Vol 76, No.5, May 1988

[4] Whitfield Diffie and Martin E Hellman, member IEEE, 'New Directions in Cryptography', Invited paper, IEEE transactions on Information Theory. Vol 22 No.6, Nov 1976

[5] Martin E Hellman, 'An Overview of Public Key Cryptography', Invited paper, IEEE Communications Society Magazine Nov 1978

[6] Whitfield Diffie, member IEEE and Martin E Hellman, senior member IEEE, 'Privacy and Authentication: An Introduction to Cryptography',Invited paper, Proceedings of the IEEE Vol 67, No.3, March 197

[7] G. Germano, et al. (2005) "Evaluation of Security Mechanisms in Wireless Sensor Networks," in Proceedings of the Systems Communications (ICW05), p.1-6.

[8] G. E. Almargni& G. Abdalla, (2012) "Design and simulation of wireless network using NS2," in second International Conference on Computer Science and Information Technology (ICCSIT), Singapore, pp. 157-161.

[9] AlanaziHamdan.O., Zaidan B.B., Zaidan A.A., Jalab Hamid A., Shabbir M. and Al-Nabhani Y., (2010) " New Comparative Study Between DES, 3DES and AES within Nine Factors" , Journal of Computing , Volume 2, issue 3, pp. 152-157.

[10] EzreikAlmargni, GheryaniAbdalla, (2012) "Design and Simulation of Wireless Network using NS2", second International Conference on Computer Science and Information Technology
(ICCSIT'2012) Singapore, pp.157-161.

[11] Jinjing ZHAO, Yan WEN, and Dongxia WANG, (2011) "A Network Security Evaluation Method Framework Based on Multiple Criteria Dicision Making Theory", Fifth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, IEEE computer society, PP. 371- 375.

[12] Singh Rajender, MisraRahul , and Kumar Vikas , (2013) "Analysis the Impact of Symmetric cryptographic Algorithms on Power Consumption for various data types", International Journal on Recent and Innovation Trends in Computing and Communication, Volume: 1 Issue: 4, pp 221-226.

[13] Verma Harsh Kumar, Singh Ravindra Kumar, (2012) "Performance Analysis of RC5, Blowfish and DES Block Cipher Algorithms", International Journal of Computer Applications, Volume 42, No.16, PP. 8-14.

[14] A. Menezes, P. van Oorschot, & S. Vanstone, (1996) Handbook of Applied Cryptography, CRC Press, 1996.

[15] S. William, (2011) Cryptography and Network Security, United States of America: Fifth Edition.