International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-2 Issue-5, November 2013

Public Key Cryptography Algorithm Using Binary Manipulation and Chinese Remainder Theorem

N. Syed Siraj Ahmed, R. Selvakumar, Akshay Taywade

Abstract - Cryptography enables all processes, transactions, and communications to be safely performed electronically. Public key achieve confidentiality and has the ability to create a digital signature where as private key achieve confidentiality. Public key Cryptography is an extremely active subject of research with important applications in electronic commerce and internet security. In particular key exchange is used in secure socket layer protected communication and public key digital signature is used to verify the malicious software. This paper explains a public-key cryptography algorithm using chinese remainder theorem and binary manipulations such as reverse, division, multiply and addition of binary number etc.,. The security of the above scheme is based on the difficulty of finding a specific solution of the binary number. The chinese remainder theorem is used to hide the technique mentioned above, before making the hidden sequence of above to be transformed modulus. This algorithm has security against any kind of forgeries.

Keyword: Binary Manipulation, Cryptography, Chinese Remainder Theorem, Public Key

I. INTRODUCTION

"Cryptography" [1] derives from the Greek word kruptos, meaning "hidden". The key to hiding data is to devise a hiding (encryption) mechanism that is very difficult to reverse (i.e., to find the original data) without using the decryption key. Usually, the harder it is to discover the key, the more secure the mechanism. More generally it is about constructing and analyzing protocols that overcome the influence of adversaries. Applications of Cryptography include ATM Cards, Computer Password and Electronic Commerce etc., . There are different types of cryptography algorithms like symmetric key cryptography, Asymmetric key cryptography and hash functions.

In Symmetric (also called "secret-key/private key") encryption, the same key (or another key fairly easily computed from the first) is used for both encryption and decryption. It is implemented in two different ways block cipher and stream cipher. A block cipher enciphers input in blocks of plaintext where as stream cipher encrypts input in terms of individual characters. Some block cipher designs are Data Encryption Standard (DES) [2], Advanced Encryption Standard (AES) [3][4] are remains quite popular due to the strong security but it is very difficult to implement in practice.

The stream ciphers like Caeser's Cipher, Transposition Cipher, Substitution Cipher [5] are not secure but easy to implement.

In Asymmetric (also called "public-key") Cryptography, one key is used for encryption and another for decryption. Many popular Asymmetric Key (Public Key) Cryptography [6] like the Elliptic Curve Cryptography (ECC) [7] technique, which is more complex and more difficult to implement due to the Elliptic Curve Discrete Logarithm problem (ECDLP), Diffie-Hellman (DH) Key agreement technique [8] also involves with large exponential operation, the RSA algorithm [9] are based on long integer decimal modular exponentiation using which computation is difficult, slow speed and also its key generation is very slow. The hash functions take a message of any length as input and outputs a short, fixed length hash which can be used in Digital Signature Algorithm (DSA) [10]. MD-4, MD-5,[11] Secure Hash Algorithms (SHA) [12] such as SHA-0, SHA-1, SHA-2, SHA-3 are some of the hash function cryptography. The MD-4, MD-5 are easily broken but SHA is very difficult to broken in practice.

The current trend towards security includes Quantum Cryptography [13] and Message Authentication Code [14] (MAC). The Quantum Cryptography is the use of quantum systems to do cryptographic tasks. The most famous example is Quantum Key Distribution (QKD) which uses quantum mechanics to guarantee secure communication. It enables two parties to produce a shared random bit string known only to them, which can be used as a key to encrypt and decrypt messages. The Message Authentication Code is similar to Cryptography Hash Functions except that a secret key can be used to authenticate the hash value.

A new Asymmetric Key (Public Key) cryptography algorithm approach has been proposed, which uses only the simple operations like conversion of decimal to binary, binary to decimal, binary multiplication, binary division, square root etc., this operations are easy to perform and hence it operate faster and no need of high speed system unlike in the other public key cryptography methods.

II. IMPORTANCEOF CRYPTOGRAPHY

In a typical situation where cryptography is used, two parties (A and B) communicate over an insecure channel. A and B want to ensure that their communication remains incomprehensible by anyone who might be listening. Furthermore, because

Revised Manuscript Received on 30 November 2013.
* Correspondence Author
Mr. N. Syed Siraj Ahmed, School of Computing Science and Engineering, Vellore Institute of Technology (VIT) (Deemed University),Vellore-632 014, Tamil Nadu, India.
Dr. R. Selva Kumar, School of Advanced Sciences, Vellore Institute of Technology (VIT) (Deemed University),Vellore-632 014, Tamil Nadu, India.
Mr. Akshay Taywade, School of Computing Science and Engineering, Vellore Institute of Technology (VIT) (Deemed University),Vellore-632 014, Tamil Nadu, India.

A and B are in remote locations, A must be sure that the information receives from B has not been modified by anyone during transmission. In addition, it must be sure that the information really does originate from B and not someone impersonating B. Cryptography is used to achieve the following goals [18]:

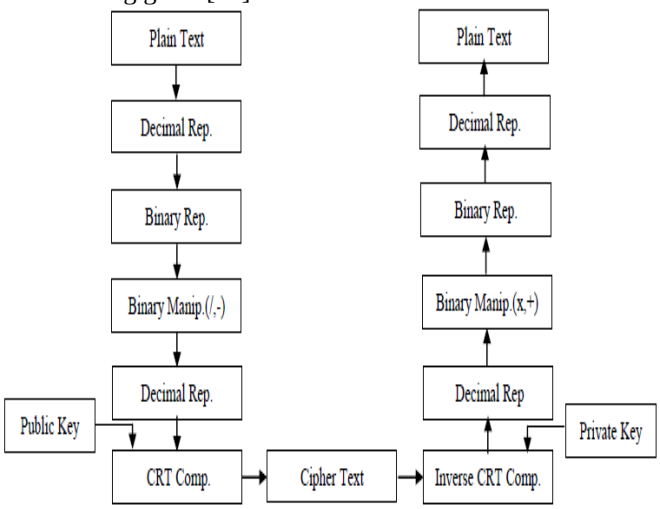

Figure 1: Encryption and Decryption by CRT

A. Confidentiality

To ensure data remains private. Confidentiality is usually achieved using encryption. Encryption algorithms (that use encryption keys) are used to convert plain text into cipher text and the equivalent decryption algorithm is used to convert the cipher text back to plain text. Symmetric encryption algorithms use the same key for encryption and decryption, while asymmetric algorithms use a public/private key pair.

B. Data Integrity

To ensure data is protected from accidental or deliberate (malicious) modification. Integrity is usually provided by message authentication codes or hashes. A hash value is a fixed length numeric value derived from a sequence of data. Hash values are used to verify the integrity of data sent through insecure channels. The hash value of received data is compared to the hash value of the data as it was sent to determine if the data was altered.

C. Authentication

To assure that data originates from a particular party Digital Certificates are used to provide authentication. Digital signatures are usually applied to hash values as these are significantly smaller than the source data that they represent.

A major difference between the above methods and this method is based on the fact that the decimal - binary - decimal combination is used to encrypt and decrypt, no longer integer, exponentiation is used to compute. This allows us to do simple computation and utilize the Chinese Remainder Theorem (CRT) in order to hide the above combination. This algorithm is excellent with a higher efficiency and better security.

III. CHINESE REMAINDER THEOREM

This theorem [15][17] has been widely used in cryptography and its applications , purely for simplifying some complex computations, and some public-key cryptography systems proposed recently based on this theorem. The main advantage of this algorithm is that it can hide the original data and can be designed as a one-way limitation. It can be described as follows: set $n_1, n_2, \ldots n_k$ are co prime and all positive integers, let $n = n_1 n_2 n_3 \ldots n_k$ so:

$$x = x_1 \bmod n_1$$
$$x = x_2 \bmod n_2$$
$$x = x_k \bmod n_k \qquad (1)$$

The set $\{0, 1, 2, \ldots, n\text{-}1\}$ has a unique solution, that is, $x = \sum x_i M_i s_i \bmod n$, with $M_i = n / n_i$,while $s_i = M_i^{-1} (\bmod n)$, $(i=0, 1, 2, \ldots, k)$.

A.MERITS

1. It increases efficiency in machine computation.
2. It reduces the space requirement for storage of data because large numbers are converted into smaller ones by linear congruencies.
3. Use of simple arithmetic operations such as addition, subtraction, multiplication, division and hence execution of MIPS is possible.
4. The computation process is very fast and hence it takes less processing time.
5. It has some application in cryptography technique, secure transmission of data and signals in military and defense applications.

IV. DESCRIPTION OF ALGORITHMS

This algorithm utilizes [16] the easiness of binary representation and manipulation problem as its limitation and uses double keys A and B in the processing of construction, then calculate S from i and j, where i = A mod V and j= B mod V , before using chinese remainder theorem to hide i and j to get a new value X, and apply some modulus transformation to X to get X*.Thus, the security is enhanced. Issue X* as public key while some related parameters and S as private keys. Experiments exposes that the speed of this algorithm is very fast in both encryption and decryption. Besides, it is easy to generate a key, and convenient for the software implementation.

The main steps of the generation of keys, encryption and decryption are shown below:

A. The Generation of the Key (shown in below figure 2)

1) Choose two keys A, B and choose modulus V, U such that V, $U < 2^m$. (where m be the number of binary bits to represent the plain text)

2) Compute i = A mod (V) , j= B mod (U) and $S= v^{-1} * i * U + u^{-1} * j * V$.

3) Choose a secret key M^{-1} such that $\gcd(M^{-1},M)=1$ where M=U*V and use Chinese remainder theorem to calculate X, aiming at (in order to) hiding A and B into X, that is:

$X = S$ or $(v^{-1} * i * U + u^{-1} * j * V) \bmod M$

Public Key: (X, m)

Private Key: (A, B, i, j, v^{-1}, V,u^{-1},U)

B. Encryption (shown in below figure 3)

1. Generate the decimal number of the plain text by r decimal digits.
2. Generate the corresponding binary value of taking n-decimal digit at a time. The binary value should be m-bits.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

3. Reverse the m-bits binary number which is generating in step2.
4. Take a k-bits long binary number W which is the square root of m-bit binary number and divide with m-bit binary number (i.e) which is generated in step 3.
5. Represent the remainder in first u-bits and quotient in next y-bits. If remainder and quotient are less than u and y bits respectively then we need to add required number of zero's in the left hand side (m = u + y).
6. Convert the binary value generated in step 5 into decimal equivalent value Z and multiply with the X.
   i.e C = Z * X

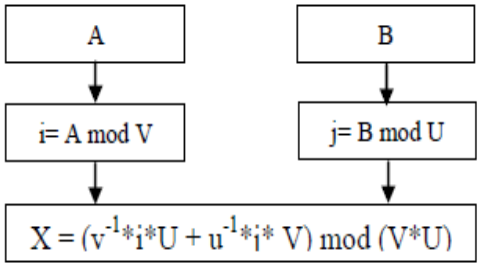

Figure 2: Key Generation

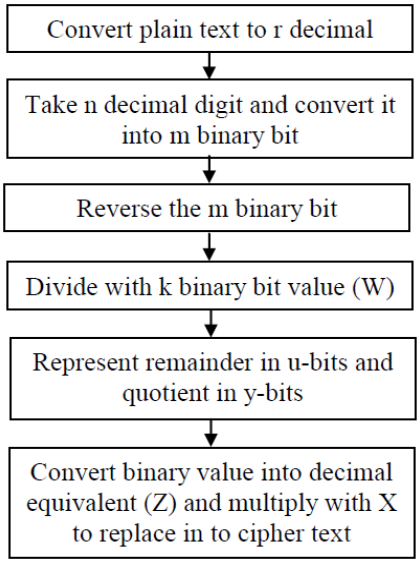

Figure 3: The Encryption Process

C. Decryption (shown in below figure 4)

1. Convert the cipher text in to decimal equivalent (C) and compute Z by using the equation, $Z = v^{-1} C \bmod (V)$.
2. Convert the binary number of the decimal equivalent generated in step1.
3. Take the last y-bit binary value and square it and add the first u-bit binary value with the result, which gives m-bit binary number.
4. Reverse the m-bits binary number which is generating in step 3.
5. Convert the m-bit binary number in to n decimal digit equivalent.
6. Convert the decimal number in to meaningful plain text by combining r decimal digit at once.

V. LIMITATION

1. This algorithm is very simple in computation.
2. It uses two reverse operations to make the algorithm more secured
3. Easy to Receive cyclic redundancy check at end users.
4. It will take less time for conversion and execution.

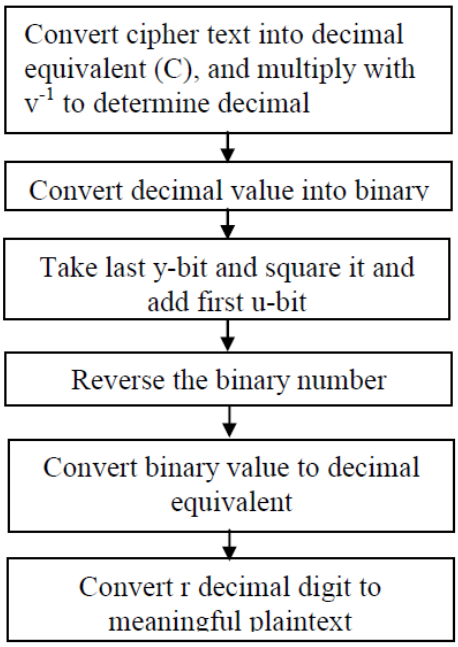

Figure 4: The Decryption Process

VI. CONCLUSION

Public Key Cryptography is used to accomplish few goals like Data integrity, Confidentiality, Authentication etc., of data which the sender sent to the receiver. Now, in order to accomplish these goals various Public Key Cryptography Algorithms are developed by various people. It has been confirmed that the algorithms which are available at this juncture are more or less difficult or complicated in nature. Because those algorithms are used to maintain high level of security against any kind of forgeries. For a minimal and medium amount of data those algorithms wouldn't be cost effective since those are not designed for minimal and medium amount of data. The aim of this work was to construct and implement a new algorithm to address this issue so that we don't have to apply those algorithms (which are not cost-effective) to encrypt a minimal and medium amount of data. Keeping this goal in mind the proposed algorithm has been designed in a quite simple manner but of-course not sacrificing the security issues.

REFERENCES

1. "Basic Cryptographic Algorithms", an article available at www.itsc.state.md.us /oldsite/info/InternetSecurity/Crypto/CryptoIntro.html
2. W.Diffie and M.E.Hellman "Exhaustive Cryptanalysis of the National Bureau of Standard (NBS) Data Encryption Standard", Computer pp. 78-84, June-1977.
3. "American National Standard for Data Encryption Algorithm (DEA)" ANSI X3.92-1981, American National Standards Institute New York.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

4. "DES modes of operation" NBS Federal Information Processing Standard P ublication 74, National Technical Information Service, Springfield, VA-1980.
5. IBM Syst.J., (Special Issue on Cryptography) Vol-17. No. 2, 1978.
6. "Introduction to Public-Key Cryptography", an article available at developer.netscape.com/docs/manuals/security/pkin/contents.html
7. Koblitz "Elliptic Curve Cryptosystem", Mathematics of Computation Vol-48, Pages 203-209, 1978.
8. W. Diffie and M. E. Hellman. New Directions in Cryptography. IEEE Transactions on Information Theory, IT-22(6) pp. 644-654, November 1976.
9. R. L. Rivest, A. Shamir, and L. Adleman. A Method for Obtaining Digital Signatures and Public Key Cryptosystems. Communications of the Association for Computing Machinery, 21(2) pp. 120-126, February 1978.
10. National Institute of Standards and Technology (NIST). FIPS Publication 186: Digital Signature Standard. National Institute for Standards and Technology, Gaithersburg, MD, USA, May 1994.
11. H.Dobbertin "Cryptanalysis of MD-4" FSE-96, PP. 53-69, 1996.
12. National Institute of Standard and Technology (NIST) " Secure Hash Standard" Federal Information Processing Standards Publication FIPS PUP 180, May-1993.
13. C.H. Bennett and G. Brassard, "Quantum Cryptography: Public-Key Distribution and Coin Tossing," Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 1984.
14. G.Brassed "On Computationally Secure Authentication Tag Requiring Short Secret Shared Keys" in Proc. Of International Cryptology Conference on Advances in Cryptology R. L. Rivest, A. Shamir, and D.Chaum Eds Plenum Press New York , 1983 PP 79-86.
15. J. Xue-juan, the origin and the solution of the "Chinese remainder theorem". Journal of jiujiang University (natural sciences) , no.3(2004), pp.102-108
16. ZHANG Yun-peng* LINXia WANG Qiang " Asymmetric Cryptography Algorithm with Chinese Remainder Theorem" Proceedings of IEEE-2011.
17. Johann GroBschadl: " The Chinese Remainder Theorem and its Application in a High-Speed RSA Crypto Chip." Proceedings of IEEE-2008.
18. IEEE P1363, Standard Specification for Public Key Cryptography", Nov-2000.

AUTHOR PROFILE

Mr. N. Syed Siraj Ahmed B.Sc., (Computer Science), M.Sc., (Computer Science), M.Phil., (Computer Science), Ph.D., (Computer Science (Pursing)). I have published a paper titled " Encryption and Decryption by Genetic Algorithm". I am doing research in Intrusion Detection by Intelligent Techniques.

Dr. R. Selva Kumar B.Sc.,(Mathematics), M.Sc.,(Mathematics), M.Phil., (Mathematics), Ph.D.,(Mathematics). I have published several papers, guiding to research scholars.

Mr. Akshay Taywade B.E.,(Computer Science and Engineering). I am doing M.Tech (Computer Science) at VIT Vellore.