Improvement in the Strength of RSA Algorithm using Bits Randomize

Prof. Brijeshkumar U Patel[1] **Prof. Archana M Naik**[2] **Prof. Kaushikkumar S Patel**[3]
[1,2,3]Department of Computer Engineering
[1,2,3]GIDC Degree Engineering College, Navsari, India

Abstract— One of the primary difficulties of asset sharing on information correspondence system is its security. This is commenced on the truth that once there is network between PCs sharing a few assets, the issue of information security gets to be discriminating. This paper introduces new technique in RSA Algorithm to provide maximum security for data over the network.

Key words: Encryption, Decryption, Key

I. Introduction

Cryptography is assuming a noteworthy part in information insurance in applications running in a system domain. It permits individuals to work together electronically without stresses of double dealing and misleading notwithstanding guaranteeing the uprightness of the message and legitimacy of the sender. It has turn out to be more basic to our regular life on the grounds that a large number of individuals connect electronically consistently; through email, e-business, ATM machines, cell telephones, and so forth. This geometric increment of data transmitted electronically has made expanded dependence on cryptography and validation by clients [1-4]. Notwithstanding the way that secured correspondence has existed for quite a long time, the key administration issue has avoided it from ordinary application. The advancement of open key cryptography has empowered vast scale system of clients that can correspond safely with each other regardless of the fact that they had never conveyed [6-8]. This paper considers a Public Key encryption technique utilizing RSA calculation that will change over the data to a structure not justifiable by the interloper in this way shielding unapproved clients from having entry to the data regardless of the fact that they find themselves able to break into the framework.

II. Methodology

There are many ways of classifying data cryptographic algorithms but for the purpose of this paper, they will be classified based on the number of keys that are employed for encryption and decryption. The three common types of algorithms are:

A. *Secret Key Cryptography (SKC):*

The SKC method uses only a single key for both encryption and decryption. The schemes are generally categorized as being either stream ciphers or block ciphers. Stream ciphers operate on a single bit (byte or computer word) at a time and implement some form of feedback mechanism so that the key is constantly changing while block cipher scheme encrypts one block of data at a time using the same key on each block. The main drawback of this method is propagation error because a distorted bit in transmission will result in n distorted bits at the receiving side. Though stream ciphers do not propagate transmission errors, they are periodic therefore the key-stream will eventually repeat. This normally results in the use of digital signature mechanisms with either large keys for the public verification function or the use of a TTP.

B. *Public Key Cryptography (PKC):*

PKC scheme uses one key for encryption and a different key for decryption. Modern PKC was first described using a two-key crypto system in which two parties could engage in a secure communication over a non-secure communications channel without having to share a secret key [5]. In PKC, one of the keys is designated the public key and may be advertised as widely as the owner wants. The other key is designated the private key and is never revealed to another party. RSA is one of the first and still most common PKC implementation that is in use today for key exchange or digital signatures. The cardinal advantage of this method is that administration of keys on a network requires the presence of only a functionally trusted TTP, as opposed to an unconditionally trusted TTP. Depending on the mode of usage, the TTP might only be required in an “off-line” manner, as opposed to in real time. Many public-key schemes yield relatively efficient signature mechanisms. The key used to describe the public verification function is typically much smaller than for the symmetric-key counterpart [6-9].

C. *Hash Functions (HF):*

The HF uses a mathematical transformation to irreversibly "encrypt" information. This algorithm does not use keys for encryption and decryption of data. It rather uses a fixed-length hash value which computed based on a plaintext that makes it impossible for either the contents or length of the plaintext to be recovered. These algorithms are typically used to provide a digital fingerprint of a file's content, often used to ensure that the file has not been altered by an intruder or virus. Hash functions are also commonly employed by many operating systems to encrypt passwords to provide some measure of the integrity of a file.

III. Related work & proposed scenario

The RSA algorithm can be used for both key exchange and digital signatures. Although employed with numbers using hundreds of digits, the mathematics behind RSA is relatively straight-forward. To create an RSA public and private key pair, the following steps can be used:

1) Choose two prime numbers, p and q. From these numbers you can calculate the modulus, n = pq
2) Select a third number, e, that is relatively prime to (i.e. it does not divide evenly into) the product (p −1)(q −1), the number e is the public exponent.
3) Calculate an integer d from the (ed-1)/ ((p-1) (q-1)). The number d is the private exponent.
4) The public key is the number pair (n,e) . Although these values are publicly known, it is computationally infeasible to determine d from n and e if p and q are large enough.

5) To encrypt a message, M, with the public key, creates the cipher-text, C, using the equation:
    - $c1 = M^{e}$ Mod n.
    - Convert c1 into binary.
    - Calculate Total Pass using c1.
    - Select PassPublickey which is less than Pass(i.e Ppukey) and generate Pass Privatekey (i.e. Pprkey).
    - C=encryption(c1,Ppukey).
6) The receiver then decrypts the cipher-text with the private key using the equation:

- p=encryption(C,Pprkey).
- Convert int bytes.
- M=P e Mod n.

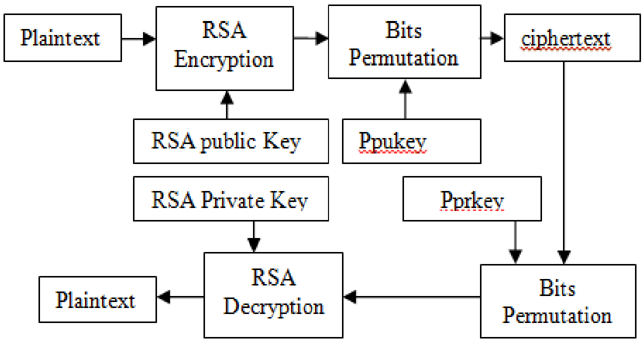

Fig. 1: Proposed Algorithm

IV. Conclusion

In this work the most famous open key cryptosystem, RSA, is made strides. The change is done in RSA algorithm so that the high calculations included towards encryption side are drop down. The proposed plan is indicated to get the progressed of RSA using bits permutation. The execution results demonstrate that other than less memory utilization, the proposed plan is effective in both encryption and unscrambling sides. The proposed plan can be productively utilized for modified RSA Algorithm using bits permutation provides better security.

References

[1] Afolabi, A.O and E.R. Adagunodo, 2012. Implementation of an Improved data encryption algorithm in a web based learning system. International Journal of research and reviews in Computer Science. Vol. 3, No. 1.

[2] Bhoopendra, S.R., Prashanna, G. and S. Yadav, 2010. An Integrated encryption scheme used in Bluetooth communication mechanism. International Journal of Computer Tech. and Electronics Engineering (IJCTEE), vol. 1, issue 2.

[3] http://www.di-mgt.com.au/rsa_alg.html.
DI management (2005) "RSA algorithm", available at:

[4] Gaurav, S., 2012. Secure file transmission scheme based On hybrid encryption technique. International Journal of management, IT and Engineering. Vol. 2, issue 1.

[5] Hellman, M. and J. Diffie, 1976. New Directions in Cryptography. IEEE transactions on Information theory, vol. IT-22, pp:644-654.

[6] Shinde, G.N. and H.S. Fade War, 2008. Faster RSA algorithm for decryption using Chinese remainder theorem. ICCES, Vol. 5, No. 4, pp. 255-261.

[7] Yang L. and S.H. Yang. 2007. A frame work of security and safety checking for internet-based control systems. International Journal of Information and Computer security. Vol.1, No. 2.

[8] Washington, L.C. 2006. Introduction to Cryptography: with coding theory by Wade Trappe. Upper Saddle River, New Jersey, Pearson Prentice Hall.

[9] Wuling Ren College of Computer and Information Engineering Zhejiang Gongshang University. 2010. A hybrid encryption algorithm based on DES and RSA in Bluetooth communication. Second International Conference on Modeling, Simulation and Visualization methods.

[10] Nentawe Y. Goshwe IJCSNS International Journal of Computer Science and Network Security, VOL.13 No.7, July 2013 Data Encryption and Decryption Using RSA Algorithm in a Network Environment