International Journal of Engineering Research and Development
e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com
Volume 8, Issue 3 (August 2013), PP. 45-51

Analyzing the speed of combined cryptographic algorithms with secret and public key

Florim Idrizi[1], Fisnik Dalipi[2], Ejup Rustemi[3]
[1,2,3] Department of IT, Faculty of Natural Sciences and Mathematics, State University of Tetova

Abstract:- Secure messages and key management have been a focal point in cryptography. In the cryptographic systems, the notion of key is referred ti an numerical value which is used by an algorithm, making the information secure and visible only to individuals that possess the proper key to discover that information. In this article we will explain the concepts of private key and public key cryptography, and combined cryptography in terms of protecting information that is being sent through Internet. Further, we will analyze some secret and public algorithms, and combined algorithms with LABView. The speed measurement of these algorithms also represents a significant contribution of this paper.

Keywords:- Cryptography, Algorithms, LabView

I. INTRODUCTION

Security is the main part of an enterprise which can be achieved by using a combined cryptography algorithms. However, the main purpose of cryptography is not only used toensure confidentiality, but also to provide solutions to problems such as: hacked integrity, authentication and non-repudiation. In cryptographic systems, the key term refers to a numerical value used by an algorithm to change the information, making that information secure and visible only to individuals who possess the appropriate key for revealing. As a result, the term of key management refers to secure management of keys for making them available to users when they need them. Currently researchers continue to find new algorithms. However, this issue is a very difficult thing because there is a need to consider many factors, such as: security, algorithm characteristics, speed and complexity.

Fig.1: Security Services

They can be categorized into Symmetric (secret) and Asymmetric (public) keys en- cryption. In Symmetric keys encryption or secret key encryption, only one key is used to encrypt and decrypt data. In Asymmetric keys, two keys are used; private and public keys. Public key is used for encryption and private key is used for decryption. Public key encryption is based on mathematical func tions, computationally intensive and is not very efficient for small mobile devices [1],[2]. There are many examples of strong and weak keys of cryptography algorithms like RC2, DES, 3DES, RC6, Blowfish, and AES. RC2 uses one 64-bit key. DES uses one 64-bits key. Triple DES uses three 64-bits keys while AES uses various 128,192,256) bits keys. Blowfish

uses various (32-448); default 128bits while RC6 is used various (128,192,256) bits keys. The most common classification of encryption techniques can be shown in Figure 2 [3].

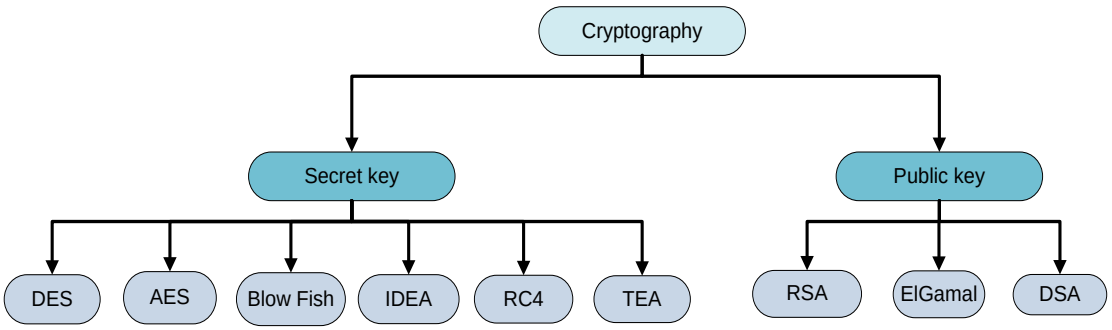

Fig. 2: .Algorithms with public and secret key

Data security is an essential part of an organization; it can be achieved by the using various methods. In order to maintain and upgrade the model still efforts are required and increase the marginally overheads. The encrypted data is safe for some time but never think it is permanently safe. After the time goes on there is chance of hacking the data by the hacker. Fake files are transmitted in the same manner as one can sends the encrypted data. The information about the key is present in the encrypt data which solves the problem of secure transport of keys from the transmitter to receiver [4],[5]. In case of practical system encrypted data is passed through the various stations which are capable to re-encrypt the data by their own key. At the time the previous keys are discarded, this will make the system more secure. There are many algorithms available in the market for encrypting the data. Encryption is the process in which plaintext has been converted into the encoded format cipher text with the help of key [6].

II. PUBLIC KEY CRYPTOGRAPHY

This section is a brief overview of the cryptography that is incorporated into a PKI. Current public key cryptography as described in this article is mostly attributed to Diffie and Hellman and Rivest, Shamir and Adleman. Because of its widespread use in e-commerce, this article focuses on the RSA (named for its creators: Rivest, Shamir and Adleman) public key cryptographic system. RSA is a public key cryptographic algorithm that is based on the hard mathematical problem of factoring composite numbers. The keys used by the RSA crypto system are based on the product of two large prime numbers that derive their cryptographic strength from the fact that it is difficult to factor large composite numbers of this kind. RSA uses a pair of keys: a public key which is made known to many entities, and a private key for which secrecy and integrity are strictly controlled and only used by the owner of that key [7].

III. SYMMETRIC KEY ENCRYPTION

An overview of public key cryptography is not complete without mentioning symmetric or secret key cryptography. The reason for this is that public key cryptographic systems lack the positive performance characteristics of symmetric systems. The ramification of this under performance is that, in practice, symmetric systems such as DES, Triple-DES, or IDEA are used to perform encipherment of data for confidentiality, where the data is more than a negligible length. In this way, symmetric key encryption supplements public key cryptographic systems. The fundamental characteristics of symmetric cryptographic systems used with PKI are that the same key is used for both encryption and decryption. Because of this symmetry the key must be kept secret and shared only between two parties [7].

Table 1: Comparison of various encryption algorithms on the basis of Key size and Block size, Type and Features [8],[9]

Algorithm	Key Size (bits)	Block Size	Type	Features
RSA	1024	128	Block Cipher	Asymmetric algorithm, speed is low
Blowfish	32- 448	64	Block Cipher	Excellent Security
AES	128	128	Block Cipher	Replacement for DES, Excellent Security
DES	64	64	Block Cipher	Most common, Not Strong Enough
Triple DES	192	64	Block Cipher	Modification of DES, Adequate Security

ECDSA	163	/	Block Cipher	
RC4	128	128	Stream Cipher	Fast Stream Cipher in SSL

IV. COMBINED CRYPTOGRAPHY

Combining the secret key and public cryptography can result in better results regarding the encryption. In this process, one must take into account the points where one algorithm is weaker than another. Encryption starts by generating secret key. The secret key used is safe and fast. During the public key encryption, a major problem was how to reach the receiver by using secret key. This is enabled by public key. In this case, the public key of the receiver is used for encrypting only the secret key. Normally, the public key cryptography is slower, nevertheless, the size of the secret key is little and this would not affect the speed limitation of encryption and decryption.

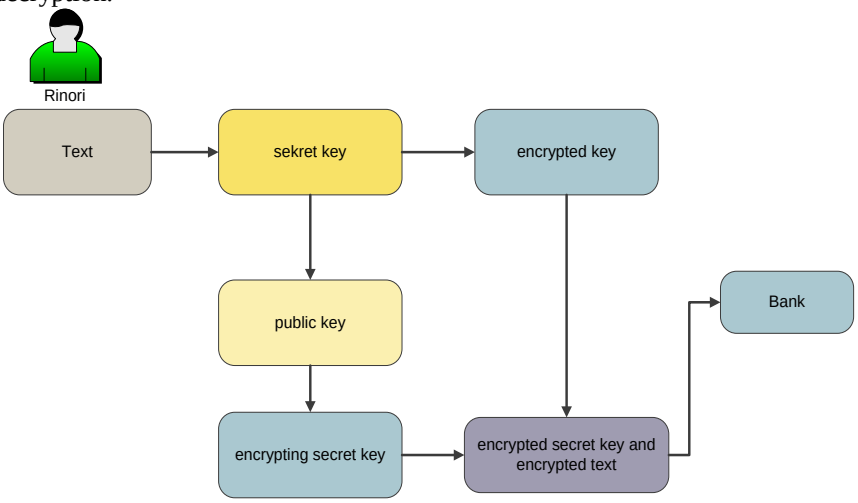

Fig. 3: Combined encryption

The last process is connecting the encrypted secret key with the encrypted text for transferring the message to the receiver. We must emphasize that transferring messages through Internet, unknown individuals cannot read this text because the secret key is encrypted by the secret key of receiver. It is only the sender who can decrypt that with the help of his private key.

The use of public/secret encryption for encrypting the secret key offers reasonable solutions by protecting the secret key from copying it through the transmission process. Also, there is no need for prior deals between peers that participate in the transmission for exchanging the secret key.

Decryption starts with the acceptation of the encrypted secret key and the encrypted text. Afterwards, the encrypted key and the encrypted text are decrypted in this way. After encrypting the secret key of the sender with the public key of the receiver, the encrypted secret key will be decrypted with the receiver secret key, which results with gaining the sender secret key. The sender secret key is used for decrypting the encrypted text where the original text appears.

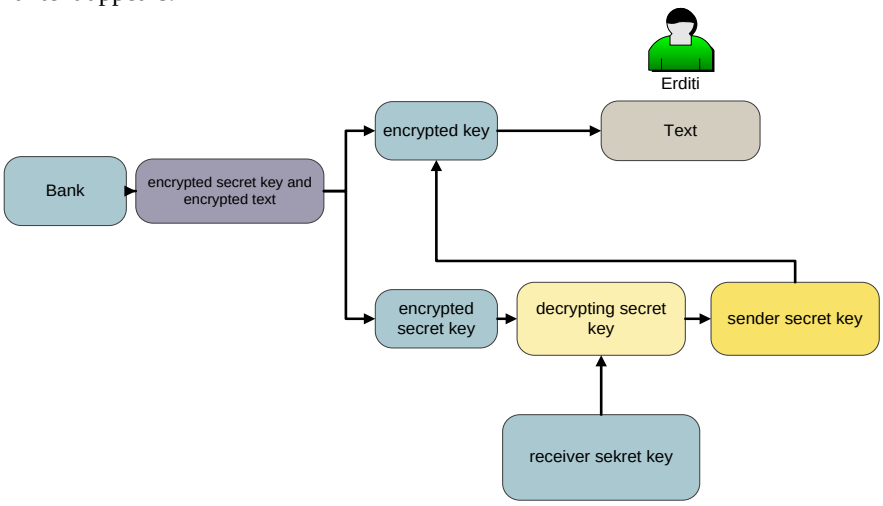

Fig. 4: Combined decryption

The combined cryptography represents the foundation for many modern encryption solutions, such as: e-main encryption, VPN encryption etc.

However, combined cryptography must assure that the encrypted message comes from the sender. It can happen that a third person can make use of the receiver public key and encrypts the secret key used for encrypting the message. The third person can share that on Internet. The receiver initially decrypts the secret key by using his private key and the message by using the secret key of the sender. The receiver has received one unwanted message by an unwanted receiver. To make sure that the message comes from the right sender, we use digital certificates

V. ANALISYS OF RSA ALGORITHM BY USING LABVIEW

RSA is a public key algorithm that is used for Encryption, Signature and Key Agreement. RSA typically uses keys of size 1024 to 2048. Since public key cryptography involves mathematical operation on large numbers, these algorithms are considerably slow compared to the symmetric key algorithm. They are so slow that it is infeasible to encrypt large amount of data. Public key encryption algorithm such as RSA can be used to encrypt small data such as 'keys' used in private key algorithm. RSA is thus used as key agreement algorithm. [10]

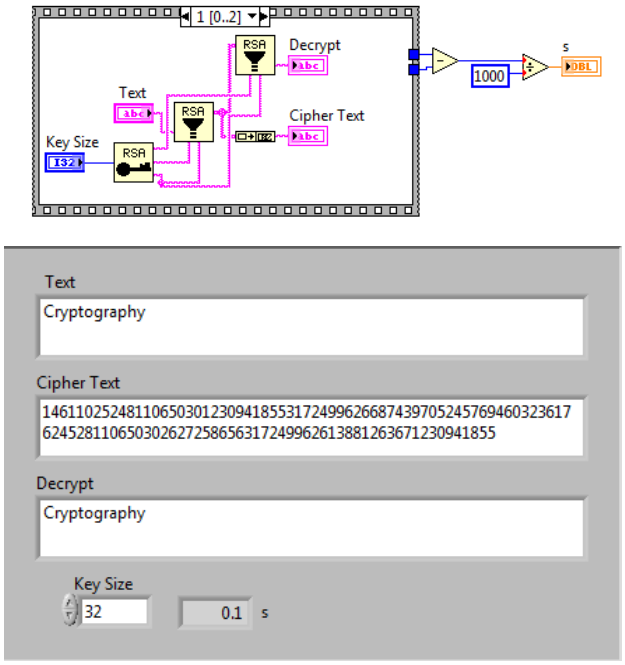

Fig.5: The realization of RSA algorithm using LabVIEW

Table 2: The speed of RSA in terms of character number encrypted and decrypted

Character number	**1000**	**2000**	**3000**	**4000**	**5000**	**10000**
Time	5.5s	10.3s	14.6s	19.3s	24.6s	53.2s

From the table we can conclude that by having 32 bit key and by increasing the number of characters for encryption and decryption, the time will be delayed progressively. This means that the speed of the algorithm depends on the number of characters that are to be encrypted and decrypted.

VI. ANALISYS OF RC4 ALGORITHM BY USING LABVIEW

RC4 stream cipher most preferred Stream cipher algorithm. In the RC4 algorithm, there are two stages process during encryption as well as decryption. The algorithm is dividing into the two parts KSA (Key scheduling Algorithm) and PRGA (Pseudo Random Generator Algorithm). KSA as the first stage of algorithm also knows as initialization of S (s is state vector) and PRGA known as stream generation in the RC4 whole process of algorithm, mean RC4 basically two stages process. In the first stages of RC4 Stream Cipher algorithm on the bases of variable sized key from 1 to 256 a State Vector (State Table) of fixed length 256 bytes is generated, after on the base of State Table, we generate the key stream that XOR with plaintext and

cipher text during encryption and decryption. During encryption the key stream is XOR with the plaintext and during decryption the cipher text XOR with key stream then convert into the plaintext. In the description of RC4, first we discussing the first stage of the algorithm known as KSA, in this stage [11]

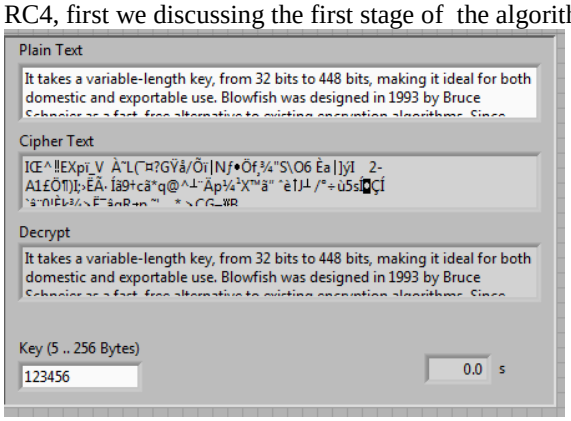

Fig.6: The realization of RC4 algorithm using LabVIEW

Table 3: The speed of RC4 in terms of character number encrypted and decrypted

Character number	**1000**	**2000**	**3000**	**4000**	**5000**	**10000**
Time	0.0s	0.0s	0.0s	0.0s	0.0s	0.0s

From the table we can conclude that by increasing the number of characters for encryption and decryption, the time will not change. This means that the speed of the algorithm is high and depends on the number of characters that are to be encrypted and decrypted.

VII. ANALISYS OF COMBINED CRYPTOGRAPHY RC4 – RSA BY USING LABVIEW

Erditi wants to send a message to Rinor. Erdit generates a one key. He uses this key together with the RC-4 algorithm to encrypt his message. After this is done, he encrypts the temporary key with Rinor public key, using RSA. He sends the encrypted message that was encrypted with RC-4 together with the temporary key that was encrypted with RSA. When Rinor receives the message, she decrypts the key with her private key. She then uses the temporary key to decrypt the message. Since only she has her private key, she will be the only person who is able to decrypt the temporary key and thus the message.

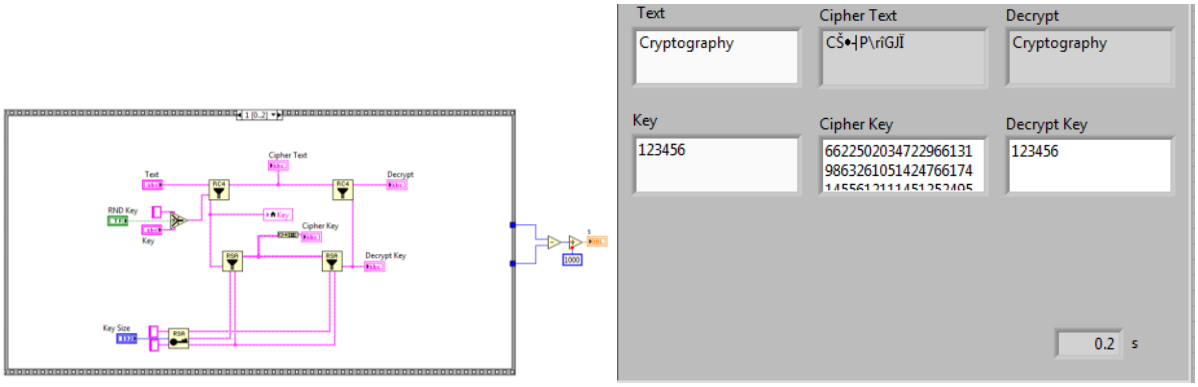

Fig. 7: The realization of RC4 – RSA algorithm using LabVIEW

Table 4: The speed of RC4 – RSA in terms of character number encrypted and decrypted

Character number	**1000**	**2000**	**3000**	**4000**	**5000**	**10000**
Time	0.1s	0.1	0.2	0.2	0.4	0.6

From the table we can conclude that by increasing the number of characters for encryption and decryption, the time will not change. This means that the speed of the algorithm is high and depends on the number of characters that are to be encrypted and decrypted.

VIII. ANALISYS OF COMBINED CRYPTOGRAPHY DES – RSA BY USING LABVIEW

RSA has two keys – one private and one public. RSA is implemented as software. It is hard to code the plaintext and to decode the ciphertext with RSA. DES has the same key for encryption and decryption. DES is implemented in hardware and it is fast. Any communication between two businesses can use different keys, and the key can be exchanged. If the key is sent separately encrypted with RSA, then the receiver can use it for decrypting the encrypted message with DES. DES is faster for generating signature but is slower in encryption. It is faster when decryption and the security can be considered comparable in equivalent way with RSA key with same size [12].

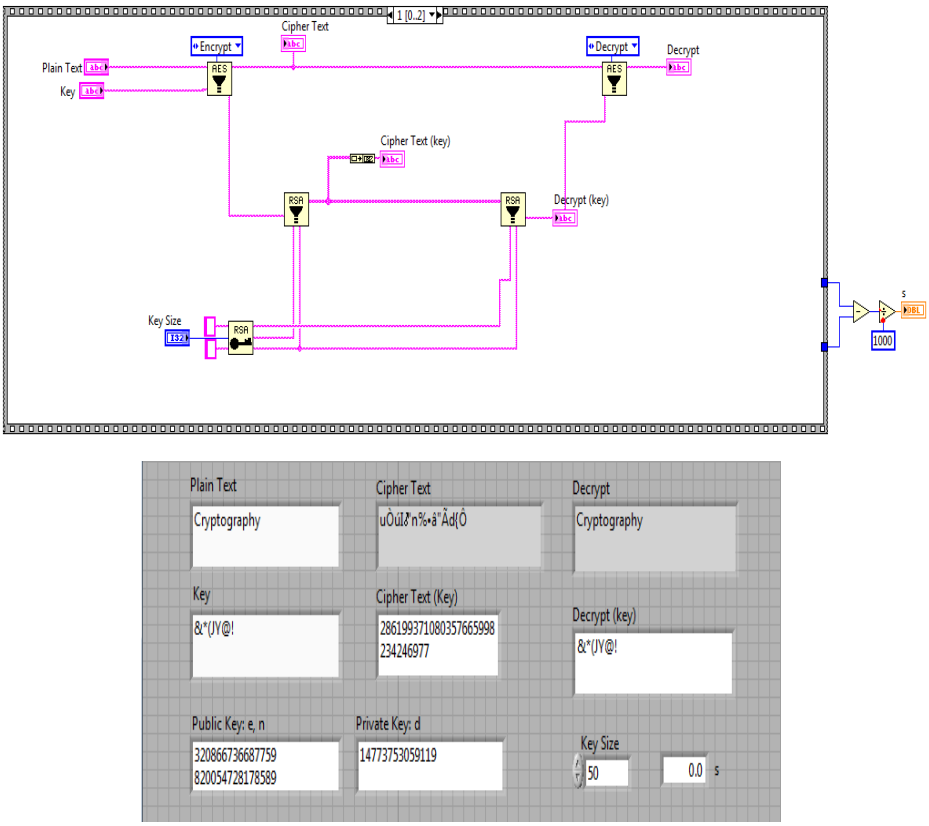

Fig. 8: The realization of DES – RSA algorithm using LabVIEW

Table 5: The speed of DES – RSA in terms of character number encrypted and decrypted

Character number	**1000**	**2000**	**3000**	**4000**	**5000**	**10000**
Time	0.2s	0.4s	0.5s	0.6s	0.8s	1.4s

From the table we can conclude that DES-RSA algorithm is slower compared to RC4-RSA, where the encryption and decryption speed was lower.

IX. CONCLUSIONS

Consequently, the information security is very important issue for companies or individuals in the global market. For this purpose, the application of cryptographic methods represents the main condition to enable a secure business communication. Due to the massive electronic communication the importance of cryptography is significant: sending sensitive data, and distance access to various information systems. On one hand, our analysis prove that secret key algorithms are faster than public key algorithms, and on the other hand we conclude that the speed of combined algorithms is not that slow.

REFERENCES

[1]. Hardjono, Security In Wireless LANS And MANS, Artech House Publishers, 2005.

[2]. P. Ruangchaijatupon, and P. Krishnamurthy, "Encryption and power consumption in wireless LANsN," The Third IEEE Workshop on Wireless LANs, pp. 148-152, Newton, Massachusetts, Sep. 27-28, 2001

[3]. Evaluating The Performance of Symmetric Encryption Algorithms, International Journal of Network Security, Vol.10, No.3, PP.216–222, May 2010

[4]. Ajay Kakkar, Dr. M. L. Singh, Dr. P. K. Bansal, "Efficient Key Mechanisms in Multinode Network for Secured Data Transmission", International Journal of Engineering Science and Technology, Vol. 2, Issue 5, 2010, pp.787-795.

[5]. Davis, R, "The data encryption standard in perspective", Communications Society Magazine, IEEE, 2003, pp. 5 – 9.

[6]. Ajay Kakkar, M. L. Singh, P.K. Bansal, Comparison of Various Encryption Algorithms and Techniques for Secured Data Communication in Multinode Network, International Journal of Engineering and Technology Volume 2 No. 1, January, 2012

[7]. Public Key Infrastructure Overview, By JoelWeise - SunPSSM Global Security Practice, Sun BluePrints™ OnLine - August 2001

[8]. "Cryptography Basics" available at weblink: http://media.wiley.com/product_data/excerpt/94/07645487/0764548794.pdf.

[9]. A Study of the Energy Consumption Characteristics of Cryptographic Algorithms and Security Protocols, IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 5, NO. 2, FEBRUARY

[10]. Public Key Cryptography - Applications Algorithms and Mathematical Explanations

[11]. International Journal of Computer Science and Network (IJCSN), Volume 1, Issue 3, June 2012 www.ijcsn.org ISSN 2277-5420

[12]. "Proposed Federal Information Processing Standard for Digital Signature Standard (DSS)," Federal Register, v. 56, n. 169, 30 Aug 1991, pp. 42980-42982.