© 2017 IJSRSET | Volume 3 | Issue 3 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Improved Data Security System Using Hybrid Cryptosystem

Olatunde Yusuf Owolabi[*1], P. B. Shola[2], Muhammed Besiru Jibrin[3]

[1,2]Computer Science Department, University of Ilorin, Ilorin, Kwara State, Nigeria
[3]Computer Science Department, Federal University Kashere, Gombe State, Nigeria

ABSTRACT

As information is send and receive through the World Wide Web, it becomes subject to inspection and access by unauthorized parties from different part of the world since it contains vital and private content that can be use for fraudulent purpose. As a result, data privacy requires more attention in order to reduce data loss and pilfering. Cryptography is one of the popular means of protecting information in order to achieve data integrity, authentication, confidentiality, accountability, accuracy and digital signatures. Symmetric & Asymmetric are the two main categories of cryptography algorithms used to protect data using the desired key. Asymmetric algorithms have been analysed by researchers to be stronger compared to Symmetric algorithms but has higher time complexity. Previous research shows that the loophole of a particular method or algorithm can be solved or minimized by another method or algorithm. Therefore, this paper proposes a method to improve data security and reduce the encryption and decryption speed of El-gamal algorithm for large volume of data using hybridization of El-gamal and Blowfish algorithm. The expected outcome of the proposed method is to achieve a more secure encryption technique to protect vital documents with faster encryption and decryption speed compare to El-Gamal algorithm.

Keywords: Algorithm, Ciphertext, Encryption, Decryption, El-gamal, Blowfish

I. INTRODUCTION

Cryptography is a subject in the field of mathematics that is applied in computer science to ensure the security primitives [7]. It is used to achieve lots of purposes like security, data integrity, non repudiation, authentication, and digital signature. It involves encrypting the original information to produce "cipher text" that is not easily interpreted by anyone [7]. The aim of cryptography is to render data in a form that is unreadable by attacker or unauthorized users [1].

There are two categories of cryptography techniques which are symmetric key and asymmetric key [5]. In symmetric key, a single key called secrete key is use for data decryption and encryption operation. Some well-recognized secrete key algorithms are 3DES (Triple Data Encryption standards), DES (Data Encryption Standard), AES aka Rijndael (Advanced Encryption Standard) [9], The International Data Encryption Algorithm (IDEA), Ron's Code (RCn) [3], Blowfish, CAST5, TEA, Twofish, RC6, Serpent, MARS [9].

Asymmetric key can also be referred to as public key encryption technique and it is based on the application of a pair of key that are mathematically related called private and public key for data security. Some asymmetric algorithms are Pretty Good Privacy (PGP, with versions using Diffie-Hellman keys and RSA) [10], Rivest, Shamir and Adleman (RSA), Elliptic Curve (EC), Diffie-Hellman (DH) [3], SSL (used for security between a web browser and server) and SSH (an alternative to telnet) [10].

In technical terms, cipher text is a meaningless text that is generated to represent vital information. The conversion of plaintext to cipher text is called Encryption. The reverse of encryption to retrieve plain text is called Decryption [8].

II. BLOWFISH ALGORITHM

Blowfish was designed by Bruce Schneier in 1993; it is one of the accepted symmetric key block cipher [11] and has a large volume of cipher suites and encryption

output. Blowfish offers a very good encryption performance rate and no standard cryptanalysis is successful on it [4]. It serves as a drop-in substitute for DES or IDEA. Blowfish algorithm has two parts [11], the first part is key expansion and the second is data encryption.

The Blowfish key expansion involves splitting the original key into series or set of sub keys. Primarily, a key of 448 bits or lesser is divided into 4168 bytes. There is a P-array as well as four S-boxes of 32-bit each. The P-array have sub keys of 32-bit which are 18 in number and each S-box has entries of 256 [11].
In encryption, 64-bit input is denote with x and Pni represents P-array (ni = number of iteration).

Blowfish Algorithm Encryption

The Steps involves

I: Partition x into two equal 32-bit that is, xLH and xRH.
II: where ni = 1,2,3,4 ...., 16, perform;
xLH = xLH XOR Pni
xRH = F(xLH) XOR xRH exchange xLH and xRH
III: After the last (16th) round exchange xLH and xRH
IV: xRH = xRH XOR P I 7 xLH = xLH XOR P18
V: Finally recombine xLH and xRH.

Blowfish Algorithm Decryption

The decrypt process is just synonymous to encryption process, but the P1, P2, P3, P4 ....., P18 are used starting from P18 to P1.

III. EL-GAMAL ALGORITHM

El-Gamal algorithm belongs to the class of asymmetric cryptosystem and is base on elliptic curve encryption system [13]. It is also comparable to the Diffie-Hellman system and widely used for data encryption as well as digital signatures. Its security relies on computation of discrete logarithm finite field.

The major feature of El-Gamal is in encryption stage, the output (ciphertext) is twofold longer compare to the corresponding plain text. The encryption generates a random N of cipher text. That is, if a particular plain text is encrypted in two different occasions; the generated ciphertext will not the same, which renders ordinary text matching attack invalid. Its loop hole includes, long cipher text (generally twice the plain text) and this algorithm encryption operation consume time.

El-Gamal is used in Internet security standard protocols such as IPSEC (Internet protocol security) [8,9], VPN (Virtual Private Network), PGP (Pretty Good Privacy) [9], SSL (Socket Secure Layer) to secure data transmitted through public networks and is mostly used in email and web.

Parameters

1. Pn → large prime number
2. g less than Pn → random number (generator)
3. y less than Pn → random number
4. compute $x = g^y \pmod{Pn}$

Encrypt message M:
Select random k such that k< Pn-1
$a = g^k \pmod{Pn}$
$b = x^k M \pmod{Pn}$
Decrypt message M
$M = (b/x^k) \pmod{Pn} = (b/g^{yk}) \pmod{Pn} = (b/a^y)$
Message signature
Select random k that are prime with p-1
Compute b: M = (ya + kb)(mod(Pn-1))
Signature (M) = (a, b)
Confirm signature:
$(x^a a^b) \pmod{Pn} = (g^m) \pmod{Pn}$

IV. RELATED WORK

In highlighting the strength of El-Gamal algorithm, [2] describes the implementation of RSA and ElGamal algorithm using JCryp Tool 1.0.0. In their paper, the comparison of the two algorithms base on security and time consumption for encryption and decryption shows that El-Gamal is more secure but encryption speed is slow.

In 2012, [7] carry out performance analysis of some algorithm such as RSA, ECC and AES considering time and complexity factors. Each algorithm is implemented in C++ and a cryptographic tool (Fidora using NS2) is used to conduct the experiment. The result shows that ECC has more cipher complexity (more secure) but spent the highest amount of time in encryption as compared to RSA and AES.

In addition, [1] agree with other researchers that El-Gamal algorithm is very secure in their research when they carryout comparative analysis between Discrete Logarithm and RSA algorithm. The algorithms were implemented in java but the simulation result also shows that El-Gamal algorithm slow performance occurs during encryption and decryption process.

DES, AES and Blowfish performance analysis was carried out in 2011 by [6]. In their research, java is use to implement and the simulation result stated that Blowfish performs better compare to other encryption algorithms. Because no known security attacks on Blowfish have successful result, this makes it to be considered as a better encryption algorithm. But more processing power required for AES contribute to it poor performance results when compared to other algorithms.

[12] Compare AES, Blowfish, and DESX in protecting files with EXE, DOC, WMV and AVI extension in their research. Java is use to implement the algorithms and the comparison result base on encryption and decryption throughput shows that Blowfish has superior performance on EXE, WMV or AVI extension as well as decryption of DOC file while AES is superior in encrypting DOC files.

V. PROPOSED METHOD

This study proposes a hybrid cryptosystem using Blowfish and El-gamal algorithm to improve data security during communication over a network. Blowfish algorithm will be use follow by El-Gamal algorithm which accept the output of Blowfish as it initial input. The hybrid cryptosystem takes the following step.

At the senders end:

1. Generate secret key using Blowfish
2. Encrypt message using the generated secret key (unknown to user)
3. Generate a pair of key using El-gamal
4. Encrypts the secret key (output of step 1) using the generated pair of key

At the receivers end:

5. Decrypt the secret key cipher text using a pair of key (unknown to user)
6. Decrypt message (cipher text) using the result of step 5.

VI. EXPECTED OUTCOME

The potency of any information security technique such as cryptography rely on simplicity and the probability to carryout it cryptanalysis. Several cryptanalysis have been carried out on both symmetric and asymmetric algorithm and the fact is, the loophole of a particular method or algorithm can be solved or minimized by another method or algorithm.

The proposed hybrid cryptosystem is expected to provide a more protected encryption and decryption process for data and information security and also improve El-Gamal algorithm performance speed in terms of encryption and decryption for large volume of data.

VII. CONCLUSION AND FUTURE WORK

In this research, we propose a cryptography method to enhance data security over a network. The network or transmission medium that is considered for communication is termed to be unsecure. The hybridize system proposed by this study compose of both asymmetric and symmetric cryptography technique using El-Gamal and Blowfish algorithm.

In this research, Blowfish generates a secret key which is use to encrypt the message containing private data or information that the sender intends to send to the receiver and pass the secret key to El-Gamal algorithm. El-Gamal algorithm continue the security processing using a pair of mathematically related, called private key and public key before the message is sent to the receiver. Figure 1 shows the pictorial view.

Despite the existence of numerous spy applications across the internet, the proposed system will enable internet users to send and receive data and information in a secure way without fear of intruder across the network.

VIII. REFERENCE

[1]. Abari Ovye John, P.B. Shola, & Simon Philip (2015). Comparative analysis of discrete logarithm and RSA Algorithm in data

cryptography. International Journal of Computer Science and Information security. (ISSN 1947-5500 Volume 13– No.2, 2015)

[2]. Ankush Sharma, Jyoti Attri, Aarti Devi & Pratibha Sharma. (2014). Implementation & Analysis of RSA and ElGamal Algorithm. Asian J. of Adv. Basic Sci.: 2(3), 125-129 ISSN (Online): 2347 – 4114

[3]. Boomija M.D. & S.V. Kasmir Raja (2016). Secure data sharing through Additive Similarity based ElGamal like Encryption. International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB16). 978-1-4673-9745-2 ©2016 IEEE

[4]. Chaitali Haldankar & Sonia Kuwelkar (2014). Implementation of AES and Blowfish algorithm. IJRET: International Journal of Research in Engineering and Technology. Volume: 03 Special Issue: 03 | May-2014 | NCRIET-2014, eISSN: 2319-1163 | pISSN: 2321-7308. Available @ http://www.ijret.org

[5]. Gary C. Kessler. (2014). An Overview of Cryptography and Handbook on Local Area Networks (Auerbach, Sept. 1998). © 1998-2016. Retrived from http://www.garykessler.net/library/crypto.html#keylen

[6]. Jawahar Thakur, & Nagesh Kumar. (2011). DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis. International Journal of Emerging Technology and Advanced Engineering (ISSN 2250-2459, Volume 1, Issue 2, December 2011)

[7]. Kumar Saurabh Er., & Ravinder Er. Singh Mann (2012). A Comparative Evaluation of Cryptographic Algorithms. Ravinder Singh Mann et al, Int. J. Computer Technology & Applications,Vol 3 (5), 1653-1657 ,ISSN:2229-6093, Sept-Oct 2012

[8]. Kumar, Chandan; Dutta, Sandip & Chakraborty, Soubhik (2015). Hiding Messages using Musical Notes: A Fuzzy Logic Approach. International Journal of Security And Its Application.

[9]. Malek jakob kakish (2012). Authenticated and secure el-gamal cryptosystem over Elliptic curves. www.arpapress.com/volumes/vol10issue2/ijrras_10_2_16.pdf. Ijrras 10 (2). February 2012

[10]. Mansoor Ebrahim , Shujaat Khan,& Umer Bin Khalid (2013). Symmetric Algorithm Survey: A Comparative Analysis. International Journal of Computer Applications (0975 – 8887) Volume 61– No.20, January 2013

[11]. Ramesh A., & Dr.A.Suruliandi ME (2013). Performance Analysis of Encryption Algorithms for Information Security. 2013International Conference on Circuits, Power and Computing Technologies [ICCPCT-2013]. 978-1-4673-4922-2/13/$31.00 ©2013 IEEE

[12]. Rishabh Arora & Sandeep Sharma. (2012). Performance Analysis of Cryptography Algorithms. International Journal of Computer Applications (0975 – 8887) Volume 48– No.21, June 2012

[13]. Zengqiang Wu, Di Su, & Gang Ding (2014). ElGamal Algorithm for Encryption of Data Transmission. 2014 International Conference on Mechatronics and Control (ICMC). July 3 - 5, 2014, Jinzhou, China. 978-1-4799-2538-4/14/$31.00 ©2014 IEEE