

HYBRIDIZATION OF EL-GAMAL AND BLOWFISH ALGORITHM FOR DATA SECURITY

*A. O. Bajeh, Y. O. Olatunde, A. G. Akintola, A. O. Balogun, M. O. Wasiu and A. T. Suleiman

Department of Computer Science
Faculty of Communication and Information Sciences
University of Ilorin, Ilorin.

*bajehamos@unilorin.edu.ng, hizyyusuf@gmail.com, abimbolar@yahoo.com,
balogun.ao1@unilorin.edu.ng, wastoy4real@gmail.com, abitao400@gmail.com

*Corresponding Author

Abstract

The internet connects all part of the world together and thus, makes it very easy and fast to communicate from different location. Reports by internet user on security issues such as hacking of E-mail account, SQL injection, unauthorized access to transactional details makes users to migrate from one platform to another. The increasing activities of hackers to overcome the existing security measures have raised the need for more and improving security technique. Therefore, this study demonstrates hybridization of Blowfish and El-Gamal algorithm to improve data security and improve the performance of El-Gamal algorithm. In the hybrid system, Blowfish is used to encrypt message containing private data using a secret key after which the secret key is encrypted by El-Gamal algorithm using public and private key which are mathematically related. The cipher text produced contains the mixture of private data and secret key. A simulation program is develop using java in order to experiment the difference between the hybrid system, blowfish and El-Gamal algorithm. The result shows that the developed hybrid system is more secure and faster compared to El-Gamal algorithm.

Keywords: Cryptography, Blowfish, El-Gamal, Algorithm, Cipher text, Encryption, Decryption

Introduction

The internet is a global network that has now become an essential (or indispensable) tool through which information are transported or shared between entities (Mossberger, 2011). It has been adopted by government, private organizations and individuals for several purposes which include dissemination of data and information among others across the world.

The volume and types of data and information that are sent or received through the internet increase on a daily basis. Such information includes sensitive matters like financial transaction, government in formation, account detail that must be kept secret away from hackers and eavesdroppers (Kaiz, 2009). It is no more news to hear of data corruption and illegal entries into systems on the internet. There are several reports of network infiltrations and cyber-attacks that are traced to political goals and nation-states (Fred, 2015).

Over the years, Cryptography is widely employed for securing data on a public network. It is a subject in the field of mathematics that is applied in computer science to ensure the security primitives. The target of cryptography is to convert data and make it incomprehensible for unauthorized user to ensure data integrity, authentication, and digital signatures (Rajan & Geeta, 2013). It involves encrypting the original information to produce “cipher text” that cannot be easily interpreted by a third party that has no key to de-cipher the encrypted text.

Symmetric cryptography and Asymmetric cryptography are mainly the two aspects of cryptography techniques shown in Figure1. Symmetric cryptographic system makes use of a single key called secret key for data encryption and decryption. In contrast, asymmetric cryptographic system is based on the application of a pair of key that are mathematically related called private and public keys for data encryption and decryption. Asymmetric cryptography poses a strong security because whoever encrypts message or perform signature verification cannot decrypt messages or create signatures. (Olatunde, Shola & Muhammed, 2017).

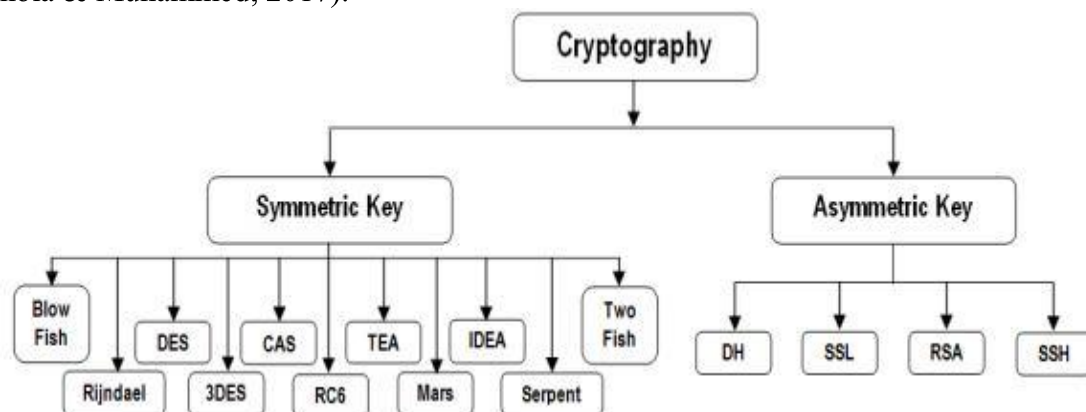


Figure 1: Different Symmetric and Asymmetric Algorithm (adopted from Kumar & Ravinder, 2012)

The main operations involved in cryptography algorithm are:

- i. Encryption: changing of text or message into cipher text or message
- ii. Decryption: the reverse of encryption
- iii. Digital signature: adding verification value to message.

2 THE ALGORITHMS

This section presents the algorithms hybridized in this study.

2.1 BLOWFISH ALGORITHM

Blowfish is one of the most popular secret key algorithm. It is a block cipher proven to have better performance compared to IDEA or DES. It uses a key length between 32 bits to 448 bits, which is to have a wide range of use. It was designed in 1993 by Bruce Schneier. It is unpatented and freely available. (Thomas & Panchami, 2015).

Blowfish Encryption Algorithm:

- Step 1: Create x as 64 bit input
- Step 2: Create i to store the number of iterations
- Step 3: Create variable xL and xR
- Step 4: $xL = x \text{ XOR } P_i$
- Step 5: $xR = F(xL) \text{ XOR } xR$
- Step 6: Exchange xL and xR
- Step 7: If $i < 16$ go to (iv) else increase i value by 1
- Step 8: Exchange xL and xR
- Step 9: $xR = xR \text{ XOR } p_{17}$
- Step 10: $xL = xL \text{ XOR } p_{18}$
- Step 11: merge xL and xR
- Step 12: End.

Blowfish Key Expansion Algorithm:

- Step 1: Create Array P with 18 3-bit subkeys
- Step 2: Create Array S-boxes with 4 32-bit values
- Step 3: Initialize S-boxes and the P-array
- Step 4: XOR P-array with the key bits. For example, $P_1 \text{ XOR (first 32 bits of key)}$, $P_2 \text{ XOR (second 32 bits of key)}$...
- Step 5: Use the method in iv to encrypt the all-zero string
- Step 6: This new output is now P3 and P4
- Repeat 521 times in order to compute new sub keys for the four S-boxes and the P-array.

Blowfish Decryption Algorithm:

This is the same as the Encryption process but in the reverse order.

2.2 El-GAMAL ALGORITHM

In 1985, Tather El-Gamal demonstrated a cryptosystem called "El-Gamal". It is one of the most secure public key encryption system. Its security rely on the (presumed) difficulty of computing discrete logs in a large prime modulus. Compare to RSA it is more secured and capable of generating random ciphertext for the same plaintext. Its drawback is that the its ciphertext is always twice the length of the plaintext. (Olatunde, Shola and Muhammed, 2017)

El-Gamal Key Generation:

In generating the pair of El-Gamal security key, the following components are required.

Step 1: Large prime number Lp

Step 2: Generator which is a primitive element Ge and cannot be any number

Step 3: A random integer Ri whereby $2 \leq Ri \leq Lp - 2$. This can be any number, it serves as the private key. It should be kept private by the user.

Step 4: Compute D such that $D \equiv Ge^{Ri} \pmod{Lp}$.

Therefore, the generated public key is (Lp, Ge, D) and private key is Ri . The public key is disclosed to unlimited number of other users.

El-Gamal Encryption Process:

In order to encrypt the secret data, the Sender B must do the following:

Step 1: Get the public key (Lp, Ge, D) from the receiver A.

Step 2: Choose an integer k such that: $2 \leq Ri \leq Lp - 2$

Step 3: Note: Represent the Secret key as an integer S where $0 < S < Lp - 1$

Step 4: Compute (Y) as follows: $Y \equiv Ge^{Ri} \pmod{Lp}$

Step 5: Compute (Z) as follows: $Z \equiv (D^{Ri} * S) \pmod{Lp}$

Step 6: The Cipher text (C) produce is: $(Y, Z) = C$

Step 7: The sender B sends C to the receiver A.

El-Gamal Decryption Process:

A pair of key is needed to decrypt the cipher text because it is encrypted using a pair of key. The decryption process is as follows: (Olatunde, Shola and Muhammed, 2017).

Step 1 Obtain the cipher text $(C = (Y, Z))$ from B.

Step 2 Compute (X) as follows: $X \equiv Y^{Lp-1-Ri} \pmod{Lp}$

Step 3 Recover the Secret as follows: $S \equiv (X * Z) \pmod{Lp}$

Report in previous research shows Blowfish algorithm possess high speed of operation and weak security strength while El-Gamal algorithm has a very high security strength but very slow performance. This motivates the hybrid system developed in this study in order to achieve a cryptosystem that is secured and consume lesser resources.

Related Work

In 2014, Christina & Joe worked on data security using Blowfish algorithm. The study emphasizes the implementation simplicity, fast and secured feature of the algorithm. In highlighting the strength of Blowfish algorithm, Rishabh & Sandeep (2014) worked on the performance analysis of cryptography algorithms. The study showed that the

performance of Blowfish is better in terms of encryption and decryption process of executables (that is, .exe) and documents (with .doc extension) file compare to AES, DESX.

Saikumar and Vasanth (2015) modify Blowfish algorithm and propose a single round of the algorithm. The simulation result obtained using Xilinx ISE with VHDL language reveals that blowfish is fast and resists several attacks. A comparative evaluation of cryptographic algorithms was done by Kumar & Ravinder (2012). In the study, El-Gamal algorithm was conclusively explained to be very strong and secure but slow in performance compared to AES and RSA. A cryptographic tool was used to perform the experiment. CPU time, used memory space, total computing time and total power were used as comparative performance metrics.

In addition, Abari, Shola and Simon (2015) in a study that compares RSA algorithm and Discrete Alogarithm using java programming language for implementation and text document for testing showed that El-Gamal algorithm is very secured explain further that El-Gamal algorithm slow performance occur during encryption and decryption process. Babatunde, Adewole, Abdulraheem and Oniyide (2014) demonstrated a network-based key exchange using El-Gamal. The study used java for implementation and it was discovered that the algorithm is highly secured by producing pseudorandom cipher text during encryption but requires double of the size of the plain text for the corresponding cipher text and it is very slow during encryption and decryption processes.

Methodology

This study uses Blowfish and El-Gamal algorithm discussed in section 2 to form a hybrid system. In the hybrid system, Blowfish is used to encrypt message containing private data using a secret key after which the secret key is encrypted by El-Gamal algorithm using public and private key which are mathematically related. The cipher text produced contains the mixture of private data and secret key. The overall process of the hybrid system is perceived by the user as an asymmetric technique rather than hybrid and this increases the level of difficulty that attackers will come across in order to have access to private data. Text document of 120kb, 216kb and 508kb are used in the experiment.

The Hybrid System Pseudo-code

- Step 1 Generate blowfish secret key denoted as F
- Step 2 Compute El-Gamal public and private key
- Step 3 Distribute the public key
- Step 4 Declare and initialize M, N and R as an empty string

Step 5	Read content of original document
Step 6	For (i =0, i <= length of document, i++)
Step 7	M = M + Encrypt character at index i (using F)
Step 8	Output M as the Secured document
Step 9	For (y =0, y <= length of F, y++)
Step 10	N = N + Encrypt character at index y (using public and private key)
Step 11	Output N as the Secured secret key
Step 12	R = M + N
Step 13	Send or receive R as the secured data
Step 14	Extract M and N from R
Step 15	Declare and initialize F and S as an empty string
Step 16	For (j =0, j <= length of N, j++)
Step 17	F = F + Decrypt character at index j (using public and private key)
Step 18	For (k =0, k <= length of M, k++)
Step 19	S = S + Decrypt character at index k (using F)
Step 20	Output S as the original document retrieved

Performance Evaluation

In this work, the performance analysis was carried out based on Encryption time, Decryption Time and Memory used.

Encryption Time: The total time a Virtual Machine (VM) or a computer takes to perform encryption of a message.

Decryption Time: The total time a Virtual Machine (VM) or a computer takes to perform decryption of a message

Memory: Memory refers to the computer hardware devices involved to store information for immediate use (primary storage) or later use in a computer. In this context, it is the total amount of storage used by a computer program to perform its operations.

Results and Discussion

Analysis of the result for Blowfish algorithm, El-Gamal algorithm and the developed hybrid method is shown in Figure 2, Figure 3 and Figure 4 respectively in terms of memory used. The portion labeled A, B, C and D;

A: the total size of the available memory (that is, total available Heap Size)

B: total memory used by the algorithm (that is, total used Heap)

C: Surviving Generators

D: Relative Time Spent in GC (Garbage Collector)

The unlabeled portion in Figure 2, Figure 3 and Figure 4 is not considered in the comparison because it denotes the number of threads and classes loaded at runtime which varies based on coding technique and professionalism of the programmer.

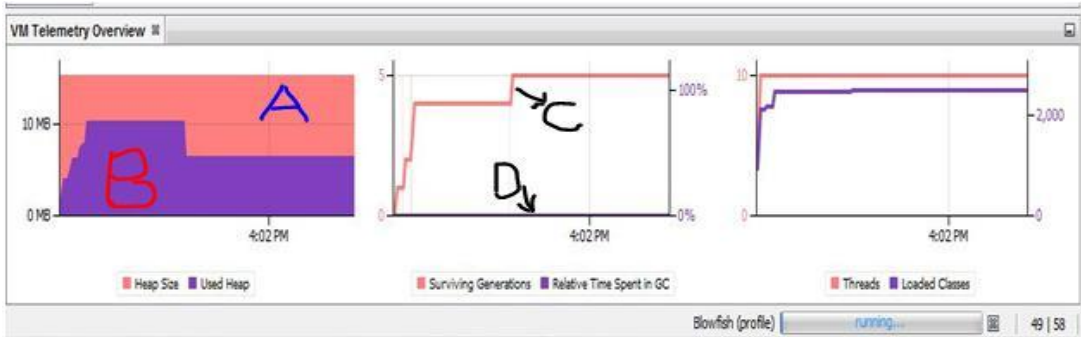


Figure 2: VM Telemetry Overview for CPU Performance of Blowfish algorithm

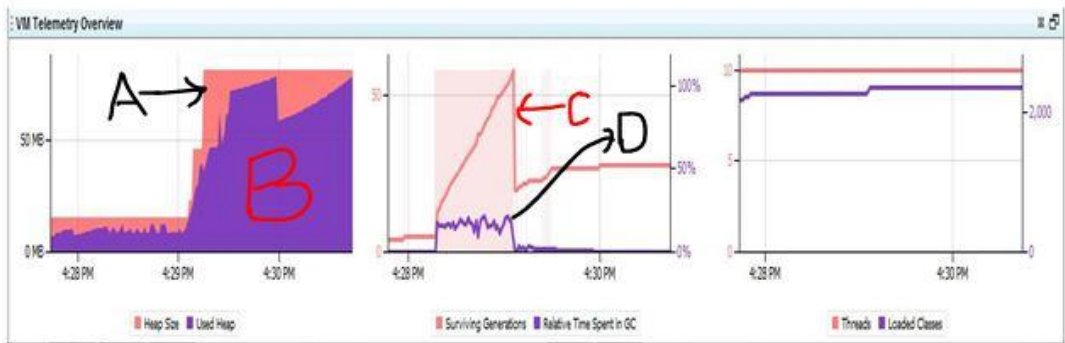


Figure 3: VM Telemetry Overview for CPU Performance in El-Gamal algorithm

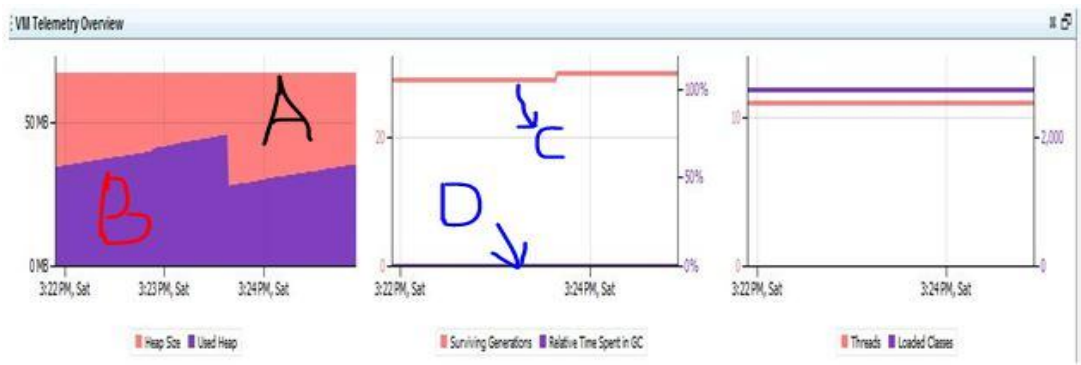


Figure 4: VM Telemetry Overview for CPU Performance in Hybrid Technique

Figure 2, 3 and 4 shows that the memory used by the hybrid system is lower compared to El-Gamal algorithm while Blowfish used the lowest memory space. In terms of

Relative Time Spent in GC, Blowfish and the hybrid technique used same amount of time which is lower compared to El-Gamal.

The comparison of Blowfish, El-Gamal and the Hybrid system in terms of encryption and decryption time is shown in Table 1.

Table 1: Comparison of Blowfish, El-Gamal and Hybrid Technique

S/N	Data Size (kb)	Algorithm	Encryption Time (Mill Sec)	Decryption Time (Mill Sec)
1	120	Blowfish	46	<1
		El-Gamal	6,084	5,351
		Hybrid	48	16
2	216	Blowfish	61	15
		El-Gamal	45,786	42,214
		Hybrid	63	32
3	508	Blowfish	63	27
		El-Gamal	4 28,143	336,508
		Hybrid	84	31
4	604	Blowfish	85	38
		El-Gamal	437,845	733,805
		Hybrid	90	67

The comparison shows that the developed hybrid system performs better than El-Gamal algorithm in all perspective. Although, this study has been able to show that there is a significant difference in the speed of operation between Blowfish, El-Gamal and the hybrid system. It should be noted that the value of encryption and decryption time in Table 1 may vary based on device configuration.

Table 2 shows comparison analysis between the mentioned algorithms based on some other attribute.

Table 2: Comparison of Blowfish, El-Gamal, Hybrid Technique based on other attribute

Attributes	Blowfish	El-Gamal	Hybrid
Date of Development	1993	1985	Proposed 2017
Key Size	32 to 448 bits	>1024 bits	Any of Blowfish and El-Gamal
Size of Block	64 bits	At least 512 bits	Any size of block in Blowfish or El-Gamal
Scalability	Scalable	Not Scalable	Scalable
Encrypt process	Fast	Very Slow	Fast
Decrypt process	Fast	Very Slow	Fast
Security	Reliable	Reliable	More Reliable
Key Used	Same	Same	Encrypted

Conclusion

One of the leading reasons for implementing an encryption-decryption scheme is privacy. As information transported through the internet, both the information and the transmission medium becomes subject to inspection and access from unofficial or unlawful individual and organization (Kaiz, 2009). In this study, encryption and decryption of plain text message was demonstrated using hybridization of Blowfish and El-Gamal algorithm. The hybrid technique provides more security and also reduces the encryption and decryption time of El-Gamal algorithm. That is, a more secured and faster algorithm is developed. In future work, comparative analysis of several hybrid techniques will be carried out based on message format in order to detect the best hybrid technique to secure message in various (text, audio, video or image) file format.

References

- Abari Ovy 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*, 13(2), 25-40.
- Babatunde A.O., K.S. Adewole, M Abdulraheem & S.A. Oniyide (2014). A Network-based Key Exchange Cryptosystem Using Elgamal Algorithm. *African Journal of Comp & ICTs*, 7, (2), 45-52.
- Christina L & Joe Irudayaraj V S (2014). Optimized Blowfish Encryption Technique. *International Journal of Innovative Research in Computer and Communication Engineering*, 2, (7), 2320-9798
- Fred schreier (2015). On cyberwarfare. DCAF HORIZON 2015, working paper no. 7 geneva, geneva centre for the democratic control of armed forces, 2015.
- Kaiz Karen, 2009. 10 Most Common Uses of Internet. Retrived on 09 Deccember, 2010 form <http://www.sooperarticles.com/internet-articles/10-most-common-uses-internet-19405.html>
- Kumar Saurabh Er., & Ravinder singh Mann Er.. (2012). A Comparative Evaluation of Cryptographic Algorithms. Ravinder Singh Mann et al. *International Journal of Computer Technology & Applications*, 3 (5), 1653-1657.
- Mossberger Karen (2011). Digital Citizenship – The Internet, Society and Participation. By Karen Mossberger, Caroline J. Tolbert, and Ramona S. McNeal." 23 Nov. 2011. ISBN 978-0-8194-5606-9
- Olatunde Yusuf Owolabi, P. B. Shola, Muhammed Besiru Jibrin. (2017); "Improved Data Security System Using Hybrid Cryptosystem", *International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET)*, Print ISSN: 2395-1990, Online ISSN : 2394-4099, Volume 3 Issue 3, pp.90-93, May June 2017. URL: <http://ijsrset.com/IJSRSET173311.php>
- Rajan, S. J., & Geeta, S. J. (2013). File Encryption and Decryption Using Secure RSA. *International Journal of Emerging Science and Engineering (IJESE)*, 1(4), pp. 11-14
- Rishabh Arora & Sandeep Sharma. (2014). Performance Analysis of Cryptography Algorithms. *International Journal of Computer Applications*, 48(21), June 2014
- Saikumar Manku & K. Vasanth. (2015). Blowfish encryption algorithm for information security. *ARPJN Journal of Engineering and Applied Sciences*, 10(10), June 2015.