Hybrid Cryptosystem Using RSA, DSA, Elgamal, And AES

Article *in* International Journal of Scientific & Technology Research · October 2019

CITATION
1

READS
566

5 authors, including:

Edwin Arboleda
Cavite State University, Indang, Cavite,Philippines
40 PUBLICATIONS **269** CITATIONS
SEE PROFILE

Rhowel Dellosa
Asia Technological School of Science and Arts
33 PUBLICATIONS **132** CITATIONS
SEE PROFILE

Hybrid Cryptosystem Using RSA, DSA, Elgamal, And AES

Levinia B. Rivera, Jazzmine A. Bay, Edwin R. Arboleda, Marlon R. Pereña and Rhowel M. Dellosa

Abstract— The integration and combination of an asymmetric and symmetric algorithm such as RSA, ElGamal, DSA, and AES were presented. Hybrid encryption has been used to ensure integrity in terms of data exchanged between the sender and receiver. The strength of the asymmetric algorithm such as RSA depends on the difficult process of factorization of large prime integers while the ElGamal's security lies on Discrete Logarithm Problem (DLP). The symmetric algorithm is known to process the encryption faster than the asymmetric algorithm. Key generation of DSA is merged in the proposed algorithm. DSA is recognized for its fast signature algorithm while the AES S-Box is used to hash the ciphertext obtained. AES strength is its fast expansion key tone. Experiment's result is presented to analyze the effectiveness of the proposed algorithm.

Index Terms—AES, Algorithm, El Gamal, DSA, RSA, Encryption, Symmetric, Asymmetric

1 INTRODUCTION

The art of reading and writing secret information is Cryptography, comprises the uses of mathematics and science in order for the protection of original information[1-3]. Cryptography covers the method of encrypting the raw information into an unintelligent form and hard to decipher by just anyone. The extraction of the original message is done through decrypting the encrypted message through the use of the key pair, public and private key[4,5]. Most Encryption Algorithms are commonly available for use in information security. Encryption algorithm has two types; namely, the Asymmetric (public) keys [6] and the Symmetric (private) keys[7]. Encryption in Symmetric key is also called secret key encryption. This type of encryption involves the use of only one key to decrypt and encrypt plaintext or data[8]. On the other hand, Asymmetric key requires the use of two keys, one is a public key typically used for encrypting while the other one is the private key, serves as the decryption key[9]. In encryption algorithm such as RSA (Rivest-Shamir-Adleman), the public key is used for encryption and the private key is used for decryption. Public key encryption is based on computationally extensive mathematical functions[10]. Data Encryption Standard (DES) and Advanced Encryption Standard (AES) are examples of cryptography algorithms that have their own strengths and weaknesses[11]. DES algorithm uses one 64-bits key, in contrast to the AES algorithm where it uses various bits' keys such as 128, 192 and 256. In encryption algorithm, one of the apparent issues is the problem regarding key distribution, Asymmetric key encryption or public-key encryption resolves this problem. Examples of Asymmetric key algorithm are the RSA and DSA where both use public and private keys; each for encryption and decryption, respectively. Users of this algorithm have to use two keys; where one key-public key, is known to the public for it used for encryption of the data while the other key-private key, is only known to the user and is used for decrypting the encrypted data [12].

Levinia B. Rivera *is from the Department of Computer and Electronics Engineering, College of Engineering and Information Technology of Cavite State University.*
Jazzmine A. Bay *is from the Department of Computer and Electronics Engineering, College of Engineering and Information Technology of Cavite State University.*
Edwin R. Arboleda *is from the Department of Computer and Electronics Engineering, College of Engineering and Information Technology of Cavite State University.*
Marlon R. Pereña *is from the Department of Information Technology, College of Engineering and Information Technology of Cavite State University.*
Rhowel M. Dellosa *is from the Computer Engineering Department of Asia Technological School of Science and Arts.*

2 TECHNICAL ASPECTS

Developed by Ron Rivers, Adi Shamir, and Leonard Adleman is public-key encryption known as RSA [13]. RSA was first recognized in use for signing and encryption. The three main steps in RSA are Key Generation, Encryption and Decryption. The weakness of RSA manifests when small encryption exponent in sending the same message to the different recipient is used. The second loophole is when same key is used for signing and encryption.

2.1 Related Studies

RSA is the acronym for Ron Rivest, Adi Shamir, and Leonard Adleman algorithm. These are the names of MIT students who first proposed an explanation of the said algorithm to the general public, the year 1977[14]. RSA is one of the Asymmetric cryptography used. RSA algorithm follows that the user must choose two prime numbers from these a supplementary value is derived. The prime number must be kept hidden from anyone but the user. The public key is used for encryption of message and from the name itself it is known to the public. There have been improvements in the algorithm of the RSA, and with the currently published methods it is difficult to crack the private key if the public key is large enough[15,16]. It takes great knowledge about prime numbers before someone (hacker) can decode the message [17-19]. The study of [26] make use of closest coordinates to develop an algorithm for indoor positioning system to improve its efficiency. The present standard for secret key encryption is the Advanced Encryption Standard Algorithm (AES). Vincent Rijmen and Joan Daemen, originated from Belgium, are the cryptographers who are the creator of the AES algorithm[20].

The advent of AES replaced the old Data Encryption Standard (DES). AES is easy to implement and processes fast in a very reasonable amount of time on a regular computer, this paves way for its success in setting the standard in asymmetric algorithm. In AES, the standardized version of the Rijndael algorithm is used by the Federal Information Processing Standard 197. The algorithm established the incorporation of Exclusive-OR operations (XOR), octet substitution with an S-box, row and column rotations, and a Mix Column in the flow of algorithm. The cipher uses number of encryption sequences which converts plain text to ciphertext. The output of each sequence algorithm is the input to the next algorithm. The output of the final algorithm is the encrypted plain text known as ciphertext. The input set by the user is entered into a matrix known as State Matrix[21] On the principle of public-key cryptography, that's where Digital Signature operates. The idea of key pairs, private and public key, is where public cryptography is constructed on. Large prime numbers make up the public and private keys. These prime numbers are produced by a mathematical algorithm. In DSA, the key pairs are primarily involved both for the process of signing and encrypting the message. The application of DSA key pairs is to authenticate the identity of the user. The Digital Signature has the same reliability as of a document and handwritten signatures[22]. In network security, DSA is acclaimed to be one of its major developments. The rapid growth of digital communications resulted in a significant need for Digital Signature. The integrity of the assigned data and the identity of the signatory is authenticated by the Digital Signal algorithm. The process of the authentication in DSA is whereby the receiver of the digital message is assured and can ensure the integrity of the identity of the sender and the message. On the other hand, RSA encryption algorithm takes up longer time due large key size and modular exponentiation operations in fortifying security. This is the reason behind the slow process in RSA's Digital Signature. There is a direct proportion between the length of the transmitted signature and the length of the transmitted message. Hence, the longer the message also create longer digital signature [23]. ElGamal is an asymmetric key algorithm. This algorithm is developed in the year 1984 by Taher Elgamal. This algorithm is an improvement to the Diffie-Hellmen key exchange protocol and works over finite fields. Foundation of the security of this algorithm is the Discrete Logarithm Problem. Thus, the ElGamal is one of the many encryption schemes that use randomization in encryption process [24]. The propositions presented in this paper is the combination of the asymmetric and symmetric encryption into one algorithm, which intends to provide a comprehensive yet secure encryption method. The prominent characteristics of RSA and ElGamal have been considered and implemented in the proposed algorithm. The use of prime numbers and the modular function is one of the powerful advantages of these algorithms. The randomization in producing keys makes it difficult to be cracked by attempters. In order to confuse hackers, the proposed algorithm is diversified with symmetric cryptosystem, DSA, and AES. The key generation of DSA is used to provide keys for ElGamal encryption, while AES provides hashing function for messages, thus producing various hexadecimal combinations to cipher the text.

RSA

The steps of the RSA algorithm are as follows: A. Generation of Public and Private keys

A. Generation of Public and Private Keys

Following are the steps for the generation of public and private keys:

1. Choose two distinct prime numbers p1 and p2.
2. Multiply them to get 'n'. \
3. Calculates (p1 -1) * (p2 -1) and mention it as ϖ(n).
4. Select 'e' as a public key, such that e and ϖ(n) are relatively prime.
5. Compute e*d = 1(mod ϖ(n)) and consider 'd' as the private key.

B. Encryption Scheme

1. The message M is encrypted into ciphertext C using the public key 'e' such that C = Me mod n.

C. Decryption

2. The ciphertext C is decrypted back to its original form M with the help of the private key 'd' such that M= Cd mod n.

ELGAMAL

Elgamal is an asymmetric key algorithm developed by Taher Elgamal in the year 1984[24]. It is based on the Diffie-Hellman key exchange algorithm and works over finite fields. The security of this algorithm is based on the Discrete Logarithm Problem (DLP). The steps of RSA algorithm are as follows: A. Generation of Public and Private keys

A. Initialization

Before the encryption and decryption process can start, the following initialization is done:

3. Choose a random prime p and a primitive root element 'a' ε Fa.
4. Private key 'x' is chosen as a random number such that 'x' ε ∪ Fa-1.
5. Public key 'y' is computed using the private key 'x'. Therefore, y = ax mod p.

B. Encryption Scheme

1. The sender chooses a random integer k ε ∪ Fa-1 and computes one-time key K = yk mod p.
2. The message M is encrypted into two parts (C1 and C2) as ak mod p and K*M mod p respectively.

C. Decryption

1. The ciphertext is decrypted as M = C2 K-1 mod p using one-time key K = C1x mod p.

DSA

Key pair generation:

p: a prime number between 512 to 1024bits long

q: a prime factor of p−1, 160bits long

g ≡ h(p−1)/q (mod p) > 1, and h <p−1

(p,q and g): public parameters

x<q: the private key, 160bits long

y ≡gx (mod p): the public key, 160bits long

Signing process (sender): k<q: a random number

r ≡ (gk mod p) (modq)

s ≡k−1 (h+xr) (modq), h=H(m) is a one-way hash function of the message m.

(r,s): signature

Verifying signature (receiver):

w ≡ s−1 (mod q)

u1≡h×w (mod q)

u2≡r ×w (mod q)

v ≡ (gu1yu2 (mod p)) (mod q)

If v =r, then the signature is verified.

AES

The Advanced Encryption Standard (AES) otherwise known as the Rijndael algorithm is a FIFS-accepted cryptographic algorithm established by Daemen and Rijmen. It is an AES candidate algorithm in 1999. The Rijndael algorithm specified as a symmetric block cipher that can process data blocks of 128 bits using cryptographic keys of 128, 192 and 256 bits [25].

3 Proposed Algorithm

The proposed algorithm is a combined method of Digital Signature Algorithm (DSA), Rivest-Shamir-Adleman Algorithm (RSA), El Gamal, and Advanced Encryption Standard (AES) cryptosystem with their unique strengths. DSA which is known for its fast signature generation and discrete logarithm problem is same as ElGamal. RSA strength lies in the difficult factorization of large integers and its use of different key for encryption and decryption. While fast expansion key time for AES S-Box. Figure 1 displays the block diagram of the proposed algorithm.

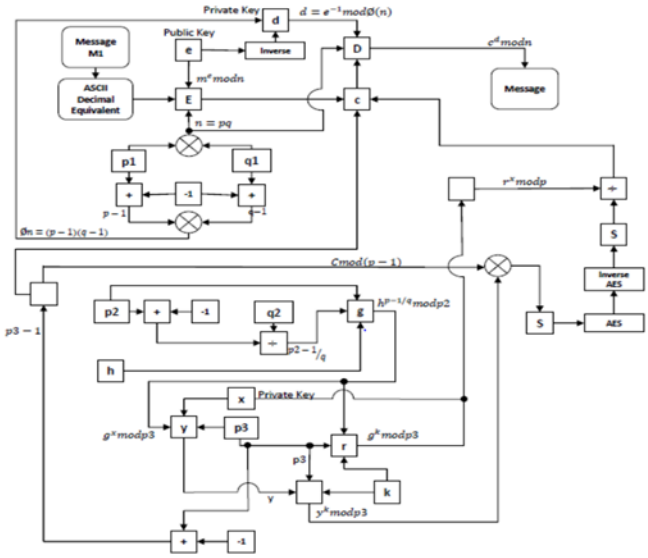

Fig. 1. Block Diagram of the Proposed Algorithm

4 Methodology

4.1 Key Generation:

1. Alice's message Mn is any mix of characters from the ASCII table. And each character of her message is converted to its ASCII decimal equivalent.
2. Alice then assigns a key p1 which is a prime number greater than the highest ASCII decimal equivalent of her characters being chosen.
3. Alice also assign a random prime number q1
4. Generate the value of n by multiplying p1 and q1. And Øn by multiplying p1-1 and q1-1.
5. Alice picks a number of encryption keys en, such that the value must be a prime number and gcd(e, ϕn)=1. Public keys can be less than or equal to the number of the message.
6. Value of d can be calculated using the Euclidean Algorithm:

$$\mathbf{d = e^{-1} \bmod Øn}$$

7. Alice again assigns a key p2 and q2, which are prime numbers.
8. Alice then chooses a random number h, equal to the number of e.
9. And generate the value of gn using the formula:

$$\mathbf{g_n = hn^{p2-1/q} \bmod p_2}$$

10. Choose a prime number p3 which is greater than Cn.
11. Bob chooses a private key x and keeps it a secret. He then sends gnx to Alice.
12. Alice computed yn using the formula:

$$\mathbf{y_n = g_n^{\,x} \bmod p_3}$$

13. Choose k which is a random number such the gcd (k, p3-1).
14. Generate the value of rn, which is the decryption key and also a private key using the formula:

$$\mathbf{r_n = g_n^{\,k} \bmod p_3}$$

For Encryption:

1. To encrypt the message, Alice computes for the value of C using the formula:

$$\mathbf{Cn = Mn \bmod n}$$

2. Alice then computes again for Sn using the formula:

$$\mathbf{S_n = (y_n^{\,k} \bmod p_3)\ [C \bmod (p_3\text{-}1)]}$$

3. The value of Sn will be hidden using AES S-Box
4. The proposed algorithm uses a repetitive cycle of key pairs that make it unique. For example, there are 6 key pairs chosen: the seventh character will apply the public key g7 = g1 and y7 = y1, so r7 = r1; the eighth character will apply the public key g8 = g2 and y8 = y2, so r8 = r2; and so on and so forth.

For Decryption:

1. To decrypt the message, Bob uses the Inverse AES S-Box.
2. Bob uses the private key x: and apply the formula:

$$\mathbf{r_n^{\,x} \bmod p_3}$$

3. Compute for C using:

$$\mathbf{C = S_n / r_n^{\,x} \bmod p_3}$$

4. And Bob will get the message using:

$$\mathbf{M_n = C^d \bmod n}$$

5 Results And Analysis

Table 1 shows the avalanche effect of the proposed hybrid algorithm on the random number keys. It proved that with the multiple numbers of k used, the ciphertext will be a lot different compared to single k. Although it is more secure to use multiple keys yet at some point, the system would be slower.

TABLE 1
THE AVALANCHE EFFECT OF THE HYBRID ALGORITHM

Message	Parameters	Random Key	Cipher Text
A large fawn jumped quickly over white zinc boxes	p1 = 131 p2 = 79 p3 = 3001 q1 = 23 q2 = 13 e1 = 83 e2 = 61 e3 = 59 e4 = 37 e5 = 23 e6 = 29 g1 = 52 g2 = 38 g3 = 64 g4 = 10 g5 = 46 g6 = 13 x = 18	k = 7	7dadcd2c, 7783d1cd, f2fc2653, 63c4d16b, 7cf53fa7, 63aa5b3f, 63ca6301, 7783d1cd, f2206f77, 63c4d16b, 6347014f, 63fa9a9d, f25a5b30, 6f13e205, f2881359, 7b460151, 7c07963f, 63936353, 6320e56f, 7783d1cd, c545dc23, f2881359, 770c0c97, 7b44c412, 6312fc53, 7cf90ccd, 6bef4f05, 6b135130, 772692dc, 7b1abc53, 63936353, 63c44638, 7783d1cd, c5474ff0, 63ca2251, 6b7bdcc7, 63926a9d, 63ca6301, 7783d1cd, 6f00dcfa, 770c0c97, 7b18404f, 7777473f, f25a5b30, 7b9682cd, 7bcd82c4, 7c3f964d, 7c4693fa,7c3f9d3f
A large fawn jumped quickly over white zinc boxes	p1 = 131 p2 = 79 p3 = 3001 q1 = 23 q2 = 13 e1 = 83 e2 = 61 e3 = 59 e4 = 37 e5 = 23 e6 = 29 g1 = 52 g2 = 38 g3 = 64 g4 = 10 g5 = 46 g6 = 13 x = 18	k1 = 9 k2 = 11 k3 = 13 k4 = 17 k5 = 19 k6 = 21	f243edc4, 7c967c92, f25afc53, 7c5146f5, 77bcaa00, 7ca59307, 63fa5bf7, 7c967c92, f26e09f7, 7c5146f5, 633f04b1, 63a5f993, 6f53a3c9, 7b0cc340, f2c4232a, c5f965bc, 77f0a063, f26e1b1b, 63b6ca5f, 7c9b7c92, f2a51712, f2c4232a, 6b1b2cf9, 6f30c900, 630c455f, 77524f07, 7bfafaa0, 6ba3cbf2, f22336f2, 6b090763, 636e1b1b, 7ca53343, 7c967c92, c57b3ffd, 63fdfabc, c581cb30, 7c207b51, 637d45f2, 7c967c92, 6f095913, 6b1b2cf9, 6bf7fab1, f2f05304, 6f53a3c9, 7c171897, 7b26131b, 772c470c, 7b825b00, 77cb5193

6 Conclusion

Encryption protects information from unwanted and unauthorized access. In this paper, the proposed combination of ElGamal, DSA, RSA, and AES algorithm using multiple keys proves a more secure and efficient way of cryptosystem encryption. The used of multiple keys will confuse the attackers from cracking the ciphered text. Along the process, the message has been twice encrypted by Asymmetric algorithm RSA and ElGamal which enhances the system of encryption. Through the use of AES, the ciphertext has been

hashed into hexadecimal.

REFERENCES

[1] M. Preetha and M. NIthaya, "A Study and Performance Analysis of RSA Algorithm," Int. J. Comput. Sci. Mob. Comput., vol. 2, no. 2320–088X, pp. 126–139, 2013.

[2] A. Sanada, Y. Nogami, K. Iokibe, and A. Khandaker, "Security Analysis of Raspberry Pi Against Side-Channel Attack with RSA Cryptography," pp. 287–288, 2017

[3] S. Dey, J. Nath, and A. Nath, "An Integrated Symmetric Key Cryptographic Method - Amalgamation of TTJSA Algorithm, Advanced Caesar Cipher Algorithm, Bit Rotation, and Reversal Method: SJA Algorithm," Int. J. Mod. Educ. Comput. Sci., vol. 4, no. 5, pp. 1–9, 2012.

[4] Malhotra M. A New Encryption Scheme Based on Enhanced RSA and ElGamal. Int J Emerg Technol Comput Appl Sci (IJETCAS). 2014;1:138–42.

[5] Arboleda ER. Secure and Fast Chaotic El Gamal Cryptosystem. Int J Eng Adv Technol. 2019;8(5):1693–9.

[6] Asaithambi N. A Study on Asymmetric Key Cryptography Algorithms. International Journal of Computer Science and Mobile Applications, Vol.3 Issue. 4, April- 2015, pg. 8-13

[7] Elminaam, Diaa Salama Abd, Abdual Kader, Hatem Mohamed & Hadhoud, Mohiy Mohamed. "Evaluating The Performance of Symmetric Encryption Algorithms". International Journal of Network Security, Vol.10, No.3, May 2010, pp. 216

[8] Thakur J, Kumar N. DES, AES, and Blowfish : Symmetric Key Cryptography Algorithms Simulation-Based Performance Analysis. International Journal of Emerging Technology and Advanced Engineering 2011;1(2):6–12.

[9] E. Zakasovskaya, A. Glushchenko, and V. Tarasov, "Construction of asymmetric cryptosystems using finite non-commutative algebraic groups," *2017 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM)*, St. Petersburg, 2017, pp. 1-5. doi: 10.1109/ICIEAM.2017.8076440

[10] Arboleda ER, Balaba JL, Espineli JCL. Chaotic Rivest-Shamir-Adlerman Algorithm with Data Encryption Standard Scheduling. Bull Electr Eng Informatics. 2017;6(3):219–27.

[11] Espalmado JMB, Arboleda ER. DARE Algorithm : A New Security Protocol by Integration of Different Cryptographic Techniques. Int J Electrical Comput Eng. 2017;7(2):1032–41.

[12] Mahajan P, Sachdeva A. A Study of Encryption Algorithms AES, DES and RSA for Security. Global Journal of Computer Science and Technology Network, Web & Security 2013;13 (15): 14-22

[13] Rivest RL, Shamir A, L. A method for obtaining digital signatures and public-key cryptosystems. Commun ACM. 1978;21(2):120-126. doi:10.1145/359340.359342

[14] Data Encryption and Decryption Using RSA Algorithm in a Network Environment. IJCSNS Int J Comput Sci Netw Secur. 2013; 13(7): 9–13.

[15] Shankar M. Hybrid Cryptographic Technique Using RSA. Int J Netw Secur Its Appl. 2014; 6(6): 39– 48.

[16] Singh G. A Study of Encryption Algorithms (RSA, DES, 3DES, and AES) for Information Security. Int J Comput Appl. 2013; 67(19): 975–8887. Available from: http://research.ijcaonline.org/volume67/number19/pxc3887224.pdf

[17] Chadha A. Dual-Layer Video Encryption using RSA Algorithm Dual-Layer Video Encryption using RSA Algorithm. Int J Adv Res Ideas Innov Technol. 2015; 116(August): 33–40.

[18] Karakra A, Alsadeh A. A-RSA: Augmented RSA. Proc 2016 SAI Comput Conf SAI 2016. 2016; (September): 1016–23.

[19] Ahmed JM, Ali ZM. The Enhancement of Computation Technique by Combining RSA and El-Gamal Cryptosystems. Proc 2011 Int Conf Electr Eng Informatics, ICEEI 2011. 2011; (July).

[20] R Pahal and V Kumar, "Efficient Implementation of AES," in International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue 7, July 2013,pp.290-295

[21] D Jayasinghe, J Fernando, R Herath, and R Ragel, "Remote Cache Timing Attack on Advanced Encryption Standard and Countermeasure," in IEEE International Conference on Information and Automation for Sustainability (ICIAFs),pp. 177-182, Dec. 2010

[22] New Comparative Study Between DES, 3DES, and AES within Nine Factors Hamdan.O. Alanazi, B.B. Zaidan, A. Zaidan, Hamid A. Jalab, M. Shabbir and Y. Al-Nabhani JOURNAL OF COMPUTING, VOLUME 2, ISSUE 3, MARCH 2010, ISSN 2151-9617

[23] Comparative Study of Symmetric and Asymmetric Cryptography Techniques by Ritu Tripathi, Sanjay Agrawal compares Symmetric and Asymmetric Cryptography Techniques using throughput, key length, tunability, speed, encryption ratio, and security attacks. IJCSMS International Journal of Computer Science and Management Studies, Vol. 11, Issue 03, Oct 2011 ISSN (Online): 2231-5268

[24] T. El Gamal, "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Trans. Inf. THEORY, vol. 31, no. 4, pp. 469–472, 1985.

[25] Efficient Implementation of AES, RituPahal, Vikaskumar, Volume 3, Issue 7, July 2013 ISSN: 2277 128X, © 2013, IJARCSSE

[26] Dellosa R, Fajardo A and Medina R. "A New Method of Location Estimation for Fingerprinting Localization Technique of Indoor Positioning System " ARPN Journal of Engineering and Applied Sciences 13 (48), 9427-9435