Hybrid Cryptography for Security Key Exchange through AES and Paillier

Pawan Kumar[a] and Vipin Saxena[b]
Department of Computer Science
Babasaheb Bhimrao Ambedkar University
Lucknow, (U.P.), 226025, INDIA
[a]*pawan0871@gmail.com and* [b]*profvipinsaxena@gmail.com*

ABSTRACT

The key is an important component for any cryptography algorithms. If the key is breached by the cyber attacker, then the cyber attacker encrypts the confidential message. In symmetric cryptographic, only one key is used for encryption and decryption, and it has weakness of symmetric cryptography. So, the problem can be solved by proposing Advanced Encryption Standard (AES) which is symmetric cryptography and Paillier system which is a asymmetric cryptography are used. The private key of AES is encrypted by Paillier cryptography. The message is encrypted by private key of AES cryptography and the private key of AES is encrypted by the public key of Paillier cryptography. The computed results are reported in the form of table and graph.

Keywords: Key Generation, Symmetric Cryptography, Asymmetric Cryptography, AES and Paillier System.

1. INTRODUCTION

In the recent days, scientific community is doing exhaustive research over the security of cloud servers, therefore, it is a developing topic of the research. The majority of businesses are switching away from conventional storage of information to cloud storage, which enables effective data access at all times and from any location around the globe. The cloud information is encrypted or decrypted by cryptography algorithms in keeping with approved standards. The cryptography protects the data stored from illegal access using encryption techniques. Hybrid cryptography is the idea that incorporates the combination of any two cryptography algorithms in between symmetric, asymmetric and hash cryptography. Data transport is taking advantage of unique sessions alongwith symmetrical encryption encourage using hybrid cryptography.

The data encryption standard (DES) was replaced by the symmetric algorithm known as AES, which was released by the National Institute of Standards and Technology (NIST) in

2001 and which is the most well-known symmetric key cryptography techniques, and uses an identical key to perform the encryption and decryption for confidential information. According to the size of the key, the AES is divided into three categories: AES-128, AES-192, and AES-256 in which the numbers 128, 192, and 256 denote the key's size as used in the cryptographic operation. A homomorphic public key system of cryptography is Paillier's system. The process of creating the public and private keys begins with the selection of two sufficiently large prime numbers, such as prn_1 and prn_2, that have an equal bit length. Based on these prime numbers, it generates public key and private key for encryption and decryption for confidential information. The present paper focuses on how to secure private key of AES cryptography with the help of Paillier cryptography.

2. RELATED WORK

Several authors have represented several hybrid cryptography algorithms which enhanced the security for information exchange across communication channels. This section discusses some of the important work related to the present work. Prakash and Rajput [1] have proposed hybrid cryptography using AES and Elliptic Curve Cryptography for wireless senser network. It generates keys by employing the ECC technique and encryption/decryption of information by applying AES. In the year 2019, Rong-Bing et al. [2] have proposed method with combination of Paillier algorithm, Horner's rule and hash function. By the use of Horner's rule then use of hash function then size of encryption and decryption were reduced and provide two-way authentication. Tsai et al. [3] have developed new AES algorithm with low power consumption for IoT devices. Low-Power Shift-Box, power gating, and control of power techniques are used in the Low-Power AES Data Encryption Architecture (LPADA), which lowers the amount of power used by AES when performing data encryption. Mohamed et al. [4] have discussed various types of hybrid cryptography for various domain and find that combination of AES and ECC hybrid cryptography very popular hybrid cryptography. Patil and Bansode [5] have proposed hybrid cryptography combinations of AES, Elliptic Curve Cryptography and SHA-256. It was discussed that the proposed method has better performance than existing algorithm for text and images data. It is providing more efficient encryption and decryption for textual information. Ghosh et al. [6] have discussed hybrid cryptography technique which secure, low-cost communication and emphasises on time consume during encryption and decryption. Ogunseyi and Bo [7] have discussed to reduce decryption time for Paillier cryptography and decryption complexity is O(log n) in relationship between size of input and time taken by decryption. In the year 2020,

Kumar and Saxena [8] have implemented a hybrid strategy in the manner of an algorithm to secure data with high integrity, speed, and secrecy. Bharathi et al. [9] have proposed a hybrid cryptography which is used AES, DES and RSA cryptography for encryption and decryption. Before transmission data is divided in to three parts and each part encrypted by AES, DES and RSA. The key is used to in the image by LSB stenography. Bermani et al. [10] have implemented method for data security strategies where data is encrypted using a hybrid cryptographic method made up of the Message-Digest algorithm (MD5), Blowfish, and Advanced Encryption Standard (AES). As a result, this kind of technology offers quick and reliable data encryption. By applying hex code operations to the encryption, the hybrid Paillier cryptosystem approach is applied to cut the number of bits from the encryption process-text [11]. In the year 2021, Alqarni [12] has discussed, to handle data created from various data sources or users in the cloud without first decrypting it. Such a strategy is used to safeguard data from assault and make encryption more difficult to preserve privacy. Seth et al. [13] have discussed, hybrid cryptography based on Blowfish and Paillier cryptography and analysed of security, attacked. Without compression, Paillier and Blowfish take around 2.5 times longer for encryption data than RSA-AES. Other important reference is Paillier cryptosystem[14].

3. METHODOLOGY

The proposed method, provides hybrid cryptography which is used through AES and Paillier crypto systems. Let us first describe the Paillier asymmetric cryptography whose algorithm is given below:

3.1 AES Cryptography

AES [3] cryptography is a symmetric cryptography which uses only one key for encryption and decryption both. AES cryptography has three key sizes of 128, 192 and 256 bits. At the time of encryption, each block is treated by AES as a 16-byte matrix in a column-major configuration 4 bytes x 4 bytes = 16 bytes = 128 bits. Each rounds takes four actions such that SubBytes, ShiftRows, MixColumns, and Add Round Key except and last round does not have MixColumns.

3.2 Paillier Cryptography

Initially Paillier cryptography takes two prime numbers of equal length of size and performs multiplication operation between prime numbers. Define $L(x) = x-1/n$ and calculate $prk = (LCM\ (prn_1-1,\ prn_2-1))$ for private key. In the following algorithm, LCM denotes Least Common Multiple and selects a random number positive number g between 1 *to* n^2. In the next step, calculate modular multiplicative inverse as $u = (L(g^{prk} \bmod n^2))^{-1}$. Public key and private key which are *pub_key (n,g), pub_key (n,g),* respectively. In the final step, encryption is done by public key and decryption is done by private key. The Paillier cryptography [14] describes below in brief:

Key Generation()

Two large prime number prn_1 and prn_2

To check $GCD(prn_1, prn_2(prn_1-1)(prn_2-1)) = 1$, if not, again take two prime number

Compute $n = prn_1 * prn_2$

Define $L(x) = x-1/n$

Compute $prk = (LCM\ (prn_1-1,\ prn_2-1))$

Select random integer number g, $g \in \mathbb{Z} * n$

Calculate $u = (L(g^{prk} \bmod n^2))^{-1}$

Public key $= pub\_key\ (n,g)$

Private key = $pri\_key\ (u, prk)$

Encryption()

m = Message , $0 <= m <= n$

Select random r, $0 < r < n$ *and* $r \in \mathbb{Z} * n$

Compute ciphertext $cipher\_text = g^m . r^n \bmod n^2$

Decryption()

Compute message $m = L(cipher\_text^{prk} \bmod n^2).u \bmod n$

3.3 Hybrid cryptography

In the following figure 1, RAM generates keys which are shared over the internet. SHYAM generates a key and encrypts the message and private key of AES. The cipher text of message and private key are shared over the internet. RAM receives both cipher texts, firstly decrypts private key of AES and the message is decrypted by AES.

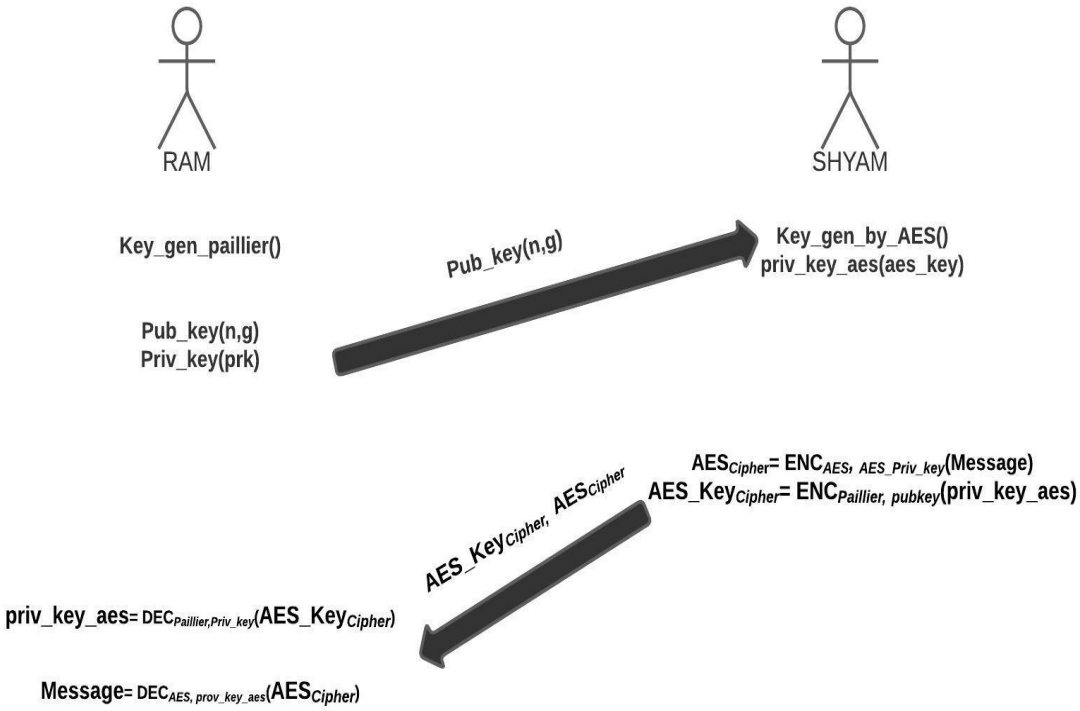

Figure 1. Proposed Method

The algorithm of proposed method is given below:

Step 1. consider two large prime number prn1 and prn2;

Step2. check if GCD(prn_1,prn_2(prn_1-1)(prn_2-1))= 1, then goto Step2. else Step1.;

*Step3. compute n =prn_1*prn_2;*

Step4. define function L(x) =x-1/n;

Step5. compute prk = (LCM (prn_1-1, prn_2-1));

*Step6. select random integer number g, g ∈ ℤ*n;*

Step7. calculate u= $(L(g^{prk} \bmod n^2))^{-1}$;

Step8. public key =pub_key (n,g);

Step9. private key = pri_key(u,prk);

Step10. share the public key over internet;

Step11. AES generate private key, priv_key_aes(aes_key)

Step12. AES_{Cipher}= $ENC_{AES,\ priv\_key\_aes}$ (Message)

Step13. AES_Key_{Cipher}= $ENC_{Paillier,\ pubkey}$(priv_key_aes)

Step14. aes_key = $DEC_{Paillier}$, priv_key (AES_Key_{Cipher})

Step15. message= $DEC_{AES,\ priv\_key\_aes}$ (AES_{Cipher})

In the proposed method, initially public and private keys are generated by Paillier cryptography. The public and private keys represent *pri_key(u,prk) and pri_key(u,prk)* respectively. The public key is shared by the receiver (RAM). The sender (SHYAM) is generated private key as *priv_key_aes(aes_key)* by AES cryptography and the message is encrypted by AES. The private key of AES is encrypted by the public key of Paillier cryptography and sends encrypted message as AES_{Cipher} and encrypted private key as AES_Key_{Cipher} of AES over insecure channel. At another end, the receiver (RAM) is decrypted private key of AES by private key of Paillier cryptography. The message is decrypted by private key of AES.

4. RESULTS AND DISCUSSION

AES cryptography has three versions which are based on size of key such that 128,192, and 256 bits. When the sender sends encrypted message which is encrypted by AES and at the same time, private key of AES is encrypted key by public key of Paillier cryptography. At the receiver side, the receiver firstly decrypts private key of AES by Paillier cryptography and then message is decrypted by AES cryptography. The experiment has completed in the environment of Windows 11 operating system with the help of Python programming language with 3.10.6 version.

Table 1. Comparison of Key Length for AES, Paillier and Hybrid Cryptography

AES (In Bits) [3]	Paillier (In Bits) [14]	Proposed Method (In Bits) (AES + Paillier)
128	128	512
128	256	1021
192	512	2047
256	1024	4093
256	2048	8186

The proposed method provides length of private key is higher and if AES cryptography is used 128 bits length of private key is needed while for Paillier cryptography, it is 128 bits length but when the present method (AES + Paillier System) is used then shared key becomes 512 bits length. The similar interpretation is given for the other bits length. The graph is representing the relationship between length of private key of AES, length of key of Paillier cryptography and length of key of the proposed method.

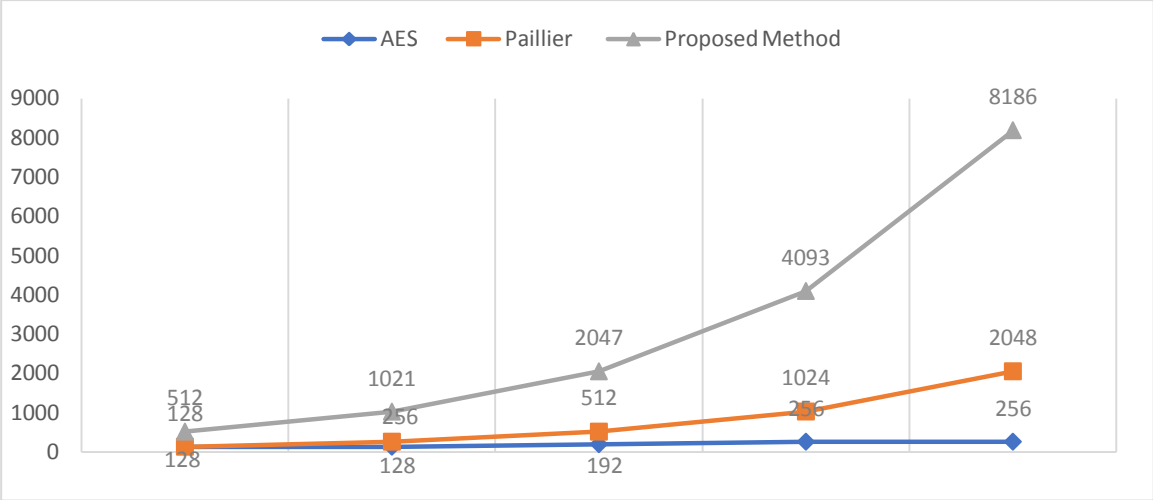

Figure 2. Comparison of the key lengths in bits for the AES cryptography, Paillier cryptography and Proposed Method

The figure 2 shows that the size of key of proposed method is increasing in the exponential manner in the respect of AES and Paillier cryptography. Blue color line represents AES, Orange color represents Paillier cryptography and gray color represents proposed method.

5. CONCLUSIONS AND FUTURE SCOPE

All the symmetric cryptography algorithms have use of one common weakness such that one key for encryption and decryption while the proposed method enhanced the AES cryptography with the help of Paillier cryptography and provides mutual authentication between sender and receiver. In the future, this proposed method can be enhanced for symmetric cryptography by the use of Paillier cryptography and cane be implemented for different types of data analysis for CPU utilization, security and compute throughput in different types of environments.

REFERENCES

1. Prakash, S. and Rajput, A. (2018), Hybrid Cryptography for Secure Data Communication in Wireless Sensor Networks, In *Ambient Communications and Computer Systems: RACCCS 2017*, (pp. 589-599), Springer Singapore, https://doi.org/10.1007/978-981-10-7386-1_50

2. Rong-Bing, W., Ya-Nan, L., Hong-Yan, X., Yong, F. and Yong-Gang, Z. (2019), Electronic Scoring Scheme Based on Real Paillier Encryption Algorithms. *IEEE Access*, *7*, 128043-128053, doi: 10.1109/ACCESS.2019.2939227.
3. Tsai, K. L., Leu, F. Y., You, I., Chang, S. W., Hu, S. J. and Park, H. (2019), Low-Power AES Data Encryption Architecture for a LoRaWAN. *IEEE Access*, Vol. *7*, pp. 146348-146357, doi: 10.1109/ACCESS.2019.2941972.
4. Mohamed, N. N., Yussoff, Y. M., Saleh, M. A. and Hashim, H. (2020), Hybrid Cryptographic Approach for Internet of Hybrid Cryptographic Approach for Internet of Things Applications: A Review, *Journal of Information and Communication Technology*, Vol. *19*, *No.*3, pp. 279-319, https://doi.org/10.32890/jict2020.19.3.1
5. Patil, P. and Bansode, R. (2020), Performance Evaluation of Hybrid Cryptography Algorithm for Secure Sharing of Text & Images, *International Research Journal of Engineering and Technology*, Vol.*7*, *No.*9, pp. 3773-3778, https://www.academia.edu/download/64789903/IRJET_V7I9664.pdf
6. Ghosh, S. K., Rana, S., Pansari, A., Hazra, J. Biswas, S. (2020, March), Hybrid Cryptography Algorithm for Secure and Low-Cost Communication. In *2020 International Conference on Computer Science, Engineering and Applications (ICCSEA)* ,(pp. 1-5). IEEE, doi: 10.1109/ICCSEA49143.2020.9132862.
7. Ogunseyi, T. B. and Bo, T. (2020, July), Fast Decryption Algorithm for Paillier Homomorphic Cryptosystem, In *2020 IEEE International Conference on Power, Intelligent Computing and Systems (ICPICS)* (pp. 803-806). IEEE, doi: 10.1109/ICPICS50287.2020.9202325.
8. Kumar, J. and Saxena, V. (2020), Hybridization of Cryptography for Security of Cloud Data, *International Journal of Future Generation Communication and Networking*, *13*(4), 4007-4014, http://sersc.org/journals/index.php/IJFGCN/article/view/34754/19261
9. Bharathi, P., Annam, G., Kandi, J. B., Duggana, V. K. and Anjali, T. (2021, July), Secure File Storage Using Hybrid Cryptography. In *2021 6th International Conference on Communication and Electronics Systems (ICCES)* (pp. 1-6). IEEE, doi: 10.1109/ICCES51350.2021.9489026.
10. Bermani, A. K., Murshedi, T. A. and Abod, Z. A. (2021), A Hybrid Cryptography Technique for Data Storage on Cloud Computing, *Journal of Discrete Mathematical Sciences and Cryptography*, Vol. *24*, *No.* 6, pp. 1613-1624, https://doi.org/10.1080/09720529.2020.1859799.

11. Kumar, J. and Saxena, V. (2021), Asymmetric Encryption Scheme to Protect Cloud Data Using Paillier-Cryptosystem, *International Journal of Applied Evolutionary Computation (IJAEC)*, Vol. *12, No.* 2, pp. 50-58, DOI: 10.4018/IJAEC.2021040104
12. Alqarni, A. A. (2021), A Secure Approach for Data Integration in Cloud Using Paillier Homomorphic Encryption, *Journal of Basic and Applied Sciences*, Vol. *5, No.*2, pp. 15-21.
13. Seth, B., Dalal, S., Le, D. N., Jaglan, V., Dahiya, N., Agrawal, A., ... & Verma, K. D. (2021), Secure Cloud Data Storage System Using Hybrid Paillier–Blowfish Algorithm, *CMC- Computers Materials & Continua*, Vol. *67, No.*1, pp. 779-798, https://www.academia.edu/download/88073731/pdf.pdf
14. Paillier, P. (1999). Public-Key Cryptosystems Based on Composite Degree Residuosity Classes, *In proceeding, International Conference on the Theory and Application of Cryptographic Techniques Prague, Czech Republic*, pp. 223-238, Springer Berlin Heidelberg.