HYBRID ENCRYPTION ALGORITHM BASED ON SYMMETRIC AND ASYMMETRIC CIPHERS

NOOR AMIRA ZURAINI BINTI MOHD ZULKIMI

A project report submitted in partial fulfilment of the
requirements for the award of the degree of
Master of Engineering (Computer and Microelectronic Systems)

School of Electrical Engineering
Faculty of Engineering
Universiti Teknologi Malaysia

JULY 2021

DEDICATION

This project report is dedicated to my family and friends who has been my source of strength and inspiration when I thought of giving up. And, to those who has been contributed directly or indirectly during this work.

ACKNOWLEDGEMENT

In the name of Allah S.W.T., the most Beneficent and Merciful, Praise be to Allah, the Lord of the worlds who has giving the strength and persistence to complete the research and thesis of final year project. First and foremost, my deepest gratitude to research's supervisor, Dr Shahidatul Sadiah Binti Abdul Manan for the continuous support for my final year project, for her patience, motivation, and great knowledge of cryptographic, and her guidance helped me in all the time of research and writing of the thesis.

Besides, my earnest appreciation to the rest of Intel colleagues the valuable information, and strong support and assistance through various stages.

My sincere thanks also goes to my parents and family who always give support and encouragement to complete the final year project in Universiti Teknologi Malaysia and also to my friends who have involved directly and indirectly in helping me to complete the final year project.

ABSTRACT

In trusted computing architecture, security is one of crucial aspects to protect the design against hardware or software attacks. The symmetric encryption method works great for fast encryption of large data. Still, it doesn't provide identity verification. Meanwhile, the asymmetric encryption method makes sure that the data is accessed by authorized recipient with public private key pair. However, this verification makes the encryption process slow when implemented at scale. Work here intends to develop and analyse the hybrid algorithms. In this study, Advanced Encryption Standard (AES) with fixed 16 bytes of block and 128-bit key length is chosen as symmetric cryptography algorithm. Meanwhile, Ron Rivest, Adi Shamir, and Leonard Adleman (RSA) with 1024, 2048 and 3072-bits key length and Elliptic Curve Cryptography (ECC) with 192, 224 and 256-bits key length with two different curves: Brain pool and NIST SECP are chosen as asymmetric algorithms. These two asymmetric algorithms are compared to determine which algorithms can produce a best performance with the combination of symmetric algorithm. Cryptographic algorithms are developed and written using Python3.8. The performance of application is evaluated using computational time for key generation, encryption and decryption phases with different input data set and key lengths. Overall, hybrid ECC has better performance in key generation phase due to its smaller key sizes and hybrid RSA has better performance in encryption and decryption due to its less complexity of algorithm. From findings, it can be summarized that AES-256-GCM + ECC-secp192r1 is the best combination of hybrid algorithm.

ABSTRAK

Dalam seni bina pengkomputeran yang dipercayai, keselamatan adalah salah satu aspek penting untuk melindungi reka bentuk daripada serangan perkakasan atau perisian. Kaedah penyulitan simetri berfungsi dengan baik untuk penyulitan cepat data besar. Namun, ia tidak memberikan pengesahan identiti. Sementara itu, kaedah penyulitan asimetri memastikan bahawa data diakses oleh penerima yang diberi kuasa dengan pasangan kunci swasta. Walau bagaimanapun, pengesahan ini menjadikan proses enkripsi menjadi perlahan ketika dilaksanakan secara besar-besaran. Kerja di sini bermaksud untuk mengembangkan dan menganalisis algoritma hibrid. Dalam kajian ini, Advanced Encryption Standard (AES) dengan tetap 16 bait blok dan panjang kunci 128-bit dipilih sebagai algoritma kriptografi simetri. Sementara itu, Ron Rivest, Adi Shamir, dan Leonard Adleman (RSA) dengan panjang kunci 1024, 2048 dan 3072-bit dan Elliptic Curve Cryptography (ECC) dengan panjang kunci 192, 224 dan 256-bit dengan dua lengkung yang berbeza: Kolam otak dan NIST SECP dipilih sebagai algoritma asimetri. Kedua-dua algoritma asimetri ini dibandingkan untuk menentukan algoritma mana yang dapat menghasilkan prestasi terbaik dengan gabungan algoritma simetri. Algoritma kriptografi dikembangkan dan ditulis menggunakan Python3.8. Prestasi aplikasi dinilai menggunakan masa komputasi untuk penjanaan kunci, fasa penyulitan dan penyahsulitan dengan set data input dan panjang kunci yang berbeza. Secara keseluruhan, ECC hibrid mempunyai prestasi yang lebih baik dalam fasa penjanaan kunci kerana saiz kunci yang lebih kecil dan RSA hibrid mempunyai prestasi yang lebih baik dalam penyulitan dan penyahsulitan kerana algoritma yang kurang kompleks. Dari hasil penemuan, dapat dirumuskan bahawa AES-256-GCM + ECC-secp192r1 adalah gabungan algoritma hibrid terbaik.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AES	-	Advanced Encryption Standard
CBC	-	Cipher Block Chaining
CTR	-	Counter
DES	-	Data Encryption Standard
ECC	-	Elliptic Curve Cryptography
ECDH	-	Elliptic-curve Diffie–Hellman
GCM	-	Galois/Counter Mode
MAC	-	Message Authentication Mode
NIST	-	National Institute Standards and Technology
PKBD	-	Password-Based Key Derivation
RNG	-	Random Number Generator
RC4	-	Rivest Cipher 4
RSA	-	Rivest, Shamir and Adleman

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Research Background

Cryptography is the practice of secure communication to protect the transfer information that known only to its sender and receiver in such a way that any third-party intercepting through the communication channel cannot extract the data. Basically, cryptographic algorithm works in combination of alphabets and numbers which implements to encrypt the plain text to cipher text. The strength of algorithm and the secrecy of the key are significant to determine the security of the encrypted data. Figure 1.1 shows the basic components of cryptosystem process.

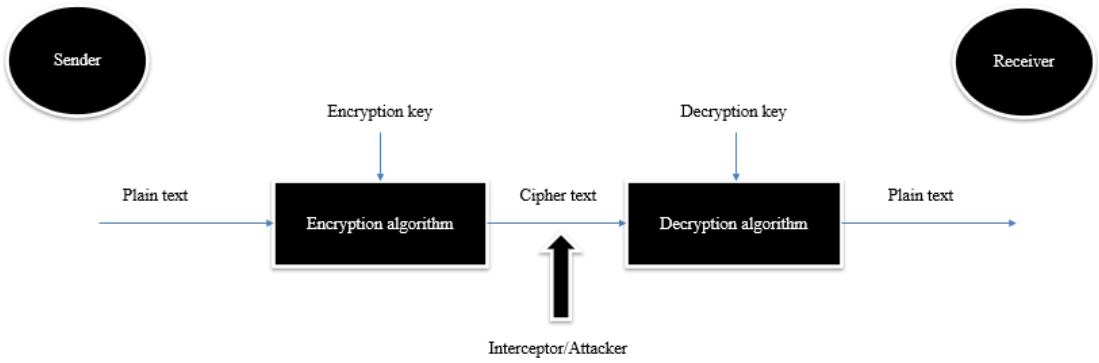


Figure 1.1: Basic components of cryptosystem

The basic components of cryptosystem are:

i. Plain text – Data to be protected during transmission.

ii. Encryption key – Combination of alphabets and words to form unique value which known to sender. The sender inputs the encryption key into the encryption algorithm along with the plaintext to compute the ciphertext.

iii. Encryption algorithm – Mathematical process which consists of cryptographic algorithm that takes plaintext and an encryption key as input and produces a ciphertext.

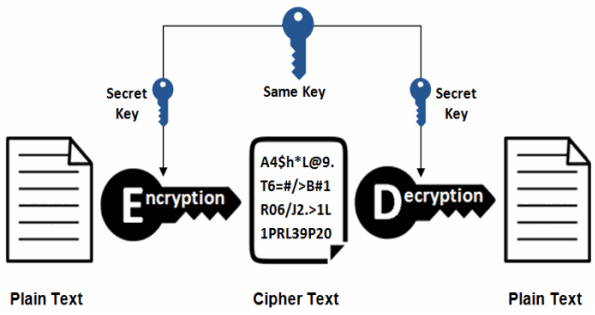
iv. Cipher text – Scrambled version of the plaintext. The ciphertext is not guarded can be intercepted by anyone who has access to the communication channel.

v. Decryption key – Combination of alphabets and words to form unique value which known to receiver. The receiver inputs the decryption key into the decryption algorithm along with the ciphertext to compute the plaintext.

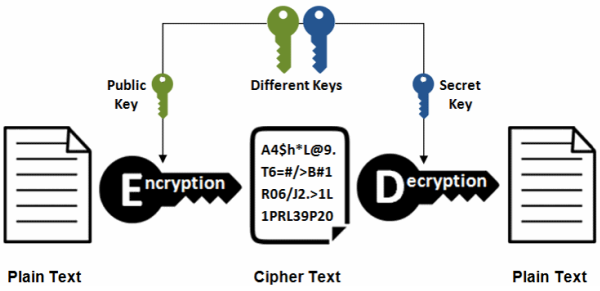
vi. Decryption algorithm – Mathematical process which consists of cryptographic algorithm that takes ciphertext and a decryption key as input and outputs a plain text.

vii. Interceptor – An unauthorized party who attempts to determine the content of plain text.

There are two types of cryptography: 1) symmetric cryptography, and 2) asymmetric cryptography. If the key is identical for encryption and decryption, this mechanism is known as symmetric cryptography as illustrated in Figure 1.2(a). Symmetric cryptography is a best-known scheme with the simplest kind of encryption that involves only one shared key to encrypt and decrypt data. Both sender and receiver have the knowledge of the shared key used in encryption and decryption. This scheme presents the benefit of being fast and often used in cryptographic. However, the drawback of this scheme is that all parties involved must exchange the shared key used to encrypt the data before they can decrypt it. Example of symmetric cryptography are Rivest Cipher 4 (RC4), Advanced Encryption Standard (AES), Data Encryption Standard (DES), etc.



(a)



(b)

Figure 1.2: Types of cryptography (a) Symmetric (b) Asymmetric [25]

On the other hand, if the key is different for encryption and decryption, this mechanism is known as asymmetric cryptography as illustrated in Figure 1.2(b). For security purpose, the encryption key is made freely available to anyone and known as a public key, and the decryption key remains as a private key so that the receiver only knows and has ability to decrypt the data. This scheme offers the benefit of more scalable and high level of security as compared to symmetric cryptography because the private key is not being shared and kept as a secret. However, the drawback of this scheme is that the computation of algorithm becomes slower with its complicated process than symmetric cryptography. Example of asymmetric cryptography are Rivest, Shamir and Adleman (RSA), El Gamal, Elliptic Curve Cryptography (ECC), etc.

AES also known as Rijndael is a family of symmetric block cipher algorithms and proposed by Vincent Rijmen and John Daemon in 2001. AES algorithm is a popular symmetric algorithm because of easy implementation, fast encryption, and decryption times. Based on the previous research, AES found to be at least size time faster than triple DES and today, there is no significant proof of attacks have been recorded towards AES. Ideally, AES has three different key lengths that are 128, 192 and 256-bits which determine the security level. Key length of 256-bits is recognized as mostly secure and standard use in industry. Figure 1.3 shows the structure of AES. It begins with key expansion and go through five main steps in each round which have its own purposes. In general, 128, 192 and 256-bits key undergo 10, 12 and 14 rounds for encryption and decryption, respectively.

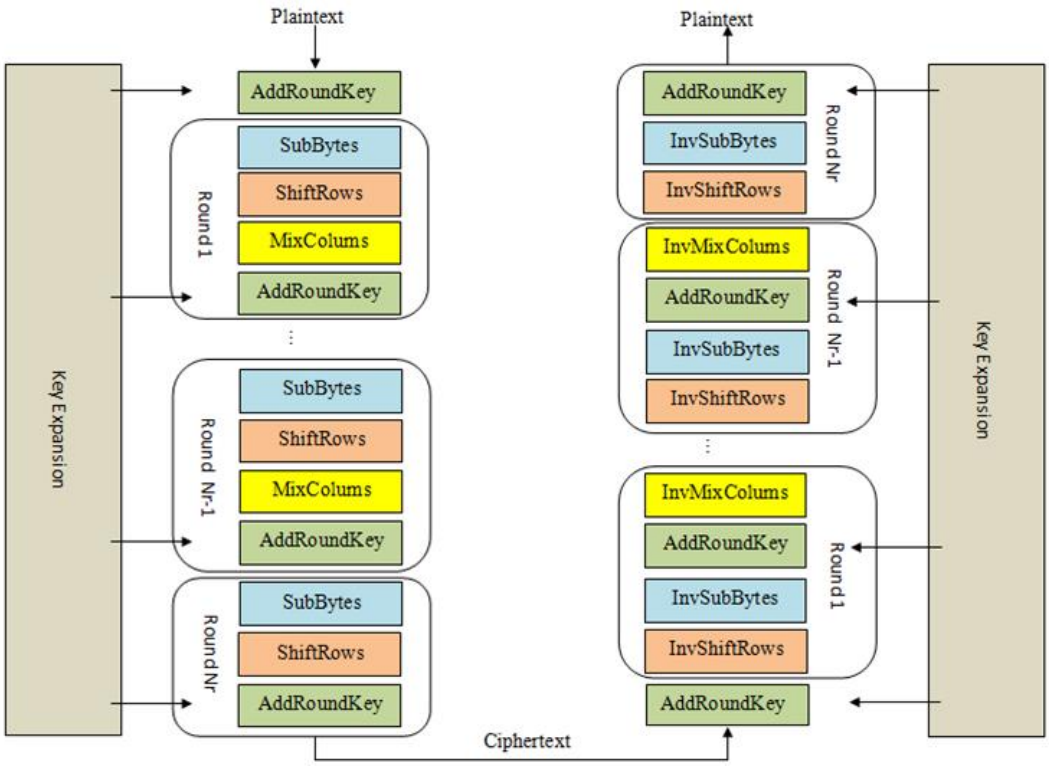


Figure 1.3: Structure of AES [26]

The plain text is divided into blocks of 128-bits before the key expansion step. Key expansion requires taking the initial key to produce a series of other keys for each round of the encryption process using computation in algorithm. Each round should not have same key otherwise the attacker can easily crack the AES. In add round key step, the initial key is added to the block of plain text using XOR cipher. Byte substitution adjusts the data to a non-linear type to create confusion to the information, and advantageous for cipher text and original plain text to be kept secret. Next, shift row or known as diffusion process is introduced to transpose the data. By shifting the rows, the data is moved from its original position horizontally, and increase the complexity of data. Mix columns step has similar implementation as shift row where it alters the data vertically. Finally, the last key generated in mixed columns will be added with the initial key.

RSA is invented in 1977 and named after its authors which are Ron Rivest, Adi Shamir, and Leonard Adleman. RSA algorithm is a popular asymmetric algorithm its

capability to derive security level from the difficulty of factoring large integers which are the product of two large prime numbers. The standard RSA key lengths are 1024, 2048, 3072, 7680, and 15360-bits. 2048-bits is the common key length in practical use. The trade of between security and speed of RSA is the longer keys provide higher security however it consumes more computational time. Figure 1.4 shows the structure of RSA. It is based on the mathematical of modular exponentiations. RSA flow begins with key generation using two random prime numbers to generate public and private key pair, then generated key pair will be stored in memory and finally perform the encryption and decryption process.

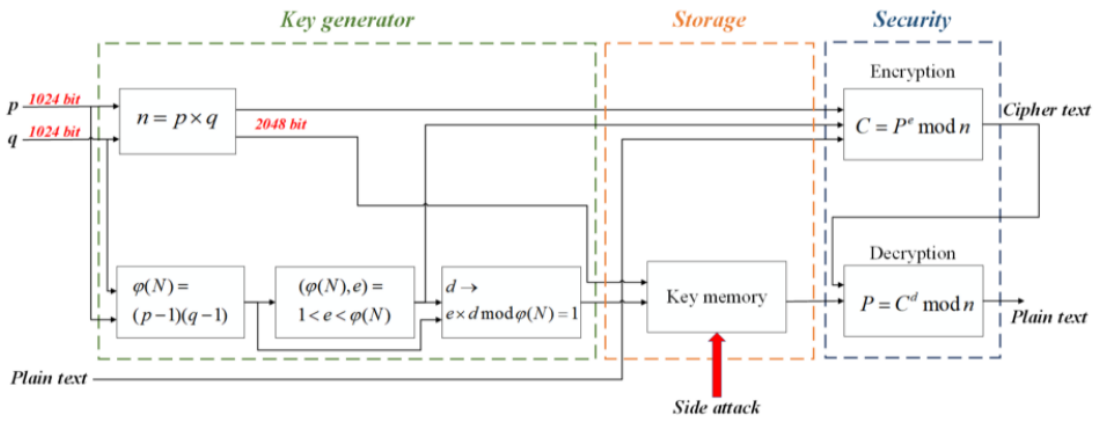


Figure 1.4: Structure of RSA [27]

ECC is discovered in 1985 by Victor Miller of IBM and Neil Koblitz. ECC is recognized as modern successor of the RSA cryptography because it uses smaller keys and signatures than RSA algorithm with the same security level and provides very fast encryption and decryption. For example, 256-bits ECC key provides about the same security as a 3072-bits RSA key. Figure 1.5 shows the general elliptical curve of ECC. ECC uses the projective property of elliptical curves to select random points in ECC key generation. It has a great trapdoor function because it is not easy to determine the curve parameters even the attacker knows the starting and ending points. To point out, this is the best mechanism introduced in ECC to protect the private key. The ECC standard key lengths are 192, 224, 256, 384 and 512-bits.

REFERENCES

[1] E. Chiranth, “Implementation of RSA Cryptosystem Using Verilog,” in international Journal for …, 2011, vol. 2, no. 5, pp. 1–7, [Online]. Available: http://www.ijser.org/researchpaper%5CImplementation_of_RSA_Cryptosystem_Using_Verilog.pdf.

[2] H. Anada, T. Yasuda, J. Kawamoto, J. Weng, and K. Sakurai, “RSA public keys with inside structure: Proofs of key generation and identities for web-of-trust,” J. Inf. Secur. Appl., vol. 45, pp. 10–19, 2019, doi: 10.1016/j.jisa.2018.12.006.

[3] G. Ramakrishnan, “Design and Verification of an RSA Encryption Core,” 2019.

[4] R. Shams, F. H. Khan, and M. Umair, “Cryptosystem an Implementation of RSA Using Verilog,” Int. J. Comput. Networks Commun. Secur., vol. 1, no. 3, pp. 102–109, 2013, [Online]. Available: www.ijcncs.org.

[5] B. C. Gillmore, “RSA in Hardware,” 2010.

[6] C. Rebeiro and D. Mukhopadhyay, “HIGH PERFORMANCE ELLIPTIC CURVE CRYPTO-PROCESSOR FOR FPGA PLATFORMS.”

[7] M. Gharib, Z. Moradlou, M. A. Doostari, and A. Movaghar, “Fully distributed ECC-based key management for mobile ad hoc networks,” in Computer Networks, 2017, vol. 113, pp. 269–283, doi: 10.1016/j.comnet.2016.12.017.

[8] M. Jaiswal and K. Lata, “Hardware Implementation of Text Encryption using Elliptic Curve Cryptography over 192 bit Prime Field,” in 2018 International Conference on Advances in Computing, Communications and Informatics, ICACCI 2018, 2018, pp. 343–349, doi: 10.1109/ICACCI.2018.8554410.

[9] G. R. K. Prasad, T. Vivek, B. Phani Rohith, and Y. Yashwanth, “Verilog implementation on cryptography encryption and decryption of 8 bit data using ECC algorithm,” in Journal of Advanced Research in Dynamical and Control Systems, 2017, vol. 9, no. Special Issue 14, pp. 2711–2719.

[10] A. Shantha, J. Renita, and N. Edna Elizabeth, “Analysis and implementation of ECC algorithm in lightweight device,” in Proceedings of the 2019 IEEE

International Conference on Communication and Signal Processing, ICCSP 2019, 2019, pp. 305–309, doi: 10.1109/ICCSP.2019.8697990.

[11] C. A. Lara-Nino, A. Diaz-Perez, and M. Morales-Sandoval, “Lightweight elliptic curve cryptography accelerator for internet of things applications,” in Ad Hoc Networks, 2020, vol. 103, p. 102159, doi: 10.1016/j.adhoc.2020.102159.

[12] N. P. Kumar and C. Shirisha, “An area-efficient ECC architecture over GF(2m) for resource-constrained applications,” in AEU - International Journal of Electronics and Communications, 2020, vol. 125, no. March, doi: 10.1016/j.aeue.2020.153383.

[13] V. B. Kute, P. R. Paradhi, and G. R. Bamnote, “A software comparison of RSA and ECC,” Int. J. Comput. Sci. Appl., vol. 2, no. 1, pp. 61–65, 2009, [Online]. Available: http://www.researchpublications.org/IJCSA/issue4/2009-IJCSA-02-01-15.pdf.

[14] M. Bafandehkar, S. M. Yasin, R. Mahmod, and Z. M. Hanapi, “Comparison of ECC and RSA algorithm in resource constrained devices,” 2013 Int. Conf. IT Converg. Secur. ICITCS 2013, no. April 2016, pp. 10–13, 2013, doi: 10.1109/ICITCS.2013.6717816.

[15] R. Sinha, H. K. Srivastava, and S. Gupta, “Performance Based Comparison Study of RSA and Elliptic Curve Cryptography,” Int. J. Sci. Eng., vol. 4, no. 5, pp. 720–725, 2013.

[16] R. Bhadada and A. Sharma, “Montgomery implantation of ECC over RSA on FPGA for public key cryptography application,” Proc. 2014 2nd Int. Conf. “Emerging Technol. Trends Electron. Commun. Networking”, ET2ECN 2014, no. 1977, pp. 0–4, 2015, doi: 10.1109/ET2ECN.2014.7044973.

[17] A. Thomas and E. M. Manuel, “Embedment of Montgomery Algorithm on Elliptic Curve Cryptography over RSA Public Key Cryptography,” Procedia Technol., vol. 24, pp. 911–917, 2016, doi: 10.1016/j.protcy.2016.05.179.

[18] M. Alam, “A Comparative Study of RSA and ECC and Implementation of ECC on Embedded Systems,” Int. J. Innov. Res. Adv. Eng., vol. 3, no. 03, pp. 86–93, 2016, [Online]. Available: http://www.ijirae.com/volumes/Vol3/iss3/15.MRAE10096.pdf.

[19] A. Kardi, R. Zagrouba, and M. Alqahtani, “Performance Evaluation of RSA and Elliptic Curve Cryptography in Wireless Sensor Networks,” 21st Saudi

Comput. Soc. Natl. Comput. Conf. NCC 2018, vol. 65537, pp. 302–306, 2018, doi: 10.1109/NCG.2018.8592963.

[20] R. Yadav, S. Srinivasan, and S. Gupta, “Security analysis of RSA and ECC in Mobile Wimax,” Int. Conf. Signal Process. Commun. Power Embed. Syst. SCOPES 2016 - Proc., pp. 1725–1729, 2017, doi: 10.1109/SCOPES.2016.7955738.

[21] D. Mahto and D. K. Yadav, “RSA and ECC: A comparative analysis,” Int. J. Appl. Eng. Res., vol. 12, no. 19, pp. 9053–9061, 2017.

[21] C. Varma, “A Study of the ECC, RSA and the Diffie-Hellman Algorithms in Network Security,” Proc. 2018 Int. Conf. Curr. Trends Towar. Converging Technol. ICCTCT 2018, pp. 2018–2021, 2018, doi: 10.1109/ICCTCT.2018.8551161.

[23] D. Mahto and D. Kumar Yadav, “Performance Analysis of RSA and Elliptic Curve Cryptography,” Int. J. Netw. Secur., vol. 20, no. 4, pp. 625–635, 2018, doi: 10.6633/IJNS.201807.

[24] F. Mallouli, A. Hellal, N. Sharief Saeed, and F. Abdulraheem Alzahrani, “A Survey on Cryptography: Comparative Study between RSA vs ECC Algorithms, and RSA vs El-Gamal Algorithms,” Proc. - 6th IEEE Int. Conf. Cyber Secur. Cloud Comput. CSCloud 2019 5th IEEE Int. Conf. Edge Comput. Scalable Cloud, EdgeCom 2019, pp. 173–176, 2019, doi: 10.1109/CSCloud/EdgeCom.2019.00022.

[25] G. Maden, F. Sonmez, M. Zontul, and O. Kaynar, "Comparison of Symmetric and Asymmetric Cryptography Algorithms and A Better Solution: Hybrid Algorithm, " International Congress of Science, Education and Technology Research, pp.19, 2018.

[26] The Advanced Encryption Standard (AES) Algorithm, March. 2021 [Online]. Available: https://www.commonlounge.com/discussion/e32fdd267aaa4240a4464723bc74d0a5

[27] H. Yu and Y. Kim, "New RSA Encryption Mechanism Using One-Time Encryption Keys and Unpredictable Bio-Signal for Wireless Communication Devices", Electronics, vol. 9, no. 2, p. 246, 2020. Available: 10.3390/electronics9020246.

[28] N. Francis and T. Monoth, An Analysis of Hybrid Cryptographic Approaches for Information Security, International Journal of Applied Engineering Research, Vol. 13, No. 3, pp. 124-127. 2018

[29] E. Ramaraj, S. Karthikeyan & M. Hemalatha, A design of security protocol using hybrid encryption technique, International Journal of the Computer, the Internet and Management, Vol. 17, No. 1, pp. 78-86. 2009.

[30] N. Garg & P. Yadav, Comparison of Asymmetric Algorithms in Cryptography. Neha Garg et al, International Journal of Computer Science and Mobile Computing A Monthly Journal of Computer Science and Information Technology. www.ijcsmc.com ISSN 2320–088X IJCSMC, Vol. 3, Issue. 4, April 2014, pg.1190 – 1196

[31] P. K. Arya, M. S. Aswal & V. Kumar, Comparative Study of Asymmetric Key Cryptographic Algorithms. International Journal of Computer Science & Communication Networks,Vol 5(1),17-21. ISSN:2249-5789 2015

[32] Cipher Block Modes, June. 2021 [Online]. Available: https://cryptobook.nakov.com/symmetric-key-ciphers/cipher-block-modes

[33] SafeCurves: Choosing safe curves for elliptic-curve cryptography, June 2021. [Online]. Available: https://safecurves.cr.yp.to/

[34] Welcome to PyCryptodome's documentation, June 2021. [Online] Available: https://pycryptodome.readthedocs.io/en/latest/index.html