International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

A Juxtapose of Symmetric Block Cipher Algorithms to Control, Analyse and Augment Efficiency of IoT Enabled Devices

K. Savima [1], **Dr. M.V.Srinath** [2]

Submitted: 26/01/2024 **Revised**: 04/03/2024 **Accepted**: 12/03/2024

Abstract: The neoteric times have contrived the utilization of automated functionalities and Internet of Things (IoT) enabled devices for quotidian working. With the increase in engaging physical entities with the virtual technologies, and the collaborative conjunction that has augmented the quality of life, it is quite natural for individuals to implement a paradigm shift in terms of upgrading to IoT enabled entities. Nonetheless, while it creates facile resolutions, the security of devices and data are under enormous risk. Hacking and data pilferage are most often evinced due to the incapability of IoT devices to sufficiently manage storage, integration, communication and the computational complexity that persists between the devices. Block cipher cryptography is a swift-developing domain that enhances the integrity of resources and mitigates intricacy in integrating the diverse operations, along with enhancing the security of functions that is usually carelessly neglected by the conventional processing devices. The previous studies relevant to this field of interest have incorporated the use of hardware services and the functionality of block ciphers to analyse their compatibility with IoT devices. However, this paper focuses to elaborate on a comparative algorithmic implementation of block ciphers to render a scrutinization from three algorithmic processes that dissect the efficiency of security. Rivest-Shamir-Adleman (RSA) algorithm with asymmetric cryptography, and an enhanced key generation of multiples of 256 is incorporated with base 64 encryption and decryption. The processing time in relevance to the encryption methods, and the effective utilization of Pseudorandom Permutational (PRP) technique that further complements the resilience of IoT devices is meticulously employed in this study. The cryptanalysis performed with Reverse, Caesar cipher and columnar- transpositional encoding mechanisms aid to analyse the efficacy of encryption and decryption to supplement competent protection of IoT devices. The simulations for the proposed study is implemented in Python, and the results are successfully procured.

Keywords: *Block Cipher, Encryption, Decryption, Internet of Things (IoT), Light-weight cryptography, Pseudorandom permutation, Reverse cipher, Caesar Cipher, Columnar-Transpositional encoding.*

1. Introduction

Technological developments and integrated systems have created a quintessential constant demand for intelligent systems and disruptive technologies. Internet of Things (IoT) is a domain that is soaring in success, due to its connectivity with the tangible and intangible entities. The sensors and the frequency spectrum [1] associated with the technology largely enables data to be transmitted through a wireless medium. Most frequently, this interaction between the components of the IoT process can employ varying platforms with different operating systems, and variable rubrics for privacy standardization, thereby making IoT devices to render fluctuating results leading to compromised functionality [2]. Block cipher technology hold the power to perform encryption on a chunk of data, rather than specific pieces as in a stream cipher technique [14]. The advantages of entailing a block cipher technology are multifarious, and are used extensively in the protection of IoT enabled devices. The fundamental motive to utilize block ciphers is the idiosyncrasy through which each chunk of data can be encrypted, thereby breaking the monotony of homogeneity in the encrypted blocks. The prominence of block cipher lies with its utilization of deterministic algorithms along with effective key generation that aids in encrypting a block of data [9], [14]. However, without the utilization of pseudorandom permutation [21], the resilience of block encryption mechanism fails in augmenting the security and efficacy of the process. There are various modes of operation [10], [20] in a block cipher algorithm, and the below framework as shown in figure 1 provides a general overview of the encryption and decryption process using the cipher block chaining method.

The other modes of operation other than the above illustrated cipher block chaining method are Cipher Feedback (CFB) and Galois/Counter Mode (GCM) [20]. The most common block cipher algorithm is the Advanced Encryption Standard (AES) that effectuates security through varying key lengths to encrypt data [17]. The Data Encryption Standard (DES) is another potent algorithm that is popular. However, the higher significance in utilizing AES over DES is the enhanced security that the former renders through the mitigation of data leakage in the key

[1] *Research Scholar, S.T.E.T Women's College (Autonomous), (Affiliated to Bharathidasan University, Tiruchirappalli), Sundarakkottai, Mannargudi - 614016, Thiruvarur Dt., Tamil Nadu, India Email: savimastet@gmail.com, Mobile No.9843221984*
[2] *Research Supervisor, S.T.E.T Women's College (Autonomous), (Affiliated to Bharathidasan University, Tiruchirappalli), Sundarakkottai, Mannargudi - 614016, Thiruvarur Dt., Tamil Nadu, India Email: sri_induja@rediffmail.com Mobile No. 9710944476*
ORCID ID : 0000-3343-7165-777X
** Corresponding Author Email: author@email.com*

generation process through their varying key lengths of 128, 192 and 256 [20]. A general architecture of AES block cipher technique used on a block of data is pictorially represented as below in figure 2.

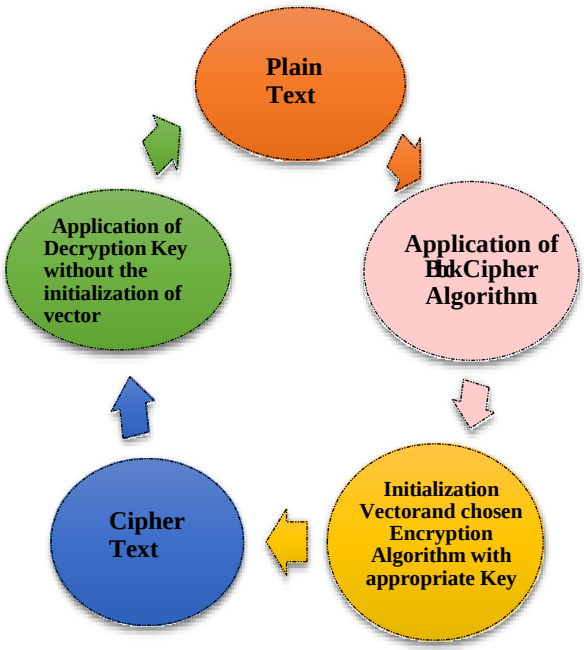

Fig. 1. Encryption and Decryption through Cipher Block Chaining – A General Overview

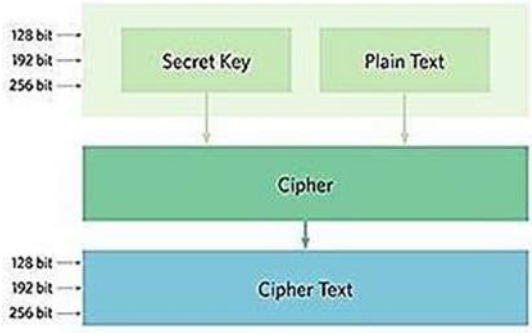

Fig. 2. Relationship between secret key, plaintext, cipher and ciphertext in a AES framework

The operation of AES is effectuated through a series of phases, and a iterative process of several rounds depending on the key that the algorithm utilizes. This variation in the number of rounds and the key length is a pivotal aspect for choosing AES in every cryptographic implementation. However, the AES follows a symmetric approach, where the generated key is the same for both the sender and receiver to encrypt and decrypt the data respectively. This can therefore cause key exhaustion [17], and is thus remedied by utilizing an asymmetric approach such as the Rivest-Shamir-Adleman (RSA) algorithm that divulges into the generation of two different keys. This study thus elaborates the incorporation of the commingled symmetric-asymmetric cryptographic methods used with Base64 encoding mechanism [15], along with delineating the different block ciphers inorder to cognize the performance efficiency and processing time that they may take. The paper is organized into the subsequent section detailing the use of symmetric and asymmetric cryptography in relevance with the different algorithms, with section III describing the proposed methodology, and sections IV and V explicating the results obtained, and the compendium of the work implemented, along with future work that can be effectuated respectively.

2. Symmetric Vs Asymmetric Cryptography

The distinction in comprehending the heterogeneity of cryptography using the symmetric and asymmetric methods aids a researcher to explicitly cognize the appropriate technique to be used for the data at hand. This section details the pros and cons of utilizing the cryptographic methods, along with the solution that the proposed approach entails inorder to incorporate the right technique of key generation and algorithmic approach.

The symmetric cryptographic algorithms utilize a common key for their process of encryption and decryption, and therefore the same key is shared between the two entities of the cryptographic process [12]. Since this key is known only to the encryptor and the decryptor, the security of the message was vouchsafed. The key can be anything that can be shared between two entities, or could be a potential random generation of passcode that is usually executed as in a OTP generation of instant randomization of passcodes [12]. This Random Number Generator (RNG) [22] are most frequently used by financial institutions and other large corporates inorder to entail dynamic passcode generation, instead of the static passcode that is vulnerable to breaches. Prominent bifurcation of this symmetric form of cryptography is imbibed by the block cipher algorithms and stream cipher algorithms [11]. AES, DES, Rivest Cipher (RC) - 4,5,6, Blowfish and International Data Encryption algorithm (IDEA) are some of the distinct algorithms implemented in most indagations [11], [14]. The pros of this cryptographic technique lies with its swift implementation. Nonetheless, the cons of this approach lie with their ability to manage the key, and can be an exhaustive process to work when the database is large. Thus, triggering the problem of key devitalization, which cannot be rolled back to the previous phase of implementation to keep it alive, thereby consequently leading to time-consumption and inefficiency.

The incorporation of asymmetric cryptography entails the utilization of embedded metadata [12] that provides unambiguous access to the lifecycle of a data, the attributes involved and the access controls to perform relevant encryption and decryption. This method also provides the user with two different keys such as the public and the private key to overcome the challenges of key devitalization and data attribution. The RSA algorithm [6] is one of the

prominent forerunners of this method of cryptography. This study entails a combinational approach of implementing the symmetric and asymmetric cryptographic methods with AES and RSA algorithms [6] that aid in balancing out on the pros and cons of each of the cryptographic processes, while ensuring to render an explicit security optimization for the algorithmic ciphers that follow.

3. Proposed Methodology

The indagation assimilated entails the elaboration of AES with the RSA algorithm, and the performance of cryptography effectuated through different ciphers such as reverse, Caesar and columnar- transpositional techniques. The encoding through base64 through the python inbuilt libraires that further accentuated the efficiency of the encryption and decryption techniques [7], [8]. The proposed algorithm thus takes into account two 128 keys for encrypting the data, and generates a 64-bit key dynamically [16]. The following diagram as shown in figure 3 depicts the basic flow of the system.

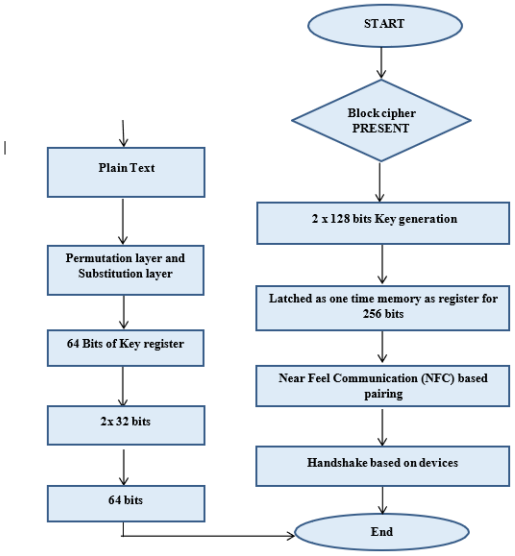

Fig. 3. Basic Flow Diagram

The study is phased out into different phases with the ciphering of data performed using three methods such as

1. Reverse cipher
2. Caesar cipher
3. Columnar transpositional cipher.

The reverse cipher [19] as the name indicates performs an inverse of the data to enable the process of encryption and decryption. It computes the length of the data and transposes each element to convert it to its equivalent cipher text. The Caesar cipher [18] utilizes a shift pattern that is commingled with a substitution method of traversing through the plain text, and performing the encryption through two phases. The uppercase characters are segregated from the lowercase, and the integer values of each position of the letters are analyzed to be used for substitution. The decryption of the method entails the reverse process or can employ the cyclic property of cipher modulo to obtain the relevant plain text from the cipher text. However, the Caesar cipher suffers the problem of brute-force attack that makes it vulnerable for it to be used. The last method of cryptography to overcome the challenges of the previous methods is effectuated through the columnar-transpositional cipher [18], in which the plain text data is arranged in the form of a matrix, with the respective data rearranged to be encrypted using transpositional row, column values. The process of deciphering entails the receiver to explicitly segregate the message length and divide it by the key value, and perform reversal ordering to obtain the relevant plain text.

The ensuing phases require the explicit key generation through base64 encoding [15], and subsequent mapping of phases through the AES combined RSA method [13]. The Base64 module in python, converts the characters into respective byte code, and then utilizes the ASCII values of each character to encode them. The decoding process entails similar reversal of the encoded data to their respective bytecode, and then reverses the ASCII values to the plain text data [15].

The symmetric and asymmetric cryptography is implemented through the combined operations of AES with the RSA algorithm [3], [13], [17]. The AES algorithm takes into account 14 rounds of iterative progression for a 256-key process, with each round utilizing differing 128- round keys, computed from the key generation of AES [4]. Each of these rounds in the process holds significant phases of implementation using the round key for encryption as delineated in the below figure 4.

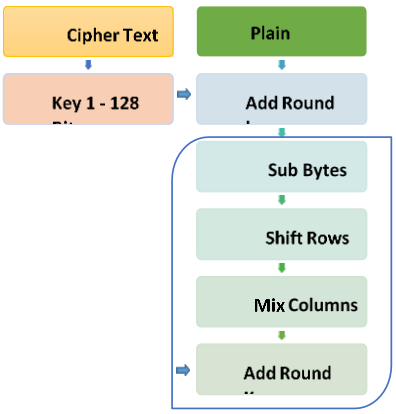

Fig. 4. Phases in each Round of AES Encryption

The byte substitution using the sub bytes fixes the 16 input bytes by looking up in the S-box table [17], and renders a matrix outcome. The shift rows accommodate the previous matrix output and shifts the rows to the left, the dropped-out values are rearranged in the subsequent row on the right. The next phase of mixing the columns utilizes a statistical computation by taking in the four bytes of a column to transform them into new set of bytes that are replaced in the original column. The output of the step thus obtained holds

new values of 16 bytes in a matrix format, which is now transformed into 128bits to be XORed to the 128-bit round key to obtain significantly relevant 128-bit values that are processed to the subsequent rounds [4], [5], else if the last round of the encryption is implemented, the ciphertext is obtained. The process of decryption is followed separately, with the inverse order of operations followed in each round inorder to obtain the decrypted data.

4. Results

This section presents the results of the ciphers obtained, along with the relevant encoding and cryptographic phases effectuated in the above delineated algorithms. The input given to the process is a block cipher effectuated through mapping data blocks. The outcome of the encryption and decryption mechanisms in the table1 below depicts the time consumed, along with the relevant output obtained from each cipher. The elapsed time for the block ciphers yield the best result with minimal time for the columnar transpositional method as compared to the reverse and Caesar cipher**.**

Table 1. Comparative output of Cipher implementations with respect to time.

Name of Algorithm	Elapsed time	Output
Caesar Cipher With key=10	0.0004	LvymuxmszrobxscxkxusxnxypxkxciwwodbsmxmszrobjxgrsmrxDrbyeqrxmyxcdkxdxwkzzsxqxfecekvvigxzbymoccocxsxpybwkdsyxxlvymucxfypdoxxtrxybxopvxlsdcglxzVsqrdgosqrdzxlvymuxmszrobxscxnsppoboxdxpbywxdroxlvymuxcyxdrkdxsdxecocxdroxkvqybsdrwcxdrkdxboaesboxvoccxmywzedsxqxzygobl
Reverse cipher	0.003	.rewop gnitupmoc ssel eriuqer taht smhtirogla eht sesu ti taht os kcolb eht morf tnereffid si rehpic kcolb "thgiewthgiL" .)stib 821 ro 46 netfo(skcolb noitamrofni sessecorp)yllausu(gnippam tnatsnochguorht hcihw ,rehpic cirtemmys a fo dnik a si rehpic kcolB
Columnar Transposition	0.002	l hi d yt h chgoami(a)osiribkon 1b)Ltg cir fnrtbk t segt tqesot eocesk amrcewhrhnnanul cenmolsf o2i.iwhbkp detohl t u oht u smiprBkp anfsecp,ituct p uyrs ot c(e4 s"hi"ocesfef coatehlisaerecugwcir io miirh o stpgslpesfano t6r8t getl hiir meoshistarmhril pno.

The results obtained from implementing the ciphers in Python are delineated as below.

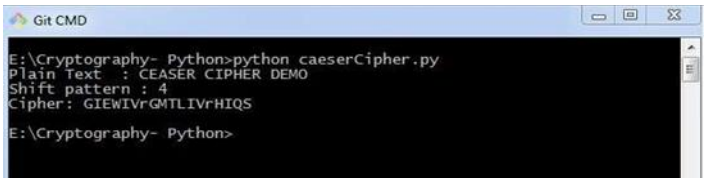

Fig. 5. Cryptography with Python - Reverse Cipher

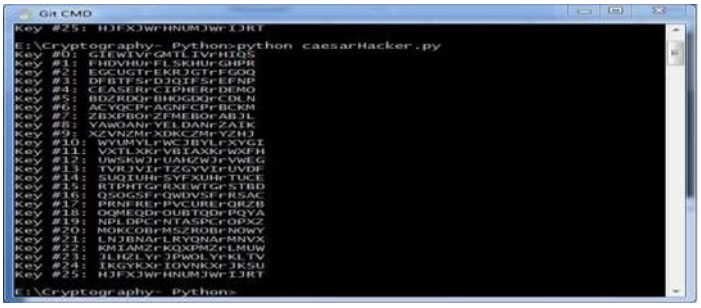

Fig. 6. Cryptography with Python - Caesar Cipher

Fig. 7. Hacking of Caesar Cipher Algorithm

Inorder to overcome the challenges with hacking and brute force attacks, the incorporation and implementation of Transpositional cipher are entailed.

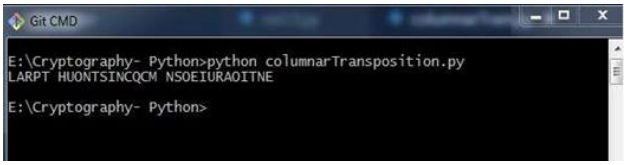

Fig. 8. Transposition Cipher

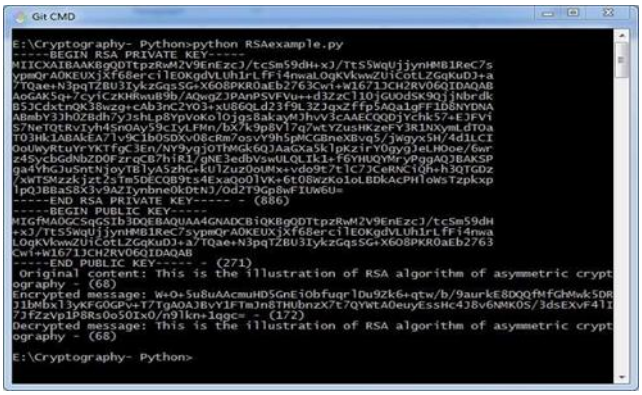

Fig. 9. Encryption of Transposition Cipher

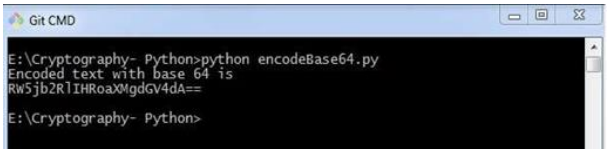

Fig. 10. Base64 Encoding and Decoding

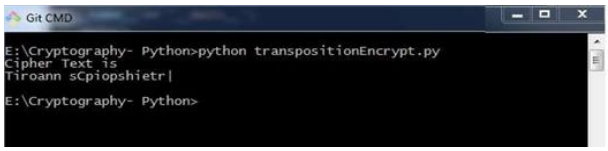

Fig. 11. Symmetric and Asymmetric Cryptography

5. Conclusion

Resilience of systems plays a crucial factor to improving the security and effectiveness. One of the prominent factors that requires impeccable scrutiny interms of using it right, and in augmenting the consistency of precise encryption mechanisms is the utilization of appropriate block ciphers that can serve as catalyst to enhancing the efficacy of IoT applications. The proposed indagation elucidated the optimization of the cryptographic process inorder to secure the data that is transmitted. With many problems such as data leak and hacking on the rise, it is essential to effectuate a hybrid approach that fulfills the constraint on successful and lossless data communication, along with ensuring optimal time of processing. The study also explicitly evinced the security mechanism with the implementation of a combined key generation in the form of symmetric and asymmetric algorithms, and the operability of AES with RSA to escalate better functionality in encryption and decryption. The juxtapose of cipher encryption and decryption through the reverse, Caesar and column-transpositional cipher methods also provided an elaborate cryptographic mechanism of encoding and decoding, with the later establishing itself to hold minimal time-consumption in processing the data. Further work on the area of interest requires a novel algorithmic approach to entail light-weight ciphers to optimize the security mechanism for efficient integration of IoT-enabled devices.

References

[1] Fatemeh Babaeian, Nemai Chandra Karmakar, "Time and Frequency Domains Analysis of Chipless RFID Back-Scattered Tag Reflection", IoT 2020, 1(1), 109-127; doi.org/10.3390/iot1010007

[2] Qusay Idrees Sarhan, "Internet of Things: A Survey of Challenges and Issues", January 2018, International Journal of Internet of Things and Cyber-Assurance, DOI:10.1504/IJITCA.2018.10011246

[3] Hengameh Delfan Azari, Dr. Prashant V Joshi, "An Efficient Implementation of Present Cipher Model With 80-Bit and 128-Bit Key over FPGA Based Hardware Architecture", International Journal of Pure and Applied Mathematics Volume 119 No. 14 2018, 1825-1832.

[4] Deepti Sehrawat and Nasib Singh Gill, "Lightweight Block Ciphers for IoT based applications: A Review", International Journal of Applied Engineering Research, ISSN 0973-4562 Volume 13, Number 5 (2018) pp. 2258-2270.

[5] Muhned Hussam, Ghassan H. Abdul-majeed, Haider K. Hooomod, "New Lightweight Hybrid Encryption Algorithm for Cloud Computing (LMGHA-128bit) by using new 5-D hyperchaos system", Turkish Journal of Computer and Mathematics Education Vol.12 No.10 (2021), 2531-2540.

[6] Mohammed Nazeh Abdul Wahid, Abdulrahman Ali, Babak Esparham and Mohamed Marwan, "A Comparison of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish for Guessing Attacks Prevention", Journal of Computer Science Applications and Information Technology, ISSN Online: 2474-9257, Aug 2018.

[7] C.G. Thorat, V.S. Inamdar, "Implementation of new hybrid lightweight cryptosystem", Applied Computing and Informatic, 2018, https://doi.org/10.1016/j.aci.2018.05.001, 2210-8327.

[8] Zaid M. Jawad Kubba1 and Haider K. Hoomod, "Modified PRESENT Encryption algorithm based on new 5D Chaotic system", IOP Conf. Series: Materials Science and Engineering 928 (2020) 032023 IOP Publishing doi:10.1088/1757-899X/928/3/032023.

[9] Sreeja Rajesh, Varghese Paul, Varun G. Menon and Mohammad R. Khosravi, "A Secure and Efficient Lightweight Symmetric Encryption Scheme for Transfer of Text Files between Embedded IoT Devices", February 2019, doi:10.3390/sym11020293.

[10] Rogaway P., Bellare M and Black J, "OCB: A block-cipher mode of operation for efficient authenticated encryption", ACM Transactions on Information and System Security (TISSEC), 6(3), pp.365-403.

[11] Soleimany, H., "Self-similarity cryptanalysis of the block cipher", IET Information Security, 9(3), pp.179-184.

[12] Yogesh K, Rajiv M, Harsh S, "Comparison of symmetric and asymmetric cryptography with existing vulnerabilities and countermeasures", International Journal of Computer Science and Management Studies. 2011;11(3):60-63.

[13] Preetha M, Nithya M, "A study and performance analysis of RSA algorithm", International Journal of Computer Science and Mobile Computing. 2013;2(6):126-139.

[14] Lavanya R, Karpagam M, Jaikumar R, "A Comparative Study on the Implementation of Block Cipher Algorithms on FPGA", 2017 IJSRST, Volume 3, Issue 8, ISSN: 2395-6011.

[15] Wojciech Muła, Daniel Lemire, "Base64 encoding and

decoding at almost the speed of a memory copy", arXiv:1910.05109v1, DOI: https://doi.org/10.1002/spe.2777, Oct 2019

[16] Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann, M.J.B. Robshaw, Y. Seurin, and C. Vikkelsoe, "PRESENT: An Ultra-Lightweight Block Cipher", September 2007 DOI: 10.1007/978-3- 540-74735-2_31

[17] Eslam w. afify, Abeer T. Khalil, Wageda I. El sobky, Reda Abo Alez, "Performance Analysis of Advanced Encryption Standard (AES) S-boxes", International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-9, Issue-1, May 2020, DOI:10.35940/ijrte.F9712.059120

[18] Syiham Mohd Lokman, Chuah Chai Wen, Nurul Hidayah Binti Ab. Rahman, Isredza Rahmi Binti A. Hamid, "A Study of Caesar Cipher and Transposition Cipher In Jawi Messages", Journal of Computational and Theoretical Nanoscience, March 2018 DOI: 10.1166/asl.2018.11130

[19] Priti V. Bhagat, Kaustubh S. Satpute, Vikas R. Palekar, "Reverse Encryption Algorithm: A Technique for Encryption & Decryption", International Journal of Latest Trends in Engineering and Technology (IJLTET), Vol. 2 Issue 1 January 2013, ISSN: 2278-621X

[20] [20] Riad Saidi, Tarek Bentahar, Atef Bentahar, "Evaluation and Analysis of Interferograms from an InSAR Radar Encrypted by an AES-Based Cryptosystem with The Five Encryption Modes", International Journal on Electrical Engineering and Informatics, December 2020, DOI: 10.15676/ijeei.2020.12.4.13.

[21] Yasir Nawaz and Lei Wang, "Block Cipher in the Ideal Cipher Model: A Dedicated Permutation Modeled as a Black-Box Public Random Permutation", December 2019, Journal of Symmetry 2019, 11, 1485; doi:10.3390/sym11121485

[22] Rubesh Anand Asari, Vidhyacharan Bhaskar, Gaurav Bajpai, Godwin Norense Osarumwense Asemota, "On the Generation of Random Numbers for Symmetric Cryptography Utilizing Astronomical Data" , Advanced Materials Research, October 2011 DOI:10.4028/www.scientific.net/AMR.367.185G.
Brandli and M. Dick, "Alternating current fed power supply," U.S. Patent 4 084 217, Nov. 4, 1978.

.