The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (EPSTEM)
ISSN: 2602-3199

The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (EPSTEM), 2022

Volume 21, Pages 469-476

IConTES 2022: International Conference on Technology, Engineering and Science

Comparative Study of Encryption Algorithms Applied to the IOT

Abdelkrim GHAZ
University Djillali Liabes, Algeria

Ali SEDDIKI
University Djillali Liabes, Algeria

Nadhir NOUIOUA
University Djillali Liabes, Algeria

Abstract: Cryptography has long been known as the mechanism for protecting secret data especially from being captured by dishonest people. Nowadays, with the rapid development of the expansion and use of digital data on the Internet and IOT applications, it has become important to develop cryptographic algorithms that guarantee the confidentiality of data, especially visual data such as digital images.In this work, we demonstrate in the comparative study between four cryptographic algorithms (DES, RSA, CR4 and SIT) for image encryption. We make an objective and visual analysis of the results to know which is the most appropriate algorithm for security data in the Internet of Things environment, which requires fast execution time, and less power consumption. We use certain measurement parameters such as PSNR, correlation, NPCR, UACI, encryption and decryption time and visual comparison of histograms before and after encryption to judge the performance between these different algorithms.

Keywords: Confidentiality, PSNR, NPCR, UACI.

Introduction

Today, the world is experiencing great development in all areas (cultural, social, and economic ...) especially the field of computing. This leads to the creation of many devices and programs to facilitate the exchange and processing of information and data in the form of images or words or signals. The majority of all digital documents manipulated and exchanged in internet networks are mainly in the form of images.

Indeed, the image affected several areas: weather, medicine, telecommunications, detection, video surveillance, etc. therefore the security of this information has become an essential necessity to preserve the authenticity and confidentiality of the messages transmitted and to avoid the intrusion of unauthorized persons, the technique ensuring this protection is called cryptography. Several encryption methods have been developed to solve the security problem (Nagesh & Thejaswini, 2017). They can be classified according to key types into two main families: symmetric and asymmetric cryptography.

The usual encryption and decryption algorithms (DES, RC4, RSA SIT) extend from powerful computers, enormous execution time and energy which present a problem in the case of the Internet of Things where one seeks to minimize time calculation and reduce energy consumption. The Internet of Things represents the network of physical objects “Things” that are integrated with sensors, software and other technologies for the purpose of exchanging data with other devices and systems on the Internet.

Literature Survey and Overview of Algorithms

During its development, cryptography has undergone a corresponding transformation In terms of problems encountered in all data security, hence the emergence of several terms in cryptography often used to characterize the secret process of sending data. Data encryption has also evolved over time from the beginning with symmetry in common Symmetric or asymmetric key for modern encryption key (Henriques &Vernekar, 2017).

Serving information from the Internet of Things (IoT) device to cloud server has several security issues, such as Intercept, modify and steal information. Communication between IoT devices and cloud servers should Protected by encryption methods. However, there are also a few Encryption technology options that fit your needs Lightweight Communication required by IoT devices.(Baiq Yuniar Yustiarini, 2022).

Due to these circumstances, a comparative study will be conducted to find the most suitable encryption algorithms for use in IoT. Therefore, we wanted to test and compare in this study The impact of cryptographic algorithms on the network The performance of IoT devices. Currently, most IoT uses Advanced Encryption Standard (AES) encryption algorithm to protect their communication lines. Therefore this study Check the effect of using DES, SIT and CR4.

The Secure Internet of Things (SIT)

The Secure Internet of Things (SIT) algorithm is a hybrid approach based on Feistel and Substitute Permutation (SP) networks. In this way, the properties of both methods are used to develop a lightweight algorithm that exhibits significant security in IoT environments while keeping the computational complexity at a moderate level. SIT is a symmetric key block cipher consisting of a 64-bit key and plaintext. In symmetric key algorithms, the encryption process consists of multiple rounds of encryption, each of which is based on a specific mathematical function to generate confusion and diffusion. Increasing the number of revolutions can provide better safety, but ultimately leads to an increase in restricted energy consumption (Chandramouli & Bapatla, 2006).

Cryptographic algorithms are usually designed to take an average of 10-20 rounds to keep the encryption process strong enough for system requirements. However, the simulation was limited to five laps to further improve energy efficiency, each encryption round includes mathematical operations that operate on 4 bits of data. Muhammad Usman and al "SIT: A Lightweight Encryption Algorithm for Secure Internet of Things,"

The Data Encryption Standard (DES)

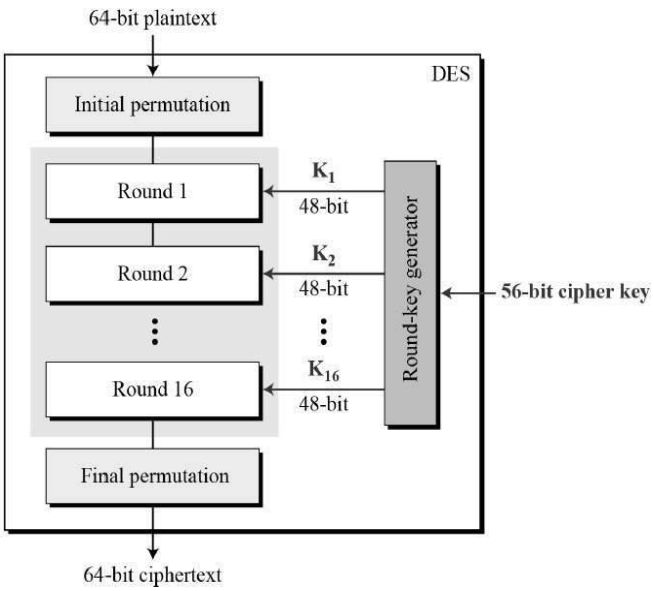

Figure 1. Structure of DES

The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST). DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only). (Coppersmith,1994). General Structure of DES is depicted in the following illustration Figure 1.

Rivest Cipher 4 CR4

Rivest Cipher 4 (RC4) is a type of cryptography that belongs to the class of stream ciphers with a symmetric key (Shyul & Chen, 2008), where this key is used for encryption and decryption. The function of RC4 is to generate a keystream using a pseudo-random number generator. The resulting keystream is manipulated using XOR and plaintext logical operations that encrypt each bit. Then perform the RC4 decryption process in the same way, and the tip bit is used as the encryption operation, because the XOR operation is symmetrical

RSA Algorithm

In 1977, Ron Rivest, Adi Shamir, and Leonard Adleman developed a new algorithm called RSA. This algorithm is a type of asymmetric cryptography because it uses different keys for encryption and decryption. The RSA algorithm includes three main steps of encryption and decryption (Ray & Potnis, 2017). These steps are shown as a flowchart in Figure 2, explaining how the algorithm works. Key Generation: In this step, two keys will be generated.

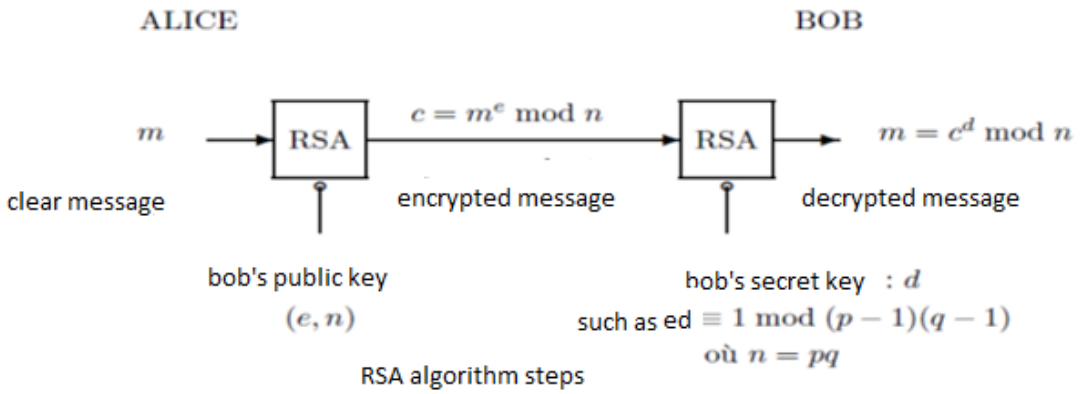

Figure 2. Principle of the RSA algorithm

Evaluation Metrics

For the sake of measuring high fidelity and robustness, some powerful metrics in the image-processing field were employed, in reason of making a fair judgment on the proposed work.

Peak Signal to Noise Ratio (PSNR)

Calculates the error among the original cover image and the encrypted image, mathematically is given by:

$$PSNR = 10\ log_{10}\ \frac{255^2}{MSE} \qquad (1)$$

Mean Square Error (MSE)

Determines mean error magnitude between two images.

Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI)

To ensure the security of the image encryption scheme for differential scanning, two quantification measures are used: NPCR (Number of Pixels Change Rate) and UACI (Unified Average Changing Intensity). NPCR measures the number of distinct pixels as a percentage of the total number of pixels between two images, whereas UACI measures the difference in mean intensity between two images.

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\% \qquad (2)$$

$$UACI = \frac{1}{M \times N}\left[\sum_{i,j} \frac{C_1(i,j) - C_2(i,j)}{255}\right] \times 100\% \qquad (3)$$

NPCR > 99.094 % and UACI > 33.4635 % ensure that an image encryption scheme is secure against differential attack. (Hasnat,& Barman, 2016).

Results and Discussion

Visual Comparison:

Comparison of Histograms

Knowing that a good encryption requires that the histogram of encrypted images must have a uniform distribution, we note that for the image lena and cameraman that the encryption algorithms SIT, DES and CR4 satisfied this condition of uniform distribution while the RSA has not this property which weakens the robustness of this algorithm, show figures 3, 4 and 5.

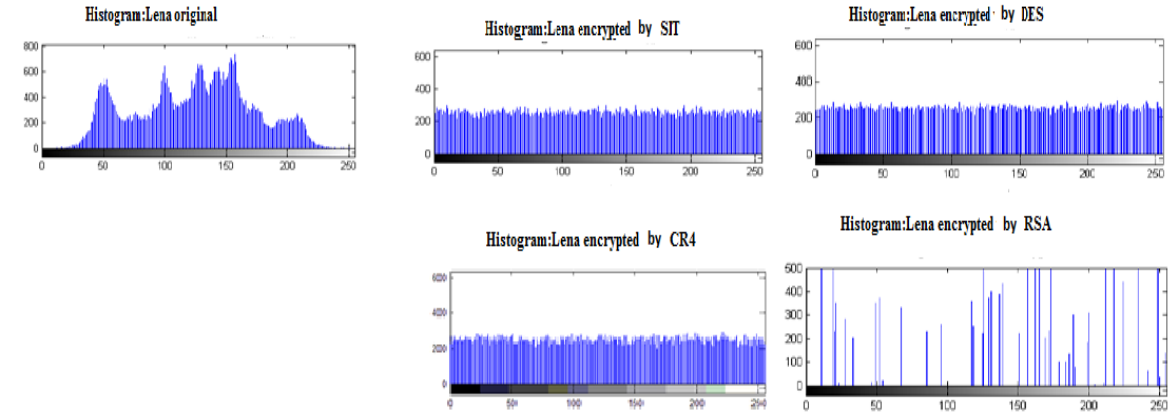

Figure 3. Histograms of the image Lena encrypted by the four algorithms

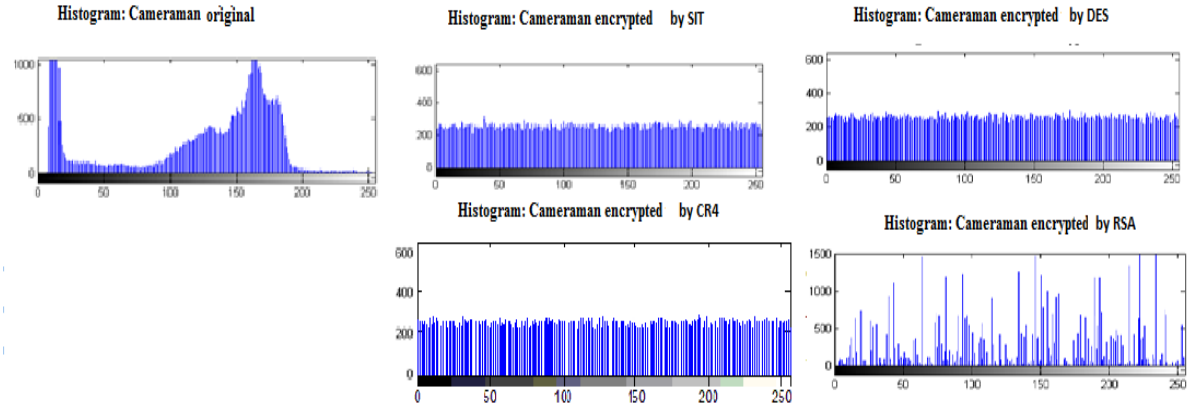

Figure 4. Histograms of the image Cameraman encrypted by the four algorithms

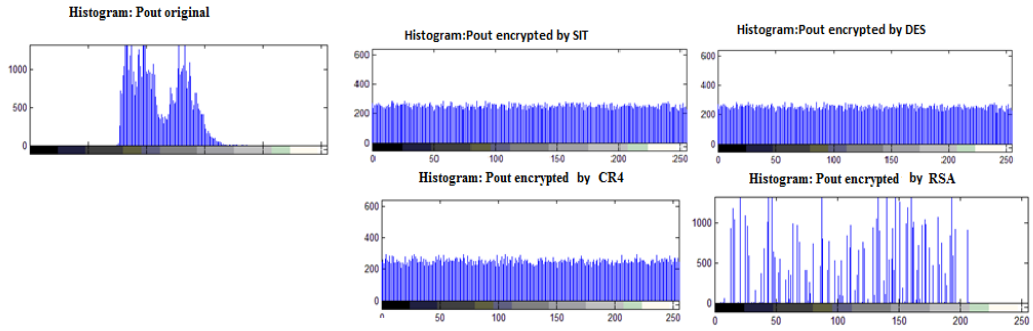

Figure 5. Histograms of the image Cameraman encrypted by the four algorithms

We have increased the size of the images (512) and have traced their histograms to see if there are changes, even figures 6. We always see that the RSA algorithm gives non -uniform histograms for all images, namely Lena, Cameraman while for the algorithms DES, SIT and RC4 the distribution remains uniform.

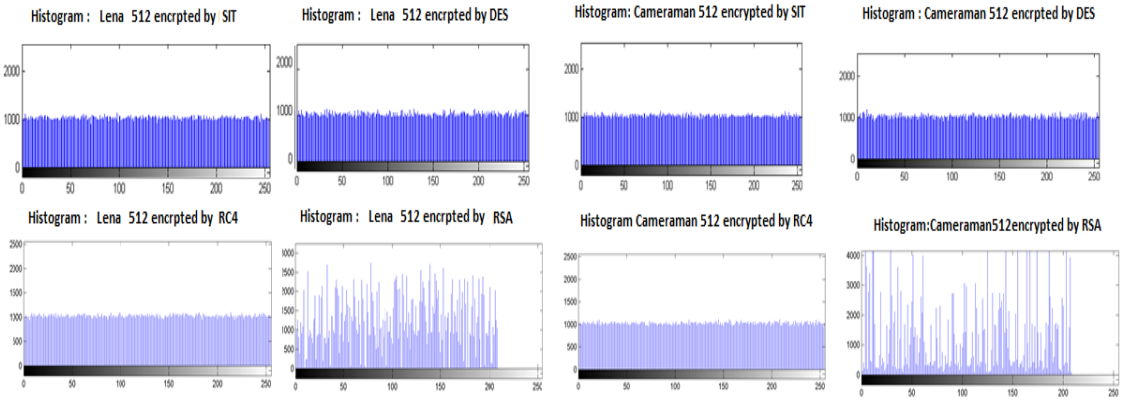

Figure 6. Histograms encrypted Lena and Cameraman

Visual Comparison of Encrypted Images

We found that the Lena image was absolutely well encrypted by 4 algorithms (especially DES, SIT, and CR4), and the RSA algorithm was slightly less robust, see Figure 7 (E). For 4 encryption algorithms, we were able to recover the decrypted image with a correlation coefficient of 1, see (C,F,I and L) above. The encryption defect of the RSA algorithm appears strongly by viewing the encrypted Pout image, where one can guess the shapes of the contours of this image which facilitates differential attacks, see Figure 8

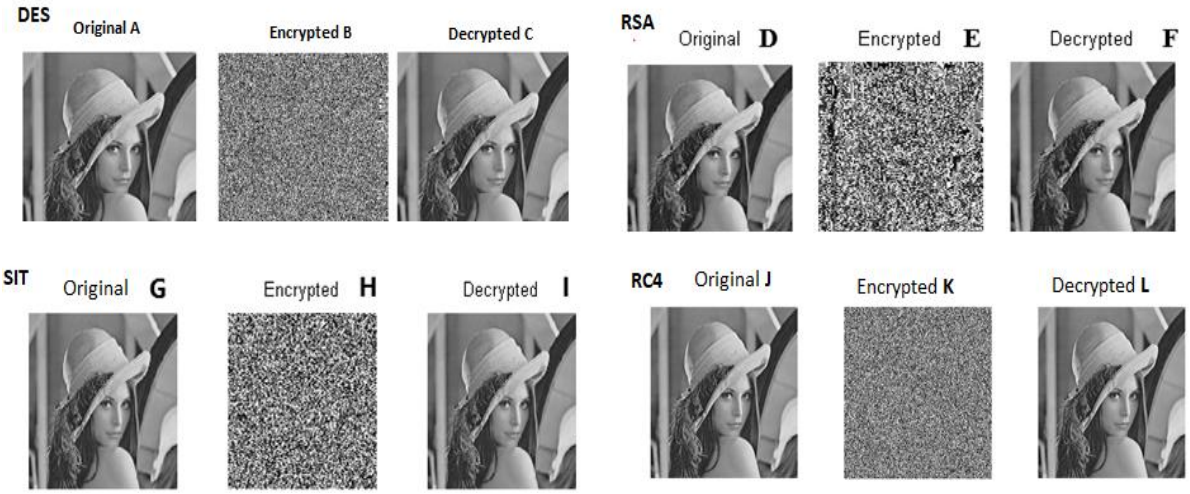

Figure 7. Encrypted and decrypted Lena and Cameraman

Figure 8. Encrypted and decrypted Pout by RSA (size: 256 and 512)

By increasing the size of the Pout image to 512 pixels, we still see that the contours of the encrypted image by the RSA remain visible, see figure 8.

Objective Comparison

Table 1 shows that the PSNR and correlation of DES, SIT and CR4 algorithms are close, we can take the Cameraman image as an example, the PSNR shows the following values (8.4156, 8.3970 and 83870) and the correlation (0.0049, 0.0037, -0.0062) while the RSA algorithm gives a lower PSNR than the previous algorithm (5.1252) we searched in the encrypted area, but a visual comparison of the images shows that the RSA encryption is less efficient. from a correlation point of view The values gives advantages to the SIT and RC4 algorithms.

Table 1. Psnr and correlation for different encryption algorithms

Images	PSNR				Correlation			
256 pixels	DES	RC4	RSA	SIT	DES	RC4	RSA	SIT
Lena	9.2190	9.2571	6.4392	9.2758	-0.0055	-0.0003	-0.0135	0.0036
Cameraman	8.4156	8.3798	5.1252	8.3970	0.0049	-0.0062	0.0430	0.0037
Pout	10.1442	10.1152	5.64	10.1554	-0.030	0.0026	0.0654	0.0052

According to the values of the measures table 2 (NPCR, UACI), larger values indicate that the encryption is strong and efficient So we can clearly see that RC4 and SIT algorithms return values close to DES in terms of NPCR compared to RSA. About UACI, we observe that the values obtained with the RSA algorithm are better, but visual comparisons show the opposite (detected contour shapes of the images encrypted by RSA).

Table 2. NPCR and UACI for different encryption algorithms

Images	NPCR				UACI			
256 pixels	DES	RC4	RSA	SIT	DES	RC4	RSA	SIT
Lena	99.5911	99.5895	99.9985	99.5972	15.0325	14.8831	45.0594	14.8598
Cameraman	99.5712	99.5895	98.8525	99.5712	17.2153	17.3143	42.8844	17.3551
Pout	99.6109	99.5895	98.2437	99.5438	16.6590	16.5358	46.6916	16.5503

Table 3 shows the advantages of the RC4 algorithm and SIT compared to DES in terms of encryption and decryption execution time, although RSA takes less time than CR4 and SIT, this can be explained by choosing p and q and public key value e below 100, i.e. if we increase p, q and e value to make encryption more efficient. We noticed a huge increase in execution time for RSA encryption (encryption time = 49.793459 seconds for Lena image, decryption time = 411.369710), almost 15 times.

Table 3. Calculation time for different Encryption and Decryption algorithms

Images	Encryption Time (Seconds)				Decryption Time (Seconds)			
256 pixels	DES	RC4	RSA	SIT	DES	RC4	RSA	SIT
Lena	525.4367	7.8586	0.000738	33.0943	524.582154	7.17554	0.098294	29.5721
Cameraman	563.35	7.5320	0.005759	33.3252	561.94	7.83811	0.051146	29.6903
Pout	558.1	6.76731	0.000979	33.1999	556.889	7.2989	0.033195	29.6782

We have found time and time again that the computation time of the RC4 algorithm is still better compared to DES, their time has greatly increased. The second is the SIT algorithm. Using RSA algorithm, by increasing the value of p, q and e to improve encryption, the time will be higher than using CR4 and SIT algorithm.

Table 4. Calculation time for different Encryption and Decryption algorithms (image 512)

Images	Encryption Time (Seconds)				Decryption Time (Seconds)			
512 pixels	DES	RC4	RSA	SIT	DES	RC4	RSA	SIT
Lena	2129.3767	42.8535	0.0037	130.0736	2132.6279	43.9544	0.5717	116.4549
Cameraman	2235.5715	43.8916	0.0023	143.4658	2239.9611	42.2810	0.3868	129.4439
Pout	2233.0038	44.3373	0.0055	133.8145	2229.2112	43.3176	0.1787	118.9075

Conclusion

From objective analysis (PSNR, correlation, NPCR, UACI, and computation time) and visual analysis (histogram, comparison of encrypted and decrypted images), it was concluded that the RC4 encryption algorithm and SIT gave better results in both encryption and decryption. Value calculation time and PSNR and correlation close to DES, the calculation time of DES is 15 times higher and requires high energy consumption, making CR4 and SIT algorithms suitable for adoption in IoT applications, with better robustness and efficiency DES and RSA are When used, the latter represents optically unsatisfactory encryption.

Scientific Ethics Declaration

The authors declare that the scientific ethical and legal responsibility of this article published in EPSTEM journal belongs to the authors.

Acknowledgements

* This article was presented as an oral presentation at the International Conference on Technology, Engineering and Science (www.icontes.net) held in Antalya/Turkey on November 16-19, 2022.

References

Chandramouli, R., Bapatla, S., Subbalakshmi, K. P., & Uma, R. N. (2006). Battery power-aware encryption. *ACM Transactions on Information and System Security (TISSEC)*, *9*(2), 162-180.

Coppersmith, D. (1994). The Data Encryption Standard (DES) and its strength against attacks. *IBM Journal of Research and Development*, *38*(3), 243-250.

Hasnat, A., Barman, D., & Mandal, S. N. (2016, October). A novel image encryption algorithm using pixel shuffling and pixel intensity reversal. In *2016 International Conference on Emerging Technological Trends (ICETT)* (pp. 1-6). IEEE.

Henriques, M. S., & Vernekar, N. K. (2017, May). Using symmetric and asymmetric cryptography to secure communication between devices in IoT. In *2017 International Conference on IoT and Application (ICIOT)* (pp. 1-4). IEEE.

Nagesh, H. R., & Thejaswini, L. (2017, March). Study on encryption methods to secure the privacy of the data and computation on encrypted data present at cloud. In *2017 International Conference on Big Data Analytics and Computational Intelligence (ICBDAC)* (pp. 383-386). IEEE.

Ray, A., Potnis, A., Dwivedy, P., Soofi, S., & Bhade, U. (2017, October). Comparative study of AES, RSA, genetic, affine transform with XOR operation, and watermarking for image encryption. In *2017 International Conference on Recent Innovations in Signal processing and Embedded Systems (RISE)* (pp. 274-278). IEEE.

Shyu, S. J., & Chen, Y. R. (2008, December). Threshold secret image sharing by Chinese remainder theorem. In *2008 IEEE Asia-Pacific Services Computing Conference* (pp. 1332-1337). IEEE.

Yustiarini, B. Y., Dewanta, F., & Nuha, H. H. (2022, July). A comparative method for securing ınternet of things (IoT) devices: AES vs Simon-Speck Encryptions. In *2022 1st International Conference on Information System & Information Technology (ICISIT)* (pp. 392-396). IEEE.

Author Information

Abdelkrim GHAZ
University Djillali Liabes**,** Algeria
Contact e-mail: *gabkarim@gmail.com*

Ali SEDDIKI
University Djillali Liabes**,** Algeria

Nadhir NOUIOUA
University Djillali Liabes**,** Algeria

To cite this article:

Ghaz, A., Seddıkı, A., & Nouıoua, N. (2022). Comparative study of encryption algorithms applied to the IOT. *The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (EPSTEM), 21,* 469-476