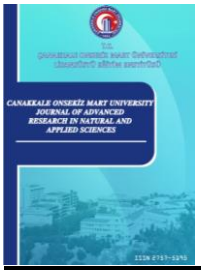
e-ISSN 2757-5195



Çanakkale Onsekiz Mart University
Journal of Advanced Research in Natural and Applied Sciences

Open Access

doi.org/10.28979/jarnas.1068884 2022, Vol. 8, Issue 4, Pages: 569-582 dergipark.org.tr/tr/pub/jarnas

Enhancing the Process of AES: A Lightweight Cryptography Algorithm AES for Ad-hoc Environments

Mustafa Al-handhal[1], Alharith A. Abdullah[2], Oğuz Ata [3, *], Çağatay Aydin[4]

[1]Department of Information Technology, Faculty of Computer Engineering, Altınbaş university, Istanbul, Türkiye
[2]Department of Information Network, Faculty of Information Technology, University of Babylon, Hillah, Iraq
[3]Department of Software Engineering, Faculty of Computer Engineering, Altınbaş university, Istanbul, Türkiye
[4]Department of Electrical-Electronics Engineering, Faculty of Engineering, Ege University, Izmir, Türkiye

Article History

Received: 07.02.2022
Accepted: 10.06.2022
Published: 15.12.2022

Research Article

Abstract − Ad hoc networks have become more widespread and important because they support mobility and can be used in different situations and some difficult areas such as rescue missions, military, and vehicular communications. Security is stated among the most significant challenges facing Ad Hoc networks due to its characteristic features such as the topology dynamicity, lack of infrastructure centralization, and open architecture. Ad hoc networks work on battery power, and this kind of networks tend to consume more power and time to process data and memory resources through data encryption, eventually requiring a higher amount of power and more time. Therefore, an AES lightweight algorithm is proposed, which is one of the complicated encryption algorithms. This algorithm will be modified to improve the security as well as reduce the amount of time and energy consumed in comparison with the original algorithm. The enhanced version is based on the outputs of sub byte and shift row, in addition to an exclusive X-OR operator between them, whereby the output of the X-OR operator is added to the round key layer. The results confirm that this enhanced algorithm is efficient, accurate, and robust against multiple types of attacks related to ad hoc networks.

Keywords − *Ad-hoc network, advanced encryption standard (aes), lightweight cryptography (LWC)*

1. Introduction

Throughout the last few decades, an exponential development is observed regarding the wireless areas. Great advances have been achieved in network infrastructures, which in turn increase the provision of wireless applications, and the appearance of omnipresent wireless devices like portable or handled computers, PDAs, and mobile phones. These devices are remarkably increasing in terms of their capabilities and tend to play a significant role in human life at the present time (Basangi et al., 2004).

Ad hoc networks consist of a set of wireless nodes which communicate in a direct way through common wireless channels(Rani et al., 2013). Ad-Hoc networks do not need any extra infrastructure like base stations or wired access points. The created network can be independent from the infrastructure network. On the other hand, these nodes are able to build their own networks. Additionally, communication among nodes only takes place whenever they are located within their transmission range. Security is an important problem in ad hoc networks, as it produces integrity, confidentiality, and availability (Elmahdi et al., 2018). Providing security

[1] mostafayousif36@gmail.com
[2] alharith@itnet.uobabylon.edu.iq
[3] oguzata@gmail.com
[4] cagatay.aydin@ege.edu.tr
*Corresponding Author

affects the power management in ad hoc networks, as the consumption of power occurs within the nodes whenever the packet is transmitted or received.

One of the efficient mechanisms which could be used for solving the security challenges in Ad Hoc networks is cryptography (Costa et al., 2017). It seems to have a major role in protecting data from opponents through converting it into a form of data that is unintelligible for unauthorized access. Lightweight cryptography is a novel sub-field designed to deal with more developed technologies (Alyas and Abdullah, 2021). Applying traditional cryptography within constrained devices is not sufficiently practical because of the mathematical complexity of cryptographic primitives (Vanda et al. 2021). Traditional cryptography requires a large memory space and relatively more power for processing. Thus, the motive behind using Lightweight algorithms is the speed of execution, the comparatively less energy and time consumed, and the need for less memory use (Abdullah and Obeid, 2021). Lightweight algorithms consist of two parts: Symmetric figures and Asymmetric figures. The symmetric ciphers consist of Block and Stream Ciphers.

Lightweight cryptography has many effective algorithms, one of which is the Advanced Encryption Standard (AES), a commonly used method in wireless environments. AES has a high security with low complexity (Agwa et al., 2017), and it has become more attractive to researchers for modification and enhancement. Several researchers have proposed different techniques to enhance the security in many networks, as outlined in the related literature reviews below.

Usman et al. (2017) present a lightweight encryption algorithm for securing IoT. A 64-bit block cipher model is proposed, requiring a 64-bit key for data encryption. It represents a hybrid between festal and uniform substituting-permutating networks. Kunchok et al. (2018) proposed three ways of security to encryption data. It combines the advantages of different encryption algorithms, so that the process of transmitting data through the network is encrypted. Aziz and Singh. (2018) proposed a compressive sensing for providing lightweight cryptographic security for IoT. They made use of compressive sensing to encrypt data, which in turn contributed to the protection of power consumption. Abdullah et al. (2018) introduced a super-encryption cryptography using international data and word auto key encryption algorithms. It combines several cryptographic algorithms for providing higher data security. Mohanty et al. (2020) introduced a lightweight algorithm with distributed throughput management in blockchain, which is applicable to IoT networks to enhance security and reduce the consumption of resources like time and power. Keshav Kumar et al. (2020) proposed AES lightweight algorithm to encrypt voice signal on peer-to-peer communication. And it is applied on Field Programmable Gate Array (FPGA) simulation. Fadhil et al. (2021) proposed Lightweight AES encryption algorithm to provide security when the data received from physical environment in IOT system. It is worked on Raspberry. Hussein M. et al. (2022) proposed AES lightweight algorithm in IoT systems to provide security and delay in time. It is implementation on Asp net.

In this paper, the AES lightweight algorithm will be used in Ad-hoc networks to provide security for data that is sent across such kinds of networks, as well as to reduce the time and power consumption required for encrypting data and transmitting packets among nodes.

The research paper could be outlined as follows. Section II describes the AES algorithm adopted in this work. Section III states the experiment and discussion result. A comparison with other previous works is drawn in Section IV, and Section V states the conclusions drawn.

2. Materials and Methods

This section discusses the modified AES lightweight algorithm that is used in this paper to reduce the power and time consumption in ad hoc networks. In the standard AES algorithm, there are four steps to encrypt and decrypt data, namely: Sub Byte, Shift Row, Mix Column and Add Round Key. In the modified form of AES lightweight algorithm, the output of both the Sub byte and Shift row are taken to create an exclusive OR (XOR) to be used instead of the MixColumns.

2.1. Encryption Process

The process of encrypting in the AES algorithm (Daemen et al, 1999) consists of a set of steps or transformations that are carried out onto the data. There are also additional steps which are iterative and fixed, also known as rounds. The number of rounds in cryptocurrencies is determined by the key length. If the available one consists of 128 bits, then the number of rounds is 10. The key lengths 192 and 256 are accompanied with 12 and 14 rounds respectively (NIST, 2001). The encryption process is shown in Figure 1.

2.2. Decryption Process

The decryption process takes place through reversing the encryption process. However, the sequence of conversions is different from the encryption process. In decryption processes, the InvSubBytes and the InvShiftRows are interchangeable with no effect on the decryption processes. 128 bit used in our work. The decrypting and encryption (William S. 2000) procedure is illustrated in Figure 1.

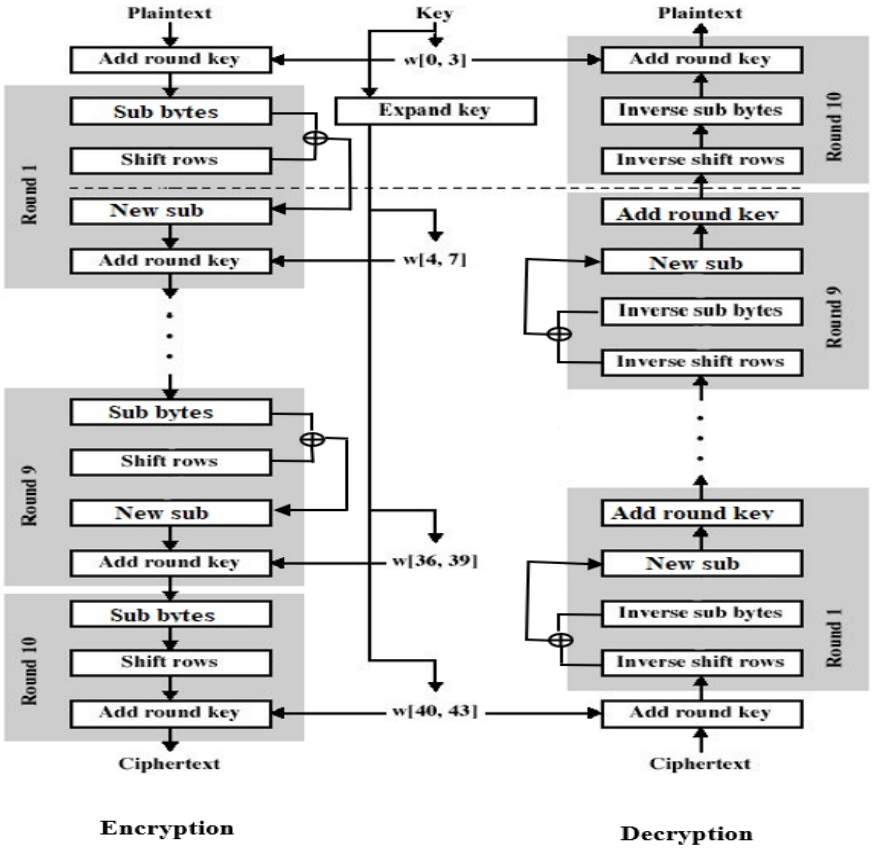


Figure 1. Encrypting and decrypting processes in the modified AES lightweight

Algorithm (1) below outlines the steps of the proposed AES lightweight

Input: Plain Text.

Output: Cipher Text.

Step1: Divide the plain text to groups, each group contains (4*4) byte. Then, perform the XOR operation with the key (This operation is called Initial key).

Step 2: Take the initial key and perform the XOR operation with S-Box (This step is called Sub Byte).

Step 3: The results of the Sub Byte are shifted. Every byte in the row shifts to the left with a certain indent. The first row undergoes no change. The second row makes a shift to the left, and the third row makes two shifts to the left (This step is called Shift Row).

Step 4: **This step is called New Sub**:

```
if (keyBits == 128) {
        for (;;) {
                temp  = rk[3];
                rk[4] = rk[0] ^
                        (Te4[(temp >> 16) & 0xff] & 0xff000000) ^
                        (Te4[(temp >>  8) & 0xff] & 0x00ff0000) ^
                        (Te4[(temp      ) & 0xff] & 0x0000ff00) ^
                        (Te4[(temp >> 24)       ] & 0x000000ff) ^
```

Step 5: Add-Round Key

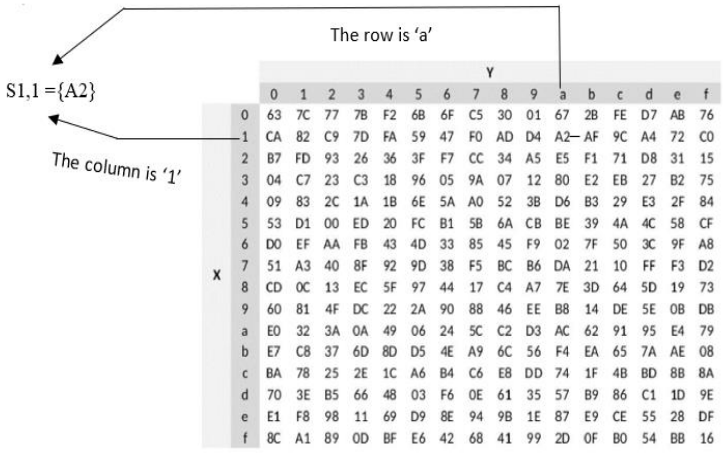
Figure 2.The steps of the proposed AES lightweight

In Figure 2 above the steps of proposed algorithm in step 4, the key is 128-bit. The term temp refers to the cipher text. Thus, Round 1 takes the Te4, representing the data in the algorithm which is determined by the bytes. Each byte has a different data, for example the data of 16 differs from the data in 8. Thus, this step (Te4[(temp >> 16) & 0xff] represents the Sub Byte and will make XOR operation with Shift Row (0xff000000). This operation reduces the New Sub to be used instead of the Mix Column. These steps will be represented in every round.

2.3. Sub Byte and Inverse Sub Byte Transformations

Each byte within the array will be replaced with an 8-byte Sub Byte taken from the S-Box. The benefit of using the Sub Byte is the non-linearity that is provided in the cipher. The S-Box is obtained through the inverse over the Galois Field (2^8) (Shastry et al. 2011). As for the Inverse Sub Byte, all bytes in the matrix are replaced by the Inverse Sub Byte that corresponds with it.

For example, if S1,1 ={1a}, then the substitution value determined by the intersected the column with index '1' and the row with index 'a'. So, the result of S1,1 will be{A2}. as shown in Figure 3.



x \ y	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
a	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
b	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
c	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
d	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
e	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
f	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Figure 3. Sub Byte Operation

2.4. Shift Row and Inverse Shift Row Transformations

In the shift row, each byte in the row undergoes a certain indent to the left. In AES, the first row remains with no changes whereas the second one makes a single shift to the left and the thirft one makes two left shifts. Meanwhile, the inverse shift row is the opposite of the forward shift row. The first row remains with no changes whereas the second shifts once to the right, and the third shifts two bytes to the right as well. The shifts are determined by the adopted matrix in (Scheier, 2015).

For example, if we have this data 85, 01, A2, ed, a4, 21, 30, b2, d2, e6, 97, 44, 53, fc, 3f and 59. So, each 4 bytes will be in row as shown in Figure 4.

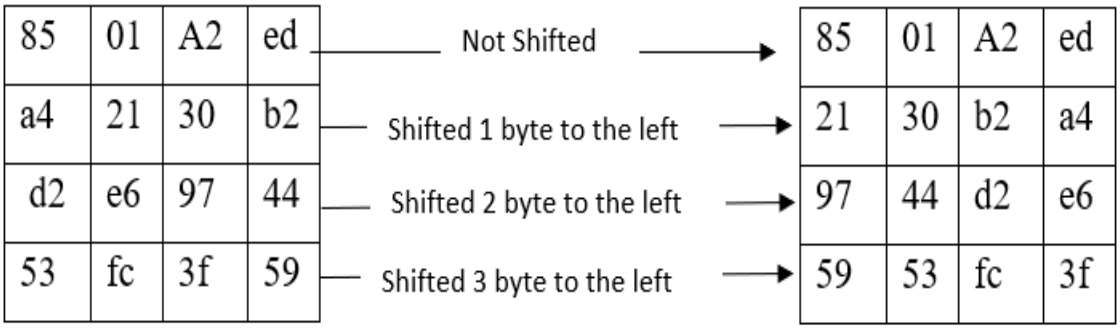


Figure 4. Shift Row Operation

2.5. New Sub

The new sub is the result of merging the Sub byte with the Shift row by using the XOR operation. The output is to be used instead of the Mix column. This operation aims to reduce time and energy consumption. Figure 5 shows the result of this step

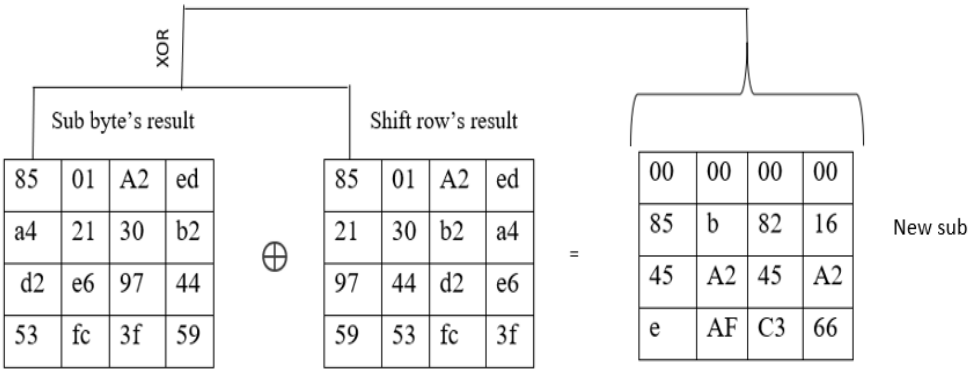


Figure 5. The New Sub

2.6. Add Round Key

Next, the round key is added to the state through the X-OR operation. The round keys are composed of several words taken from the key table. The round key undergoes the X0OR operation for every byte in the state matrix, generating a new round key for each round through altering the cipher key.

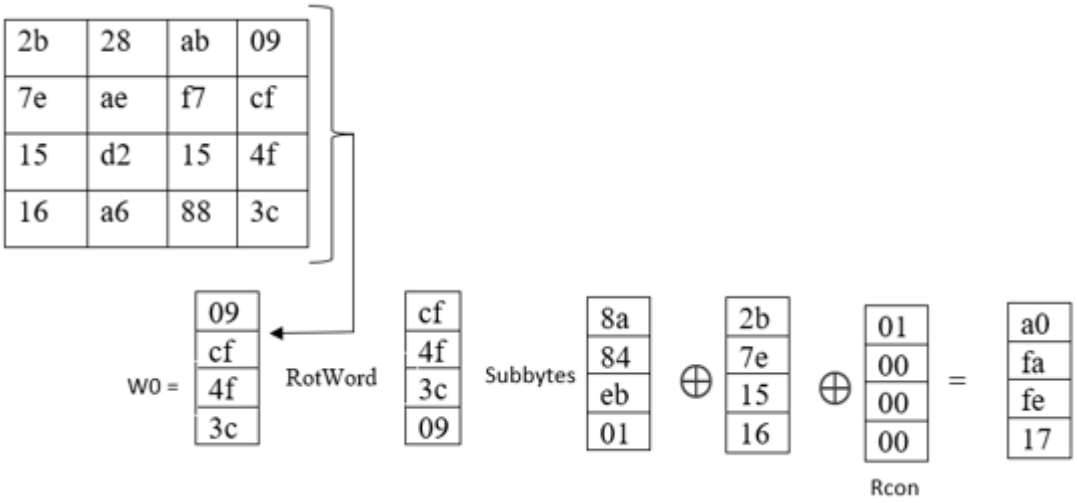


Figure 6. Add Round Key Operation

2.7. Key Schedule

The key schedule takes the original key (the length of 128 bit , 192 bit, and 256 bit) then the subkeys will derive in AES. The subkeys number is equal to the number of rounds plus one. So, the key length of 128 bit is nr =10 and there are 11 subkeys beacuse the plus one

3. Results and Discussion

After designing the Ad-Hoc network, it is used within this simulation after which the connection between the clients and server is observed. Figure 7 shows this Ad-Hoc network. To prove the enhancement of the AES lightweight algorithm, the implementation of the Ad-Hoc network in the cooja simulator is shown and discussed. Cooja is used for the reduction of power and time consumption.

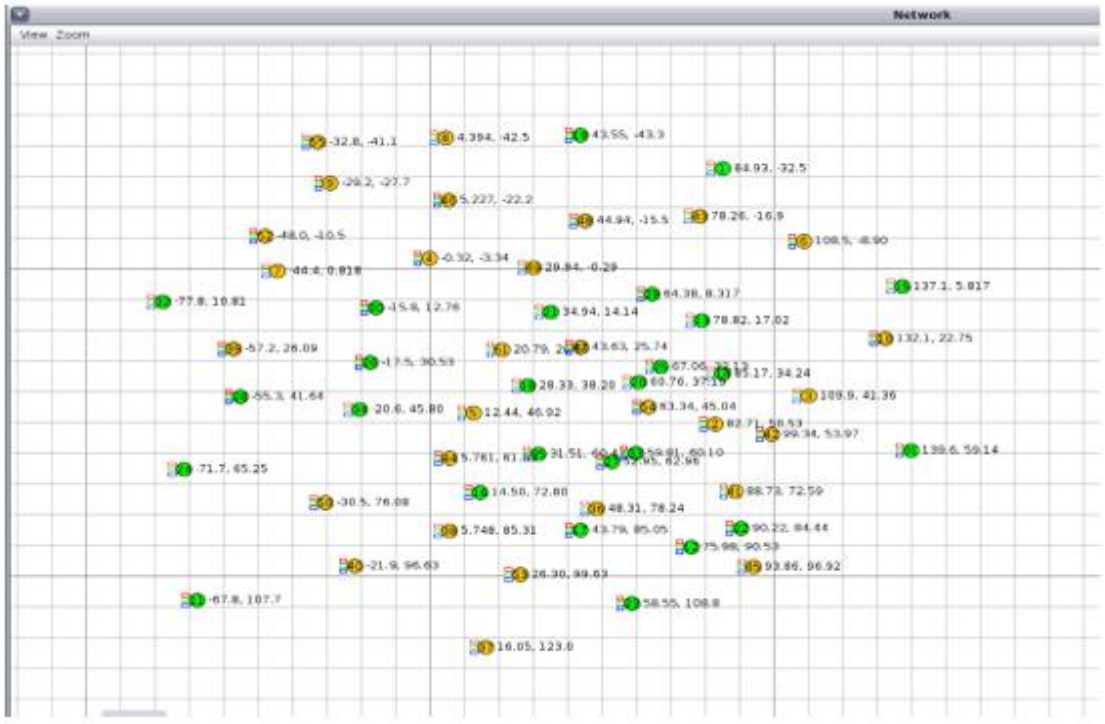


Figure 7. Ad-hoc network implementation.

In Figure 8 below presents the output of the network. It shows the time that is consumed when the message sent between motes as sender and receiver.

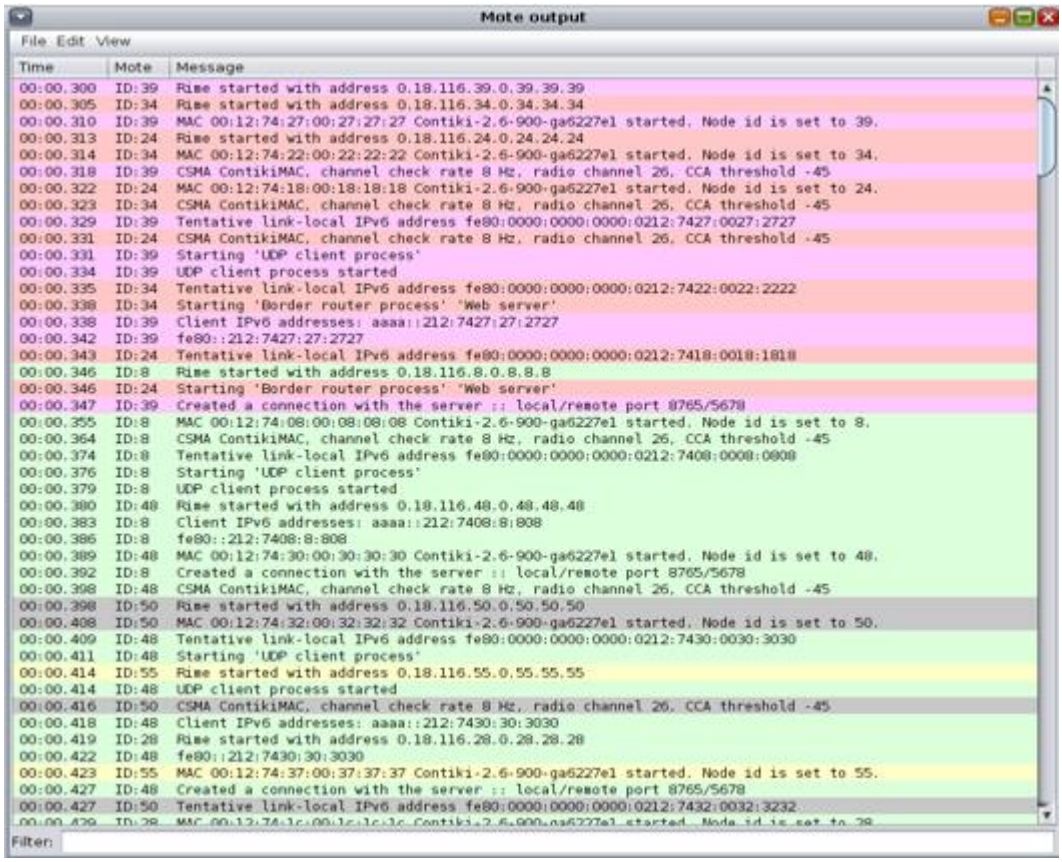


Figure 8. The output of ad hoc network implementation.

In power trace, a loss in power is observed when using the Standard AES algorithm to send data between sender (Radio TX) and receiver (Radio RX), as shown in Table 1. Therefore, the lost power in Radio TX and RX for 55 mote (node) for a lot of nodes. The total loss in power for Radio TX is 0.32% and for Radio RX is 0.03%.

Table 1
The power trace for Standard AES algorithm

Mote	Radio on (%)	Radio TX (%)	Radio RX (%)
Sky1	0.00%	0.00%	0.00%
Sky 2	1.34%	0.48%	0.02%
Sky 3	1.28%	0.49%	0.00%
Sky 4	0.80%	0.00%	0.07%
Sky 5	1.39%	0.48%	0.06%
Sky 6	1.4 1%	0.48%	0.03%
Sky 7	0.73%	0.00%	0.03%
Sky 8	0.73%	0.00%	0.02%
Sky 9	1.37%	0.48%	0.03%
Sky 10	1.37%	0.49%	0.02%
Sky 11	0.81%	0.00%	0.04%
Sky 12	0.78%	0.00%	0.04%
Sky 13	1.37%	0.49%	0.02%
Sky 14	1.32%	0.48%	0.01%
Sky 15	0.85%	0.00%	0.09%
Sky 16	1.46%	0.48%	0.05%
Sky 17	1.35%	0.49%	0.02%
Sky 18	1.48%	0.48%	0.07%
Sky 19	0.68%	0.00%	0.02%
Sky 20	1.36%	0.48%	0.03%
Sky 21	1.33%	0.49%	0.02%
Sky 22	1.34%	0.49%	0.03%
Sky 23	0.74%	0.00%	0.03%
Sky 24	1.38%	0.49%	0.03%
Sky 25	1.39%	0.48%	0.05%
Sky 26	1.39%	0.48%	0.03%
Sky 27	0.79%	0.00%	0.05%
Sky 28	1.49%	0.49%	0.09%
Sky 29	1.29%	0.49%	0.00%
Sky 30	0.77%	0.00%	0.03%
Sky 31	0.82%	0.00%	0.06%
Sky 32	1.4 1%	0.48%	0.03%
Sky 34	1.47%	0.48%	0.04%
Sky 35	0.71%	0.00%	0.03%
Sky 36	1.31%	0.48%	0.00%
Sky 37	1.32%	0.49%	0.02%
Sky 38	1.33%	0.48%	0.03%
Sky 39	0.73%	0.00%	0.05%
Sky 40	1.38%	0.49%	0.01%
Sky 41	1.38%	0.49%	0.02%
Sky 42	1.30%	0.49%	0.00%
Sky 43	0.75%	0.00%	0.03%
Sky 45	1.36%	0.48%	0.03%
Sky 46	1.47%	0.48%	0.06%
Sky 47	1.38%	0.48%	0.01%
Sky 48	0.85%	0.00%	0.07%
Sky 49	1.40%	0.49%	0.03%
Sky 50	0.81%	0.00%	0.08%
Sky 51	1.35%	0.48%	0.03%
Sky 52	1.34%	0.48%	0.03%
Sky 53	0.81%	0.00%	0.06%
Sky 54	1.47%	0.48%	0.03%
Sky 55	1.35%	0.49%	0.02%
Average	1.16%	0.32%	0.03%

In proposed AES lightweight algorithm, the power loss for sender and receiver is better than the standard algorithm. Table 2 presents the power trace for the proposed algorithm.

Table 2
The power trace for the proposed AES algorithm

Mote	Radio on (%)	Radio TX (%)	Radio RX (%)
Sky1	0.00%	0.00%	0.00%
Sky 2	1.48%	0.48%	0.06%
Sky 3	1.39%	0.48%	0.00%
Sky 4	0.76%	0.00%	0.07%
Sky 5	1.43%	0.48%	0.06%
Sky 6	1.38%	0.48%	0.03%
Sky 7	0.75%	0.00%	0.03%
Sky 8	0.74%	0.00%	0.02%
Sky 9	1.34%	0.48%	0.03%
Sky 10	1.36%	0.48%	0.03%
Sky 11	0.00%	0.00%	0.00%
Sky 12	0.00%	0.00%	0.00%
Sky 13	0.00%	0.00%	0.00%
Sky 14	0.00%	0.00%	0.00%
Sky 15	0.00%	0.00%	0.00%
Sky 16	0.00%	0.00%	0.00%
Sky 17	0.00%	0.00%	0.00%
Sky 18	0.00%	0.00%	0.00%
Sky 19	0.00%	0.00%	0.00%
Sky 20	0.00%	0.00%	0.00%
Sky 21	0.00%	0.00%	0.00%
Sky 22	0.00%	0.00%	0.00%
Sky 23	0.00%	0.00%	0.00%
Sky 24	0.00%	0.00%	0.00%
Sky 25	0.00%	0.00%	0.00%
Sky 26	0.00%	0.00%	0.00%
Sky 27	0.00%	0.00%	0.00%
Sky 28	0.00%	0.00%	0.00%
Sky 29	0.00%	0.00%	0.00%
Sky 30	0.00%	0.00%	0.00%
Sky 31	0.00%	0.00%	0.00%
Sky 32	0.00%	0.00%	0.00%
Sky 34	0.00%	0.00%	0.00%
Sky 35	0.00%	0.00%	0.00%
Sky 36	1.37%	0.48%	0.03%
Sky 37	1.33%	0.48%	0.02%
Sky 38	0.80%	0.00%	0.05%
Sky 39	1.35%	0.48%	0.02%
Sky 40	1.35%	0.48%	0.04%
Sky 41	1.46%	0.48%	0.07%
Sky 42	0.82%	0.00%	0.02%
Sky 43	1.35%	0.48%	0.04%
Sky 45	1.34%	0.48%	0.01%
Sky 46	0.75%	0.00%	0.05%
Sky 47	1.36%	0.48%	0.03%
Sky 48	1.38%	0.48%	0.01%
Sky 49	0.72%	0.00%	0.03%
Sky 50	0.73%	0.00%	0.00%
Sky 51	1.35%	0.48%	0.02%
Sky 52	1.36%	0.48%	0.01%
Sky 53	0.76%	0.00%	0.03%
Sky 54	1.43%	0.48%	0.05%
Sky 55	1.34%	0.48%	0.02%
Average	0.69%	0.19%	0.02%

As shown in tables above, the power loss for the sender (Radio Tx) is better than the Standard in many motes (nodes), as the power lost in Radio TX and Radio RX is relatively low. The total loss in power is 0.19% for Radio TX and 0.02% for Radio RX. This is an improvement by merging Sub Byte and Shift Row, which results in the formation of a new sub instead of Mix Column. This leads to less consumption of time and power in the proposed algorithm. Additionally, these values are presented as charts below to show the difference between algorithms:

Figure 9 below shows the motes, Radio TX and Radio RX in proposed algorithm. The motes from 11 to 35 show no power lost for Radio TX and Radio RX, being 0. Meanwhile, other motes have values that represent the loss of power.

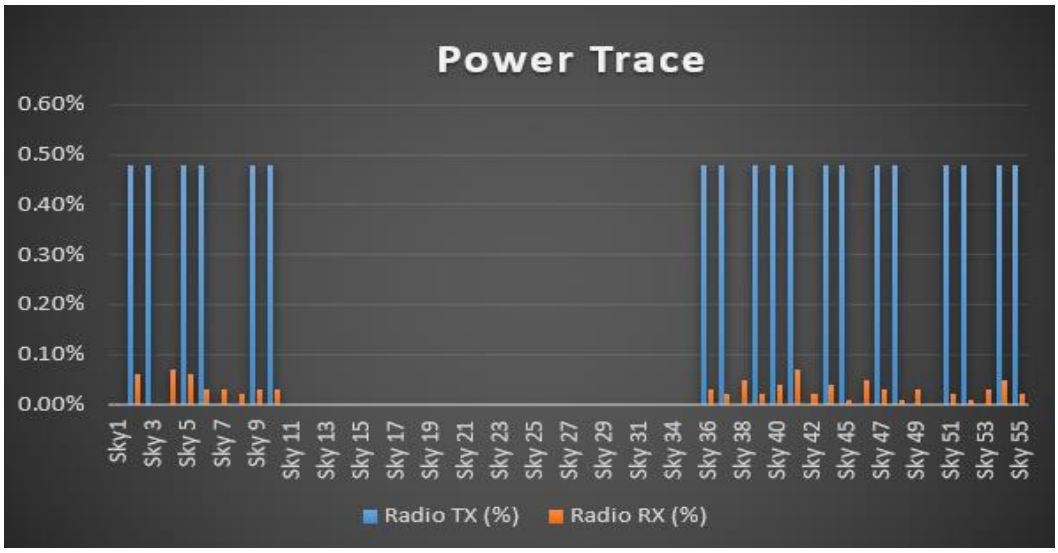


Figure 9. The power trace for the proposed algorithm

In addition, Figure 10 shows the motes, Radio TX and Radio RX in the standard algorithm. A large amount of power is lost in a lot of motes in Radio TX and Radio RX as compared to the proposed algorithm

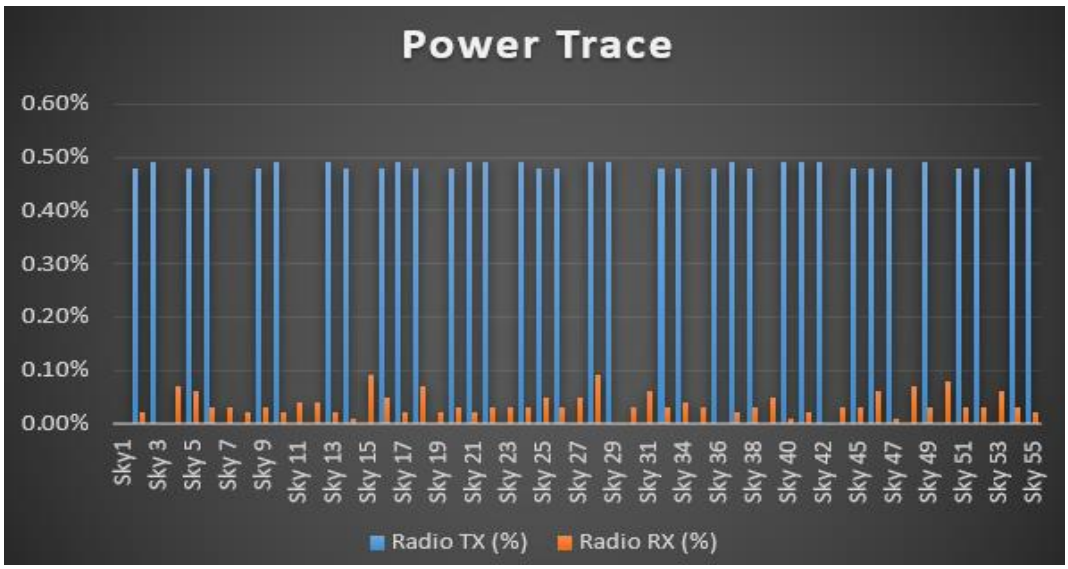


Figure 10. The power trace for the Standard algorithm

The result of the work analysis is presented using the Wireshark, Figure 11 represents the captured packet using the proposed AES lightweight algorithm for clients and servers, Ip Address for the source and destination, clarification of the throughput, and packet loss of Ad-Hoc network.

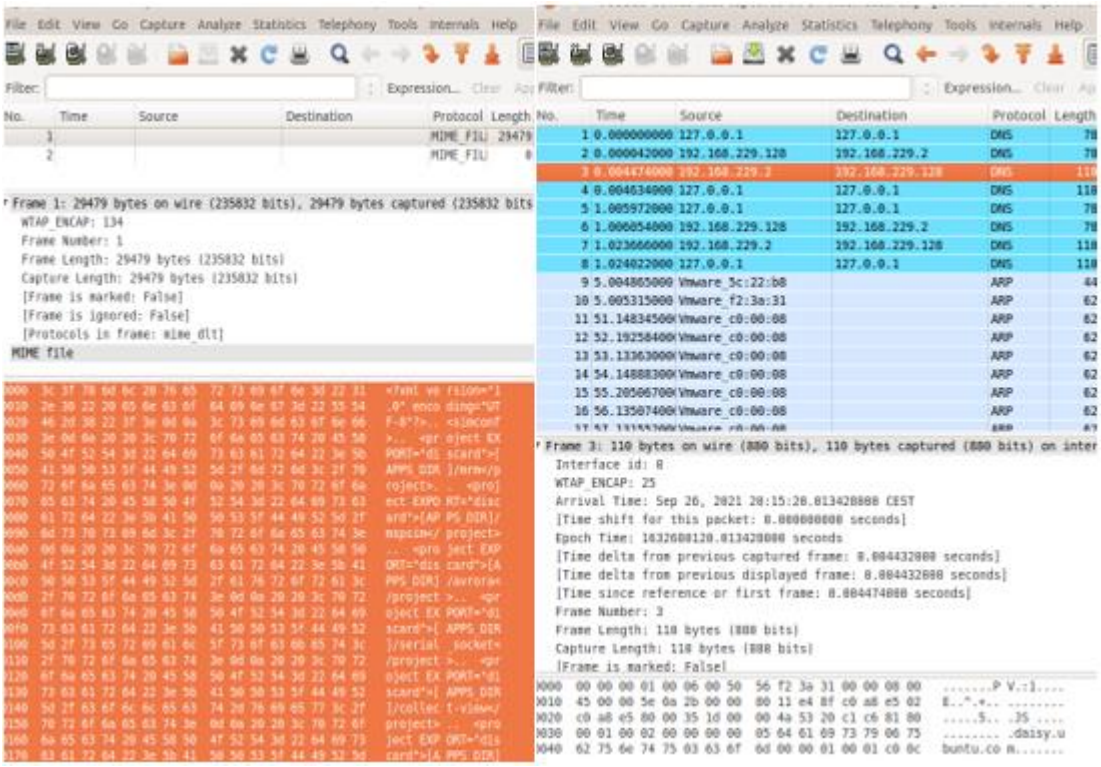


Figure 11. Wireshark Analysis Results

According to the simulation and Wireshark analysis, it is concluded that the time used in the proposed AES lightweight algorithm is less than that of the standard AES algorithm by **8 seconds and some milliseconds**, as shown in Figure 12.

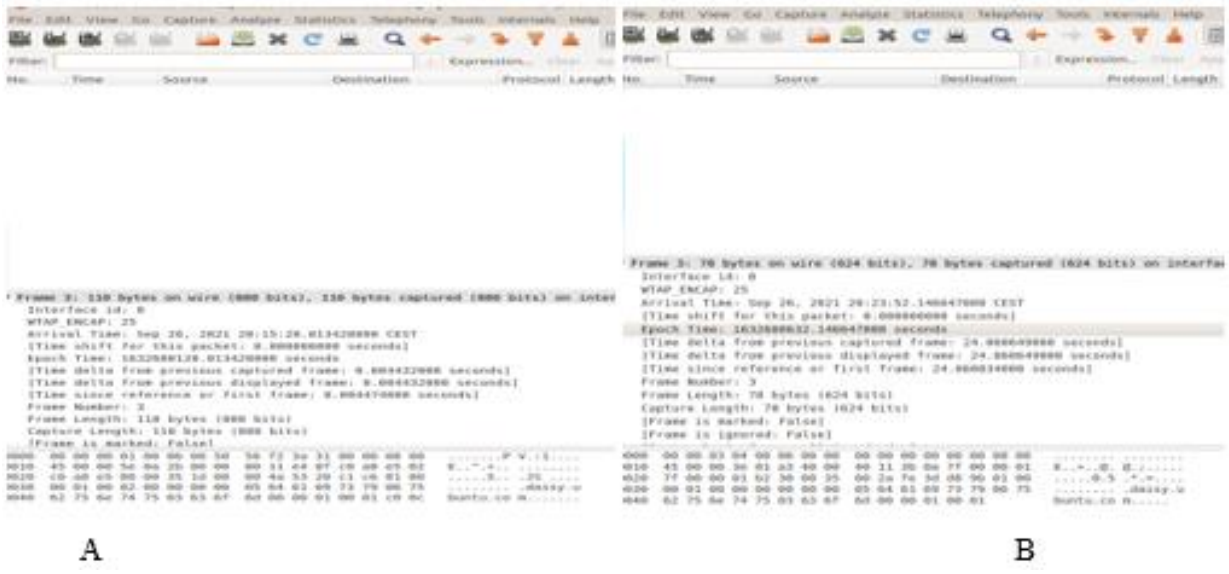


Figure 12. A. Arrival time for the proposed algorithm, B. Arrival time for the Standard algorithm.

4. Comparison of Previous Works

The present work is considered an extension of previous works, with the main objective of solving security problems in Ad-hoc networks. This section draws a comparison between this work and earlier related researches, as summarized in Table 3.

Table 3
Comparison of previous works

Ref No.	Algorithm used	Technology used	Environment work	Implementation tool	Enhance security	Enhance time and power consuming
Usman et al. (2017)	Secure IoT (SIT).	mix of feistel and uniform substituting-permutating networks.	IOT	MATLAB	✓	×
Kunchok and Kirunbanand (2018)	Lightweight hybrid encryption system with ECDH and AES.	ECDH key exchange mechanism to generate keys and establish connections, digital signatures for authenticating, followed by the AES algorithm to encrypt and decrypt user data files.	IOT	IOT	✓	×
Aziz and Singh (2019)	efficient lightweight security scheme (LSS).	CS method used to solve security issue and energy.	IOT	Intel Berkeley research lab	✓	×
Mohanty et al. (2018)	lightweight integrated Blockchain (ELIB)	ELIB with public blockchain for enhancing security and privacy.	IOT	Block chain	✓	×
Keshav Kumar et al. (2020)	AES lightweight algorithm	AES lightweight algorithm to encrypt voice signal on peer-to-peer communication.	IOT	FPGA	✓	×
Fadhil et al. (2021)	Lightweight AES encryption algorithm	Lightweight AES encryption algorithm to provide in IOT system. It is worked on Raspberry	IOT	Raspberry	✓	×
Hussein M. et al. (2022)	AES lightweight algorithm	Lightweight AES encryption algorithm to provide security in IOT system. However, enhance the delay in time	IOT	Asp.net	✓	✓
The proposed work	AES lightweight algorithm	Using the outputs of Sub byte and Shift row to make an exclusive or (XOR) to be used instead of the MixColumns	Ad-Hoc	Cooja	✓	✓

5. Comparison of Standard AES and Enhanced AES Lightweight Algorithm

Table 4
Comparison between standard AES and enhanced AES lightweight algorithm

Item	Standard AES	Enhanced AES lightweight
Security	High	High
Time	Using a lot of time	Using a little time
Key Exchange Algorithm	Classical Algorithms	Lightweight algorithms
Packet loss	More	Less
Power saving	Less	More

5. Conclusion

Lightweight cryptography is a technique used for securing information in a developed manner that uses low assets and gives high throughput while consuming less power. This paper proposed an AES lightweight algorithm for reducing the amount of time and power that is consumed in ad hoc network. An XOR operation is conducted between the Sub byte and the Shift row, resulting in a new sub. This sub is used as a replacement of the Mix Column, thereby eventually resulting in the reduction of overall time and power consumption. The results for the proposed AES lightweight algorithm are found to be better than the standard AES algorithm in power and time consumption when transmitting the packets between nodes.

Author Contributions

Mustafa AL-handhal: Collected data and wrote the article.

Alharith A. Abdullah: Planned the analysis and wrote the article.

Oğuz Ata: Made the statistical analysis.

Çağatay Aydin: Worked on simulations.

Conflicts of Interest

The authors declare no conflict of interest.

References

Abdullah, A. A., & Obeid, N. R. (2021). Efficient Implementation for PRINCE Algorithm in FPGA Based on the BB84 Protocol. In Journal of Physics: *Conference Series* , 1818(1) , 122-216. Retrieved from: http://psychologyandeducation.net/pae/index.php/pae/article/view/3215/2869

Abdullah, D.; Rahim, R.; Siahaan, A.P.U.; Ulva, A.F.; Fitri, Z.; Malahayati, M.; Harun, H. (2018). Super-Encryption Cryptography with IDEA and WAKE Algorithm. Journal of Physics: *Conference Series.*doi: https://doi.org/10.1088/1742-6596/1019/1/012039

Alyas, H. H., & Abdullah, A. A. (2021). Enhancement the ChaCha20 Encryption Algorithm Based on Chaotic Maps. In Next Generation of Internet of Things *Springer, Singapore,* 91-107. doi: https://doi.org/10.1007/978-981-16-0666-3_10

Aziz, A., & Singh, K. (2018). Lightweight security scheme for Internet of Things. Wireless personcommunication Issue, *Springer online available* doi:https://doi.org/10.1007/s11277-018-6035-4.

Basagni, S., Conti, M., Giordano, S., & Stojmenovic, I. (Eds.). (2004). Mobile ad hoc networking. *John Wiley& Sons* Retrieved from: https://doc.lagout.org/network/Mobile%20Ad%20Hoc%20Networking.pdf

Costa, D. G., Figuerêdo, S., & Oliveira, G. (2017). Cryptography in wireless multimedia sensor networks: A

survey and research directions. Cryptography, 1(1), 4. doi:https://doi.org/10.3390/cryptography1010004

Elmahdi, E., Yoo, S. M., & Sharshembiev, K. (2018). Securing data forwarding against blackhole attacks in mobile ad hoc networks. *In IEEE 8th annual computing and communication workshop and conference (CCWC),* 463-467. doi: https://doi.org/ 10.1109/CCWC.2018.8301683

Fadhil, Meryam Saad, Alaa Kadhim Farhan, and Mohammad Natiq Fadhil. (2021)"A lightweight AES Algorithm Implementation for Secure IoT Environment." *Iraqi Journal of Science* 62.8: 2759-2770. doi:10.24996/ijs.2021.62.8.29

Hussein M. Mohammad, Alharith A. Abdullah. (2022). Enhancement process of AES: a lightweight cryptography algorithm-AES for constrained devices, Journal of TELKOMNIKA Telecommunication Computing Electronics and Control, 551-560. doi: 10.12928/TELKOMNIKA.v20i3.23297

I.Vanda, L. Buttyán . (2003).Lightweight authentication protocols for low-cost RFID tags, *in Second Workshop on Security in Ubiquitous Computing–Ubicomp*. Retrieved from: http://www.mscs.mu.edu/~iq/papers/rfid/Lightweight%20Authentication%20protocols%20for%20low%20cost%20RFIDs.pdf

J. Daemen, V. Rijmen, and K. U. Leuven.(1999), AES Proposal: Rijndael. (NIST), *National Institute of Standards* Retrieved from: http://citeseerx.ist.psu.edu/viewdoc/summary?

Kumar, K., Ramkumar, K.R., Kaur, A., (2020) A Lightweight AES Algorithm Implementation for Encrypting Voice Messages using Field Programmable Gate Arrays, *Journal of King Saud University - Computer and Information Sciences.* doi: https://doi.org/10.1016/j.jksuci.2020.08.005

Mohanty, S.N.; Ramya, K.C.; Rani, S.S.; Gupta, D.; Shankar, K.; Lakshmanaprabu, S.K.; Khanna, A. (2020).An efficient Lightweight integrated Blockchain (ELIB) model for IoT security and privacy. *Future Generation. Computer System,* doi: https://doi.org/10.1016/j.future.2019.09.050

Muhammad Usman, Irfan Ahmed, M. Imran Aslam, Shujaat Khan and Usman Ali Shah.(2017). SIT: A Lightweight Encryption Algorithm for Secure Internet of Things, *International Journal of Advanced Computer Science and Applications,* 8(1). Retrieved from: https://arxiv.org/pdf/1704.08688.pdf

N. I. of Standards-(NIST), Advanced Encryption Standard (AES). (2001). *Federal Information Processing Standards Publication197.* Retrieved from: https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.197.pdf.

P.V.S. Shastry, A. Agnihotri, D. Kachhwaha, J. Singh and M.S. Sutaone.(2011). A Combinational Logic Implementation of S-Box of AES, *IEEE 54th Int. Midwest Symp on Circuits and Systems (MWSCAS),* 1-4. doi: https://doi.org/10.1109/MWSCAS.2011.6026559 .

S. Agwa, E. Yahya, and Y. Ismail. (2017). Power efficient AES core for IoT constrained devices implemented in 130nm CMOS, Proc. - *IEEE International Symposium on Circuits & System.,* 2–5. doi: https://doi.org/10.1109/ISCAS.2017.8050361

Schneier, B. (2015). Secrets and lies: digital security in a networked world. John Wiley & Sons. Retrieved,from:https://www.wiley.com/enus/Secrets+and+Lies%3A+Digital+Security+in+a+Networked+World%2C+15th+Anniversary+Edition-p-9781119092438

Tenzin Kunchok, Prof. Kirubanand V. B. (2018). A lightweight hybrid encryption technique to secure IoT data transmission, *International Journal of Engineering & Technology,* 7 (2), 236-240. doi: https://doi.org/ 10.14419/ijet.v7i2.6.10776

V.Rani, Dr. Renu Dhir. (2013). A Study of Ad Hoc Network: A Review, *International Journal of Advanced Research in Computer and Communication Engineering,* 3, Issue 3. Retrieved from: http://www.ijarcsse.com.

William Stallings.(2000). Cryptography and Network Security: Advanced Encryption Standard.Retrieved from: http://www.cs.man.ac.uk/~banach/COMP61411.Info/CourseSlides/Wk2.3.AES.pdf

.