International Journal for Modern Trends in Science and Technology, 9(05): 848-853, 2023

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0905145
Available online at: http://www.ijmtst.com/vol9issue05.html

Security Enhancement of Information using ultilayered Cryptographic Algorithm

S. Girish Gandhi, D. Sai Rushitha, G. Swapna, K. Pavithra, A. Nandhini

Department of Electronics and Communication Engineering, Narayana Engineering College, Nellore, Andhra Pradesh, India

To Cite this Article
S. Girish Gandhi, D. Sai Rushitha, G. Swapna, K. Pavithra, A. Nandhini. Security Enhancement of Information using ultilayered Cryptographic Algorithm. International Journal for Modern Trends in Science and Technology 2023, 9(05), pp. 848-853. https://doi.org/10.46501/IJMTST0905145

Article Info
Received: 21 April 2023; Accepted: 20 May 2023; Published: 24 May 2023.

ABSTRACT

As the technology is getting advanced continuously the problem for the security of data is also increasing. The hackers are equipped with new advanced tools and techniques to break any security systems. So, for protecting data communications, computer networks have led to development of several cryptography algorithms. The Advanced Encryption Standard (AES) is a computer security standard issued by the National Institute of Standards and Technology (NIST) intended for protecting electronic data. This algorithm can be used to encrypt/decrypt blocks of 128 bits and can use cipher keys of 128 bits wide (AES128). In this project, a hardware implementation of the AES 128 encryption algorithm is proposed using Xilinx ISE. In this algorithm encryption and decryption is done using same key. A unique feature of the proposed pipelined design is that the round keys, which are consumed during different iterations of encryption, are generated in parallel with the encryption process. This lowers the delay associated with each round of encryption and reduces the overall encryption delay of a plaintext block and improves speed of the algorithm.

KEYWORDS: ***Encryption, AES Decryption, Xilinx ISE, Security, Rounding, Key expansion***

1. INTRODUCTION

Cryptography is implemented in software and hardware throughout the world to encrypt sensitive data. It is essential for government computer security, cyber security, and electronic data protection. AES was created for the U.S. government with additional voluntary, free use in public or private, commercial, or noncommercial programs that provide encryption services. NIST specified the new AES algorithm must be a block cipher capable of handling 128-bit blocks, using keys sized at 128, 192 and 256 bits.

AES is short for Advanced Encryption Standard and is a United States encryption standard defined in Federal Information Processing Standard (FIPS) 192, published in November 2001. It was ratified as a federal standard in May 2002. AES is the most recent of the four current algorithms approved for federal us in the United States. One should not compare AES with RSA, another standard algorithm, as RSA is a different category of algorithm. Bulk encryption of information itself is seldom performed with RSA.RSA is used to transfer other encryption keys for use by AES for example, and for digital signatures.

AES is a symmetric encryption algorithm processing data in block of 128 bits. A bit can take the values zero and one, in effect a binary digit with two possible values

as opposed to decimal digits, which can take one of 10 values. Under the influence of a key, a 128-bit block is encrypted by transforming it in a unique way into a new block of the same size. AES is symmetric since the same key is used for encryption and the reverse transformation, decryption. The only secret necessary to keep for security is the key. AES may configure to use different key lengths, the standard defines 3 lengths and the resulting algorithms are named AES-128, AES-192 and AES-256 respectively to indicate the length in bits of the key. Each additional bit in the key effectively doubles the strength of the algorithm, when defined as the time necessary for an attacker to stage a brute force attack, i.e., an exhaustive search of all possible key combinations in order to find the right one.

Attackers can bypass cryptography, hack into computers that are responsible for data encryption and decryption, and exploit weak implementations, such as the use of default keys. However, cryptography makes it harder for attackers to access messages and data protected by encryption algorithms

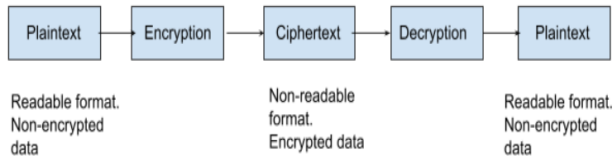


Fig 1 : Block diagram of cryptography

2. LITERATURE SURVEY

In [1], the authors have the authors have implemented a combination of Private-Public-Private key algorithm for encryption-decryption in two layers and a public key for key generation in both AES and DES algorithms. This implementation of AES provided a delay of 4.4 sec.

In [2], the authors present the analysis of various parameters of DES and AES encryption schemes. Based on the results the authors concluded that the AES takes less encryption and decryption time when compared to the DES algorithm.

The authors of [3] compared the AES and 3DES to determine the most secure algorithm.3DES is nothing but the equivalent to the application of DES three times. Compared to AES, 3DES is limited to encrypted key of length 56 bits , meaning that 3DES can have encryption key lengths of 168, 112, or 56 bits. 3DES has a shorter length and weaker encryption keys when compared to AES, and 3DES repeatedly applies encryption keys while AES does not. Hence the author concludes that the AES is the most secure algorithm undoubtedly.

In [4], the authors implemented AES on FPGA using five different techniques as CB-KB-S, CB-KB-P, CB-KC-S, CB-KC-P, CC-KC-S. From the results it was concluded that the CC-KC-S technique requires the greatest number of LUTs as it is implementing both its cipher module, key expansion module's S-box using combinational blocks. Because the techniques using BRAMs for their S-box implementation require a smaller number of LUTs as compared to techniques using combinational blocks for the S-box implementation.

In [5], the authors proposed an efficient hardware architecture design & implementation of Advanced Encryption Standard (AES). Xilinx ISE 12.3i software is used for simulation with Device XC6vlx240t of Xilinx Vertex Family. They tested each program with some of the sample vectors provided by NIST and concluded that the proposed implementation is suitable for the hardware critical applications.

The authors of [6] explains the survey is done on some of the more popular and interesting cryptography algorithms currently in use and their advantages and disadvantages. In this paper the authors analyze the encryption and decryption time of various algorithms on different settings of data. They considered the performance of algorithms like DES,3 DES, AES and Blowfish. The experimental results of the project shows that the Blowfish

3. PROPOSED METHOD

A. AES Algorithm

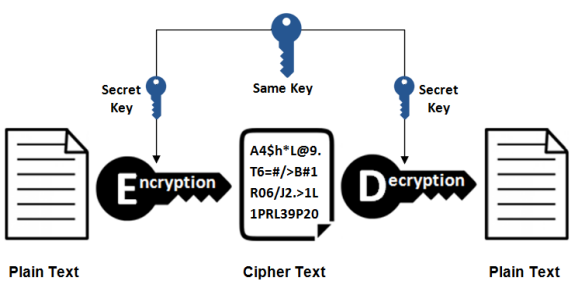


Fig 2 : Symmetric Encryption

The AES Encryption algorithm (also known as the Rijndael algorithm) is a symmetric block cipher

algorithm with a block/chunk size of 128 bits. Symmetric algorithm means it uses the same key for both encryption and decryption process. It converts these individual blocks using keys of 128, 192, and 256 bits. Once it encrypts these blocks, it joins them together to form the cipher text.

B. Operation of AES Algorithm

The AES encryption involves the process of encrypting a message with the key and provides a cipher text. To obtain the cipher text we need to perform several operations which involves the process of rounding and key expansion. The number of rounds in encryption and decryption depends upon the key length. In this paper, only the (AES-128) encryption scheme with 128-bit keys is considered. So there will be total 10 number of rounds.

Key length	Rounds
128 bits	10
192 bits	12
256 bits	14

Table 1 : Number of rounds

C. Basic Structure of AES Algorithm

The main operations of the encryption algorithm include: key expansion and rounding in which rounding consists of three steps as bytes substitution (Sub Bytes), the row shift (Shift Rows), column mixing (Mix Columns), and the round key adding (Add Round Key).

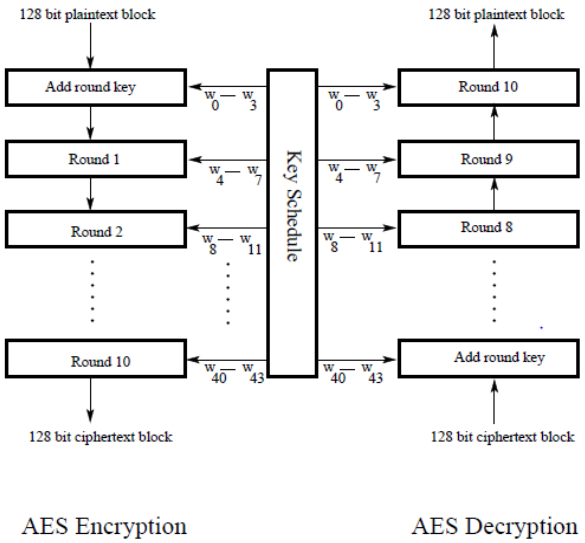


Fig. 3 : Basic Structure ofAES

D. Rounding Transformation

STEP 1 : In the Sub Bytes step, each byte in the matrix is updated using an 8-bit substitution box, the Rijndael S-box. This operation provides the non-linearity in the cipher**.**

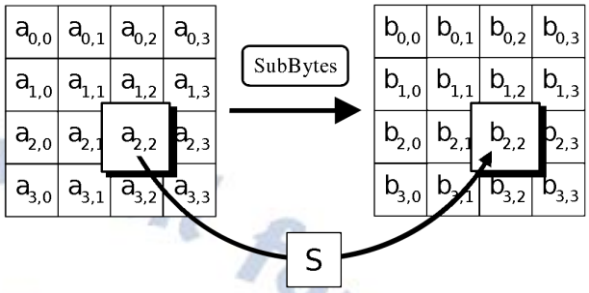


Fig 5 : Substitution bytes

	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
10	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
20	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
30	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
40	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
50	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
60	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
70	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
80	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
90	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a0	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b0	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c0	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d0	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e0	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f0	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Fig 6: S-box

STEP 2 : The Shift Rows transformation consists of

(i) not shifting the first row of the state array at all

(ii) circularly shifting the second row by one byte to the left

(iii) circularly shifting the third row by two bytes to the left

(iv) circularly shifting the last row by three bytes to the left

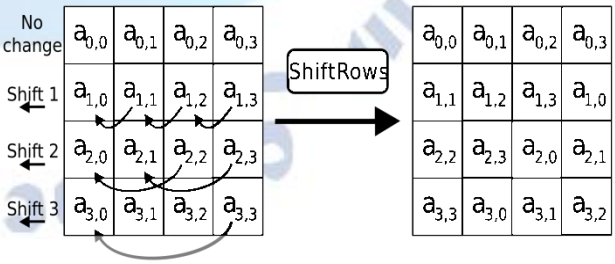
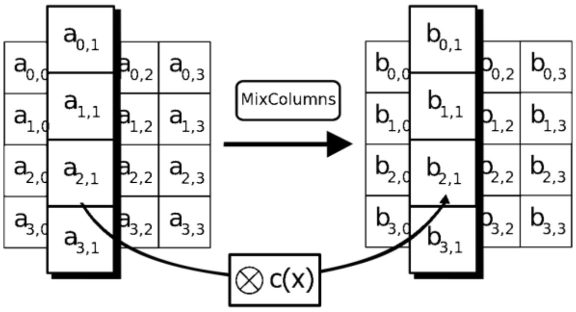


Fig 7 : Shift Rows

STEP 3:Another crucial step occurs of the state is Mix Column. The multiplication is carried out of the state. Each byte of one row in matrix transformation multiply by each value (byte) of the state column. In another word, each row of matrix transformation.



STEP 4 : In the Add Round Key step, the sub key is combined with the state. For each round, a sub key is derived from the main key using Rijndael's key schedule; each sub key is the same size as the state. The sub key is added by combining each byte of the state with the corresponding byte of the sub key using bitwise XOR.

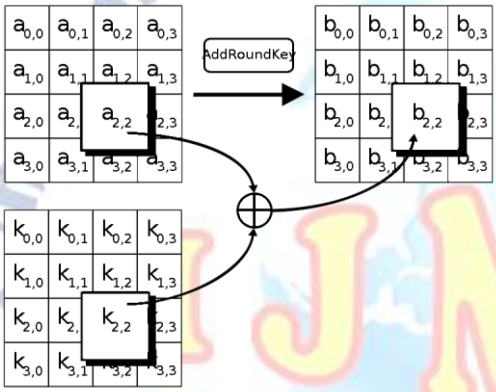


Fig 8 : Add round key step

E. Key Expansion

The key is also arranged in the form of an array of 4 × 4 bytes. The first word from first column of the array, and so on. The four column words of the key array are expanded into a schedule of 44 words.

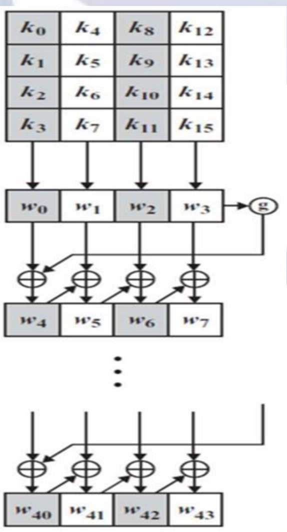


Fig 9 : Key Expansion

Each round consumes four words from the key schedule the first four words are used for adding to the input state array before any rounding processing can begin, and the remaining 40 words used for the ten rounds of processing that are required for the case a 128-bit encryption key.

4. EXPERIMENTAL RESULTS

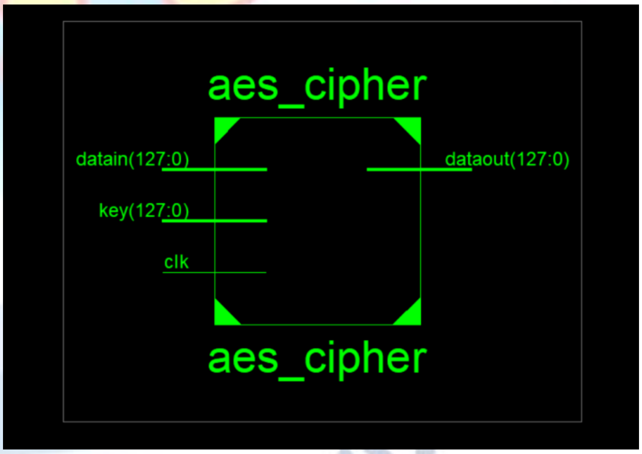
The experimental results show the RTL schematic of both encryption and decryption process and simulation results of AES algorithm.

Data in:
000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000
00000000000000000000000000001010

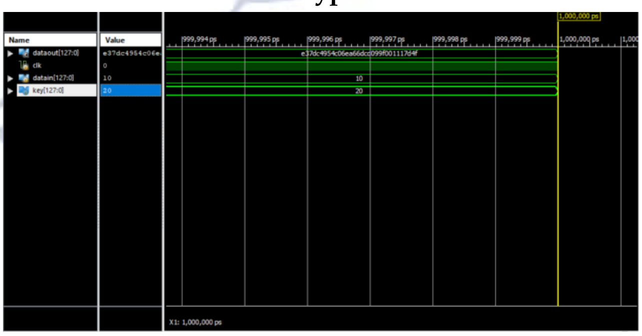
Key :
000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000
00000000000000000000000000010100

Cipher text : e37dc4954c06ea66dcc099f001117d4f

A. RTL Schematic of AES encryption



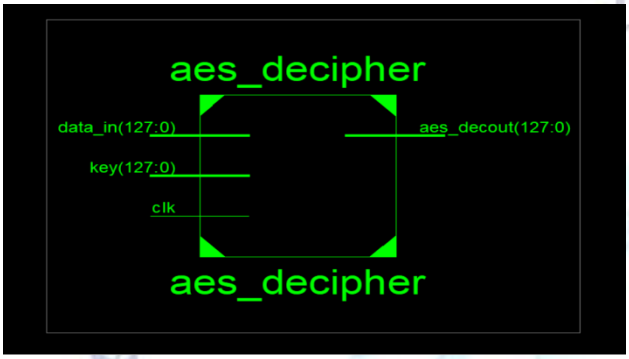
B. Simulation of AES encryption



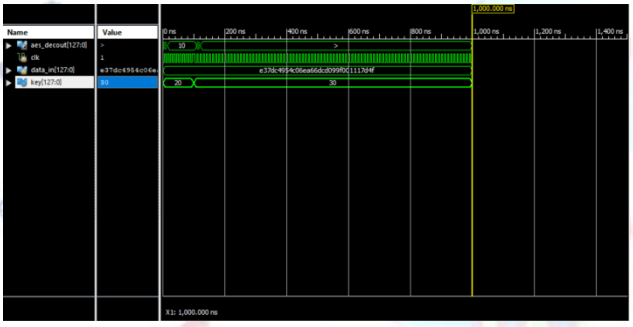
After performing encryption of data and key the obtained cipher text is shown above . Similarly, the

results of decryption are obtained by checking with different keys. When the key is matched with the original key then the output will be displayed otherwise there will be no data output . Through this who have the key accessibility can view the original data and others cannot. Hence, we will ensure data security.

C. RTL schematic of AES decryption



D. Simulation of AES decryption



5. CONCLUSIONS

In this work, we have compared our design implementation of the AES algorithm from the previous implemented designs of the AES algorithm. The parameters which are considered for comparison are LUTs ,SR flipflops and I/O.

A. Comparison of slice flipflops

Figure shows the comparison of slice flipflops with our design and with the previously implemented design. In paper [5] the researchers used 256 number of slice registers. Whereas in our design the number of flipflops used are 128.

Table 2: Device Utilization Summary

Logic Utilization	Used	Available	Utilization
Number of Slices	16803	42176	39%
Number of Slice Flipflops	128	84352	0%
Number of 4 input LUTs	32281	84352	38%
Number of bonded IOBs	385	576	66%
Number of FIFO 16/RAM16s	10	376	2%
Number of GCLKs	1	32	3%

B. Delay

The number of LUTs used in previous implemented designs[1] are more compared to the proposed design . Hence the delay is reduced and the speed of the operation is improved.

For Encryption :

Delay : 3.793ns

Total time for Xst completion : 177.00 secs

For Decryption :

Delay : 74.510ns

Total time for Xst completion : 247.00 sec

6. FUTURE SCOPE

The Advanced Encryption Standard (AES) is a widely used encryption algorithm that provides strong cryptographic security for various applications. As for the future scope of AES, here are a few potential areas where it could continue to be relevant:

A. Internet of Things (IoT) Security:

With the increasing number of connected devices in the IoT ecosystem, the need for secure communication and data privacy is also growing. AES could play a significant role in securing these devices and their communication channels.

B. Cloud Security: Cloud computing has become a popular platform for storing and processing sensitive data. AES could be used to provide end-to-end encryption for data stored in the cloud, thus ensuring its confidentiality and integrity.

C. Post-Quantum Cryptography: With the emergence of quantum computing, traditional cryptographic algorithms are becoming vulnerable to attacks. AES could be adapted to resist quantum attacks and continue to provide secure communication and data protection.

D. Work on selecting large key size :This AES algorithm can be implemented with a greater number of bits further. When we implement this algorithm with 192or 256 bits the overall delay will

be more compared to the implementation of 128 bits ,since the number of rounds will be more if the bit size increase. But implementation of aes with a greater number of bits is more secure and robust.

E. **Image Processing** : Possible improvements include getting back the decrypted image in color. To encrypt videos by extracting each frame and encrypting the images simultaneously. To encrypt the frame and the sounds simultaneously we can also use this AES algorithm for future reference.

F. **Blockchain Security**: Blockchain technology relies on cryptographic algorithms to secure transactions and data. AES could be used as a building block for designing secure blockchain systems.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] Mitali, Vijay Kumar and Arvind Sharma "A Survey on Various Cryptography Techniques" in International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Volume 3,Issue 4, July-August 2014 ISSN 2278-6856.https://www.ijettcs.org/Volume3Issue4/IJETTCS-2014-08-25-137.pdf

[2] M. Bedoui, H. Mestiri, B. Bouallegue, and M. Machhout. "A reliable fault detection scheme for the AES hardware implementation." In 2016 International Symposium on Signal, Image, Video, and Communications (ISIVC), pp. 47-52. IEEE,2016.https://ieeexplore.ieee.org/document/7893960

[3] RituTripathi,SanjayAgrawal "Comparative Study of Symmetric and Asymmetric Cryptography Techniques" in International Journal of Advance Foundation and Research in Computer (IJAFRC) Volume 1, Issue 6, June 2014. ISSN 2348 –4853http://www.ijirset.com/upload/2015/march/43_A_COMPARATIVE.pdf

[4] U.Farooq r,and M. F. Aslam. "Comparative analysis of different AES implementation techniques for efficient resource usage and better performance of an FPGA." Journal of King Saud University-no. 3 (2017): 295-302 https://www.sciencedirect.com/science/article/pii/S1319157816300143

[5] Noura Aleisa "Comparison of the 3DES and AES Encryption Standards" in International Journal of Security and Its ApplicationsVol.9, No.7 (2015), ISSN: 1738-9976 http://article.nadiapub.com/IJSIA/vol9_no7/21.pdf

[6] PushpLata, V. Anitha, "Multi-Layered Cryptographic Processor for Network Security" in International Journal of Scientific and Research Publications, Volume 2,Issue10,October 2012 1 ISSN 2250-3153.https://www.ijsrp.org/research-paper-1012/ijsrp-p1030.pdf