iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** VIII **Month of publication:** August 2021

DOI: https://doi.org/10.22214/ijraset.2021.37839

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VIII Aug 2021- Available at www.ijraset.com

Enhancing Encryption Algorithms through Parallelizing

Varre Divya Sai Manikanta[1], Penumarthi Satya Lohith[2]
[1, 2]*Vellore Institute of Technology, Vellore*

Abstract: ***Encryption Algorithms are necessary part of the data sharing today as every bit of data need encryption so that it could be transferred from one place to another without the fear of data leaking. Every lost bit of data puts the system to danger. Encryption algorithms compose of necessary steps involving a key that helps converting plain text to cipher text. All the steps must be performed carefully to ensure that the data encrypted is found back. Thus, many algorithms are made to run sequentially and in serial. This makes the algorithm to take much computation time.***
Keywords: Parallelize, encryption algorithms, multi-threading.

I. LITERATURE SURVEY

With the growing amount of data and communications, data exchange has increased. According to an estimate in 2017, around 15 million texts are sent each day. We live in a connected network where everything we type, speak or command are recorded. In such a place, we want our conversation and our activity to be safe and not ending up in a data market, waiting to be exploited by certain individuals or organizations. Data surpassed oil in value in May 2017. This brings to question the safety of how the data is stored is stored and transferred and that's where encryption comes in. Encryption is a field where the humans have done good contributions to the field and made up good algorithms that make data almost impossible to decrypt by unwanted eyes

A. IDEA

The International Data Encryption Algorithm (IDEA) algorithm is a mainstream secure key cryptographic algorithm. Thought was used as the symmetric figure which has well Privacy cryptosystem. Thought was to build up a solid encryption algorithm, which would supplant the DES method created in the U.S.A. in the seventies. It is likewise intriguing in that it altogether stays away from the utilization of any query tables or S-boxes. When the well-known PGP email and record encryption item was planned by Phil Zimmermann, the designers were searching for most extreme security. Thought was their first decision for data encryption dependent on its demonstrated structure and its incredible notoriety. gives elevated level security not founded on staying quiet about the algorithm, but endless supply of the secret key, is completely determined and effortlessly comprehended, can be used efficiently, may be exported world wide and is patent protected to prevent fraud and piracy.

B. RSA

RSA is an asymmetric process where public key and private key are used in this process. First of all sender send a message or data then the encryption process will start. Sender makes a cipher text by using public key and it send to the receiver. Then receiver will get the encrypted data then receiver will decrypt the encrypted data by the using of private key. Here the key is not shared. Hence the receiver will get the original data here 1024 bits or more length key is used to it's quite impossible to break the security. It gives security in high performance computer also. We can break this process in three-part Key Generation, Encryption and Decryption. The cipher text will follow this rule (C=Me mod n) and in decryption site (P=Cd mod n) where C= cipher text, P= plain text and M= Message.

C. Rivest Cipher 5

RC5 is ought to be a Symmetric block cipher used for encoding and decoding which utilizes similar cryptographic key. It contains fixed length bit arrangements i.e. plain text and cipher text. It is faster and reasonable for coding. All the required operational activities got to be the administrator's. RC5 varies with cores of different word length. The user can control the interchange of higher speed and protection. The number of rounds 'r' is the second parameter. The security can be managed by the user according to his information. The third parameter is key length which is in byte form. Although,

RC5 gives high security but it is difficult to execute. According to sub-ordinate pivots, RC5 features support evaluation of cryptographic quality.It is block symmetric key encryption algorithm planned in 1994. This algorithm is eminent for being straightforward and quick (by virtue of utilizing just crude PC tasks like XOR, move and so forth) and devours less memory. Contingent upon input content (block and key) size , number of rounds.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VIII Aug 2021- Available at www.ijraset.com

II. PROBLEM DESCRIPTION

Encryption Algorithm comprises of a number of steps that are generally performed sequentially. Our problem focuses on parallelizing these algorithms. The algorithms are analysed for ways to break it down to remove all the data dependencies and inter-dependent steps that can be resolved so as to be executed by different threads parallelly.

Hence two cases can be made from the above scenario

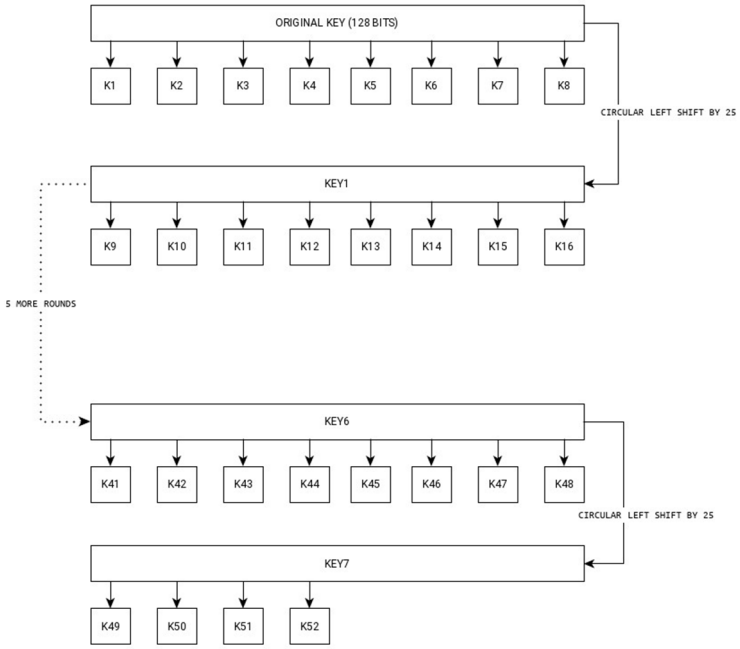
1) The algorithm steps as well as the pre-processing can be parallelized along with the instruction
2) The algorithm steps cannot be parallelized but pre-processing can be parallelized along with the instruction.
3) Neither the algorithm steps nor the pre-processing can be parallelized but instructions can be

III. SYSTEM DESIGN

A. IDEA

IDEA is a block cipher. It operates on blocks of text. According to IDEA standards, the input text for the algorithm is 64bits in length. The algorithm divides the input text into blocks of 16bits each and operates them with sub-keys of length 16bits. The key is 128bits in length. There is a total of 52 subkeys. The first 8 rounds use 6 sub-keys while the last round use.

1) *Key Generation Process:* The key is 128bits in length. This key is used to generate eight sub-keys. The initial six being sub-keys of the first round while the 2 keys be the first 2 sub-keys of the 2nd round . The original key is then shifted left by 25 and the resulting key is used to generate 8 other sub-keys.



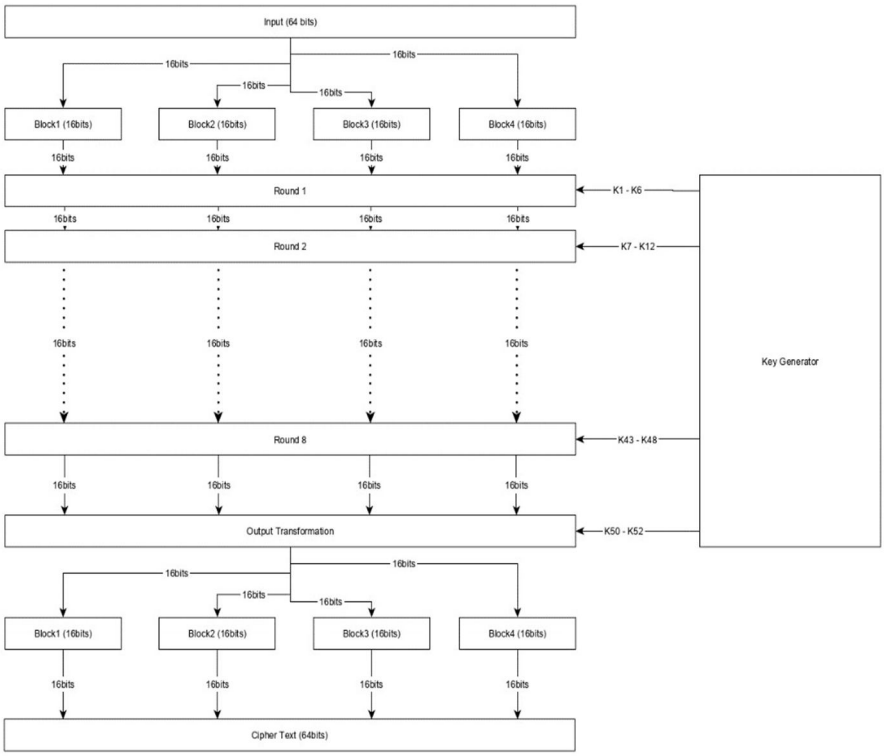
2) *Decryption Key Generation:* For generating keys for decryption, the following equation is followed:

$$K_1 = \frac{1}{K_{49}}$$
$$K_2 = -K_{50}$$
$$K_3 = -K_{51}$$
$$K_4 = \frac{1}{K_{52}}$$
$$K_5 = K_{47}$$
$$K_5 = K_{48}$$

Here, 1 / K_i indicates the multiplicative inverse for K_i and -K_i indicates the 2's compliment of K_i Algorithm

There are 9 rounds in IDEA. The first 8 are called as general rounds and they use 6 16bits sub-keys each. The operations performed in the general rounds are

- Multiplication Modulo $2^{16}+1$
- Addition Modulo $2^{16}+1$
- Xclusive OR



The general round is performed as:

- STEP 1 : Multiply PT1 and Key1
- STEP 2 : Add PT2 and Key 2
- STEP 3 : Add PT3 and Key 3
- STEP 4 : Multiply PT4 and Key K4
- STEP 5 : Result of Step 1 XOR result of step 3
- STEP 6 : Result of Step 2 XOR result of step 4
- STEP 7 : Multiply step 5 with Key 5
- STEP 8 : Add result of step 6 and step 7
- STEP 9 : Multiply result of step 8 with Key 6.
- STEP 10 : Add result of step 7 and step 9.
- STEP 11 : Result of steps 1 XOR result of step 9.
- STEP 12 : Result of steps 3 XOR result of step 9.
- STEP 13 : Result of steps 2 XOR result of step 10.
- STEP 14 **:** Result of steps 4 XOR result of step 10.

The last round is termed as Output Transformation. It uses 4 16bits sub-keys each. The operations performed in the Output Transformation round are

- Multiplication Modulo $2^{16}+1$
- Addition Modulo $2^{16}+1$

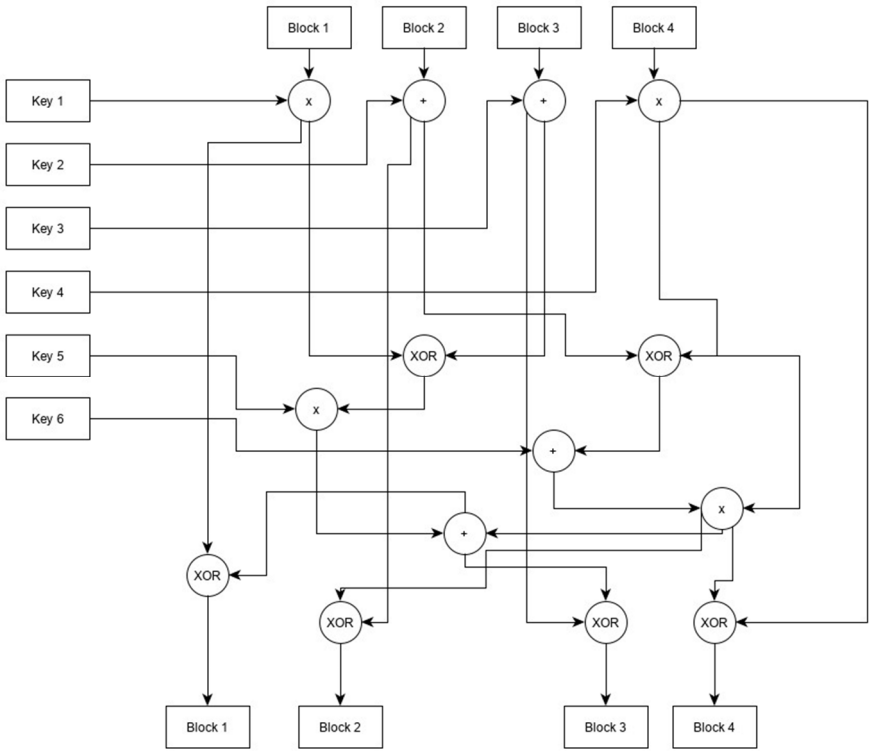
3) Output Transformation Round

a) Step 1: Multiply R1 with Key 49.

b) Step 2: Add R2 and Key 50.

c) Step 3: Add R3 and Key 51.

d) Step 4: Multiply R4 and Key 52.



4) Serial Execution Approach: In order to execute the code, the input was considered as a text containing ASCII characters. All these characters would lie between 1 – 128 only. Thus, all of these characters would take a maximum of 8bits space in the memory. Hence, the plain text was appended with extra spaces are added to make it of length which is a multiple of 8. Thus, the new text that was formed would occupy a memory size which is a multiple of 64bits. The text was then converted to a binary format and divided into pieces of 64bits.

Each piece was taken and divided into blocks of 16bits each and the entire 9 rounds were performed on them. The resulting blocks were concatenated and then appended to an ongoing **cipher text** string.

The decryption keys are now generated and the cipher text block is sent for decryption.

Finally, the resulting string from decryption is trimmed and matched with the original plaintext.

5) Parallel Execution Approach

The coding language used here was Java SE 12. In order to divide the task into various threads, the *ExecutorService* class was called.

In Java, the maximum number of threads that can execute concurrently is the number of processors in the system. Hence, the number of processors was found out by calling

Runtime.getRuntime().available Processors(). IDEA consists of 14 steps that should be carried out sequentially with one result being dependent on the other. Hence, the core processing of the algorithm cannot be altered. In order to parallelize the procedure, the following things were broken down and fed to other threads to execute.

a) Key Generation

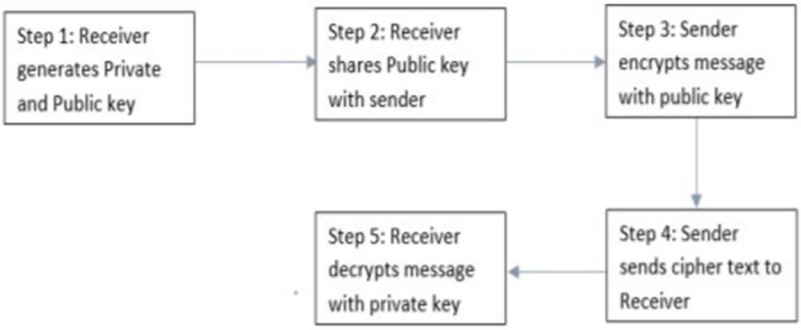
b) Input text going through Encryption Process

c) Decryption Key Generation

B. RSA

PUBLIC KEY BASED CRYPTO ALGORITHMIC APPROACH

Public key based cryptographic calculations utilize two sort of keys for encryption and decryption. It is consequently these calculations are alluded to as Asymmetric Cryptographic Algorithms. For secure information correspondence among sender and collector, beneficiary creates private and public key. Then, at that point collector sends the public key to the sender over a got medium and solicitations him to start the correspondence. Presently, utilizing public key sender encodes the information and sends the code message to recipient. With the assistance of comparing private key, beneficiary decodes the code message and gets the first message. The entire system is displayed in beneath figure as a stream chart.



RSA chips away at the numerical idea of factorization of exceptionally enormous number, for example discovering two enormous indivisible numbers whose item is that number. The size of RSA keys is taken huge enough to make for all intents and purposes hard to distinguish these numbers. This makes factorization to require some investment in spite of the utilization of most popular calculations. The RSA security measure is profoundly subject to the size of the key taken which expands the irregularity of the assurance of components of the number. It has been surveyed that if the key length is of 1024 pieces or more, it is almost difficult to penetrate the security of RSA encryption in any event, when working with elite PCs. RSA calculation works in three stages Key Generation stage, Encryption stage and Decryption stage.

C. Rivest Cipher 5

RC5 is a symmetric key block encryption algorithm designed by Ron Rivest in 1994. It is notable for being simple, fast (on account of using only primitive computer operations like XOR, shift, etc.) and consumes less memory.

Key: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Plain Text: 00000000 00000000
Cipher Text: EEDBA521 6D8F4B15

RC5 is a block cipher and addresses two-word blocks at a time. Depending on input plain text block size, number of rounds and key size, various instances of RC5 can be defined and each instance is denoted as RC5-w/r/b where w=word size in bits, r=number of rounds and b=key size in bytes.

1) Algorithm

a) Step-1: Initialization of constants P and Q.

RC5 makes use of 2 magic constants P and Q whose value is defined by the word size w.

WORD SIZE (BITS)	P (HEXADECIMAL)	Q (HEXADECIMAL)
16	b7e1	9e37
32	b7e15163	9e3779b9
64	b7e151628aed2a6b	9e3779b97f4a7c15

b) Step-2: Converting secret key K from bytes to words.

Secret key K of size b bytes is used to initialize array L consisting of c words where c = b/u, u = w/8 and w = word size used for that particular instance of RC5. For example, if we choose w=32 bits and Key k is of size 96 bytes then, u=32/8=4, c=b/u=96/4=24.
L is pre initialized to 0 value before adding secret key K to it. for i=b-1 to 0

L[i/u] = (L[u/i] <<< 8) + K[i]

c) Step-3: Initializing sub-key S.

Sub-key S of size t=2(r+1) is initialized using magic constants P and Q.
S[0] = P
for i = 1 to 2(r+1)-1

S[i] = S[i-1] + Q)

d) Step-4: Sub-key mixing.

The RC5 encryption algorithm uses Sub key S. L is merely, a temporary array formed on the basis of user entered secret key.

Mix in user's secret key with S and L.
i = j = 0 A = B = 0 do 3 * max(t, c) times:

A = S[i] = (S[i] + A + B) <<< 3 B = L[j] = (L[j] + A + B) <<< (A + B) i = (i + 1) % t j = (j + 1) % c

e) Step-5: Encryption.

We divide the input plain text block into two registers A and B each of size w bits. After undergoing the encryption process the result of A and B together forms the cipher text block.

A = A + S[0] B = B + S[1] for i = 1 to r do:

A = ((A ^ B) <<< B) + S[2 * i] B = ((B ^ A) <<< A) + S[2 * i + 1] return A, B

f) Step-6: Decryption.

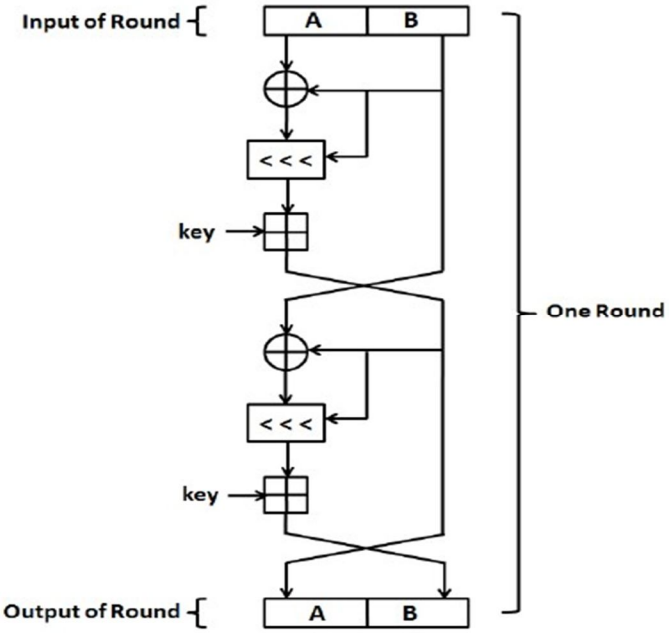
for i = r down to 1 do:

a. = ((B - S[2 * i + 1]) >>> A) ^ A

A = ((A - S[2 * i]) >>> B) ^ B

g) = B - S[1] A = A - S[0] return A, B

Block diagram for the one-round in RC5



IV. CONCLUSION

A. *Summary*

We tested this algorithm to the very extent. From a bare minimum of 60 characters to a maximum of 15,000 characters. The algorithm was programmed to break the instruction stream into small chunks that are vectorized and split into tasks by the threading service. In cases of symmetric encryption, the key generation / expansion process was also parallelized to give a better and a more efficient code.

B. *Conclusion*

1) Advantages of Parallelization

a) Less execution times
b) Efficient code
c) Distribution of instructions to threads automated

2) Disadvantages

a) Overhead cost outweighs the time saved in case of small strings
b) Memory usage multiplies by the number of threads/processors used
c) Weight of performance on processor increases exponentially with the increase in number of processors

C. *Future Study*

With the hope of better parallelization algorithms and improvement in the encryption algorithms, this process can be accelerated much faster than its usual speed. Data dependency among the steps must be made a little less complicated so that they are easy to be modularised into various components. Certain algorithms must be developed that actually parallelize the core components of these algorithms.

REFERENCES

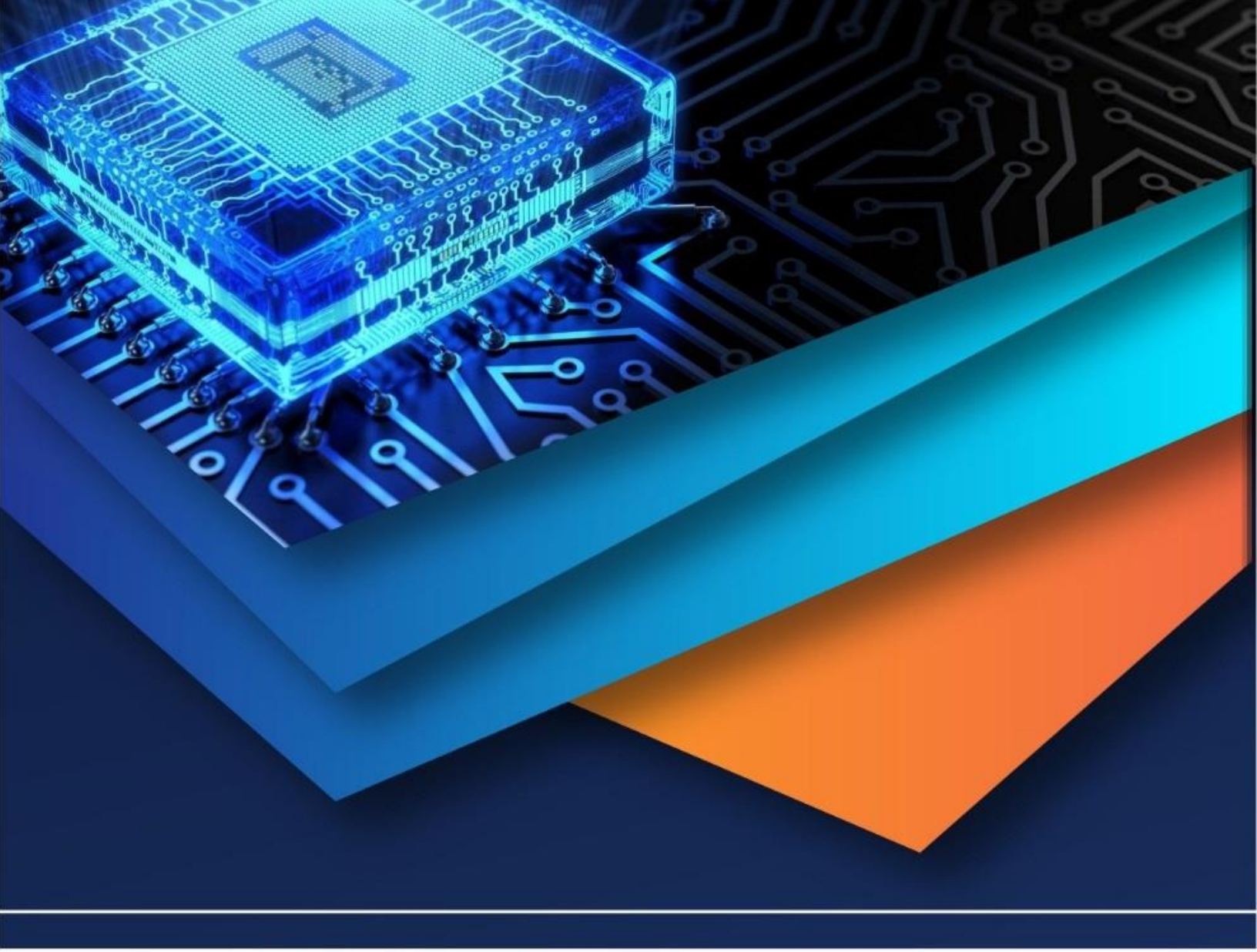
[1] Basu, Sandipan. (2011). INTERNATIONAL DATA ENCRYPTION ALGORITHM (IDEA) – A TYPICAL ILLUSTRATION. Volume 2, No. 7, July 2011 Journal of Global Research in Computer Science
[2] Xin Zhou, Xiaofei Tang-- Research and implementation of RSA algorithm for encryption and decryption Published in: Proceedings of 2011 6th International Forum on Strategic Technology
[3] Ronald L. Rivest The RC5 encryption algorithm Part of the Lecture Notes in Computer Science book series (LNCS, volume 1008)

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VIII Aug 2021- Available at www.ijraset.com

Appendix

Appendix 1 : Test Cases

1) 59 characters Sonos Port has a built-in digital-to-analog converter (DAC)
2) In 2017, Apple introduced Face ID for the iPhone X as a replacement to Touch ID, its fingerprint technology
3) Pre-orders for the Sonos Port begin today, and it'll be available starting September 12 in the U.S., with a global rollout to follow early next year.
4) If you've played with the most recent smartphones from Samsung, Huawei and other Android manufacturers, you know that in-screen fingerprint readers already work quite well.
5) A lot of the Port's specs are similar to the outgoing Connect's, but the more compact package, and its new matte-black look seem much better in terms of integrating unobtrusively with your existing setup.
6) The asking price may seem a bit steep for what is essentially a connectivity accessory, but the Sonos Connect basically replaces a DAC entirely, which can be quite expensive on its own, and uniquely provides Sonos connectivity and streaming capabilities as well.
7) The Sonos Port includes two built-in 10/100 Mbps Ethernet ports, so you can wire right into your router if you need a more reliable connection, and it has a 12V power trigger, which means it'll automatically turn on stereo or receiver equipment when they're connected and in standby mode.
8) The Sonos Port includes two built-in 10/100 Mbps Ethernet ports, so you can wire right into your router if you need a more reliable connection, and it has a 12V power trigger, which means it'll automatically turn on stereo or receiver equipment when they're connected and in standby mode. Sonos Port has a built-in digital-to-analog converter (DAC)
9) The Sonos Port includes two built-in 10/100 Mbps Ethernet ports, so you can wire right into your router if you need a more reliable connection, and it has a 12V power trigger, which means it'll automatically turn on stereo or receiver equipment when they're connected and in standby mode. If you've played with the most recent smartphones from Samsung, Huawei and other Android manufacturers, you know that in-screen fingerprint readers already work quite well.
10) The asking price may seem a bit steep for what is essentially a connectivity accessory, but the Sonos Connect basically replaces a DAC entirely, which can be quite expensive on its own, and uniquely provides Sonos connectivity and streaming capabilities as well. The Sonos Port includes two built-in 10/100 Mbps Ethernet ports, so you can wire right into your router if you need a more reliable connection, and it has a 12V power trigger, which means it'll automatically turn on stereo or receiver equipment when they're connected and in standby mode.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY