Mahaviracharya Encryption Algorithm (MEA) Comparing with AES, Blowish Using Short Length Data

Nagaraju Bollepalli
Assistant Professor (c),
Ph.D in University College of Engineering,
Osmania University.

Prof. Ramkumar.P
Retd. Professor,
Dept. of CSE,
University College of Engineering, OU.

Abstract: *In these days of new cyber-attacks, the task of creating a new algorithm can be considered very important. Mahaviracharya Encryption Algorithm is a newly designed cryptography algorithm. Mahaviracharya Encryption Algorithm is being compared with existing algorithms AES and Blowfish. The Experiment results are described in this paper.*

Keywords: *Symmetric Encryption Algorithm, Rasilabdacheda misravibhaga sutram Mahaviracharya Encryption Algorithm.*

I. INTRODUCTION

Cryptography techniques are critical for providing data secrecy through encryption. Algorithms are classified into two types: symmetric cryptosystems and asymmetric cryptosystems. The Mahaviracharya encryption algorithm is both symmetric and block cypher in nature.

Mahaviracharya was a renowned mathematician who was born in India. He was born in the ninth century. He wrote an algebra and geometry textbook. Ganitha Saara Sangraha is the title of the book. He discusses a formula in this book. Specifically, "Rasilabdacheda misravibhaga sutram" is used to separate the undisclosed dividend integer, divisor, and quotient from their combined sum. [1].

Rasilabdacheda misravibhaga sutram:“any suitable optionally chosen number subtracted from the given combined sum happens to be the divisor. On dividing, by this divisor as increased by one, the remainder (left after subtracting the optionally chosen number from the given combined sum), the required quotient is arrived at. The very same remainder (above mentioned), as diminished by (this) quotient becomes the required dividend number” [1].

Rasilabdacheda misravibhaga sutram was used to create a new cypher known as the Mahaviracharya Encryption Algorithm (MEA). In this approach, original text is treated as a divisor (a), secret key as a quotient (c), and encrypted text as a combined total (x). We must choose a number while decrypting the cypher text x in order to retrieve the plain text a, i.e. divisor in the formula (k). However, for different k numbers, we will discover separate a, b, and c values. So, in order to obtain an accurate number here, we must first choose an adequate k value. In the decryption algorithm, a formula for determining the optimal k value is provided below. [2]

A. Encryption Method

$$b=a * c$$

$$x = a + b + c$$

x is the cipher text

B. Decryption Method

$$k=c(x+1) / (c+1)$$

$a=x-k$

a is the plain text.

We can change above decryption algorithm. The revised decryption algorithm is:

$$a = (x - c)/(c + 1)$$

II. BACKGROUND

We published a paper with title "Mahaviracharya Encryption Algorithm (MEA) with Modified Counter Mode and Comparing with AES Algorithm" [3]. This paper describes a method for implementing counter mode on the Mahaviracharya Encryption Algorithm. In counter mode, a random number is typically assigned to the counter and then added by one for each subsequent block. Counter mode is, as it is, not yet utilized in MEA. The Mahaviracharya Encryption Algorithm treats the full plain text as a single block. Because counter mode is only used for that particular block, increasing the counter number is not required. [3].

In Mahaviracharya Encryption Algorithm plain text (P), counter value(R), secrete key (K) are variable length values and must greater than or equal to 128 bits. Ciphertext, which is the output of MEA algorithm, length is equal to the plain text length.

The encryption and decryption methods are:

A. Encryption Method

1.Plain text: $P=p_1\ p_2\ p_3\ p_4\ \ldots p_m$

- P contains m number of digits and P should minimum 128 bits.

2.Counter value: $R=r_1\ r_2\ r_3\ r_4\ \ldots\ldots r_s$

- R is Randomnumber, contains s number of digits and R should minimum 128 bits.

3.Secrete Key: $K=k_1\ k_2\ k_3\ k_4\ldots k_q$

- K contains q number of digits and K should minimum 128 bits.

4. $B=R*K$

5. $X=R+B+K = x_1\ x_2\ x_3\ldots x_m\ x_{m+1}\ x_{m+2}\ldots x_{m+n}$

- X length (number of digits: $m+n$) should be greater than Plaintext (P) length (number of digits).
- If X length less than P length then X should be expanded to x_{m+n}.To expand X, in this paper, we used BigInteger(X.getBytes("us-ascii")) java code iteratively.

6. $X'= x_1x_2\ x_3\ \ldots\ldots x_m.$

7. Cipertext: $C=X' \oplus P$. [3]

B. Decryption Method

1.Cipertext: $C=c_1\ c_2\ c_3\ c_4\ \ldots c_m$

- C contains m number of digits and C should be minimum 128 bits.

2. Counter value: $R=r_1r_2\ r_3\ r_4\ \ldots\ldots r_s$

- R is Random[5] number, contains s number of digits and R should be minimum 128 bits.

3. Secrete Key: $K=k_1\ k_2\ k_3\ k_4....k_q$

- K contains q number of digits and K should minimum 128 bits.

4. $B=R*K$

5. $X=R+B+K = x_1\ x_2\ x_3\ldots\ldots\ x_m\ x_{m+1}\ x_{m+2}\ldots\ldots x_{m+n}$

- X length (number of digits: $m+n$) should be greater than cipertext (C) length (number of digits).
- If X length less than C length, then X should be expanded to x_{m+n}. To expand X, in this paper, we used BigInteger(X.getBytes("us-ascii")) java code iteratively.

6. $X'= x_1\ x_2\ x_3\ \ldots\ldots x_m$

7. Plain text: $P=X' \oplus C$.[3]

An article was published by Chiranth B O and Shashikala B. "The fresh comparative review among DES, 3DES, and AES was discussed in this paper using some factors those are key length, cypher type, block size, developed, cryptanalysis resistance, security, possibility key, possible ACSII printable character keys, required time to test completely possible keys at 50 billion seconds, and these showed that AES is better than DES and 3DES" [6].

Shaza D. Rihan and colleagues compared the DES and AES algorithms. "Their study compares the performance of two ciphers, AES and DES. For varying text sizes, the performance of encryption methods is calculated in terms of processing time, CPU utilization, and encryption throughput on the Windows and Mac environment. According to the simulation findings, AES is quicker than DES in terms of execution time for the two environments. AES outperforms DES in terms of throughput. For two systems, DES utilizes less CPU than AES" [7].

Shaify Kansal et al. published an article. "The research evaluates the performance of symmetric key ciphers for pictures and text. The findings reveal that the encryption time and decryption time of the AES is less than other ciphers because the no. of rounds is significantly smaller in AES, but 3DES has longer encryption time and decryption time since it uses the process 3 times. The encryption time or decryption time has an inverse relationship with throughput. As a result, AES has a higher throughput and 3DES has a lesser throughput than the other methods. AES consumes extra storage than the other symmetric key encryption techniques, but DES consumes less memory" [8].

Dr. Najib A. Kofahi submitted a paper in "International Journal of Security and Its Applications" [9] titled "An Empirical Study to Compare the Performance of Some Symmetric and Asymmetric Ciphers"[9]. They show empirical results acquired using a Java program of the Elliptic-Curve-Cryptosystem (ECC) as public key cipher and a set of conventional ciphers, notably Triple Data Encryption Standard (T_DES), Blowfish , and Advanced Encryption Standard (AES). Under Windows XP and Linux, performance is evaluated based on CPU execution time. They employed the "Java programming language, Java Cryptography Architecture (JCA), and Java Cryptography Extension in their implementation (JCE)" [9]. The performance of these ciphers is evaluated for secretkey creation, encryption, and decryption activities. The experimental findings reveal that the Blowfish method is the quickest of the three conventional ciphers.

In the "Journal of Global Research in Computer Science, Pratap Chandra Mandal published a paper titled Evaluation of Performance of Symmetric Key Algorithms: DES, 3DES, AES, and Blowfish. This study compares four of the most commonly used symmetric key algorithms: DES, 3DES, AES, and Blowfish. The following characteristics were compared: rounds, block size, key size, encryption / decryption time, CPU

process time in the form of throughput, and power consumption. These findings indicate that blowfish is more appropriate than AES. Java programming is used to implement the simulation software" [10].

In the "International Journal of Innovative Research in Computer and Communication Engineering, Srinivas B.L, Anish Shanbhag, and Austin Solomon D'Souza published an article. A Comparative Performance Analysis of DES and Blowfish Symmetric Algorithms is the title of the paper. This study compares the symmetric key encryption methods DES and Blowfish with different parameters such as data type, data size, and key size. The experimental work was done on the DES and Blowfish algorithms in order to demonstrate the performance of this method by adjusting some of these parameters. The execution time was investigated as a function of the encryption key length and file size; this has been described as complexity and security. Various data types were examined, and the roles of the data types were also highlighted. Based on the results of the execution, it is determined that encryption time is independent of data type and data size. According to the research, the encryption time is solely determined by the quantity of bytes in the file. It also found that encryption duration varied significantly to data size. Encryption time increases with increasing key size for all block cipher algorithms studied, but decreases with increasing key size for DES. Blowfish is the fastest block cipher, while DES looks to be the quickest of all ciphers tested" [11].

Apoorva and Yogesh Kumar submitted a paper titled "Comparative Study of Different Symmetric Key Cryptography Algorithms in the International Journal of Application or Innovation in Engineering and Management (IJAIEM). This study compares four of the most used symmetric key encryption algorithms: AES, Twofish, CAST-256, and Blowfish. The comparison considers the algorithm's behavior and performance when different data loads are employed, since their primary objective here is to evaluate the performance of algorithms under diverse situations. The following criteria are used in the comparison: speed, block size, and key size. The results suggest that the blowfish method outperforms other algorithms in terms of speed. However, when the data size is very little, this distinction is not readily apparent. However, for files more than 100KB in size, it is quite evident" [12].

Table.1 summaries various studies on the performance analysis of symmetric cyphers.

S.No	Title	Journal	Authors	Algorithms	Parameters	Result
1	Survey of Performance Comparison of DES, 3DES and AES Algorithms	International Journal of Data & Network Security	Chiranth B O, Shashikala B	DES, 3DES and AES	key length, cipher type, block size, cryptanalysis resistance, security, possibility key.	AES
2	A Performance Comparison of Encryption Algorithms AES and DES	International Journal of Engineering Research & Technology	Shaza D. Rihan, Ahmed Khalid	AES and DES	processing time, CPU usage and encryption throughput	AES
3	Performance Evaluation of Various Symmetric	International Conference on Parallel,	Shaify Kansal, Meenakshi Mittal	DES, 3DES and AES	Encryption time and decryption time	AES

	Encryption Algorithms	Distributed and Grid Computing.				
4	An Empirical Study to Compare the Performance of some Symmetric and Asymmetric Ciphers	International Journal of Security and Its Applications	Dr. Najib A. kofahi	3DES, AES, Blowfish	Execution time	Blowfish
5	Evaluation of performance of the Symmetric Key Algorithms: DES, 3DES ,AES and Blowfish	Journal of Global Research in Computer Science	Pratap Chandra Mandal	DES 3DES AES and Blowfish	rounds, block size, key size, encryption time decryption time CPU process time in the form of throughput and power consumption	Blowfish
6	A Comparative Performance Analysis of DES and BLOWFISH Symmetric Algorithm	International Journal of Innovative Research in Computer and Communication Engineering.	Srinivas B.L, Anish Shanbhag Austin Solomon D'Souza	DES and Blowfish	Performance analysis applying different data types, data sizes and key sizes.	Blowfish
7	Comparative Study of Different Symmetric Key Cryptography Algorithms	International Journal of Application or Innovation in Engineering & Management.	Apoorva , Yogesh Kumar	AES, Twofish CAST-256 and Blowfish	speed, block size, and key size	Blowfish

According to the findings of the preceding articles, the AES and Blowfish algorithmsare performing well. As a result, we want to compare the Mahaviracharya Encryption Method (MEA) with AESand Blowfish algorithms.

III. EXPERIMENT RESULTS AND ANALYSIS

In "Mahaviracharya Encryption Algorithm (MEA) with Modified Counter Mode and Comparing with AES Algorithm" [3] paper, we presented the tests performed on the Advanced Encryption Algorithm (AES), Mahaviracharya Encryption Algorithm (MEA). In addition, in this paper, we assessed the experiment outcomes. We used encryption time and decryption time as parameters to compare these two techniques. Based on this data, we could concluded that the Mahaviracharya Encryption Algorithm (MEA) executes faster than the Advanced Encryption Algorithm (AES).

Now we conducted experiments on Advanced Encryption Algorithm (AES), Blowfish algorithm, and Mahaviracharya Encryption Algorithm (MEA)using small data sizes 128-bits, 256-bits, 384-bits, 512-bits, 640-bits, 768-bits, 896-bits, 1 KB, 2 KB, 3 KB, 4 KB, and 5 KB of data as plain text.

For this experiment, data files of 128-bits, 256-bits, 384-bits, 512-bits, 640-bits, 768-bits, 896-bits, 1 KB, 2 KB, 3 KB, 4 KB, and 5 KB are separated into two groups. The data sizes in the first set are 128-bits, 256-bits, 384-bits, 512-bits, 640-bits, 768-bits, and 896-bits. Each data block size is raised by 128 bits in this group. The second set includes data sizes of 1KB, 2KB, 3KB, 4KB, and 5KB. Each data block size is raised by 1 KB in the second group. The results of the experiments are detailed below. Encryption and decryption times for several text data sizes are computed here. To carry out this experiment, a Jdk windows-x64 bin java language, Apache Net Beans IDE, Windows 10 pro 64 bit operating system, and an Intel(R) Core(TM) i5-4310U CPU @ 2.00GHz GHz laptop are employed.

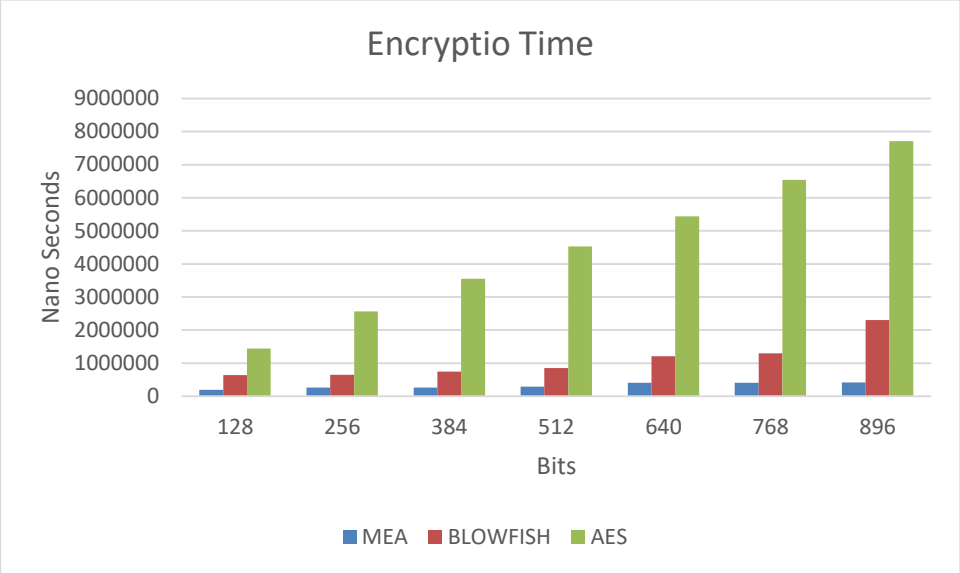
The First Group Results:

We calculate the encryption times of text messages of various length using the Advanced Encryption Algorithm (AES), the Blowfish cipher, as well as the Mahaviracharya Encryption Algorithm (MEA). The specifics are shown in the Table.2. The average data size for the data items under consideration is 512 bits, the average encryption time for Mahaviracharya Encryption Algorithm (MEA) is 322151.4 Nano seconds, the average encryption time for Blowfish Algorithm is 1103365.714 Nano seconds, and the average encryption time for Advanced Encryption Algorithm (AES) is 4540908 Nano seconds. This table clearly shows that MEA is faster than Blowfish, Advanced Encryption Algorithm (AES).

Table.2: The Encryption Procedure

	Data Size	MEA	BLOWFISH	AES
	128 bits	197240 ns	644400 ns	1444461 ns
	256 bits	264800 ns	654820 ns	2563050 ns
	384 bits	266440 ns	745720 ns	3552021 ns
	512 bits	294700 ns	855800 ns	4525564 ns
	640 bits	406380 ns	1215440 ns	5443760 ns
	768 bits	409580 ns	1303060 ns	6542900 ns
	896 bits	415920 ns	2304320 ns	7714599 ns
Average:	**512 bits**	**322151.4 ns**	**1103365.714 ns**	**4540908 ns**

*ns is an abbreviation for Nanoseconds.

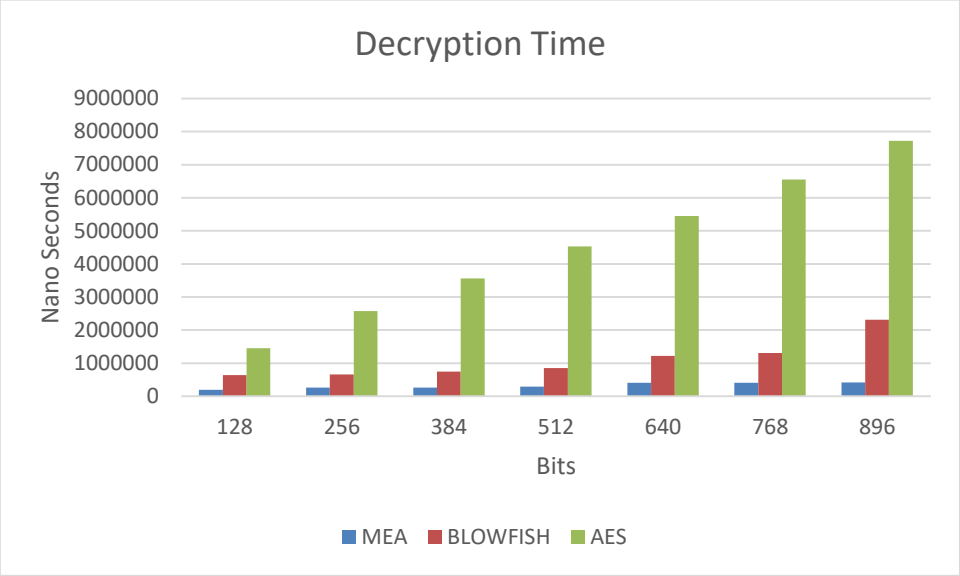


Graph.1: Encryption Method

We calculate the decryption timings of text messages of various length using the Advanced Encryption Technique (AES), the Blowfish algorithm, as well as the Mahaviracharya Encryption Algorithm (MEA). The specifics are shown in the Table.3. The average data size for the investigated data items is 512 bits, while the average encryption time for Mahaviracharya Encryption Algorithm (MEA) is 323069.6 Nano seconds, 1107790 Nano seconds for Blowfish Algorithm, and 4549922 Nano seconds for Advanced Encryption Algorithm (AEA). This table clearly shows that MEA is faster than Blowfish, Advanced Encryption Algorithm (AEA).

Table.3: Decryption Process

	Data Size	MEA	BLOWFISH	AES
	128 bits	198150 ns	645361 ns	1453528 ns
	256 bits	265732 ns	655718 ns	2574147 ns
	384 bits	267356 ns	746815 ns	3561408 ns
	512 bits	295671 ns	856716 ns	4533681 ns
	640 bits	407273 ns	1224256 ns	5451982 ns
	768 bits	410391 ns	1312447 ns	6550893 ns
	896 bits	416914 ns	2313216 ns	7723817 ns
Average:	**512 bits**	**323069.6 ns**	**1107790 ns**	**4549922 ns**



Graph. 2: Decryption Process

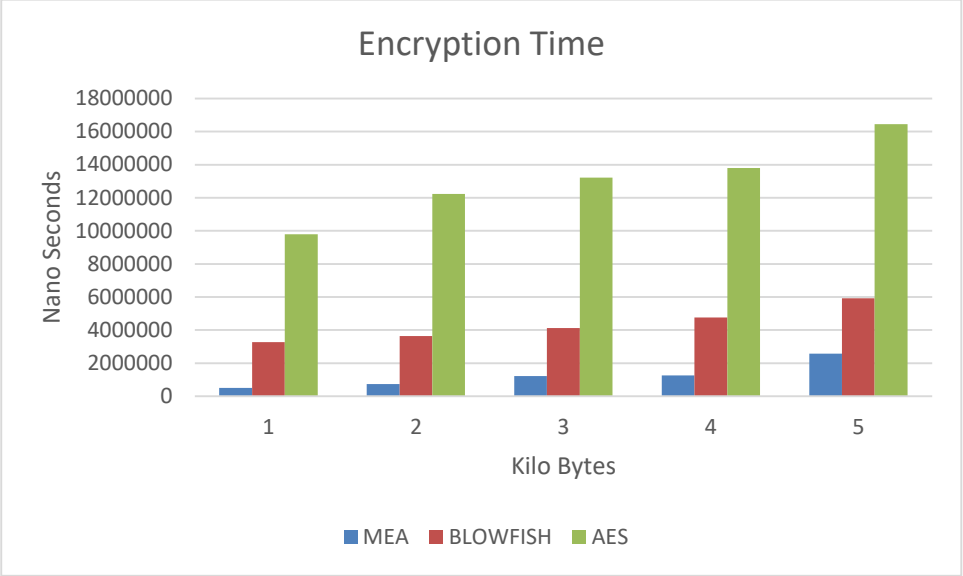
The Second Group Results:s

We calculate the encryption times of text messages of various length using the Advanced Encryption Algorithm (AES), the Blowfish cipher, as well as the Mahaviracharya Encryption Algorithm (MEA). The specifics are shown in the table-. The average data size for the investigated data items is 3 KB, while the average encryption time for Mahaviracharya Encryption Algorithm (MEA) is 1261766 Nano seconds, 4343968 Nano seconds for Blowfish Algorithm, and 13094480 Nano seconds for Advanced Encryption Algorithm (AEA). This table clearly shows that MEA is faster than Blowfish, Advanced Encryption Algorithm (AEA).

Table.4: The Encryption Procedure

	Data Size	MEA	BLOWFISH	AES
	1 KB	504332 ns	3280060 ns	9786580 ns
	2 KB	742880 ns	3640020 ns	12228580 ns
	3 KB	1226520 ns	4124000 ns	13211440 ns
	4 KB	1263280 ns	4757760 ns	13794920 ns
	5 KB	2571820 ns	5918000 ns	16450880 ns
Average:	**3 KB**	**1261766ns**	**4343968ns**	**13094480 ns**

*ns is an abbreviation for Nanoseconds.

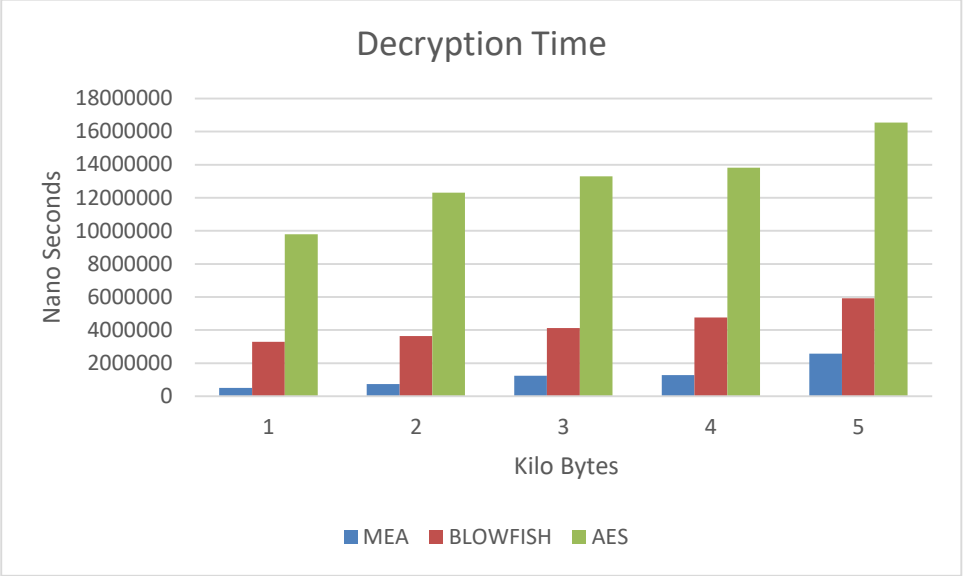


Graph.3: Encryption Method

We calculate the decryption timings of text messages of various length using the Advanced Encryption Technique (AES), the Blowfish cipher, as well as the Mahaviracharya Encryption Algorithm (MEA). The specifics are shown in the table-. The average data size for the investigated data items is 3 KB, while the average encryption time for Mahaviracharya Encryption Algorithm (MEA) is 1267513 Nano seconds, 4351803 Nano seconds for Blowfish Algorithm, and 13150723 Nano seconds for Advanced Encryption Algorithm (AEA). This table clearly shows that MEA is faster than Blowfish, Advanced Encryption Algorithm (AES).

Table.5: Decryption Process

	Data Size	MEA	BLOWFISH	AES
	1 KB	505257 ns	3291241 ns	9794729 ns
	2 KB	743794 ns	3650205 ns	12309700 ns
	3 KB	1235709 ns	4132958 ns	13300791 ns
	4 KB	1272349 ns	4765591 ns	13809896 ns
	5 KB	2580456 ns	5919021 ns	16538497 ns
Average:	**3KB**	**1267513ns**	**4351803ns**	**13150723ns**



Graph.4: Decryption Method

Experiment to analyse Brute-force Attack on MEA:

The key size of the Data Encryption Standard (DES) algorithm is merely 56 bits. It is too little to withstand a brute force attack. To combat brute force attacks, the Advanced Encryption Algorithm (AES) with a key length of 128 bits was created.

The Mahaviracharya Encryption Algorithm (MEA) supports varied length keys, however to avoid brute force attacks, we chose 128 bits as the minimum length for the secret key. However, in this experiment, we used different lengths of the secret key to produce cipher text and calculated the time required to break the cipher text using a brute force assault. The findings of the experiment are shown in the table below.

Table.6: The time requisite to breach various key spaces using the brute force assault.

Key length	No. of Keys	Time to Break in Milliseconds
8 bits	256	138
12 bits	4096	2960 = 2.960s
16 bits	65536	29152=29.152s
20 bits	1048576	459483=459.483s=7.65805m
Average:	**279616 keys**	**122933.25 milliseconds**

To carry out this experiment, a Jdk windows-x64 bin java language, Apache Net Beans IDE, Windows 10 pro 64 bit operating system, and an Intel(R) Core(TM) i5-4310U CPU @ 2.00GHz GHz laptop are employed.

We can determine the average no. of secrete keys and the average time to break the cipher text using the table above. The average no. of secrete keys tested is 279616, and the time to break these keys is 122933.25 milliseconds. Using the computer system described in the preceding paragraph, it can test 2.274 alternative keys in 1 millisecond, which means it can test 2,274 alternative keys in one second to crack the encrypted text. If we choose a 128-bit key, it will take about 10^{29} years to crack the cypher text using a brute force attack on a laptop with the above mentioned system settings.

The table below depicts the architecture of some prominent symmetric encryption algorithms utilizing various factors such as algorithm structure, block size, key size, number of S boxes used in each method, and number of rounds used in each algorithm. To compare current methods, Mahaviracharya Encryption Algorithm is also

included in this table. The Mahaviracharya Encryption Algorithm does not take into account parameters such as method structure, the number of S boxes used in algorithm, and the number of rounds used in algorithm.

Table.7: Summary of Symmetric Algorithms Architecture

Algorithm	Structure	Block Size	Key Size	# S Boxes	# of Rounds
DES	Festial structure	64 bits	56 bits	8	16
3DES	Festial structure	64 bits	168 bits	8	48
Rijndael	SPN	128 bits	128/192/256 bits	1	10/12/14
MARS	Festial structure	128 bits	128-448 bits	1	32
RC6	Festial structure	128 bits	128/192/256 bits	N/A	20
Serpent	Festial structure	128 bits	128/192/256 bits	8	32
Twofish	Festial structure	128 bits	128/192/256 bits	4	16
IDEA	Lai–Massey scheme	64 bits	128 bits	N/A	8
Blowfish	Festial structure	64 bits	32-448 bits	4	16
MEA	N/A	>=128 bits*	>=128 bits#	N/A	N/A

*Block size is flexible, starting at 8 bits, although according to AES committee recommendations, 128 bits is considered the minimum length, with no restriction on maximum length.

#Key length is varied, starting with 8 bits, although according to AES committee rules, 128 bits is considered the minimum length, with no limit on maximum length.

IV. CONCLUSION

Mahaviracharya Encryption Algorithmis a new algorithm which has the good features like easy to understand, easy to implement. It is giving good security against brute-force attack, ciphertext-only and known-plaintext attacks. It is taking less time for encryption and decryption methods than the AES andBlowfish algorithms for short length data.

REFERENCES

1. Rangacarya.M, “Ganitha-Sara- Sangraha of Mahaviracarya”, Cosmo Publication New Delhi, India.
2. B.Nagaraju, P.Ramkukar, “A New Method for Symmetric Key Cryptography”, International Journal of Computer Applications (0975 – 8887), Volume 142 – No.8, May 2016.
3. Bollepalli.Nagaraju, and Penu.Ramkumar, “Mahaviracharya Encryption Algorithm (MEA) with Modified Counter Mode and Comparing with AES Algorithm” , Proceedings of the International Conference on Emerging Trends in Engineering (ICETE), Vol. 1.,Springer publications-2019.

4. W. Stallings, "Cryptography and network security: principles and practices". Pearson Education India, 20014.

5. Chiranth B O, Shashikala B, Survey of Performance Comparison of DES, 3DES and AES Algorithms, International Journal of Data & Network Security, Volume 1 No.3, Dec10, 2012.

6. Shaza D. Rihan, Ahmed Khalid, A Performance Comparison of Encryption Algorithms AES and DES, International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 www.ijert.orgIJERTV4IS120227, Vol. 4 Issue 12, December-2015.

7. Shaify Kansal, Meenakshi Mittal, Performance Evaluation of Various Symmetric Encryption Algorithms, 2014 International Conference on Parallel, Distributed and Grid Computing.

8. Dr. Najib A. kofahi, "An Empirical Study to Compare the Performance of some Symmetric and Asymmetric Ciphers", International Journal of Security and Its Applications Vol.7, No.5 (2013), pp.1-16 http://dx.doi.org/10.14257/ijsia.2013.7.5.01.

9. Pratap Chandra Mandal, "Evaluation of performance of the Symmetric Key Algorithms: DES, 3DES ,AES and Blowfish", Journal of Global Research in Computer Science, ISSN:2229-371X

10. Srinivas B.L , Anish Shanbhag , Austin Solomon D'Souza, "A Comparative Performance Analysis of DES and BLOWFISH Symmetric Algorithm", International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 5, October 2014, ISSN(Online): 2320-9801 , ISSN (Print): 2320-9798

11. Apoorva , Yogesh Kumar, "Comparative Study of Different Symmetric Key Cryptography Algorithms", International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 2, Issue 7, July 2013 ISSN 2319 – 4847.