A Study on current scenario of cryptographic algorithms

Happy Joshi [1], Nidhi Bhatt [2]

[1] *P.G student, Communication system engineering, SAL institute of technology and engineering research, Ahmedabad, Gujarat, India*
[2] *Assistant professor, Head of E.C department, SAL institute of technology and engineering research, Ahmedabad, Gujarat, India*

ABSTRACT

Secure system is most important part in the data communication. A digital media can be transmitted easily in real time anywhere at any time due to the multimedia technology and internet, but to maintaining a security of information is a biggest problem now a days. Cryptography playing a major role to provide security. The main aim to protect the data from unauthorized access. The encryption and decryption processes involves in cryptographic concept. There are many cryptographic approaches has been used to provide security such as Data encryption standard, Advanced encryption standard , Blowfish, Two fish, RSA, Modified Advanced encryption standard. A comparison is made between all these approaches shows that Modified AES provides more security than other approaches.

Keyword: -*Cryptography, MAES, Encryption, and Decryption, S-box etc.*

1. INTRODUCTION

Human being from ages had two inherent needs: (a) to communicate and share information and (b) to communicate selectively. These two needs gave rise to the art of coding the messages in such a way that only the intended people could have access to the information. Unauthorized people could not extract any information, even if the scrambled messages fell in their hand. The art and science of concealing the messages to introduce secrecy in information security is recognized as cryptography. Cryptography is the art and science of making a cryptosystem that is capable of providing information security. Cryptography deals with the actual securing of digital data. It refers to the design of mechanisms based on mathematical algorithms that provide fundamental information security services. You can think of cryptography as the establishment of a large toolkit containing different techniques in security applications. [1]

1.1 How to secure the information?

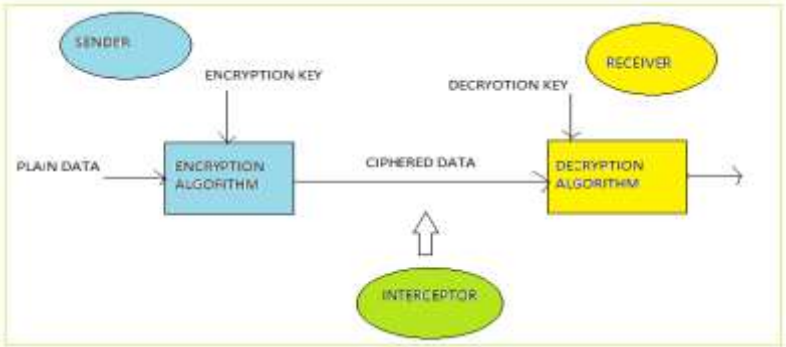

Figure 1: Basic idea how to secure the data

As shown in above figure plain data such as audio, video, image, text, etc will be send by the sender the plain data will be encrypted by the encryption algorithm. That encrypted data is also known as ciphered data. The encryption and decryption is done with encryption and decryption key.

1.2 Types of Cryptographic algorithm

1. DES (Data encryption standard): Data encryption standard algorithm was developed in 1971 by IBM for US government. The plain text is processed in 64 bit block length. The key is 56 bit in length which is divided into 16 sub keys for 16 round processing. Decryption is same as encryption where cipher data is used as input to DES and sub keys are used now in reverse order wuth 56 bit key size there are 2^{56} =7.20× 10^{16} possible keys available to provide good security.[9]
2. 3DES (Triple data encryption standard): It is also used encryption and decryption. It is also working on 64 bit plain text but key size is 168 bit. But it is slower than DES because it requires three keys and three executions at every sequence. It occupy 3 times more rounds then DES .[9]
3. Blowfish: Blowfish provides good performance into software. It has 64 bit block size and variable key length from 32 bits to 448 bit. The algorithm is divided into two parts – 1)A key expansion , 2) Data encryption part. The main role of key expansion is to covert a key of at most 448 bit into several sub key arrays of 4168 bytes. Blowfish is successor of two fish. It suffers from week key problems, so some attacks are possible against it.[9]
4. Two fish: It is highly suited for large microprocessors and smart card microprocessor. Two fish was designed to meet NIST'S design criteria for AES. Specifically there are 128 bit symmetric block cipher with key length of 128, 192, 256 bits .[9]
5. AES (Advanced encryption standard):Both AES and DES are not good approaches for long term security. NIST in 1997 issues a call for proposal for a new advanced encryption standard out of proposal in 1st round, 15 algorithms were shortlisted out of which in 2nd round 5 algorithm were short listed out of them NIST select RSA and AES algorithm. AES algorithm provides 128 bit block size and a key length that is 128, 192, 256 bits .[9]

Parameter	DES	Blowfish	AES
Type of algorithm	Symmetric key	Symmetric key	Symmetric key
Key length	56 bit	64 bit	128, 192 , 256 bits
Data hiding speed	Slow	Speedy than DES	High speed but for video slightly slower
Data detection	Sometimes easy to detect	Not easy to detect	Very difficult to detect
flexibility	Less	Medium	More flexible
			Approved by us government for Data security

Table 1: Comparison between different algorithms [6]

Among all of this algorithm AES is most trusted algorithm which is used for encryption and decryption. AES works efficiently for images and audio but for video encryption and decryption it becomes slightly slower due to its mix column structure. Thus there was some modification in AES algorithm to overcome the limitation.

2. Modified AES

Modified AES algorithm is a fast lightweight encryption algorithm for security of multimedia data. To overcome the problem of high calculation and computational overhead, We analyze the Advanced Encryption Standard (AES) and modify it, to reduce the calculation of algorithm and for improving the encryption performance. Modified AES is used for all kind of data. The modified AES algorithm adjusts to provide better encryption speed. In Modified AES the block length and the key length are specified according to AES. MAES is uses the dynamic S Box instead of static s-box. [6]

The main five different stages we use for modified AES algorithm are

1. Dynamic s box
2. Substitute byte
3. Shift rows
4. Permutation
5. Add round key

Substitution Bytes, Shift Rows and Add Round Key remain unaffected as it is in the AES. Here the important function is Permutation which is used instead of Mix column. These rounds are managed by the IP table. Permutation is widely used in cryptographic algorithms. [6]

2.1 What is permutation?

Permutation operations are interesting and important from both cryptographic and architectural points of view. The DES algorithm will provide us permutation tables. The inputs to the IP table consist of 128 bits. Modified-AES algorithm takes 128 bits as input. The functions Substitution Bytes and Shift Rows are also interpreted as 128 bits whereas the Permutation function also takes 128 bits. In the permutation table each entry indicates a specific position of a numbered input bit may also consist of 256 bits in the output. While reading the table from left to right and then from top to bottom, we observe that the 242 th bit of the 256-bit block is in first position, the 226th is in second position and so forth. After applying permutation on 128 bits we again complete set of 128 bits and then perform next remaining functions of algorithm. If we take the inverse permutation it gives again the original bits, the output result is a 128-bit cipher text. For the full decryption of Modified-AES algorithm the transformation processes are, Inverse sub byte, Inverse Shift rows, Inverse Permutation, and the Add round key.

3. Basic Structure of MAES

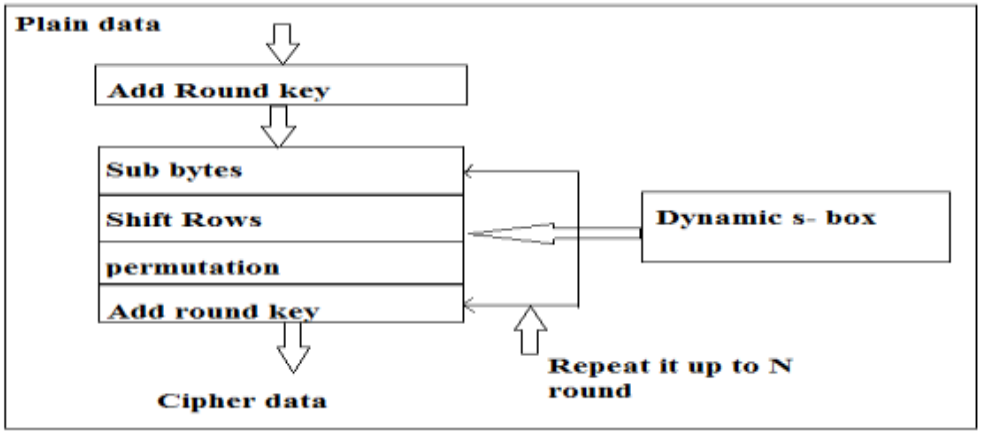

Figure 2: Basic structure of Modified AES algorithm [3]

4. CONCLUSION

Light weight and secure algorithms are very attractive for multimedia application.We have achieved fast lightweight encryption algorithm to secure our multimedia data from unauthorized access. For the security of multimedia data, we have reviewed that encryption algorithm that is based on AES using symmetric key encryption algorithm. In version of security analysis and experimental results it is proved that MAES scheme is fast and on the other hand it provides good security and adds very less overhead on the data. Theoretical analysis of the achievement makes it very suitable for high rate and less overhead on the data. For all these compensation it is suitable for any large scale text and image and video transfer.

5. REFERENCES

[1] Sumedh H. Nagdeve, Ujwala S.Ghodeswar "Synthesis of Advanced Encryption Standards using Xilinx 13.4", IEEE2015

[2] Vikas Kaul, Dr.V. A. Bharadi, P. Choudhari, Dhvani Shah, Dr. S. K. Narayankhedkar "Security Enhancement for Data Transmission in 3G/4G Networks" International conference on computing communication control and automation IEEE 2015

[3] Vikas Kaul, Dr. V. A. Bharadi, P. Choudhari, Dhvani Shah, Dr. S. K. Narayankhedkar "Security Enhancement for Data Transmission in 4G Networks" International conference on computing communication control and automation IEEE 2014

[4] Dhananjay M. Dumbere "Video Encryption Using AES Algorithm" International conference on current trends in engineering and technology IEEE 2014.

[5]Swinder Kaur, Prof. Renu Vig "Efficient Implementation of AES Algorithm in FPGA Device" International conference on computational intelligence and multimedia application IEEE 2007

[6] Neel Khatri , Nandlal Dhandhukia "MAES Based Efficient architecture for Real time Audio" M.E. Student IJARIIE-ISSN(O)-2395-4396-2016

[7] C. Narsimha Raju, Ganugula Umadevi, Kannan Srinathan "Fast and Secure Real-Time Video Encryption" IEEE 2010.

[8] Pravin Kawle, Avinash Hiwase, Gautam Bagde, Ekant Tekam, Rahul Kalbande "Modified Advanced Encryption Standard", International Journal of Soft Computing and Engineering (IJSCE), Volume-4, Issue-1, March 2014.

[9]. Rashmi A. Gandhi ,Atul M. Gosai" A Study on Current Scenario of Audio Encryption", International Journal of Computer Applications Volume 116 –No. 7, April 2015.