Chetan Rathod et al. International Journal of Recent Research Aspects ISSN: 2349-7688, Vol. 5, Issue 2, June 2018, pp. 32-35

Comparative Analysis of Encryption and Decryption Algorithms for Audio

*Chetan Rathod[1], †Nilesh Advani[2], Prof. (Dr.) Atul Gonsai[3]

[1]Vivekanand College for Advance Computer and Information Science, VNSGU, Surat
[2]Marvadi Education Foundation's Group of Institutions, Rajkot
[3]Dept. of Computer Science, Saurashtra University, Rajkot

Abstract: **The use of the web exceeds day by day. Information security is a challenging issue in today's hi-tech world. Cryptography plays a main role within the field of network security. There is a broad range of cryptographic algorithms that are used for securing networks. In this study is made for the cryptography algorithms, particularly algorithms- AES, DES, 3DES, RC4,RC6, RSA, Blowfish, MUGI, ARIA, Salsa20 and Serpent are compared and performance is evaluated. This paper chiefly focuses on encryption techniques for audio knowledge. This presents a study and comparison of basic encoding standards and a literature survey of encryption technique that used for encoding on audio data. Comparing between symmetric and asymmetric cryptography, symmetric cryptographic techniques take less time than asymmetric technique.**

Keywords: **Cryptography; Encryption; Decryption; Cipher; RSA; Blowfish; AES; DES;Triple DES;RC4; RC6; XOR;MUGI; ARIA; Salsa20;Serpent**

I. INTRODUCTION

Human being had two inherent needs – (1) communication and sharing information and (2) Communication with the selected. These two needs increase the art of coding the messages in such a way that only the genuine people could have access to the information. It is badly need to secure the data. Information Security has now become a very important aspect of data communication as people spend alarge amount of time connected to a network. Unauthorized people could not get any data, even if the twisted messages fell in their hand. Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. The 'cryptography' is combination of two Greek words, 'Krypto' meaning hidden and 'graphene' meaning writing. Cryptography is a combination of encryption and decryption process.

Normally user share their data and information with their group using computer network. This information may be various media like text, image, audio and video. When these media contents transmit in computer network, it faces many security threats. For example, the CEO of a company discuss about their future marketing policies through online. Some people may be stole this information and shared it to another companies. If army wants to share some important data there is a fear to share this to unauthorized person. So it is necessary to protect the information from unauthorized user. The solution is cryptograph. The main consideration in designing an encryption algorithm has to be the security of the algorithm against undesirable attacks. However, in the real world, performance and implementation cost is also important concerns. In this paper, security, Block Size, Key Size, Number of Rounds and Cipher Type has been compared. The primary focus is on comparing the encryption algorithms on the basis of their performance and ease of implementation.

An encryption algorithm plays an important role in securing the data in storing or transferring it. The encryption algorithms are categorized into Symmetric (secret) and Asymmetric (public) keys encryption. In Symmetric key encryption or secret key encryption, only one key is used for both encryption and decryption of data. E.g.: Data encryption standard(DES), Triple DES, Advanced Encryption Standard(AES), RC4, RC6and Blowfish Encryption Algorithm. In asymmetric key encryption or public key encryption uses two keys, one for encryption and other for decryption. E.g.: RSA.

Block Cipher and Stream Cipher: Encryption technique commonly used is based on the form of input data they operate on. The two types are Stream cipher and Block Cipher. "A Cipher is an algorithm for performing encryption (reverse decryption).

Block Cipher- In this method data encryption and decryption is done in form of blocks of data. In it's the plain text is divide into blocks then feed into the cipher system to produce blocks of cipher text. The basic form of block cipher is ECB (Electronic Codebook Mode) is where data blocks are encrypted directly to generate its corresponding cipher blocks.

Stream Cipher- this method data encryption and decryption is done on a stream of data by operating on it by bits. It has two main components: a key stream generator, and a mixing function. Key stream generator is the main unit in stream cipher encryption technique while, mixing function is usually just an XOR function. For example, if the key stream generator produces series of zeroes, the outputted ciphered stream will be identical to the original plain text.

II. IMPLEMENTED ALGORITHMS

The following encryption algorithms were chosen for implementation:

* Research Scholar of Dept. of Computer Science, Saurashtra University, Rajkot
† Research Scholar of Dept. of Computer Science, Saurashtra University, Rajkot

DES:[2][1][5][9]

Data Encryption Standard developed in March 1975 by IBM was later adopted in 1977 by NIST. It is most widely used as an encryption algorithm in the world. DES is a block cipher key algorithm it takes 64-bit block size Plain Text as an input and gives 64 bit cipher text as an output. Key Size is 64bits and it has 16 Round. Each block of 64 bits is divided into two 32 bits block L and R(Left and Right). If encryption is done individually for each 64-bit block, then the mode of encryption is called Electronic Code Book (ECB) mode. There are two other modes of DES encryption, 1. Chain Block Coding (CBC) and 2. Cipher Feedback (CFB), which make each cipher block dependent on all the previous messages blocks through an initial XOR operation. DES is not robust enough. Several attacks recorded against it.

Triple DES:[2][1][5]

This is a new form of DES. This was created by IBM in 1978. DES used key size of 56 bits which is not robust again brute force attacks and other attacks. Triple DES was created by using same rules of DES algorithm with long key size. Performance of triple DES is trice (48 Rounds)that's why it is slower then DES but compare to DES it extend the security. It is block cipher with key size of 168 bits(three 56-bit DES keys) and block size of 64 bits. Triple DES has low performance in terms of power consumption and outturn compared with DES. Several attacks also recorded against it.

AES:[1][2][3][5][9]

The Advanced Encryption Standard (AES) algorithm is a symmetric block. It is most broadly adopted encryption standard. AES was originally referred to as rijndael. This was created by Joan Daemen and Vincent Rijmen in 1998. AES can do encryption on plain text and decryption on cipher text of 128 bits. AES has 128-bit block size and a variable length key of size 128,192 or 256 bits. Number of rounds in the encryption or decryption processes depends on the key size.

- 10 cycles of repetition for 128 bit keys.
- 12 cycles of repetition for 192 bit keys.
- 14 cycles of repetition for 256 bit keys.

Each round of encryption process requires the following four types of operations: Sub-Bytes, ShiftRows, MixColumns, XorRoundkey. Decryption is the reverse process of encryption and using inverse functions.

BLOWFISH:[2][1][3][5]

Blowfish was designed in 1993 by Bruce Scheier as a fast, alternative to existing encryption algorithms. Blowfish symmetric block cipher algorithm encrypts block data of 64-bits at a time. It will follow the 16 round feistel network and this algorithm is divided into two parts. **1. Key-expansion:** It will convert a key of at most 448 bits into several sub key arrays totaling 4168 bytes **2. Data-encryption:** It is having a function to iterate 16 times of network. Each round consists of a key-dependent permutation, and a key- and data- dependent substitution. All operations are XORs and additions on 32-bit words. The algorithm keeps two sub key arrays: the **P-array** consists of 18x32-bit sub keys and also four 32bits **S-boxes** with 256 entries each. Blowfish is the best performing algorithm under the speed and the security was taken into the consideration. Blowfish is not only the fastest but also provides the great security through the strong key size which enables it to be used in many applications like Bulk Encryption, Random Bit Generation , Internet Based Security (network security) , Packet Encryption and so many of applications. the problem is it takes more time to initialize the algorithm with key.

RC4:[2] [6][7]

It is a stream cipher algorithm designed in 1987 by Ron Rivest for RSA Security. It works with byte-oriented operations. The algorithm is based on the use of a random permutation. The RC4 algorithm is simple and quite easy to explain. RC4 has a use in both encryption and decryption while the data stream undergoes XOR together with a series of generated keys. It takes in keys of random lengths (40 to 2048 bits) and this is known as a producer of pseudo arbitrary umbers. The output is then XORed together with the stream of data in order to generate a newly-encrypted data. Weak pont of this algorithm is a related key vulnerability, which applies when part of the key presented to the KSA is exposed to the attacker. It consists of the observation that when the same secret part of the key is used with numerous different exposed values, an attacker can receive the secret part by analyzing the initial word of the key streams with relatively less effort.

RC6:[1][11][12][13]

In RC6 it is exactly specified as RC6-w/r/b where the word size is **w** bits, encryption rounds **r (**nonnegative number**)**, and **b** is the length of the encryption key in bytes. RC6 uses a block size of 128 bits and having key sizes of 128, 192 and 256 bits. It is symmetric cipher algorithm. The standard value of w = 32, b=16 and r = 20. RC6 is vulnerable to brute force attacks. It is a simple, fast, and secure block cipher. It has modified Feistel structure and disadvantage is that it has different algorithm between encryption and decryption. Thus, the RC6 algorithm needs double space compared with the same structure of encryption and decryption when it implemented on hardware.

RSA:[2][3][4][9][10]

RSA is a most popular and secure asymmetric cryptography algorithm. In 1977 three mathematician "Ron Rivest", "Adi Shamir" and "Leonard Adleman" describe this algorithm. It has two key **encryption key**(public) and **decryption key**(private). RSA is based on the mathematical concept that is easy to find the private and public keys based on the very large prime numbers. **Encryption:** compute c = m^e*mod* n, where the e and n are the public key, and m is the message block. The c is the encrypted message. **Decryption:** The private key d is used to decrypt messages. Compute: m = c^d*mod* n, where n is the modulus and d is the private key. In RSA, decryption process takes more time then encryption..This algorithm is very reliable, and the longer the

keys, the more difficult it is to break it. For i.e the cracking of the longest key is 768 bits, that is to say 1024 and 2048 - bit RSA keys are very safe.

MUGI: [14][15]

MUGI that is designed for use as a stream cipher. MUGI has a 256-bit input. It has 128-bit secret key and a 128-bit public key. It produce outputs a 64-bit random data block for each round(Total 32 Rounds).Its design is based on linear feedback shift registers(LFSRs). Because of their linearity and predictability, they cannot be used in their actual forms. Several techniques have been used to improve their security, such as the combination generator, non-linear filtering and clock control. Stream cipher seem to be designed in an ad hoc way, as a PANAMA. "Panama is based on generic design principles, comparable to those of block ciphers". Panama can be used both as a KSG and as a hash function MUGI is only suitable as a KSG. MUGI's performance is equal to or even better than AES but MUGI is not vulnerable to common attacks on block ciphers and also to some attacks on stream ciphers.

Serpent: [16] [17]

Serpent is a symmetric block cipher algorithm belongs to a class of substitution-permutation networks (SPN).It was developed by Ross Anderson, Eli Biham, and Lars Knudsen. This was a finalist in the AES where it was ranked second to Rijndael. Serpent has 32 round network working on four 32 bits words(128 Bits block size). Each round applies one of eight 4-bits S-boxes 32 times in parallel. It support a key sizes of 128, 192 and 256 bits. Serpent is a better design than DES. Not much protected against different attacks.

AREA: [18]

ARIA is a block cipher designed in 2003 by a large group of South Korean researchers. The algorithm uses a substitution-permutation network structure based on AES. The interface is the same as AES: 128-bit block size with key size of 128, 192, or 256 bits. The number of rounds is 12, 14, or 16, depending on the key size. ARIA uses two 8×8-bit S-boxes and their inverses in alternate rounds; one of these is the Rijndael S-box. According to authors of [18], they could not find any weakness and have not inserted any hidden weakness. ARIA is suitable for most platforms and can be widely used.

Salsa20: [19]

Salsa20 is a stream cipher algorithm for encryption submitted to eSTREAM by Daniel J. Bernstein. Its used key of 256-bit, a 64-bit nonce, and a 64-bit stream position to a 512-bit block of the key stream.It is built on a pseudorandom function based on add-rotate-xor (ARX) operations — 32-bit addition, bitwise addition (XOR) and rotation operations. User can efficiently seek to any position in the key stream in constant time.Some attacks are noticed.

III. COMPARISON AND ANALYSIS

The performance comparison of the algorithms mentioned above is conducted with different types of files. The performance matrices are: Round Block, Block Size, Key Size, Round, Cipher Type and Security

Algorithm	Block Size	Key Size	Round	Cipher Type	Security
AES	128 bits	128, 192, 256 bits	10/ 12/ 14	Symmetric Block Cipher	Secured
DES	64 bits	56+8 bits	16	Symmetric Block Cipher	Inadequate
3DES	64 bits	168, 112 or 56 bits	48	Symmetric Block Cipher	Inadequate
RC4	Byte Oriented	40 to 2048 bits	1	Symmetric Stream Cipher	Weak Security
RC6	128 bits	128 , 192 or 256 bits	20	Symmetric Block Cipher	Vulnerable
Blowfish	64 bits	32 – 448 bits	16	Symmetric Block Cipher	Secured
RSA	Minimum 512 bits	Greater then1024 bits	1	Asymmetric Algorithm	Secured
MUGI	64 bits	256	32	Block/Stream Cipher	Vulnerable
Serpent	128 bits	128 , 192 or 256 bits	32	Block Cipher	Vulnerable
ARIA	128 bits	128 , 192 or 256 bits	12, 14 or 16	Block Cipher	Secure
Salsa20	512 bits(State Size)	256 bits	20	Stream Cipher	Vulnerable

Table 1: Comparison and Analysis of Symmetric and Asymmeric Algorithms

IV. CONCLUSION

In this paper, we have discussed various encryption algorithms for audio data, which provides network security also. We see the different types of algorithm Symmetric or Asymmetric. Symmetric is faster in execution than asymmetric. Because of large computation, the calculation speed is slow in asymmetric algorithm. Public-key encryption is based on mathematical problem solving, number needs a large number of mathematical operations. We compare it based on key, block Cipher or Stream cipher, by block size, key size no of rounds and security purpose. We conclude that in symmetric category AES and Blowfish algorithm is better than other algorithm in base of security reason. A new developed ARIA is also secured algorithm for block cipher. RSA is best choice algorithm based on stream cipher but it is suitable for small amount of data encryption. Blowfish is the best performing algorithm under the speed and the security was taken into the consideration. Blowfish is not only the fastest but also provides the great security through the strong key size which enables it to be used in many applications. Only the problem is, it takes more time to initialize the algorithm with key which yet to be rectified and explored.We will propose a new method for generating S-boxes and P-arrays which are considered as the main building elements of the Blowfish algorithm. This new generating method will lead to a reduction in time complexity of generating S-boxes and P-arrays.

With the help of these algorithms, one can generate their own algorithm by making modifications into existing algorithms to make data more secure. In future, also one can use the existing algorithms and develop more secure and faster encryption techniques.

1 References

[1] M. V. B. Pawar, P. P. A. Tijare, and P. S. N. Sawalkar, "A Review Paper on Audio Encryption," vol. 2, no. 12, pp. 45–48.

[2] Z. Hercigonja, D. Gimnazija, and C. Varazdin, "Comparative Analysis of Cryptographic Algorithms and Advanced Cryptographic Algorithms," *Int. J. Digit. Technol. Econ.*, vol. 1, no. 2, pp. 1–8, 2016.

[3] M. Ahamad and I. Abdullah, "Comparison of Encryption Algorithms for Multimedia," vol. 44, pp. 131–139, 2016.

[4] M. Panda, "Performance analysis of encryption algorithms for security," *Int. Conf. Signal Process. Commun. Power Embed. Syst. SCOPES 2016 - Proc.*, pp. 278–284, 2017.

[5] A. Nadeem and M. Y. Javed, "Comparison of," *2005 Int. Conf. Inf. Commun. Technol.*, pp. 84–89, 2005.

[6] A. K. Singh, S. G. Samaddar, S. R. Sahoo, and G. Mathew, "Increasing robustness of RC4 family for automated selection of ciphersuites," *Procedia Eng.*, vol. 30, no. 2011, pp. 45–52, 2012.

[7] P. Jindal and B. Singh, "RC4 Encryption-A Literature Survey," *Procedia Comput. Sci.*, vol. 46, no. Icict 2014, pp. 697–705, 2015.

[8] A. A. Tamimi and '', "Performance Analysis of Data Encryption Algorithms," *Retrieved Oct.*, vol. 1, pp. 399–403, 2008.

[9] G. Singh, "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security," *Int. J. Comput. Appl.*, vol. 67, no. 19, pp. 975–8887, 2013.

[10] I. G. Amalarethinam and H. M. Leena, "Enhanced RSA Algorithm with Varying Key Sizes for Data Security in Cloud," *2017 World Congr. Comput. Commun. Technol.*, pp. 172–175, 2017.

[11] G.-H. Kim, J.-N. Kim, and G.-Y. Cho, "An improved RC6 algorithm with the same structure of encryption and decryption BT - 11th International Conference on Advanced Communication Technology, ICACT 2009, February 15, 2009 - February 18, 2009," vol. 2, pp. 1211–1215, 2009.

[12] A. B. Mohamed, G. Zaibi, and A. Kachouri, "Implementation of RC5 and RC6 block ciphers on digital images," *Int. Multi-Conference Syst. Signals Devices, SSD'11 - Summ. Proc.*, 2011.

[13] K. Aggarwal, "Comparison of RC6, modified RC6 & enhancement of RC6," *Conf. Proceeding - 2015 Int. Conf. Adv. Comput. Eng. Appl. ICACEA 2015*, pp. 444–449, 2015.

[14] J. Daemen, "A new keystream generator MUGI. ," *Proc. 9th Int. Work. Fast Softw. Encryption*, vol. 2365, pp. 179–194, 2003.

[15] J. D. Golic, "A Weakness of the Linear Part of Stream Cipher {MUGI}," *\ifnum\shortbib=1{FSE}\else{Fast Softw. Encryption -- {FSE}}\fi~2004*, vol. 3017, pp. 178–192, 2004.

[16] R. Anderson and E. Biham, "Serpent: A flexible block cipher with maximum assurance," *first AES ...*, no. 1, pp. 1–10, 1998.

[17] J. Sugier, "Implementing Serpent Cipher in Field Programmable Gate Arrays," 2011.

[18] D. Kwon *et al.*, "New Block Cipher: ARIA," *Inf. Secur. Cryptol. - ICISC 2003*, vol. 2971, pp. 432–445, 2004.

[19] D. J. Bernstein, "The salsa20 family of stream ciphers," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 4986 LNCS, pp. 84–97, 2008.

