IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)
An International Open Access, Peer-reviewed, Refereed Journal

A Study and Comparative Analysis of some Advanced Symmetric Block Cipher Techniques

[1]Shipra Srivastava, [2]Binayak Parashar
[1]Research Scholar, [2]Assistant Professor
[1]Computer Science and Engineering
[1]DR.K.N.Modi University, Newai, Rajasthan, India

***Abstract* - Symmetric key algorithm also known as secret key, uses same key for encryption and decryption. In future we will have more powerful, faster and better technology, so there will be requirement of advanced cryptographic algorithm for information security. This paper discusses about some advanced cryptographic algorithm with their advantages and disadvantages.**

***Index Terms* – Symmetric key algorithm, AES, GOST, Kuznyechik, Magma, CAST, Serpent, SEED**

I. INTRODUCTION

It is the art of secret writing [1]. Cryptography is the art and science of making a cryptosystem that is capable of providing information security. Cryptography is used to convert the plain text into cipher text using some encryption technique. The cipher text is then transmitted over a insecure channel to the authorized receiver. The receiver decrypts the cipher text and converts it back into plain text using decryption algorithm. A cryptosystem is an implementation of cryptographic techniques and their accompanying infrastructure to provide information security services [1].

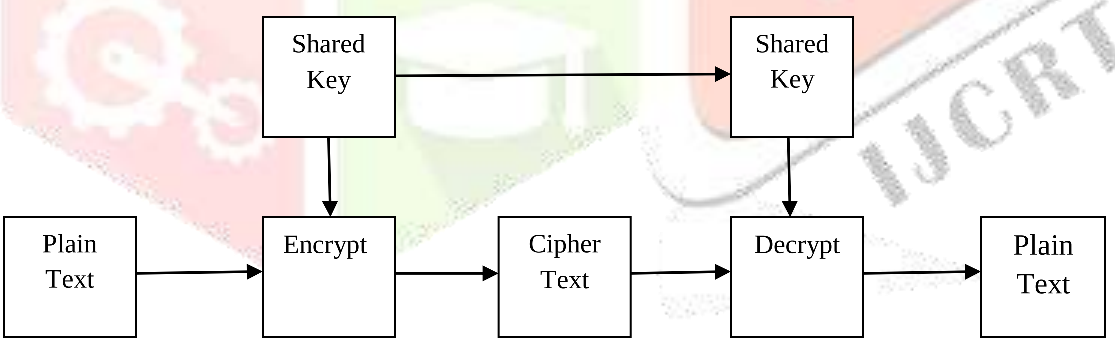

Fig.1. Symmetric Key Cryptography

II. SECURITY GOALS OF CRYPTOGRAPHY

A. Confidentiality- It keeps the information secure between authorized users.
B. Integrity-Integrity assures that no data is altered during the transmission.
C. Authentication- Authentication provides the identification of the originator.
D. Non-repudiation-None of the party can deny the creation or transmission of the said data to a recipient or third party.

III. ADVANCED SYMMETRIC ALGORITHM

A. Advanced Encryption Standard (AES)

AES is considered to be the strongest symmetric block encryption technique with a fixed block size of 128-bits.AES comes in a variant of 128-bit key length with 10 rounds, 192-bit with 12 rounds and 256 bits with 14 rounds. The structure of AES is based on substitution-permutation network. Each round consists of four types of transformations: byte substitution, shift row, mix column and key addition.AES is faster in computation in comparison to other symmetric encryption techniques.AES is implemented in both hardware and a software in order to encrypt the data. AES is secured against any kind of attack till date.

B. GOST

GOST is a 256-bit symmetric block encryption technique introduced by the Russian encrypted standard. It is based on the Fiestel structure with 64-bit block cipher having key length of 64-bits and 32 rounds of operation. Each round consists of a key addition of a modulo 2^{32}. It uses set of 8 bijective S-boxes on 4-bits.The encryption standard was used by the central Bank of Russian Federation and its associated branches for secure communication in order to protect their assets and billions of dollars against fraud. When calculated it was found that he implementation cost and hardware cost for GOST is less as compared to AES and TDES [2].On 16 October 2016 it was discovered that GOST encryption technique can be broken by an algebraic attack and Reflection attack [2].The encryption which was said to be very secure now could not prove its security required by the ISO.

C. Kuznyechik

Kuznyechik is a symmetric block encryption technique having block size of 128-bits with key size of 256-bits and 9 rounds of operation. The 9 rounds of operation contains tree transformations : addition having round sub-keys, substitution with S-boxes and linear transformation.256-bit master key is used for generation of the sub keys for the ten rounds [3].This encryption algorithm is considered to be secure for future computing against fraud.

D. Magma

Magma is another encryption technique introduced by The Russian Federal standard [GOST R 3412- 2015].The algorithm is based on Fiestel structure which takes 64-bit block of data as input and after conversion 64-bit of encrypted data is received as a output by 256-bits of keys. The number of S-boxes used by Magma is 8 and these 8 S-boxes converts 4-bits of input to 4-bits of output. The encryption standard is used for protecting the information and information processing which provides the basic security services like confidentiality, integrity and authenticity of the information to be transmitted as well as storage in computer aided system [3].

E. CAST

CAST encryption technique was developed by Carlisle Adams and Stafford Tavares. This is also a symmetric block cipher technique with two variants 128-bit and 256-bits.CAST-128 (or CAST – 5) follows Fiestel scheme having 64-bit of block size with the key size of between 40-bits and 128-bits.The number of rounds of operation required can be either12 or 16 depending on the key size. If the key size is larger than 80-bits, full round of operation is required that uses 8 X 32 bit of S-boxes [5].CAST-256 (or CAST -6) was an extension of CAST-128 suitable for block size of 128-bits.The number of rounds of operation required is 48. The algorithm follows Fiestel chain structure that uses non-linear transformation and modular arithmetic [5].This algorithm provides a good result, good performance [4] and is considered to be very reliable and secure for future computing.

F. Serpent

Serpent encryption algorithm also falls in the category of symmetric block cipher and was developed by Ross Anderson, Eli Biham and Lars knedsen. It supports block size of 128-bits and a key size of 128, 192 and 256-bits.The number of operational round required is 32 before and after the beginning respectively with a substitution permutation network operating on a block of 32 bit-words. These blocks are called initial permutation and final permutation. This is one of the symmetric algorithms that is not based on Fiestel scheme. Width of all data line are equal to the size of input block which is of 128-bits [6].Serpent cipher is stronger but slower than AES.As serpent cipher is highly sensitive to key and plain text, It successfully hides the pattern..Till date no attack is found to be succeeded on serpent cipher [6].

G. SEED

SEED is created by KISA (Korea Information Security agency) in 1998 which is 128-bit symmetric block cipher. It uses two 8 X 8 S-boxes with permutations. The design is based on Fiestel scheme having 16 rounds of operations. This encryption technique is considered to be stronger than Differential cryptanalysis and linear cryptanalysis in terms of attack [7]. A 128-bit input is divided into two blocks 64-bit each. The right 64-bit block is acts as input to the round function F, having 64-bit sub-key. L is the most significant 64-bits f 128 bit input and R is the least significant 64 –bits [6]. Use of SEED algorithm requires use of object identifiers explained in Lee et al. [7]. Republic of Korea the encryption technique for confidential services like electronic commerce, financial service, wired and wireless communication.

4. CONCLUSION

This paper tells about the advanced symmetric key algorithm like AES, GOST, Kuzneychik, Magma, CAST, Serpent and SEED for future computing. Depending on the block size and security provided to information we can choose the best algorithm from above mentioned. For future computing symmetric algorithm plays very important role.

REFERENCES

[1] W. Stallings, Cryptography and Network security Principles and Practices Fourth edition, Pearson Education, Prentice Hall, 2009.

[2] Nicolas, T. Courtois, University College London, Gower Street, London, UK, “Security Evaluation of GOST 28147-89 in View Of International Standardisation”.

[3] Ishchukova Evgeniya and Maxim Anikeev. “Two simplified versions of Kuznyechik cipher (GOST R 34.12-2015)” Conference paper: October 2017, DOI: 10.1145/3136825.3136856.

[4] Carlisle Adams “The CAST-256 Encryption Algorithm”, http://adonis. .ee.queensu.ca:8000

[5] Andrushkevych, Alina, Tatyana Kuznetsova, Ivan Bilozertsev, and Sergii Bohucharskyi. "The block symmetric ciphers in the post-quantum period." In 2016 Third International Scientific-Practical Conference Problems of Infocommunications Science

[6] Mreza Naeemabadi, Ordoubadi, B. S., Alireza Mehri Dehnavi and Kambiz Bahaadinbeigy “Comparison of Serpent, Twofish and Rijndel encryption algorithms in tele-ophthalmology system.

[7] Lee, H. J., Lee, S. J., Yoon, J. H., Cheon, D. H., Lee, J. I. “The Seed Encryption Algorithm” RFC 4269, December 2005, Network Working Group.