Comparison and Analysis on Symmetric Cryptography Algorithms

Dr. C. Thiyagarajan[1], V. Rahul dharshan[2]
[1]Associate Professor
[1, 2] PSG College of Arts and Science, Coimbatore, Tamilnadu, India

Abstract- *Daily progress is being made in technology. Information security is a requirement for faster and better technology. Data authentication is necessary at the execution levels for this. A useful technology for establishing secure data independence is cryptography. For secure data communication, it employs the two fundamental procedures of encryption and decryption. Numerous cryptographic methods have been suggested and used up to this point. In this article, we have reviewed a number of the suggested symmetric key cryptography techniques and conducted a preliminary comparative analysis between them. This paper discusses the fundamental characteristics, benefits, limitations, and applications of several symmetric key cryptography methods.*

Keywords- Cryptography, Encryption, Symmetric Key.

I. INTRODUCTION

Data privacy is ensured by the art of converting readable text (plain text) into unreadable text (cipher text). The terms "cryptography" and "crypto" both refer to writing and hiding. Information security, data encryption, data authentication, and access control are all issues that are addressed. Both symmetric key (also known as secret key) and asymmetric key (also known as public key) cryptography exist. We have covered a few of the proposed methods for symmetric key cryptography in this succinct article. In symmetric key cryptography, the secret key is used as both an encryption and decryption key.

It is therefore more efficient than its Asymmetric Key sibling. To date, numerousmethods and algorithms have been created to implement symmetric key cryptography. Some of them have been discussed in the following sections.

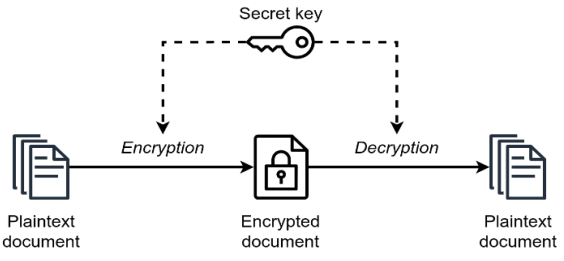

Fig 1. Symmetric Key Cryptograph

II. ANALYSISON SYMMETIC KEYS

Cryptography

Plaintext or clear text refers to information that can be read and understood without additional security measures.Encryption is the process of masking the contents of plaintext by hiding the appearance of the plaintext.When plaintext is encrypted, the outcome is ciphertext, which is unintelligible nonsense. Decryption is the process of converting cipher-text back to its original plaintext.

A common cryptographic scenario involves two parties (X and Y) communicating through an unsecure channel. X and Y want to be sure that anyone who might be listening is unable to understand what they are saying. Furthermore, since X and Y are separated by great distances, X must ensure that the data she gets from Y was not altered during transmission. She must also confirm that Y genuinely provided the information and that a fraudster did not provide it.The following objectives are attained by the usage of cryptography:

Confidentiality

To ensure data privacy. In most cases, confidentiality is attained by encryption. Plain text is converted into cipher text using encryption algorithms (which employ encryption keys), and cipher text is then converted back to plain text using the corresponding decryption procedure. Asymmetric encryption techniques use a public/private key pair, whereas symmetric encryption algorithms use the same key for encryption and decryption.

Data Integrity

To make sure that data is shielded against alterations that might be malicious or unintentional. Hashes or message authentication codes typically offer integrity. A fixed length numeric value created from a series of data is called a hash value. The integrity of data received across unsecured channels is checked using hash values.To ascertain whether

the data was altered, the hash value of the received data is compared to the hash value of the data as it was provided.

Authentication

To ensure that a specific party is the source of the data. Authentication is provided by digital certificates. Since hash values are far smaller than the underlying material they represent, digital signatures are typically applied to them.

Overview of Symmetric Key Algorithms

We always use the same key for both the encryption and decryption processes when using symmetric key encryption. The key advantages of this algorithm are its quick processing speed and minimal computational requirements. This method separates into block ciphers and stream ciphers as its two divisional modes. All data would be divided into chunks or blocks when using a block cipher. Data based on block size and a key would be provided for data encryption. Following the application of the encryption rule, the data will be divided into bits like 0101010101 and randomized using a stream cipher.The symmetric algorithm is quicker than the asymmetric algorithm.

Some General Algorithms for Symmetric Key

For symmetric key cryptography, there are many different algorithms available. We have discussed some fundamental symmetric key methods in this section.

- AES
- DES
- 3DES
- RC4
- Blowfish
- Twofish

Advanced Encryption Standards (AES)

AES was introduced by NIST (National Institute of Standards and Technology) in January 1997. It has a minimum block size of 128 bits for both encryption and decryption and is more reliable than the DES method. First the bytes are replaced, then the rows are moved, then the columns are shuffled, and finally a circular key is added. It can be used to secure both sensitive and non-classified goods.

Data Encryption Standard (DES)

This algorithm, which uses a block size of 64 bits, was created by IBM in 1997. Eight S-Boxes make up each of the 16 steps of the encryption process. The bits are first shuffled, followed by non linear substitutions, and lastly the XOR operation is used to obtain the result. The result is combined with the subkey of the given round using the XOR function. Subkeys are reversed throughout the decryption procedure.

Triple Data Encryption Standard (3DES)

It is one of the advanced version of the DES algorithm. This key has a total length of 192 bits and is very reliable. The key is initially divided into three separate subkeys, each 64-bit. The following steps are the same as in the DES algorithm, except that they are performed three times. The data is encrypted with the first key and then decrypted with the second key. Decrypted data is re-encrypted with a third key. However, there is a limited ability to keep data safe for longer.

RC4 Algorithm

Ronald Rivest created this algorithm. Continually exchanging state entries based on key sequence is necessary.The length of the key varies and can range from 1 to 256 bytes.It creates a stream using pseudo-random bytes, which is then XORed to change plain text into encrypted text. In comparison to the DES algorithm, the encryption method is ten times faster.

Blowfish

It is the most effective encryption algorithm currently in use. The length of the key varies and can be between 32 and 448 bits.The block size of it is 64 bits. There are only two fundamental steps to the process. Key expansion is carried out initially. There are 18 subkeys of 32 bits each in the P-array. There are four 32-bit S-boxes, each with 256 entries.Then, XOR techniques are used to encrypt the data. It has many uses for which the key is not regularly altered. Blowfish was created in 1993 by Bruce Schneier as an alternative to traditional encryption methods.

Two Fish Algorithm

The symmetric key block cipher Twofish has key sizes up to 256 bits and a block size of 128 bits.Although it placed in the top five in the AES competition, it was not chosen for standardization. Based on the older block cipher Blowfish, Twofish was created. Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, and Niels Ferguson were involved in its creation. The reference implementation of the Twofish cipher is now in the public domain, and the

algorithm itself is not protected by a patent. As a result, there are no constraints whatsoever on who can utilize the Two fish algorithm.One or two ciphers, including this one, are part of the OpenPGP standard (RFC 4880). However, compared to Blowfish, which has been around longer, Twofish has not experienced as much usage. The use of pre-computed key-dependent S-boxes and a moderately complex key schedule are two of Twofish's distinguishing characteristics. The actual encryption key is made up of one half of an n-bit key, and the other half is utilized to alter the encryption algorithm.

Secret Key Algorithm

Cryptography with a secret key A single key is utilized in secret key cryptography for both encryption and decryption. The sender encrypts the plaintext using the key (or a set of rules) before sending the ciphertext to the recipient. To decode the message and obtain the plaintext, the recipient uses the same key. Secret key cryptography is also referred to as symmetric encryption because a single key is utilized for both purposes. The key, which is actually the secret in this type of encryption, must be known by both the sender and the recipient. The distribution of the key presents the biggest challenge with this strategy, of course.

III. COMPARISON OF VARIOUS SYMMETRIC KEY ALGORITHMS

In this section, various aspects of the above mentioned algorithms are listed in form of a table to provide a clearer understanding of their commonalities & contrasts. The table provides a comparison of six of the contemporary encryption algorithm by looking at seven of their features.

Algorithm	Creator	Block Size	Key Lengths	Rounds	Algorithm	Effectiveness	Attacks
DES	IBM (1975)	64 bits	56 bits	16	Fiestel Network	Slow	Brute Force
3DES	64 bits	64 bits	64*3 = 192 bits	48	Fiestel Network	Slow specially in Software	Theoretically Possible
AES	J.Daemen and V.Rijmen (1998)	64 bits	128,192, 256 bits	9, 11, 13	Substitution Permutation Network	Effective in both Hardware & Software	Side Channel Attacks
RC4	Ron Rivest (RSA Security) (1994)	2064 bits, 1684 effective	40 – 2048 bits	256	Fiestel Network	Slow	Differential Attack
BLOWFISH	Bruce Schneier (1993)	64 bits	32 – 488 bits (128 default)	16	Fiestel Network	Efficient in Software	Differential Attack , Pseudorandom Permutation
TWOFISH	Bruce Schneier et al. (1998)	128 bits	128, 192, 256 bits	16	Fiestel Network	Efficient in Software	Truncated Differential Cryptanalysis (Partially Broken)

IV. FUTURE SCOPE ON SYMMETRIC CRYPTOGRAPHY

Several approaches based on symmetric key encryption have been proposed in the past. They ensure advanced information security. However, several questions remained unresolved. Effective revocation methods must be established for Oblivious Attribute certificates. To ensure equal security, data recovery must be fast and able to handle multiple computers. SOA can be used for large data transmission. Public key self-certification improves data security, but requires a lot of storage space. Therefore, techniques can be created that reduce both storage and handling requirements at the same time. Many parameters of digital watermarking include flexibility, transparency, security, capacity, complexity, etc. But we cannot reach them all at once. Based on this fact, a suitable algorithm can be created. One can explore how a huge message can be woven together in such a way that its force is preserved. Better encryption techniques improve system performance and work well in different situations.

V. CONCLUSION

Symmetric key algorithms play a crucial role in securing digital communication and data integrity. They rely on a shared secret key for both encryption and decryption processes, making them efficient and fast. However, their main challenge lies in securely distributing and managing these keys. Despite this, symmetric key algorithms are widely used in various applications, from securing internet connections (TLS/SSL) to encrypting sensitive files (AES). With proper implementation and key management practices, symmetric key algorithms provide a robust foundation for ensuring confidentiality and privacy in the digital realm. As technology advances, it is essential to continuously evaluate and adapt symmetric key algorithms to address emerging security threats and challenges.

REFERENCES

[1] Stallings W., “Cryptography and Network Security: Principles and Practices”, 4’th Ed., Pearson Education 2006, ISBN:81-7758-774-9

[2] Diffie W., Hellman M.E., New Directions in Cryptography”, IEEE Transactions on Information Theory, Vol. IT22 No. 6, November 1976, pp. 644-654

[3] E. Surya, C.Diviya, “A Survey on Symmetric Key Encryption Algorithms”, IJCSCN, Vol 2(4), 475-477, ISSN:2249-5789

[4] E. Thambiraja, G. Ramesh, Dr. R. Umarani, “A Survey on Various Most Common Encryption Techniques”,

IJARCSSE, Volume 2, Issue 7, July 2012 ISSN: 2277 128X

[5] Kapsepatil A., Prof. Shah P., "A Literature Survey on Symmetric Encryption Algorithms for Digital data", IJAIR, 2012 pp. 306-308, ISSN: 2278-7844

[6] Patil A, Goudar R, "A Comparative Survey Of Symmetric Encryption Techniques For Wireless Devices", IJSTR, Vol 2, Issue 8, Aug 2013, pp. 61-65, ISSN 2277-8616

[7] http://en.wikipedia.org/wiki/Cryptography

[8] Kahate, Atul. Cryptography and network security. Tata McGraw-Hill Education, 2013

[9] Raychev, Nikolay. "Classical cryptography in quantumcontext."Proceedings of the IEEE 10 (2012): 2015