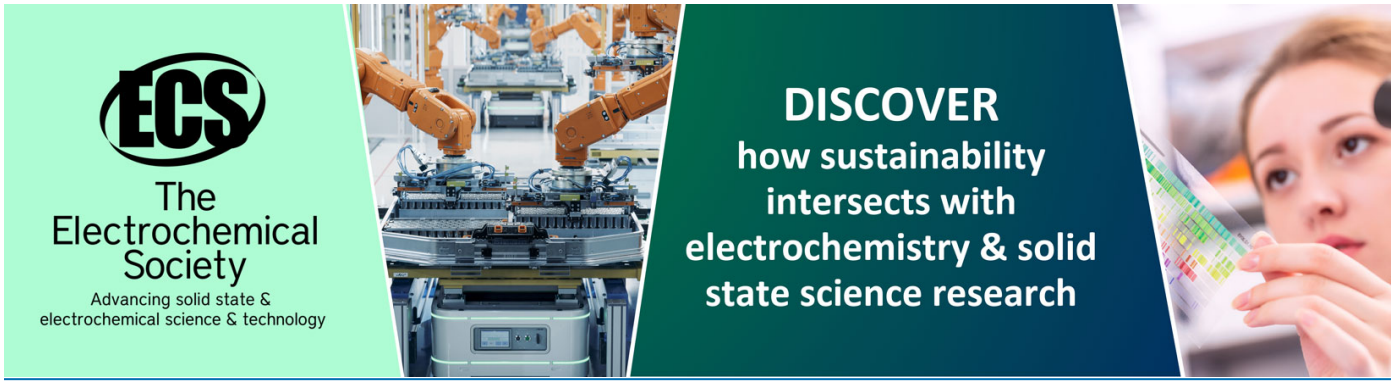
Systematic literature review: comparison study of symmetric key and asymmetric key algorithm



IOP Conf. Series: Materials Science and Engineering **420** (2018) 012111 doi:10.1088/1757-899X/420/1/012111

Systematic literature review: comparison study of symmetric key and asymmetric key algorithm

Priasnyomo Prima Santoso[1], Elkin Rilvani[1], Ahmad Budi Trisnawan[1], Krisna Adiyarta[1], Darmawan Napitupulu[1,2], Tata Sutabri[3], Robbi Rahim[4]

[1]Program Studi Magister Ilmu Komputer, Universitas Budi Luhur, Jakarta, Indonesia
[2]Research Center for Quality System and Testing Technology, Indonesian Institute of Sciences, Banten, Indonesia
[3]Fakultas Teknologi Informasi, Universitas Respati Indonesia, Jakarta, Indonesia
[4]School of Computer and Communication Engineering, Universiti Malaysia Perlis, Malaysia

Email: pnyomo@gmail.com, elkin.rilvani@pelitabangsa.ac.id, abudit75@gmail.com, krisna.adiyarta@budiluhur.ac.id, darwan.na70@gmail.com, tata.sutabri@urindo.ac.id, usurobbi85@zoho.com

Abstract. Cryptography is a science that studies how to keep data or messages safe when sent, from sender to recipient without interference from third parties. This paper presents a comparison of cryptographic algorithms of simetris keys and asymmetric keys. Cryptographic research related journals are collected and analyzed to find the correct comparison of cryptographic algorithms to implement. The results of this study, namely: symmetric and asymmetric keys have differences in the process of encryption and decryption. There are many cryptographic algorithms that can be applied to symmetric and asymmetric keys, but the selection and use of certain algorithms cannot be said to be forever the best because they depend on the circumstances encountered in developing the applied system.

1. Introduction

During the development of information technology in the computer world, the data security model plays a very important role. Security not only focuses on the data but also focuses on network security as data exchange traffic. Network security is a vital part of information security because it is responsible for maintaining the confidentiality of data on computer networks. One of the techniques applied to maintain data confidentiality in computer networks is cryptography.

Cryptography is a science that studies how to keep data or messages safe when sent, from sender to recipient without interference from third parties. This is in line with the development of computer network technology and the internet, the more applications that arise by utilizing network technology and demanding application level of secure data delivery.

Based on its type, cryptographic algorithm is divided into two types, namely: symmetric algorithm and asymmetric algorithm. The symmetric algorithm uses only one key to lock and open a message called a private key, while the asymmetric algorithm uses two different keys, one key to encrypt messages and another key to open or decrypt messages. But with the rapid development of cryptographic technology, the problems in the field is difficult to choose which cryptographic algorithm is appropriate to use and the process of application.

Symmetric algorithm is an algorithm where the encryption key used is the same as the decryption key so that the algorithm is also called a single-key algorithm. The key must be provided during the communication process for the encryption and decryption process. Based on the amount of data processed, symmetric key cryptography is divided into two types: block chiper and stream chiper. In the block chiper, the data is formed into blocks or data groups with certain data lengths (in a few bytes), so in a single encryption or decryption process the incoming data has the same size. While in the stream chiper, the data is divided into single bits or sometimes in a byte, so the data format is a stream of bits to then encrypt and decrypt [2].

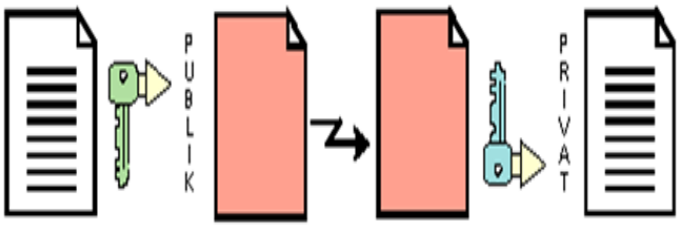


Figure 1. Symmetric key cryptography

The advantages of symmetric algorithms are higher operating speeds than asymmetric algorithms that can be used in real time systems. While the symmetrical algorithm weakness that lies in the difficulty in key management because it takes a different key for each different user. Examples of symmetric algorithms include Blow Fish, DES, AES.

Asymmetric algorithm is an algorithm where the encryption key used is not the same as the decryption key. In this algorithm used two keys namely public key (public key) and private key (private key). Public keys are publicly distributed, while private keys are kept confidentially by the user.Although the public key is known but it will be very difficult to know which private key is used [3]. Asymmetric algorithms have advantages at the security level where the keys are used differently for encryption and decryption processes and the keys used are longer than symmetric algorithms. While the weakness of the asymmetric algorithm with the increase in key length then increased also overhead on the data packet, resulting in lower operating speed. Examples of asymmetric algorithms include: RSA, DSA, Diffie-Hellman.

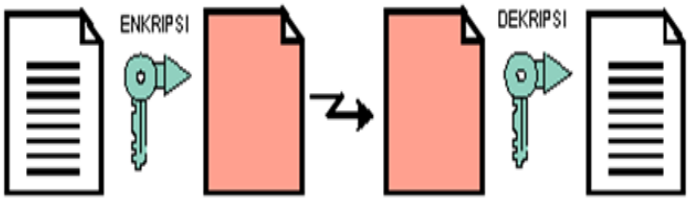


Figure 2. Asymmetric Key Cryptography

This study aims to conduct a review literature on the development of cryptographic algorithms and its application so that it can be known comparison cryptographic algorithm based on several criteria such as the strength of encryption, speed of operation, cost, Thus the state of the art can be obtained related to the advantages and disadvantages of various

cryptographic algorithms that exist today. In this study, the authors synthesize some literature related to the theme of research.

2. Methodology

The author obtained data, theory, and analysis derived from research that has been done in the form of papers and journals. The author uses google search engine with keyword "cryptography", then google will display the results of these keywords. Then the authors open the Wikipedia site that describes the specific cryptography and techniques that can be used. The author then did a keyword query back in google with keyword "cryptography journal". This keyword successfully displays journals and papers related to cryptographic techniques. The complete search and screening process of scientific articles can be presented in Figure 3 below:

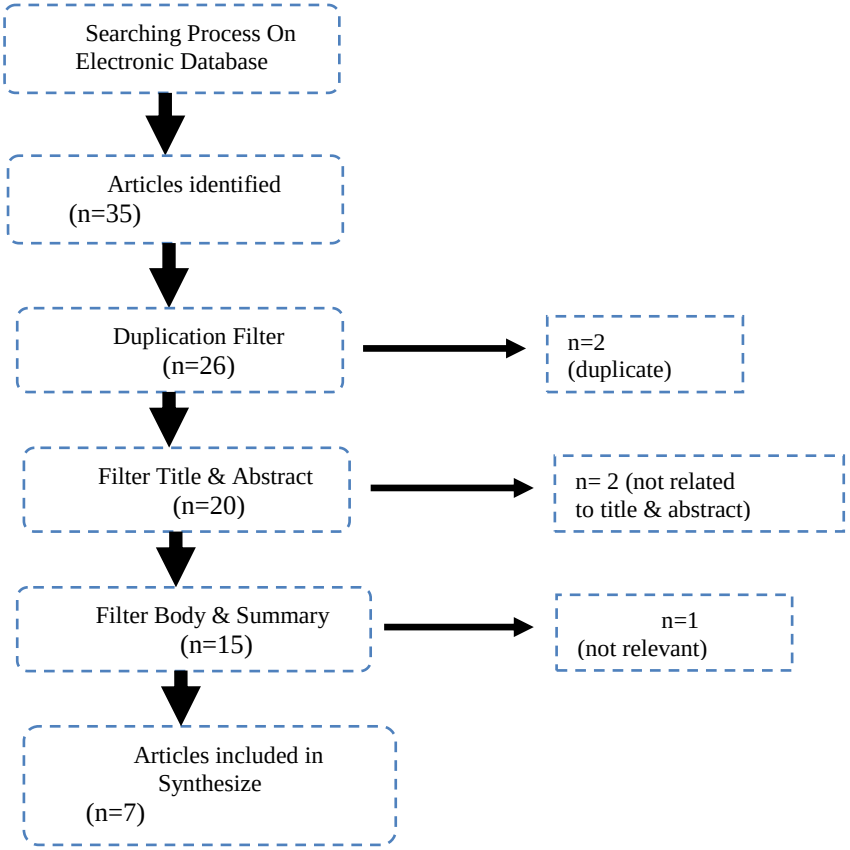


Figure 3. Article filtering process

The author gets a total of 12 articles related to cryptography, but only 7 articles are relevant to the research domain as follows: 3 journal articles derived from search results google search engine, while 4 other journal articles the author get from IEEE electronic database with keyword "cryptography algorithm". The entire seven (7) articles will be included in this study for analysis as they are considered to be significantly relevant to the context of this study. The algorithms are compared: cryptographic key algorithms (Blow Fish, DES, AES) and asymmetric keys (RSA, DSA, Diffie-Hellman). Parameters that are compared, among others: key types used, key length, encryption strength, tunability, speed of operation, implementation and power consumption used.

3. Result and Discussion

This section discusses various key symmetric cryptographic algorithms and asymmetric keys from several related literature review articles such as:

Research [1] presents a commonly applicable cryptographic method, in general classification consisting of two, Symmetrical and asymmetric methods. An analysis in the data security perspective and computational complexity using two types of cryptographic methods, in the test it is seen that both methods have the same accuracy, but more complexity on Asymmetric method, and time used in asimetric comput class criptography process tends to be more complex, but the data security level is more either using Asymmetric method.

Research [2] presents a comparison of studies between various encryption algorithms such as AES, DES, RSA and DIFFIE-HELLMAN, by comparing the different factors of both symmetric keys and asymmetric key encryption algorithms. Then the result of encryption technique in terms of symmetric lock and asymmetric key algorithm analyzed that symmetric key algorithm is considered good in speed and power consumption while asymmetric key algorithm in terms of tunability.

Research [3] presents the basic factor of insecurity over the internet is how much security the channel provides when transmitting data. Cryptography technology is one of the techniques that enable secure data transmission without loss of confidentiality and integrity. Based on the key distributions, cryptography is classified into two main types - symmetric key cryptography and asymmetric key cryptography. By comparing the importance of these two cryptographic techniques, the proposed algorithm proves to be very efficient on the basis of each but there are certain areas that remain open, linked to this algorithm, and have not been fully addressed. The paper also provides an appropriate future scope related to this open field.

Research [4] presents an overview of asymmetric key algorithms, beginning with the start of asymmetric cryptography from 1976 to the present. This article provides a description of the operation of encryption and decryption on each algorithm, showing it basic security, field of implementation, advantages and disadvantages during operation. The journal also shows an existing gap based on the conclusions drawn from the review, with particular emphasis on algorithms that are best suited to the application industry given the current trends.

Research [5] evaluates the performance of cryptographic algorithms to find out the best algorithms to use for the future. This paper compares the symmetric algorithms (AES, DES, Blowfish) asymmetric algorithms (RSA) with different file types such as binary, text and image files. A comparison has been performed using evaluation parameters such as encryption time, and decryption throughput. The simulation results are given to demonstrate the effectiveness of each algorithm.

Research [6] has surveyed several proposed mechanisms based on symmetric key cryptography and has made a comparative study base. This paper discusses the basic features, advantages, disadvantages and applications of various symmetric key cryptographic algorithms.

Research [7] presents peer analysis in the field of encryption algorithms and concentrates on private key blocks of ciphers commonly used for bulk data and encryption links. In this study also performed a comparison of some popular and efficient algorithms. This paper also focuses on the comparative study of all encryption techniques as a literature survey. The purpose of experimental research. This article extends to the performance parameters used in the process of encryption and analysis of security issues.

This section also presents performance comparisons of some key symmetric cryptographic algorithms (Blow Fish, DES, AES) and asymmetric keys (RSA, DSA, Diffie-Hellman) with various parameters. Parameters measured include key types used, key length, encryption strength, tunability, operating speed, implementation and power consumption used. The synthesis process results from all literatures related to the symmetric and asymmetric key algorithms could be presented in table 1 as follows:

Table1. Result of synthesize process

Algorithm	**Symmetric Key**			**Asymmetric Key**		
	BlowFish	**DES**	**AES**	**RSA**	**DSA**	**Diffie-Hellman**
Encryption and Decryption Key	Same **[3,5,6]**	Same **[1,2,3,4,5,6]**	Same **[2,3,5,6,7]**	Different **[1,2,4,5,7]**	Different **[3,4]**	Different **[2,3,5]**
Key Length	32 bits ‘till 448 bits **[3,5,6]**	56 bits **[1,2,3,4,5,6]**	128,192 or 256 bits **[2,3,5,6,7]**	>1024 bits **[1,2,4,5,7]**	5012 ‘till 1024 bits **[3,4]**	>1024 bits **[2,3,5]**
Encryption Strength	High **[3,5,6]**	Medium **[1,2,3,4,5,6]**	High **[2,3,5,6,7]**	High **[1,2,4,5,7]**	High **[3,4]**	High **[2,3,5]**
Tunability	Yes **[3,5,6]**	No **[1,2,3,4,5,6]**	No **[2,3,5,6,7]**	Yes **[1,2,4,5,7]**	Yes **[3,4]**	Yes **[2,3,5]**
Operating Speed	Fast **[3,5,6]**	Fast **[1,2,3,4,5,6]**	Fast **[2,3,5,6,7]**	Fast **[1,2,4,5,7]**	Fast **[3,4]**	Slow **[2,3,5]**
Cost	Expensive **[3,5,6]**	Expensive **[1,2,3,4,5,6]**	Cheap **[2,3,5,6,7]**	Expensive **[1,2,4,5,7]**	Expensive **[3,4]**	Depend on key **[2,3,5]**
Power Consumption	Very Low **[3,5,6]**	Higher than AES **[1,2,3,4,5,6]**	Higher thanBlow Fish **[2,3,5,6,7]**	High **[1,2,4,5,7]**	High **[3,4]**	High **[2,3,5]**

4. Conclusion

Based on the results of research that has been done can be concluded as follow scryptography has a fugsi as a keeper of message store mains a feand can be sent without any ganggan. That symmetric and asymmetric keys have their respective advantages and disadvantages in the use of the results of the synthesis that has been done.

Further researchsuggestions can be added comparative measurement variables, forex ample: variables calability, variable accuracy, ease of use variables and others. Subsequent research can also use the frame work in measuring variables when comparing types of cryptographic algorithms as symmetric and asymmetric keys, so the comparison process becomes easier and more specific.

5. References

[1] Basri B, 2016, Kriptografi Simetris dan Asimetris dalam Perspektif Keamanan Data dan Kompleksitas Komputasi, Jurnal Ilmu Komputer**2**, 2 p. 17–23.

[2] Bisht N and Singh S, 2015, A Comparative Study of Some Symmetric and Asymmetric Key Cryptography Algorithms International Journal of Innovative Research in Science, Engineering and Technology**4**, 3 p. 1028–1031.

[3] Chandra S, 2014, A comparative survey of symmetric and asymmetric key cryptography in International Conference on Electronics, Communication and Computational Engineering p. 83–93.

[4] Gaithuru J, 2015, A Comprehensive Literature Review of Asymmetric Key Cryptography Algorithms for Establishment of the Existing Gap, Malaysian Software Engineering Conference p. 236-244.

[5] Tripathi R and Agrawal S, 2014, Comparative Study of Symmetric and Asymmetric Cryptography Techniques, International Journal of Advanced Foundation and Research in Computer**1**, 6 p. 68–76.

[6] Chandra S Bhattacharyya S Paira S and Alam S, 2014, A Study and Analysis on Symmetric Cryptography in International Conference on Science, Engineering and Management Research IEEEp. 1-9.

[7] Mathur H and Alam P, 2015, Cryptology Algorithm, Int. J. Elmerging Trends Technol. Comput. Sci. **4**, 1, p. 4–6.