International Journal of Computer Networks and Communications Security

VOL. 7, NO. 5, MAY 2019, 96–103
Available online at: www.ijcncs.org
E-ISSN 2308-9830 (Online) / ISSN 2410-0595 (Print)

Comparative Study of Cryptography Algorithms and Its' Applications

Md. Navid Bin Anwar[1], Mahmud Hasan[2], Md. Mahade Hasan[3], Jafrin Zafar Loren[4] and S.M.Tanjim Hossain[5]

[1, 2, 3, 4, 5] Faculty of Computer Science, American International University- Bangladesh, Dhaka, Bangladesh

[1]navid826@hotmail.com, [2]mahmudh.jion@yahoo.com, [3]mehedi.jim@gmail.com, [4]lloren328@gmail.com, [5]tanjimhossain41@gmail.com

ABSTRACT

In modern world, security is the most valuable term in the field of communication system. Security comes along with many technologies and methods, where one of the most secure technologies is Cryptography where ordinary plain text is converted into cipher text for transferring data to the valid user. Cryptography algorithms can be divided into two types based on the number of keys such as Symmetric and Asymmetric where Symmetric algorithm works with one single key and Asymmetric algorithm works with two different keys. However, selecting the appropriate algorithms for specific application has been always a challenging task because of the latency, key size, and security issues. Cryptographic algorithms face different type of attacks like brute force attack, man in the middle attack, cycle attacks etc., which are still remained as threads. This paper presents the performance analysis, based on different performance metrics and threads, of various techniques of cryptographic algorithms and identifies the suitable algorithms for different types of applications.

Keywords: *Encryption, Algorithms, Symmetric, Asymmetric, Applications*.

1 INTRODUCTION

Cryptography is a process of translating the original plain text in to cipher text. The sender translates the plaintext in to cipher text. In this way when the data sends to receiver the sender translate the plaintext into chipper text. Then the receiver converts it to plaintext for reading data. The passion of the cryptography is to protect data from unauthorized access. When the data sends to receiver as chipper text, then third party can't access the data as the original form. The way that the plaintext hides the data is called encryption. The way of the encrypting the input or plaintext which is unreadable is called chipper text. The way that takes encrypting message to the receiver and translates as readable form is called decryption. Algorithms, use for Cryptography, can be divided into two main categories - Symmetric key cryptography and asymmetric key cryptography.

In Symmetric key cryptography, it's uses only one key to send data from sender to receiver. It uses private key and secret key number which can be number, word and also string. To use this method both parties (sender and receiver) must need to know the same key. Two common modes are use in this type of cryptography, one is called block ciphers and another one is stream ciphers [1]. Block ciphers handle groups of bits known as blocks where each block is processed multiple number of times. In block chippers the blocks are converted into a fixed-length blocks of plain text. In every round the key is applied in a manner which should be unique. Unlike block chippers, stream ciphers operates on one bit at a time where the data is encrypted by dividing it into small single bits. This is achieved by doing bitwise XOR operation.

In asymmetric key cryptography, two types of keys are used: one is used for encrypting the plaintext and another one is used for decrypting the cipher text. In this method, the key that is used for encryption is known as act as public key and it can be advertised by the owner to others, and the other key, used for decryption, which is only known to the valid user called the private key. [1][2].

In [1], comparison was done between symmetric (DES, 3DES, AES, Blowfish) and asymmetric (RSA, Diffe-Hellman, ECC) key algorithms based

of advantages and disadvantages along with the importance.

On a paper [3] some of selected algorithm for example DES, 3DES, AES, Blowfish (Symmetric) and RSA and Diffie Hellmen (Asymmetric) are analyzed based on key length where they found that DES works better.

In [4] performance analysis has been done based on security and challenge issues of different symmetric algorithms, such as - AES, DES, Blowfish and RSA algorithm in terms of using them in cloud computing.

From the above literature study, it has been found that the effectiveness of the symmetric and/or asymmetric algorithms varies greatly depending on different parameters, such as security threads, latency, key size.

In this paper we have focused on the performance analysis of the different algorithms for both symmetric and asymmetric cryptography based on their applications and security threads alongside with other parameters. This will enable the researchers or other network security service providers to select the appropriate algorithms for their system.

The paper presents the research works in according to the following sections, in section 3, different types of Symmetric Cryptographic Algorithms are presented, section 4. Presents different types of Asymmetric Cryptographic Algorithms. Performance analysis of different cryptographic algorithms according to their application is presented in section 5 and section 6 is the conclusion of the paper.

2 SYMMETRIC CRYPTOGRAPHY ALGORITHM

In this section various type of symmetric algorithms are individually discussed in terms of their working procedure, advantages and disadvantages.

2.1 AES Algorithm

AES (Advanced *Encryption* Standard) was first presented by Rijndael in Oct-2000. It was Designed by Vincent Rijmen and Joan Daemen in Belgium. It is a symmetric block cipher which can be in different block sizes, such as- 128, 192 and 256 bits. Essentially, encryption calculations are separated into three noteworthy classifications; simple division by key, substitution, and transposition. AES utilizes a round function that is thought about of four distinctive byte-arranged changes, for example, Sub byte, Shift row, Mix column, Add round key. Number of rounds to be utilized relies upon the length of key [3].

These numbers of rounds, AES compare between its own three block ciphers: AES-128, AES-192 and AES- 256. Each of this type both encrypts and decrypts data in block of 128 bits in measures of cryptographic keys. In this method of cryptography there is no extra room for acceptance additional block sizes and key length. The AES encryption algorithm performs in different stage of transformation. At first the cipher use the data to put into an array and after that it performs a number of encryption rounds. This round is based on key length such as 10 rounds for 128 bits, 12 rounds for 192 bit and 14 rounds for 265 bit keys. Then when this transformation is over creating a table of substitution with the data performs the second transformation with shifting the data in rows and then mixes columns. Finally, there is an exclusive or XOR operation at the different part of the keys.

As AES implemented in system as robust security protocol, the higher length of keys such as 128, 192 and 256 bits are encrypted in this method easily. The main uses of AES come with applications of wireless communication, financial transaction and e-commerce business. While the limitation of AES based on simplified algebraic architecture and as every block is encrypted.

2.2 BLOWFISH Algorithm

Blowfish algorithm uses variable length block cipher with the key size of 64-bit. It was discovered in 1993 by Bruce Schneier [5][6[7]. In Blowfish the key length can be varied from 32 to 448 bits. This calculation is a 16 round Fiestel figure and it utilizes a huge key ward S-boxes [6]. Blowfish requires around 5KB of memory. Blowfish as a rule utilizes a one of a kind type of key generation [8]. In the key expansion phase, it creates a table (4168 bytes) of sub-keys by converting the single key up to 448bits [8]. This generating sub-keys increase security. Blowfish can make longer key with the goal that it's so hard to endeavor to hack the key.

The algorithm comprises of two sections: first one known as key-expansion part and next one is data encryption part [9]. Key expansion changes over a key of at most 448 bits into a few sub-key clusters totaling 4168 bytes. Data encryption happens commonly by means of a 16-round arrangement. There is a key-dependent permutation in each round, and substitution is done by a key and data. By using XORs and additions on 32-bit words all of these operations are done. A four indexed array data looksup operation is also done additional to the above operations [9].

Blowfish is uninhibitedly utilized. After the key timetable has finished, Blowfish is a moderately quick block cipher, because of the modest number of rounds (sixteen) and the straightforwardness of the round [10].

Blowfish algorithm can't give confirmation and non-denial as two individuals have same key. The key timetable in Blowfish is somewhat tedious. The small block size of Blowfish (64 bits) is more helpless against the attacks than the 128 bits utilized by AES [10].

2.3 DES Algorithm

DES (Data Encryption Standard) was developed in 1970 at IBM by Horst Feistel. This encryption standard was recommended by National Institute of Standards Technology [11].

DES deals with the input that is 64 bits of plain text where it constructs cipher text. The cipher text is 64 bits. Regardless of whether 64 bit key is the genuine input, the key length is 56 for this calculation. DES perform it's operation by substitution and permutation in total of 16 rounds. Consequently, key and data bits are permutated, XORed, shifted and then they are passing through 8 boxes. Following the lookup table is a basic step of DES algorithm. The Decryption process is performed in reverse. This makes it a symmetric key algorithm [4]

The DES algorithm's encryption and decryption speed is fast in terms of other symmetric algorithms. One of the important advantages is with having used DES; swifter public-key techniques can be made. DES uses the least memory while encryption time [11]. On the other hand, DES is considered weak and insecure because it was recorded with many attacks as the key length is 56 which are too small [12]. The application of DES is popular encryption technique where this processes images like JPEG format and Bitmap image.

2.4 3DES Algorithm

3DES or the Triple Data Encryption Algorithm was produced to address the conspicuous defects in DES without de-marking a radical new cryptosystem [13]. To make a sufficiently robust cryptosystem the advancement of 3DES is done. As the double DES was unable to provide sufficient protection of a compromise user; therefore, 2DES was supplanted by 3DES. [14]

3DES works similarly as DES, with the exception of that experiences three times amid the encryption procedure, followed by encryption, unscrambling, and another encryption. The key length uses in 3DES is 192 bits (64 bits x 3 keys), however its genuine quality is 168 bits (56 bits x 3 keys). Although, 3DES is more secure than DES, but additionally it implies that it is more (3x) slower in processing [15]. One thing is critical that every one of the three keys must be extraordinary. On the off chance that any of the keys are observed to be same, it will be less demanding for an intruder to find the plaintext.

3DES cipher experiences a crucial shortcoming connected to its little (64-bit) block size. Additionally, there is currently a reasonable, moderately quick attack on 64-bit block cipher that gives aggressors a chance to recoup validation treats and different qualifications from HTTPS-secured sessions [16]. Along with this still 3DES use in password protection of user content and system data.

3 ASYMMETRIC CRYPTOGRAPHY ALGORITHMS

In this section various type of asymmetric algorithms are individually discussed in terms of their working procedure, advantages and disadvantages.

3.1 RSA Algorithm

In 1978 RSA was composed by Ron Rivest, Adi Shamir, and Leonard Adleman .It is the most popular public key algorithm. It's a standout amongst other known open key cryptosystems [17].

RSA is an asymmetric cryptosystem. There are two diverse keys. RSA is most widely known as public key cryptosystem, since one of them is shared with everybody. The other key is private since its kept secret. RSA is based on mathematical fact.

The RSA is considered reliable and safe for its secrecy and privacy features. RSA also offers integrity where the content stays in its original form in exchange phase. Disadvantages of RSA is that it takes longest encryption time.it requires of similar lengths for c and which is not easy to meet the requirement .Padding techniques are required in this case which leads to more processing time [18]. RSA is used mostly in hybrid encryption schemes and digital signatures and also in web browsers, chat applications, email, VPNs and some other kinds of interchanges that require safely sending information to servers or individuals.

3.2 DSA Algorithm

A digital signature algorithm (DSA) alludes to a standard for digital signatures [19]. The National Institute of Standards and Technology (NIST) presented DSA in 1991 for making digital signatures. DSA does not encode message digests utilizing private key or decode message digests utilizing public key. Rather, it utilizes extraordinary scientific capacities to make a digital signature comprising of two 160-bit numbers [19].

In DSA If the digital signature isn't checked by the general public key, at that point the recipient should just stamp the message as invalid [21]. Additionally, in some states and nations does not have any laws considering digital and innovation issues. In spite of the fact, digital signature gives validness yet it doesn't guarantee secrecy. Keeping in mind the end goal is to give the security, some other method, such as- encryption and unscrambling should be utilized. DSA used in web application where user data and content transfer during email.

3.3 ECC Algorithm

Elliptic curve cryptography was presented in the mid-1980s,by Koblitz and Miller as a promising option for cryptographic conventions in light of the discrete logarithm issue in the multiplicative gathering of a limited field [22[23].

ECC is same as RSA but different is that it has fast solving capacity and has different way of cryptographic algorithm. The ECC's security key length is smaller than other asymmetric algorithms and its key length is only 163 bit. ECC and RSA takes full-exponential time and sub-exponential time respectively. For a case, if the key size of RSA is m then 1024 piece takes 4*10m MIPS years with best known assault ECC with 160 piece key size takes 12.6*10m MIPS. It uses elective curve equation in lieu of traditional prime numbers. Most of the execution time spends on scalar multiplication. ECC provides same security as other algorithms but in smaller key sizes.

The whole security of ECC rely upon the capacity to figure a direct increase and powerlessness toward process the multiplicand given the first and item point [22]. The ECC provides decent authentication in RFID system. For small key size it can use in wireless sensor networks like tablet, mobile phones.

Most significant privilege is that ECC provides good security with small key size which provides faster computational capabilities. On the other hand, it expands the extent of the encrypted message essentially more than RSA encryption. This algorithm is more confounded and hard to actualize than RSA, which improves the probability of usage blunders, subsequently lessening the security of the algorithm. ECC is utilized as a part of key trade for internet browser use additionally in a portable setting, including mobile phones and the Internet of Things.

4 PERFORMANCE ANALYSIS

The performance result analysis of different symmetric and asymmetric algorithms is done based on various performance metrics. These metrics decide which algorithm performs better than others. The following performance metrics are analyzed-

- ***Key length:*** Key length is the number of bits in a key used by a cryptographic algorithm which determined the time complexity of transferring the data to the sender and receiver ends.
- ***Block Size:*** A block is an arrangement of bytes or bits, typically containing some entire number of records, having a greatest length, a block size. data in this way organized are considered to be blocked.
- ***Round:*** Round is a function, which measures how much time the operation needs to perform for retrieve data.
- ***Vulnerabilities:*** Weakness points of a system which can be exploited by attacker.
- ***Efficiency:*** Determines how fast or slow it behaves when implemented in hardware and software.
- ***Applications:*** Performance area of algorithm with specific function directly for the user or, in some cases, for another application program. Identify the best protocol for different applications in computer networking system.

Table 1: Performance Analysis of Symmetric Cryptography Algorithms

Performance Metrics	AES	BLOWFISH	DES	3DES
Key-Length (bits)	128,192,256	32-448	56	112,168
Developed	2000	1993	1975	1978
Block Size	128	64	64	64
Security	Mostly Secure	Unpatented and royalty-free	Proven Inadequate	Adequate security
Possible thread	Side channel attack	Brute force attack	Brute force attack, man in the middle attack	Channel attacks
Rounds	10,12,14	16	16	48
Efficiency	Fast	Fast	Slow	Fast for hardware but Slow in software
Applications	Wireless communication ,Bank	Database Security, E-Commerce Software	Image processing	Smart Card, e-payment

TABLE 2: Performance Analysis of Asymmetric Cryptography Algorithms

Performance Metrics	RSA	DSA	ECC
Key-Length (bits)	1024-2048	2048-3072	160
Developed	1977	1991	1980
Block Size	192	Variable	80
Security	Medium high level of security	Mostly Secure	Mostly Secure
Possible thread	Cycle Attacks, Sharing of common modules	Set of parameters can be generated for pre-chosen message	Curve generation attacks, zero-value point attack
Rounds	1	16	1
Efficiency	Slow in hardware specially when decryption	Slow for both software and hardware	Slow for both software and hardware
Applications	Internet Banking	Web application and email verification	Key exchange over web and mobile.

5 DISCUSSION

After analyzing AES in table1 we can see that breaking a 128 bit AES key could take more than the age of the universe while use a supercomputer is being used and boxcryptor even uses 256 bit keys [24][25][26][27]. Till now there is no specific attack against AES has been reported, therefore AES is considered the encryption standard for wireless communications, governments, banks, where the high level security is the main concern [24][26]. Blowfish algorithm is used for database security(ex: IDS Server) and E-Commerce Software(ex: Avactis Shopping Cart, CS-Cart) [28][29]. As the key does not change frequently therefore Blowfish is suitable for these kinds of application. It works faster than most of other encryption algorithms where the large data caches are being considered on a 32-bit microprocessor. Blowfish also is a relatively fast block cipher due to the small number of rounds and simplicity of the round operation [30]. For Image processing system DES is better, as it has small key and block size which will enable high transmission rate with moderate security during image transmission [31][32]. For smart card (integrated circuit card) or e-payment purpose 3DES algorithm can be used although it's performance is slow in terms of software because of triple phases of DES but it is very cheap for hardware implementation [33].

The result analysis for RSA in table 2 explains that this algorithm can be used for mobile banking system [34][35]. RSA has higher key length , block size and slower efficiency which increases time complexity. Besides RSA provides a secure transmission over transmission channel which provides the system a good security. While DSA can be used in web application and email verification based on performance metrics [36] [37]. Since it has a larger number of key lengths and block size depends on variable along with measurement, higher security and efficiency which makes the system much secure. ECC works better in key exchange over web, mobile [38][39]. ECC's efficiency is lower terms of all performance metrics except numbers of round. Because of small key sizes it performs faster than remaining both.

6 CONCLUSION

In this paper a comprehensive study is done based on the performance of different cryptographic algorithms to determine which algorithm is best for a specific field of application. The performance analysis is done based on following parameters - Key-Length, Block Size, Security, Possible thread, Rounds, Efficiency. Although symmetric and asymmetric algorithms both are well popular techniques for protecting the data but based on the result analysis and discussion we can conclude that symmetric cryptography algorithms such as – AES, BLOWFISH, DES, 3DES are more suitable for the applications like wireless communication, JFile, image processing, smart card or e-commerce type of serveries respectively. On the other hand, asymmetric cryptography algorithms such as – RSA, DSA, ECC are the best choice for the applications like Internet banking, web application, email verification, key exchange over web, mobile. This work can be extended in the future by evaluating more cryptographic techniques and schemes to identify their possible field of applications.

7 REFERENCES

[1] Sourabh Chandra, Smita Paira, Sk Safikul Alam, Dr.(Prof.) Goutam Sanyal "A comparative survey of symmetric and asymmetric key cryptography", IEEE 2nd International Conference on Electronics, Communication and Computational Engineering (ICECCE), 2014.

[2] RSA Laboratories- Chryptographic tools; section 2.1.5. unpublished;http://www.rsa.com/rsalabs/node.asp?id=2174.

[3] Ritu Tripathi, Sanjay Agrawal "Comparative Study of Symmetric and Asymmetric Cryptography Techniques" International Journal of Advance Foundation and Research in Computer (IJAFRC) Volume 1, Issue 6, June 2014. ISSN 2348 – 4853.

[4] Rachna Arora, Anshu Parashar, "Secure User Data in Cloud Computing Using Encryption Algorithms", International Journal of Engineering Research and Applications (IJERA) , Vol. 3, Issue 4, Jul-Aug 2013, pp.1922-1926.

[5] Schneier, B.: "Description of a New Variable-Length Key, 64-BitBlock Cipher (Blowfish)", Fast Software Encryption, Cambridge Security Workshop Proceedings(Dec. 1993), Lecture Notes in Computer Science(LNCS) Springler verlag Vol. 809, pp. 191-204,1993, ISBN 3-540-58108-1.

[6] https://ieeexplore.ieee.org/abstract/document/5942029/

[7] B. Schneier, "Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)", Fast Software Encryption, Cambridge Security Workshop proceedings December 1993, Springer-Verlag, 1994, pp. 191-204 .

[8] https://study.com/academy/lesson/blowfish-encryption-strength-example.html

[9] Nie, T., & Zhang, T. (2009). "A study of DES and Blowfish encryption algorithm". In TENCON 2009 - 2009 IEEE Region 10 Conference. IEEE

[10] https://www.commonlounge.com/discussion/d95616beecc 148daaa23f35178691c35

[11] Yvo Desmedt, Jean-Jacques Quisquater, "Public-Key Systems Based on the Difficulty of Tampering (Is there a difference between DES and RSA)".

[12] Yogesh Kumar, Rajiv Munjal, Harsh Sharma," Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures", IJCSMS International Journal of Computer Science and Management Studies, Vol. 11, Issue 03, Oct 2011.

[13] "3DES", http://www.cryptosys.net/3des.html

[14] T. Sobh, K. Elleithy and A. Mahmood, "Novel Algorithms and Techniques In Telecommunications", Automation and Industrial Electronics. Springer Science Business Media B. V., Bridgeport. (n.d.).

[15] http://codenamekidnextdoor.blogspot.com/2011/09/explaining-triple-data-encryption.html

[16] https://www.infoworld.com/article/3112324/security/ new-collision-attacks-against-triple-des-blowfish-break-https-sessions.html

[17] Gurpreet Singh, Supriya, "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security", International Journal of Computer Applications (0975 – 8887) Volume 67– No.19, April 20

[18] Dr. Prerna Mahajan & Abhishek Sachdeva, "A Study of Encryption Algorithms AES, DES and RSA for Security", Global Journal of Computer Science and Technology Network, Web & Security Volume 13 Issue 15 Version 1.0 Year 2013.

[19] https://www.techopedia.com/definition/27504/digital-signature-algorithm-dsa.

[20] https://www.di-mgt.com.au/public-key-crypto-discrete-logs-4-dsa.html

[21] https://lerablog.org/technology/data-security/advantages-and-disadvantages-of-digital-signatures/

[22] Rahat Afreen and S.C. Mehrotra, "A Review on Elliptic Curve Cryptography for Embedded Systems", International Journal of Computer Science & Information Technology (IJCSIT), Vol 3, No 3, June 2011.

[23] https://searchsecurity.techtarget.com/definition/elliptical-curve-cryptography148daaa23f35178691c35

[24] .https://www.quora.com/What-are-the-applications-and-advantages-of-AES

[25] https://www.eetimes.com/document.asp?doc_id=1275908

[26] https://www.jscape.com/blog/aes-encryption

[27] http://www.rfwireless-world.com/Terminology/Advantages-and-disadvantages-of-AES.html

[28] https://www.schneier.com/academic/blowfish/products.html

[29] https://www.ukessays.com/essays/computer-science/blowfish-algorithm-history-and-background-computer-science-essay.php

[30] https://www.commonlounge.com/discussion/d95616beecc148daaa23f35178691c35

[31] Qian Gong-bin, Jiang Qing-feng, & Qiu Shui-sheng. (2009), "A new image encryption scheme based on DES algorithm and Chua's circuit". In 2009 IEEE International Workshop on Imaging Systems and Techniques. IEEE.

[32] https://www.scientific.net/AMM.644-650.2202

[33] Tsague, H. D., Nelwamondo, F., & Msimang, N. (2012), "An Advanced Mutual-authentication Algorithm Using 3DES for Smart Card Systems". In 2012 Second International Conference on Cloud and Green Computing. IEEE.

[34] https://www.researchgate.net/publication/272816109_Mobile_Payment_Method_Based_on_Public-Key_Cryptography

[35] https://sushi2k.gitbooks.io/the-owasp-mobile-security-testing-guide/content/0x04g-Testing-Cryptography.html

[36] Chen Tianhuang, & Xu Xiaoguang. (2010), "Digital signature in the application of e-commerce security". In 2010 International Conference on E-Health Networking Digital Ecosystems and Technologies (EDT). IEEE.

[37] https://security.stackexchange.com/questions/164743/dsa-digital-signature-algorithm-how-is-it-applied-in-web-applications-layman-e

[38] https://resources.infosecinstitute.com/ecc-case-mobile-encryption/#gref

[39] http://www.ijarcst.com/doc/vol4issue1/cnithiya

AUTHOR PROFILES:

Md Navid Bin Anwar received Master of Science (M.Sc) in the domain of Electrical Engineering, Information Technology and Computer Engineering from the RWTH Aachen University, Germany. His research interest includes Information Security, Internet of Things and wireless sensor networks.

MAHMUD HASAN received Bachelor of Science (BSc) in Computer Science and Engineering from the American International University-Bangladesh (AIUB) in 2018. His

research interest includes Systems & Networking, Cryptography and Software Engineering.

MD.MAHADE HASAN received Bachelor of Science (BSc) in Computer Science and Engineering from the American International University-Bangladesh (AIUB) in 2018. His research interest includes Information Security, Artificial Intelligence and Software Engineering.

S.M.TANJIM HOSSAIN received Bachelor of Science (BSc) in Computer Science and Engineering from the American International University-Bangladesh (AIUB) in 2018. His research interest includes Data Science, Networking and IOT.

JAFRIN ZAFAR LOREN received Bachelor of Science (BSc) in Computer Science and Engineering from the American International University-Bangladesh (AIUB) in 2018. Her research interest includes Networking, Artificial Intelligence and Software Engineering.