Symmetric and Asymmetric Encryption Algorithms in Cryptography

M.Sowmiya, S.Prabavathi

Abstract*: *Security is the most challenging issue in today's internet world. Internet related applications and its relevant data are need to be exchanged over the internet increasingly. Hence it is necessary to provide security for the data to be transmitted. Cryptography is one such category, that provides security for data. The security of data over internet transmission is achieved through several encryption algorithms developed in Cryptography. This paper analyzes the performance of various encryption algorithms used in Cryptography and indicates which is the best algorithm based on some parameters.

Index Terms: Security, Cryptography, Encryption.

I. INTRODUCTION

The development in networking technologies has made the data to be exchanged drastically. The transmitted data is vulnerable to several attacks by intruders. The data can be copied or altered by the external parties of the network, who are called as attackers or hackers. So, Cryptography took place in creating some new techniques for protecting the data of the user. Cryptography is the art of making the data secure by converting the actual data into other forms such that it is unknown to the attacker even if the information is hacked. It makes the data to be scrambled for unauthorized users. Cryptography defines two basic types of secrecy, called as encryption and decryption. Encryption is the method of making the facts unknown or scrawled to the attacker. It has many types of algorithms for scrambling the data. The data to be transmitted is called as plain text, whereas the data created by means of the encryption algorithm is called as secret message.

Decryption is the procedure of breaking out the secret message into original data. The attacks on the plaintext can vary into two types namely, Active attacks, and Passive attacks. Active attacks are those that reads as well as alters the plain text message that has been transmitted. Passive attacks are those that can only read the plain text message. This type of attacks is unknown to the user. Cryptography is mainly designed to ensure four important security functionalities. They are defined in the following section.

Primary Functions of Cryptography Confidentiality: Ensuring that except the planned receiver, no one can read the message. Authentication Verifying the identity of the sender of the information and ensuring the received data has been sent only by the authorized user.

Revised Manuscript Received on December 22, 2018.

M.Sowmiya, Department of IT, M.Kumarasamy College of Engineering, Karur, 639 113.
sowmiya.m90@gmail.com
S.Prabavathi, AP / IT,M.Kumarasamy College of Engineering,Karur, Prabavathis.it@mkce.ac.in

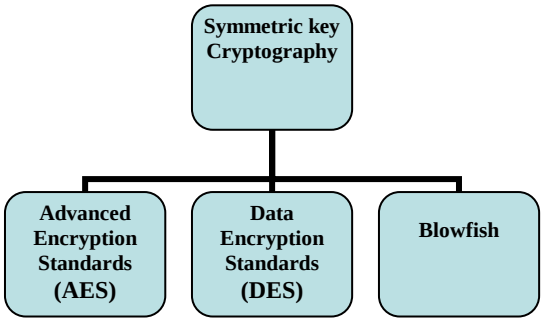
Integrity Guaranteeing the receiver that the established message has not lost its uniqueness. Non-repudiation:

It is a functionality that assures the sender as well as the receiver for data communication. Access control Only approved parties are permitted to admittance the information.

Classification of Cryptographic Algorithms:

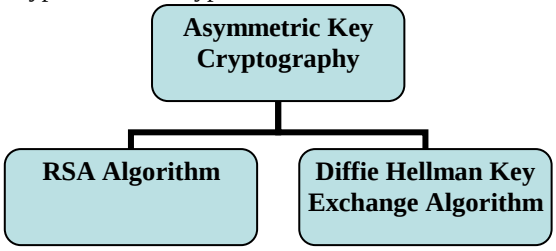
Cryptography is broadly classified into two categories:

Symmetric key Cryptography This technique uses a sole key for both encryption and decryption. Hence it requires less computing time and reduced processing overhead. Symmetric key cryptography can be employed in two ways namely, block cipher and stream cipher. Block cipher mode of operation, works by taking the complete message as a single block. Stream cipher works by separating the data into single bits. The separated bits are then randomized, and then made use for encryption. Symmetric algorithms are further classified as follows:



Asymmetric key Cryptography

This method practices two diverse keys for both encryption and decryption. They are termed as public key and private key. Public key is known to both the sender and the receiver whereas private key is known only to themselves. Private key is used to encode the plain text message and public key is used to decrypt the cipher text. Asymmetric key Cryptography needs more processing since, different key is used for encryption and decryption.



2.0. Related Works:

This section discusses about various methodologies and techniques for encryption.

Ritu Tripathi has made a comparison of symmetric and Asymmetric key algorithms and used some of the parameters like throughput,

time consumption, key length etc.,

E. Surya has proposed a study on the comparison of various symmetric key algorithms and concluded one of the algorithms to be the best of use. This paper shows the variable use of the symmetric key algorithms.Dr. Prerna Mahajan have analysed AES, DES and RSA algorithms for their ability to secure data and the time spent on encryption and decryption. Analysis of the encryption techniques used for securing the data has been made by John Justin.M and he concluded that symmetric algorithms are better in performance when compared to asymmetric cryptography algorithms in terms of time, speed.

3.0. Overview of Symmetric key Encryption Algorithms:

The proposed work makes a comparison on different encryption algorithms based on few parameters such as key length, plain text length, speed and several other factors too.

3.1 Advanced Encryption Standards (AES):

AES was established in the year 2001 by National Institute of Standard and Technology (NIST). AES is a symmetric encryption technique that follows a block cipher approach. The block size of the plain text can be 128 bits. The key length is often 16 or 24 or 32 bytes. Supported, the key length the AES can be termed as AES-128, AES-192, or AES-256. This algorithm performs operations on 8 – bit bytes.

It takes each block as a single 128bit block into 4 × 4 square matrix and stores it into an array called state array. State array is changed at every stage of encryption and decryption. Based on the size of key the algorithm follows different rounds such as:

128 bits – 10 rounds

192 bits – 12 rounds

256 bit – 14 rounds.

The key is expanded and used in AES. The AES algorithm performs its task by using four transformation functions. They are explained as follows;

Substitute Bytes:

S-Box implementation is used in substitute bytes transformation. The size of the S-Box is 16 × 16 matrix. The size of input and output is 8 bits. The first four bits are assumed to be the row number and the next four bits are assumed to be the column number.

The output of the previous transformation function is stored in the sate array and processed in this step as follows. The function considers each column input as one word. It multiplies it with a predefined matrix and again stores it into state array.

Add Round key:

This is the stage where the key is actually used. It performs XOR operation with the state array and the key. Thus, this stage gives the final output of the algorithm.

The decryption of AES algorithm is made reversing each stages of the transformation function. The Substitute byte, Shift Rows and Mix Column functions makes use of the inverse functions where as the XOR operation done at the Add Round Key stage is done as such, without any inverse function.

3.2 Data Encryption Standards (DES):

DES was one of the commonly used encryption schemes in the earlier days, before the establishment of AES algorithms. DES was developed in the year 1977 by National Institute of Standard and Technology. It is form of block cipher approach, in which the input is taken as 64bit block and the size of the key 56bits. This technique uses the equivalent key for both encryption and decryption. The algorithm begins by passing the plain text into initial permutation (IP), which rearranges the bits of plaintext. This algorithm performs permutation and substitution operation in sixteen rounds. For each round, a subkey is formed by performing permutation and left circular shift on the keys. The leftward and rightward halves of the output of the last round is swapped to form a preoutput. This is then passed to IP-1 to get the final output.

The decryption process of DES is the use of same algorithm excepting that the application of subkeys is reversed. Also, the primary and concluding permutations are inverted.

3.3 Blowfish:

Blowfish is one of the familiar techniques of symmetric key block cipher encryption scheme. This method was designed in the year 1993 by Bruce Schneier. The structure of blowfish is Feistel Cipher technique. The algorithm takes 64bit block as input and the key size may vary from 32-448 bits. The key size is greater as it is hard to breakdown the cipher.

4.0 Overview of Asymmetric key Encryption Algorithms:

This section discusses about the RSA algorithm and Diffie Hellman Key Exchange algorithm. These two algorithms remain for evaluation to understand the asymmetric key concept.

II. RSA ALGORITHM:

RSA algorithm is a new approach of public key cryptosystems. The algorithm was developed in the year 1977 and published in the year 1978 by Rivest, Adi Shamir and Len Adleman. This algorithm takes numbers as input of size 0 to n-1 for some n.

Typically, the size of n is 1024 bits. The encryption algorithm is as follows:

Let the plain text be M < n

Select two prime numbers p, q

Compute n = p × q

Compute $\phi(n) = (p-1)(q-1)$

Choose integer e

Compute $d = e^{-1} \pmod{\phi(n)}$

Public key – {e,n}

Private key – {d,n}

Therefore, the ciphertext is $C = M^e \bmod n$

The decryption process computes the plain text from the received cipher text:

$M = C^d \bmod n$.

RSA algorithm shows satisfactory level of security if the size of the key is high.

4.2 Diffie Hellman Key Exchange Algorithm:

Diffie Hellman Key Exchange algorithm is used to enable two users to exchange the secret key in a secure manner. The procedure itself is limited to exchange of secret values.

The algorithm works by choosing a prime number q and an integer α which is the primitive root of q. These two values are publicly known numbers to the user A and user

B. Then both the users choose random integers as their respective private keys such that XA<q and XB<q.
Then the users compute public key using the formula, YA = α XA mod q & YB = α XB mod q.
The key to be exchanged is then computed using the following formula:
User A: K = (YB) XA mod q
User B: K = (YA) XB mod q
The results of both the users are exchanged as a secret value.
5.0 Results:
The comparison table of symmetric and asymmetric algorithms is shown below on the basis of their input size, key length, speed, key used, and power consumption. It will be much better to understand the concept of all the described algorithms by making an interpretation on the table. Further the encryption/decryption time of the AES, DES & RAS algorithms for varying message size is also shown in the graph

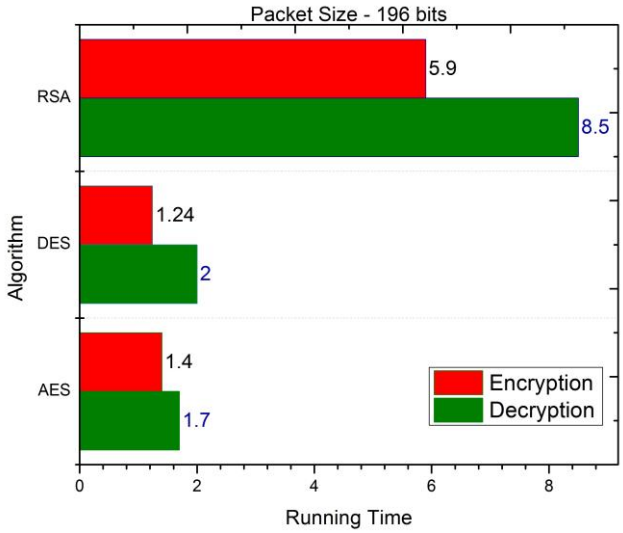


Fig 1: Comparison graph chart to show the performance level of AES, DES and RSA algorithms, for the packet size of 196 bits.

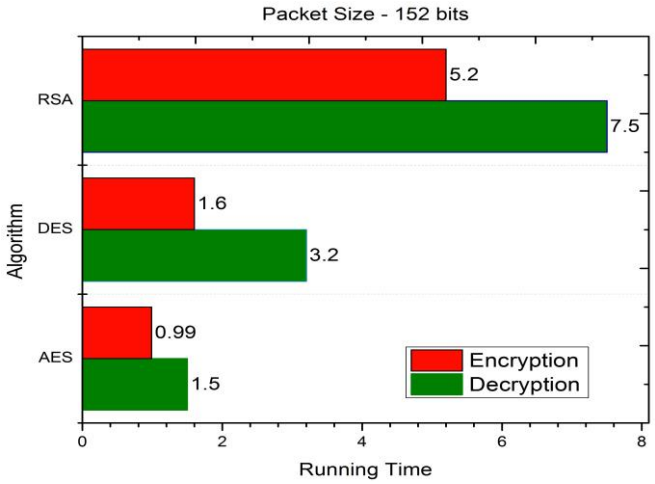


Fig 2: Comparison graph chart to show the performance level of AES, DES and RSA algorithms, for the packet size of 152 bits.

III. CONCLUSION

From the analysis made on various algorithms, it can be concluded that symmetric algorithm shows less time consumption since it uses a single key for encryption and decryption. Speed level of symmetric algorithms seem to be better than asymmetric algorithm. When compared to security, RSA algorithm shows high level of security since it uses the factoring of high prime number for key formation. From the graph it is evident that AES and DES algorithms shows less encryption/decryption time whereas RSA shows the longest encryption/decryption time.

REFERENCES

1. International Journal of Advancements in Research & Technology, Volume 1, Issue 6, November-2012 ISSN 2278-7763.
2. Consumer Perception and Buying Decisions by SyedaQuratulainKazmi.
3. Journal of Marketing and Consumer Research www.iiste.org ISSN 2422-8451 An International Peer-reviewed Journal Vol.13,2015.
4. https://www.techopedia.com/definition/26363/online-marketing
5. https://usatodaytn.com/blog/what-is-online-marketing
6. https://www.thebalancecareers.com/get-to-know-and-use-aida-39273
7. The McCraw-Hill 36 Hour Course "Online Marketing" by Lorrie Thomas
8. The Impact of Customer Satisfaction on Online Purchasing: A Case Study Analysis in Thailand by TaweeratJiradilok, SettapongMalisuwan, NavneetMadan, and JesadaSivaraks; Journal of Economics, Business and Management, Vol. 2, No. 1, February 2014 Page 5-11.
9. Customer Satisfaction in Online Shopping: a study into the reasons for motivations and inhibitionsbyRashed Al Karim; IOSR Journal of Business and Management (IOSR-JBM) e-ISSN: 2278-487X, p-ISSN: 2319-7668. Volume 11, Issue 6 (Jul. - Aug. 2013), PP 13-20 www.iosrjournals.org
10. A Study on Customer Satisfaction towards Online Shopping by P Jayasubramanian, D Sivasakthi, K AnanthiPriya; International Journal of Applied Research 2015;1(8):P 489-495.
11. A Study on Customer Satisfaction on Online Marketing in India by S. Chitra, E. Shobana; International Research Journal of Management, IT & Social Sciences (IRJMIS) Available online at http://ijcu.us/online/journal/index.php/irjmis Vol. 4 Issue 1, January 2017, pages: 93~98.
12. Customer satisfaction toward Online Marketing - An empirical study by Dr. M. Rajarajan; International Journal of World Research, Vol: I Issue XXXIV, October 2016 P 72-78
13. https://www.digitalvidya.com/blog/growth-of-digital-marketing-industry-in-india/
14. https://www.business-standard.com/article/current-affairs/india-is-adding-10-million-active-internet-users-per-month-google-118062700882_1.html
15. https://www.semrush.com/blog/internet-users-in-india-a-fresh-audience-for-brands/
16. https://www.acewebacademy.com/blog/emergence-digital-marketing-coming-years/
17. Rajesh, M., and J. M. Gnanasekar. "Path Observation Based Physical Routing Protocol for Wireless Ad Hoc Networks." Wireless Personal Communications 97.1 (2017): 1267-1289.
18. Rajesh, M., and J. M. Gnanasekar. "Sector Routing Protocol (SRP) in Ad-hoc Networks." Control Network and Complex Systems 5.7 (2015): 1-4.
19. Rajesh, M. "A Review on Excellence Analysis of Relationship Spur Advance in Wireless Ad Hoc Networks." International Journal of Pure and Applied Mathematics 118.9 (2018): 407-412.
20. Rajesh, M., et al. "SENSITIVE DATA SECURITY IN CLOUD COMPUTING AID OF DIFFERENT ENCRYPTION TECHNIQUES." Journal of Advanced Research in Dynamical and Control Systems 18.