ISSN: 2249 – 2593 /doi:10.14445/22492593/IJCOT-V11I1P301

Analysis of Encryption Approaches And Varieties

Sumaiyh Bani Oraba, Malak Saleh Mohammed Al-Hizami, Amira Abdullah Al-Jaafariya, Sumaiyh Bani Oraba, Ramesh Palanisamy

Information Technology, University of technology Appliance and Sciences-IBRA-Sultanate of Oman.

Abstract *- We live in an accelerated world of technological advancement. The world has now witnessed an evolution that is increasing day by day. But there are many hackers for this technology. So, we must protect the data that we use in this technology from any attack. Encryption techniques are the essential technologies that help to protect Data. Encryption techniques are in which data are encapsulated and cannot read by the attacker. These make it difficult for an attacker to crack the encryption used. Encrypted text can only read when it reaches the recipient. Several keys are used to encrypt and decrypt data. This paper covers encryption methodologies, what types of encryption algorithms, and how we can protect data from attack.*

Keywords – *Encryption, algorithms, symmetric, asymmetric*

Introduction

Today we live in a world of rapid technological development. Therefore, we must protect all data from any attacks or threats. Data encryption and decryption are the most substantial protection for data that cannot be easily penetrated [1]. Encryption is for data to be hidden and not reading [8]. Most network communication is via computers or cell phones, and these networks are open and comfortable for the attacker to penetrate. Still, when using encryption technology, it is difficult or prevented for the attackers to access the information, and it is changed or forged [2]. Also, most organizations require encryption techniques to use the cloud to store enterprise data and reduce many errors regarding the breach of that Data and the collapse of the enterprise [3,4]. Encryption technology is used to protect that Data when moving through the medium [5]. There are many data encryption types and decryption, including AES, DES, and RSA [6,9]. DES is the most widely used type of encryption [7]. There are two main types of data encryption keys: symmetric and asymmetric keys [8]. There are obstacles and issues and encryption techniques for each technology, which are some attacks that have been studied recently [11].

Related Work

Encryption is one of the essential security techniques for networks as it stores information for long periods. This information can be transferred over insecure networks, but no one can read it until only when it reaches the intended person. When the Data is decrypted, then the recipient can read the text [1]. There are specific keys for encrypting the sent data. The length of the sent message is determined for the use of large or small keys. When the message reaches the recipient, the Data is decrypted into the required text or original text [2]. Encryption is necessary because it is highly reliable to protect data stored in the cloud online [3]. Because the cloud makes it easy for the user to use his Data anywhere and anytime, the Data is encrypted and difficult to penetrate [4]. When using the same key in encryption, the same key must also be used for decryption; otherwise, decryption will not occur [5]. As for asymmetric keys, two keys (public and private) can be used. The encryption shall be in the public access while the decryption shall be in the private key [6]. The most used resolution is DES, where sensitive information is stored through encryption [7]. Encryption techniques work through many mathematical algorithms to encode and decode data. The encryption of any information, be it numbers, words, or phrases [8]. There are several types of algorithms, including Data Encryption Standard (DES), Triple Data Encryption Standard (DES), and Advanced Encryption Standard (AES) [9]. For every security technology, there are hackers for that secured information. Some security aspects help protect encryption from any attack [10,11].

Encryption methodologies

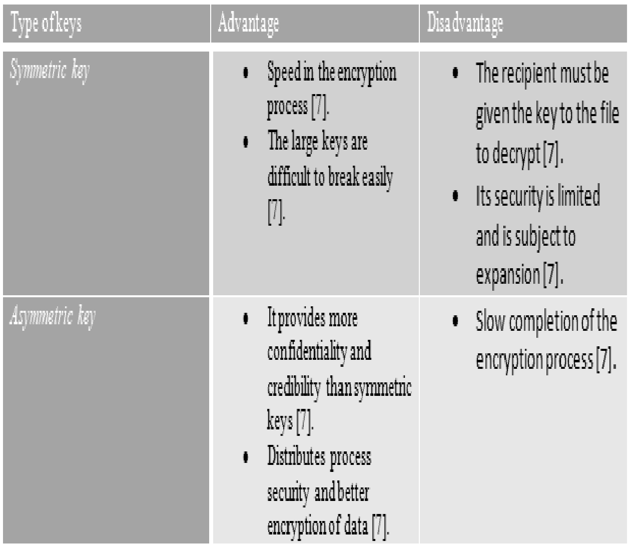
Encryption is encapsulated data that you do not allow anyone to read, only using the private encryption keys for the used encryption. The advantage of encryption is that even if a hacker gets access to the data, he cannot read it only if you have using the encryption key [4]. It is a well-known technology for protecting data. It is a combination of public access and the special one that helps hide the information and its clarity for the recipient [6]. Some algorithms convert standard text to encoded using mathematical formulas. The key is the number of bits that one type of algorithm takes to encrypt [7]. Cloud encryption is the process of converting customer data stored in the cloud into encrypted text using encryption algorithms. In the past, the encryption in the cloud provider was limited to passwords and account numbers, but nowadays, it encrypts an entire database but is very expensive. So, they encrypt it before sending it to the storage in the cloud [4]. There are two types of encryption, whether symmetric or asymmetric encryption. The encryption methods could be increased with more robust and secure encryption in the future [9].

- **Encryption time:** It calculates the total time taken for encryption to produce the data and calculate the algorithm rate when moving the encrypted data [9]. The more time spent in the encryption process, the slower the encryption goes and its energy consumption [9].
- **Decryption time:** The time is taken to decode the text and convert it into the original, readable text. The more time spent in the decryption process, the slower the encryption speed goes and its energy consumption [9].

How the Symmetric and Asymmetric encryption work:

Symmetric encryption (secret keys) works by agreement between the two parties on the type of key used to deal with each other in an encrypted way. The first party encrypts the message and the second party (the receiver) decrypts this message with the same key. As for asymmetric encryption (public keys), it is by two tickets. One of them is public, which is for the whole audience, and the other is mostly specific to the recipient. The receiver sends the type of public key to the sender, and then the sender sends the encrypted message to the recipient for decryption using the private key [4,5, 7]. Here we conclude that the asymmetric key is better than the symmetric key because it is more confidential and secure. However, it is slower than an asymmetric switch [4].

Comparison between symmetric and asymmetric keys:



Type of keys	Advantage	Disadvantage
Symmetric key	• Speed in the encryption process [7]. • The large keys are difficult to break easily [7].	• The recipient must be given the key to the file to decrypt [7]. • Its security is limited and is subject to expansion [7].
Asymmetric key	• It provides more confidentiality and credibility than symmetric keys [7]. • Distributes process security and better encryption of data [7].	• Slow completion of the encryption process [7].

What types of encryption algorithms

Algorithms are the main component of encryption. Many algorithms are used to protect information from attack. There are many types, including DES, TripleDES, RC2, RC4, Blowfish, Twofish, and Rijndael (AES) [1]. Symmetric and asymmetric encryption exists. In symmetric encryption, one file key is used for the sender and the recipient, and when sending to the recipient, it must receive the type of crucial used [2,3].

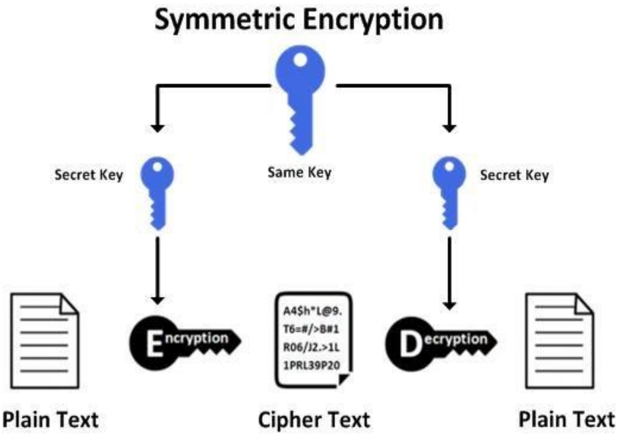
The type of algorithm used in symmetric encryption:

A. Data Encryption Standard (DES): The first encryption algorithm used to encrypt data [2, 8]. It was widely used. It is not easy to break because it goes through several encryption rounds [2, 7]. After this type of encryption has been fraudulent, some weaknesses were noted for advances in power computer processing [2,9]. The encryption process in this type consists of 8 steps to complete the process [5,7]. This type of encryption is mostly used in video conferences and ATMs [7].

B. Advanced Encryption Standard (AES): Group functions are organized circularly at many different times and repeatedly. There are four steps to making the functions circular: byte substitution, changing rows, mixing columns, and adding keys. AES replaces the Data Encryption Standard (DES) algorithm. The size of blocks for encryption in this type is 192, 128 and 256 [1, 2,5,9].

***C. Blowfish*:** It is one of the most common encryption tools used for computer security. It is also used for software security, but its keys are weak. The critical length of the encryption block is 64 bytes [2]. It is a robust encryption algorithm, but it is slowly accepted and used as an alternative to DES [9].

D. Triple DES: It is the slowest encryption method because it put on the algorithm three times for each block of data [9].



As for asymmetric encryption, it uses two keys: a public key used for everyone who wants to communicate and the text that will be encrypted. The recipient receives the text decryption by private access to this text [2].

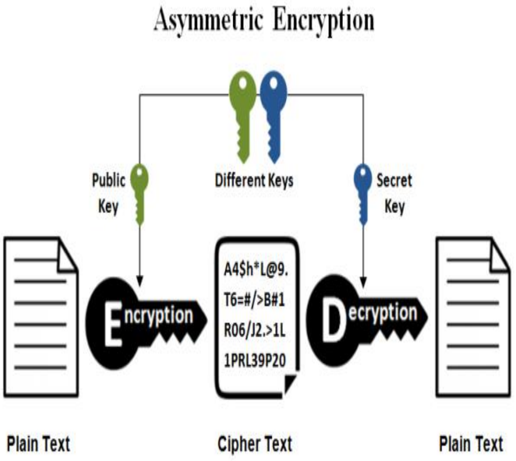
The type of algorithm used in asymmetric encryption:

1 - Rivest, Adi Shamir, and Leonard Adleman (RSA): It is more common for asymmetric keys, and it is used to decrypt Microsoft and Netscape [2].

2 - Digital Signature (DSA): By encrypting the public key, the recipient verifies the content of the message sent to him [2].

How we can protect data from attack.

Network security is paramount to protect data from any software breaches. Some users create weak passwords that are easy to decipher. They must create strong passwords of seven or more varied between letters, numbers, and signs. not write old passwords. To ensure more data security, make updates from time to time for where the Data is kept [11]. The concern with symmetric encryption is if the key used to encrypt the Data is known so that the hacker can gain access to the entire system, then it is destroyed [4].



Conclusion

In conclusion, security for networks is essential in preserving information for institutions, officials, and others. Encryption is encapsulating data so that no one can read it, only the intended person. Encryption is a robust technology to enable users to protect data better. We must use the appropriate type and methods of encryption keys to preserving the information from any attack.

Reference

[1] obaida Mohammad awad al-hazaimeh," a new approach for complex encrypting and decrypting data," international journal of computer networks & communications (ijcnc) vol.5, no.2, march 2013.

[2] Ezeofor C. J.1, Ulasi A. G.2," Analysis of Network Data Encryption & Decryption Techniques in Communication Systems", International Journal of Innovative Research in Science, Engineering, and Technology (An ISO 3297: 2007 Certified Organization)Vol. 3, Issue 12, December 2014.

[3] Mohammad Ubaidullah Bokhari & Qahtan Makki Shallal," A Review on Symmetric Key Encryption Techniques in Cryptography, "International Journal of Computer Applications (0975 – 8887) Volume 147 – No.10, August 2016.

[4] Okeke Stephen," The Study of the Application of Data Encryption Techniques in Cloud Storage to Ensure Stored Data Integrity and Availability," International Journal of Scientific and Research Publications, Volume 4, Issue 10, October 2014.

[5] N.krishna Chaitanya, A.Suman Kumar Reddy," Simple And Efficient Data Encryption Algorithm" INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 8, ISSUE 12, DECEMBER 2019.

[6] 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 the Year 2013.

[7] Indumathi Saikumar, "DES- Data Encryption Standard," International Research Journal of Engineering and Technology (IRJET) Volume: 04 Issue: 03 | Mar -2017.

[8] Ayushi A Symmetric Key Cryptographic Algorithm", ©2010 International Journal of Computer Applications (0975 - 8887)Volume 1 – No. 15.

[9] Article by Mahendra Kumar Shrivas[1,] Antwi Baffour Boasiako[2,] Sangeetha Krishanan[3,] Thomas Yeboah[4]," Enhanced Simplified Symmetric Key Encryption Algorithm," Texila International Journal of Academic Research Volume 3, Issue 2, Dec 2016.

[10] Poornachander V#," Security Issues on Cryptography and Network Security," Poornachander V / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 7 (3), 2016, 1648-1654.

[11] Gahan A V 1, Geetha D Devanagavi2," An Empirical Study of Security Issues In Encryption Techniques," International Journal of Applied Engineering Research ISSN 0973-4562 Volume 14, Number 5 (2019) pp.