Data Encryption Standard (DES)

 Student’s Name

Institutional Affiliation

Data Encryption Standard (DES)

**Introduction**

Understandably, in cryptography encryption is a cybersecurity measure meant to protect private and personal data using unique codes that scramble data, thus making impossible for the intrusion to occur. In the recent past, the discussion of cybersecurity especially encryption has gained momentum especially because of the increasing number of attacks that put company’s data at risk. However, with the application of ideal data encryption algorithm, it becomes impossible for the intruders to tap or access data. In this assignment, the goal is use Data Encryption Standard (DES), to explain and show how secure communication is performed. This paper also provides an overview of reflective summary of the current cybersecurity threats landscape.

**Overview of Data Encryption Standard (DES)**

 DES is asymmetric key blocker cipher or algorithm, meant for digital data, published by the National Institute of Standards and Technology. DES has been implemented through Feistel of 16 round structure. Ideally, this encryption algorithm uses 16 rounds of Feistel structure with a block size of 64 bit. Additionally, the effective length of this encryption algorithm is 56 bits, because 8 out of 64 bits is unusable. In terms of the main operations of DES, they include permutation, XOR, and substitution. According to Kenekayoro (2010), encryption of asymmetric ciphers consists of confusion and diffusion whereby confusion is for establishing the relationship between the plain text and cipher text complexity. On the other hand, the concept of diffusion in DES is meant to spread the change in cipher text with the aim of hiding any statistical feature. Moreover, substitution is applied in DES to achieve confusion and permutation diffusion.

 Data encryption as far as DES is concerned is known as Forward “Cipher Operation” and data decryption is termed as “Inverse Cipher Operation”. Ideally, in the forward cipher operation, each of 64 bit data changed based on a mathematical method that comprises of 16 rounds. Similarly, inverse cipher transformation utilizes the same steps as encryption algorithm but the rule is to use the same block of keys using in each round of encryption as the ones used in decryption round. In this case, R16 L16 is used as input of decryption, where K16 is used for that iteration, K15 for K15 L15 etc. (Rabah, 2005). The effectiveness of DES is based on secure implementation of cipher which is achieved through the application of permutation transportation technique. Transportation comprises of exchange of two main components of an ordered list. The diagram below represents the general structure of DES

Figure 1: General Structure of DES

Based on the above diagram, each round make use of 48 bit round key captured from the cipher as per the predefined algorithm. The above diagram has also captured the key elements of DES cipher at encryption site.

**Secure Data Communication using DES**

 DES is a widely accepted algorithm for data encryption that use private (secret) key that is difficult to break. In any given message, the key is generated randomly among massive number of keys. Just like any other private key cryptographic techniques, both the sender and the receiver must be well are of the key and must utilize it (Kessler, 2010). Many organizations use DES to secure the transfer of data over unsecure networks. Therefore, the proposal of secure data transfer through the implementation of DES encryption and decryption applications is ideal for the communication over remote computers.

**Reflective Summary of the Current Cybersecurity Threat Landscape**

 Notably, internet infrastructure is geared towards supporting global exchange of information via both physical and logical assets which include protocols, services, and other devices. Such assets suffer from different kinds of threats which may hamper data plus other valuable information. As threat landscape, this research provides detailed overview of the current cybersecurity threats and their trends, so that organizations can improve the security of their systems using the best cybersecurity practices. Ideally, the threats of internet infrastructure may include unauthorized access, sabotage, information breach, denial of service, among others. Such threats can be grouped based on threats types, which include physical attacks, disaster, the conditioning of insufficient functioning of internet infrastructure asset, unintentional damage, eavesdropping, among others (Lévy-Bencheton, 2015). These threats have been consolidated by ENISA (European Union Agency for Cybersecurity).

 Based on specific cyber threats of the infrastructure, such threats are applicable to information and telecommunication technology in general. However, considering the scope of this research is based on cybersecurity, is a need to dig deeper. The main groups of threats in the current cybersecurity landscape can be categorized into DNS threats, routing threats, DDoS threats, and generic threats, which are not specific to the internet infrastructure. Therefore, the threats discussed in this paper provides a clear picture of the current state of play. Rout threats as stated above involve harming of network interconnection and operation of single networks. Additionally, a smooth running of routing infrastructure is important in enhancing the robustness for internet (Lévy-Bencheton, 2015). Routing threats mostly occur through hijacking of network and internet resources, misconfiguration of network and internet resources, interception of assigned numbers, among other things. The current cybersecurity trend shows that there is increasing number of threats. The diagram below shows an overview of the routing threats

Table 1: Application of Important Specific Threat to Routing

 Another key threat type in the current cybersecurity landscape is nefarious activity/ abuse with the specific threat identified as autonomous system (AS) hijacking. The main objective of AS by the attackers is conducting the malicious activity with the hijacked networks and are masked to appear as if it has been carried out on behalf of the victim. This can be presented in a forensic case study on autonomous system hijacking from attacker’s perspective. In the nefarious activity type, address space hijacking can still follow under it and it occurs when the victim is announcement of victim’s prefixes has been done by a rogue BGP peer. A good example of this is when the hacker tries to redirect traffic different service providers, with the aim of stealing bitcoins.

**Specification of Inspiring Encryption Algorithms with Examples**

 Notably, the DES specifies two Federal Information Processing Standards (FIPS) approved cryptographic algorithms which is a requirement in line with FIPS 140-1.When applied together with ANSI X9.52 standard, it offers mathematical specification and algorithm for encrypting and decrypting information that is binary coded. Encryption of data is geared towards converting data into unintelligible format known as cipher, while decrypting is meant to return data to its original form. The diagram below represents full specifications of DES based on 64 –bits block of plain text, that invoking 16 rounds of permutations (Kessler, 2010) . Based on this diagram, 64 bit block that requires encryption undergoes the first permutation moving each bit to a new bit position e.g. first, second, an third bits are moved to new positions respectively. Then the permuted 64 bit is divided into32 bit blocks referred to as left and right and denoted as L0 and R0. Additionally, there are sixteen rounds of operation on L and R within the iteration, which can be determined via the iteration from 1 to 16. The following formulae is applicable





 Figure 2: DES Encryption Algorithm

 Based on the analysis of the strengths of DES, it generally lies on two aspects, which include the application of 56-bits key-which is applicable in encryption. Additionally, there are 256 possible keys, which makes it practically impossible to have a brute force attacks on the computer networks as well as in the internet communication. Secondly, the strength of DES is based on the nature of algorithm. Ideally, cryptanalysts can perform cryptoanalysis through the exploitation of the features of DES algorithm; however, no one has succeeded in identifying the weakness. On the other hand, there are two weaknesses with DES especially on the design of cipher. Which include two chosen input to an S-box that can create the same output. Also, the goal of initial and final permutation is not clear.

 Notably, several network security standards have been recommended and broadly implemented in home and business environment to offer protection from unauthorized access and communication/ information over the internet. Nevertheless, the implementation of such standards is mostly done by the network administrators or network security specialists without knowing the standard weaknesses (Guillen et al., 2009). Additionally, network intrusion and detection system have been broadly implemented with the aim of building layered information security infrastructure. Consideration of DES encryption algorithm in network security is paramount.

**Full Specification of my Encryption Algorithm**

Ideally, DES comprises of initial and final permutations, which takes a 64-bit input and permutes them based on predefined rule. For example, in the initial permutation the 58th bit changes to be the first bit in the output. Similarly, in the final permutation, the first bit becomes the 58th bit in the output (Siahaan, 2018). The permutation rules for the P-boxes (both initial and final permutations are as shown on the table below.



Table 2: Initial and Final Permutation Table

 As per DES specification, the key length is 64-bit. Additionally, there are 8 bytes, whereby in each byte type, the 8 bit is a parity-check bit. Also, each parity-check bit is the XOR the previous 7 bits. The whole process can be describes as shown in the diagram below.



Figure 3: Parity -Check Bits in DES Specification

Notably, these permutation s do not possess any cryptography significance in Data Encryption Standards (DES). In this case, all the permutations are considered to be keyless and predetermined. The reason for their inclusion is not clear and this has not been explained by DES designers. Based on the DES function and specifications, this mostly applies 48- bit key to the rightmost 32 bits to generate a 32 -bit results. This function/ specification is made up of 4 sections, which include an expansion D -box. Whitener that adds key, a group of S- boxes as well as a group of straight D-box as shown on the image below.



Figure 4: DES Function/ Specifications

In the application of DES, several block ciphers are based on structure proposed by Feistel. Additionally, Feistel network is fully specified based on the block size i.e., 2W, number of rounds, -d rounds function i.e.f1, …., fd: {0,1}w-{0,1}w/. The whole process of encryption and decryption over the network systems and internet occurs based on the following.

***For Encryption in DES***

***– L1 = R 0 R 1 = L 0 ⊕ f 1(R 0 )***

 ***– L 2 = R 1 R 2 = L 1 ⊕ f 2(R 1)***

***…***

***– L d = Rd-1 R d = Ld-1 ⊕ fd(Rd-1 )***

***For Decryption in DES***

***– R 0 = L 1; L 0 = R 1 ⊕ f 1(L 1 )***



Figure 5: DES Specification: Encryption and Decryption

Ideally, DES perform encryption of data in blocks of size, each having 64 bit, meaning 64 bits of pain text is the one that goes as an input to DES to produce 64 bits of cipher text. Additionally, the same algorithm as well as key are applied in encryption and decryption with minor differences. The whole process of encryption and decryption is based on 2 fundamental attributes of cryptography substitution, also known as confusion and transportation, also known as diffusion. The section below shows all the steps involved in key generation.

***Step 1: Handing over the 64 bit plain text block to an initial permutation function.***

The diagram below shows the whole process of encryption and decryption in DES In this process, the 64 bit key is transformed to 56 bit-key. From this, Different 48 bit key is generated in each round through the transformation process.

*A good example is when the round position 1, 2,9, or even 16, shifting is done by the only position for other rounds. Additionally, circular shifts is done by the 2 positions. Also, the shifting of the number of key bits is done as shown in the figure below.*

Figure 6: Step 1: Key Transformation-Number of Key Bits- Shifted Per Round

After the first shift permutation has occurred, the second shift must occur through the process called compression permutation. As a result of this permutation, a different subset of key is applied in each round, thus making DES not easy to track.

**Step 2: The Initial Permutation is Performed on Plain Text**

This is achieved through expansion permutation whereby initially there were two 32 bit text areas known as Left Plain Text (LPT) as well Right Plain Text (LPT). In the process of expansion, the RPT is extended/ expanded from 32 bits to 64 bits. Additionally, the whole process involves permuting bits through the process of expansion permutations which occurs by dividing 32 bits into 8 blocks with each block having 4 bits. Moreover, each of the 4 bit is then expanded to a corresponding 6-bit block that the 4 bit block then addition of 2 more bits. The figure below represents the whole process.



Figure 7: Initial Permutation on Plain Text.

Notably, the process amounts to expansion and input permutation while creating the output. It is worth noting that the process of key transformation do involve compressing the 56-bits key to 48 bits key, while the expansion process entails expanding 32 bit RPT into 48 bits. When implementing DES algorithm with respect to this research, the idea started with generation of keys- where the whole process involved 16 rounds of encryption each comprising of a different key. The key was generated using the C++ program as captured on the code screenshot below.







Figure 7: DES Generation of Key Code Snippet

Upon running the above code, it generated 8 different keys as shown on the screenshot below.

Figure 8: Output of Key Generated

When creating an algorithm for encrypting plain text to generate cypher text, the ideal involved transposition of plain text and then dividing it into two halves to undergo the whole process of encryption and decryption. After executing the whole code for encryption, below was the output.



Figure 9: Encrypting Plain Text to Generate Cypher Text

Similarly, to decrypt the plain text, the process of reversing the order of keys was done in round keys that is 16 becomes etc.) and application of DES () function. After executing this code, the output below were obtained.



**Strength and Weaknesses of Algorithm and its Best Application**

Based on this algorithm, DES is strong from differential cryptanalysis perspective. This makes it more powerful in protecting against differential attacks. As noted through research resistance to differential attacks is ascertained through differential characteristics offered by the S-box. In terms of the weaknesses, DES is not known to be modified/ written against linear cryptanalysis (GeeksforGeeks, 2020). Arguably, the mentioned the attacks in Des consist of a practical break as plaintext can be easily changed, thus changing the meaning and hence the cypher text generated. It is also evident that DES weak keys that are technically not common.

References

Kenekayoro Patrick, T. (2010). The data encryption standard thirty-four years later: An overview. African Journal of Mathematics and Computer Science Research, 3(10), 267-269.

Siahaan, A. P. U. (2018). Encryption of DES Algorithm in Information Security.

Guillen, E., Padilla, D., & Colorado, Y. (2009, September). Weaknesses and strengths analysis over network-based intrusion detection and prevention systems. In *2009 IEEE Latin-American Conference on Communications* (pp. 1-5). IEEE.

Kessler, G. C. (2010). An overview of cryptography. Online: http://www. garykessler. net/library/crypto. html,[Last accesed: 01/10/09].

Lévy-Bencheton, C., Marinos, L., Mattioli, R., King, T., Dietzel, C., & Stumpf, J. (2015). Threat landscape and good practice guide for internet infrastructure. EU Agency for Network and Information Security (ENISA).

Rabah, K. (2005). Theory and implementation of data encryption standard: A review. Information Technology Journal, 4(4), 307-325.

GeeksforGeeks. (2020, August 18). Strength of Data Encryption Standard (DES). Retrieved from <https://www.geeksforgeeks.org/strength-of-data-encryption-standard-des/>

Aleisa, N. (2015). A Comparison of the 3DES and AES Encryption Standards. *International Journal of Security and Its Applications*, *9*(7), 241-246.

Kartalopoulos, S. V. (2008, May). Differentiating data security and network security. In *2008 IEEE International Conference on Communications* (pp. 1469-1473). IEEE.

Mahajan, P., & Sachdeva, A. (2013). A study of encryption algorithms AES, DES and RSA for security. *Global Journal of Computer Science and Technology*.

|  |
| --- |
|  |
| Forouzan, B. A., & Mukhopadhyay, D. (2015). *Cryptography and network security*. New York, NY: Mc Graw Hill Education (India) Private Limited. |
| Lakhtaria, K. I. (2011, April). Protecting computer network with encryption technique: A Study. In *International Conference on Ubiquitous Computing and Multimedia Applications* (pp. 381-390). Springer, Berlin, Heidelberg. |  |