A Comparison of Data Encryption Algorithms

Name

Course Title

Professor's Name

Date

A Comparison of Data Encryption Algorithms

Data security is arguably the most significant and persistent obstacle to ongoing technological advancements. Encryption has emerged as an effective solution to data security, supporting secure electronic data transfer through the web (Abood & Guirguis, 2018). However, equipped with better tools and their growing expertise, cyber-adversaries are increasing thwarting weak encryption techniques. Therefore, this creates a need among cybersecurity to identify the most effective encryption algorithms. Several metrics are used to describe high performing encryption algorithms, including resilience, speed, and efficiency. This paper reviews popular encryption algorithms, i.e., DES, 3DES, AES, and Blowfish, to determine the most resilient technique. Each algorithm's strength depends on its key size, block size, number of rounds, and algorithm complexity (round description).

Data Encryption Standard (DES) refers to a symmetric encryption method that encrypts and decrypts blocks of data consisting of 64 bits (Ratnadewi et al., 2018). While DES's input key is 64 bits in length, the actual key is only 56 bits long. Thus, the algorithm disregards 8 bits of the 64-bit key and then uses the compressed 56-bit key derived from 64 bits key to encrypt data in block sizes of 64 bits (Ratnadewi et al., 2018). DES uses the Feistel structure with 16 rounds. DES inputs 64-bit plain text and produces a 64-bit ciphertext. The algorithm starts with submitting a 64-bit plain text block to an initial permutation (IP) function, which executes on the input (plain text). Subsequently, IP produces two halves of the permuted block, i.e., Right Plain Text (RPT) and Left Plain Text (LPT) (Wahid et al., 2018). Both RPT and LPT are subjected through sixteen rounds of the encryption process (Wahid et al., 2018). Finally, the RPT and LPT are combined, and the algorithm performs a Final Permutation (FP) on the combined block.

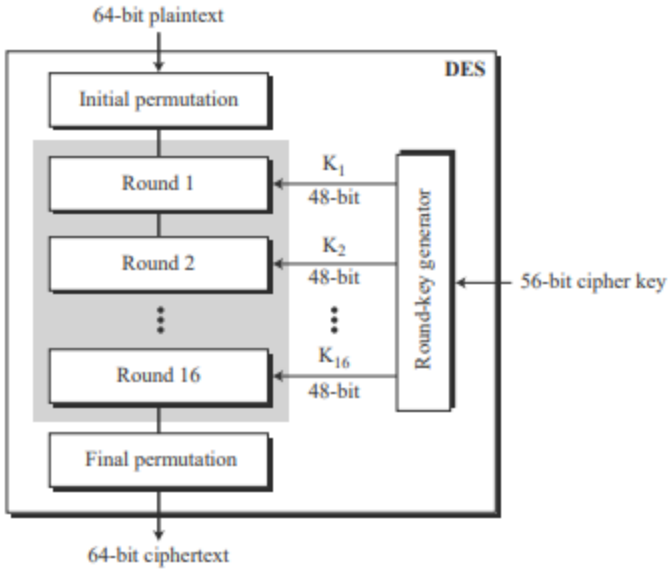

Figure 1: DES Round Algorithm

Triple-DES (3DES) was proposed to address the flaws in DES while preserving the same cryptography. 3DES runs an encryption approach and structure similar to the original DES. However, in 3DES, the process is applied three times to enhance the encryption level (Wahid et al., 2018). Besides, 3DES uses the same key size as DES (56-bit). However, since the algorithm is applied triple successively with three multiple keys, its actual size is 168 bits. DES uses 48 DES-equivalent rounds. Each 3DES round executes, as shown below.

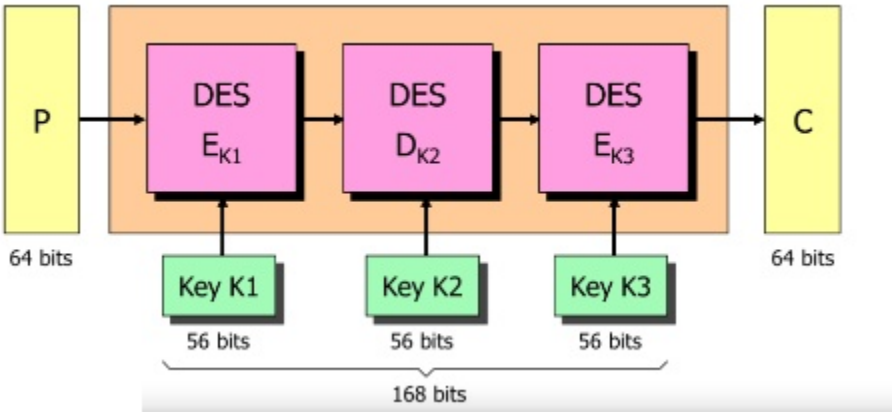

Figure 2: 3DES Round Algorithm

The National Institute of Standards and Technology (NIST) proposed the Advanced Encryption Standard (AES) to replace the frail DES technique (Devi & Kotha, 2019). This block cipher has a variable number of rounds and key length, executing ten rounds for 128-bit keys, twelve rounds for 192-bit keys, and fourteen rounds for 256-bit keys (Devi & Kotha, 2019). AES allows 128-bit long data, grouped into four fundamental active blocks. Each round entails byte substitution, shift rows, mix columns, and add-around key functions (Devi & Kotha, 2019). These blocks are perceived as an array of bytes and classified into four-by-four column matrices. The data is then shifted from its initial position to produce diffusion. Every round key attached to the plaintext through the additive XOR algorithm to scatter the data further (Devi & Kotha, 2019). The encryption produces a new matrix with 16 new bytes. The process starts again and is executed as per the number of rounds.

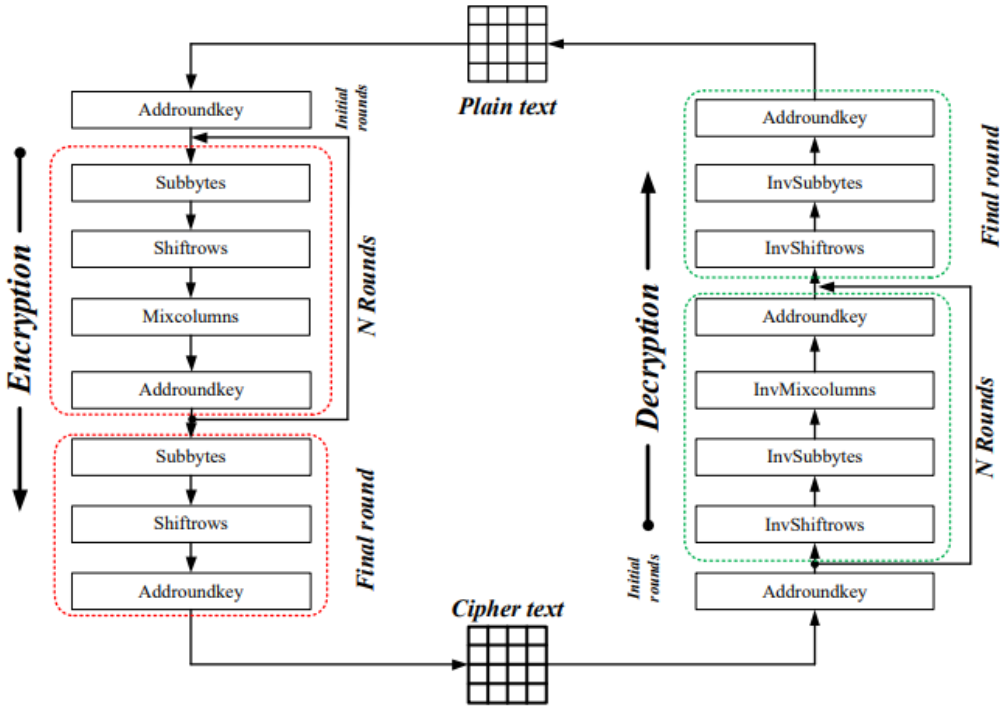

Figure 3: AES Round Algorithm

Finally, Blowfish is a symmetric-key block cipher with the Feistel network structure (Asassfeh, Qatawneh, & AL-Azzeh, 2018). The encryption method takes a variable-length key, ranging between 32 bits and 448 bits, with a block length of 64 bits. Blowfish runs for 16 rounds and uses massive key-dependent S-boxes. As shown in figure 4 below, Blowfish's F-function divides the 32-bit input into four eight-bit quarters and utilizes the quarters as input to the S-boxes (Asassfeh, Qatawneh, & AL-Azzeh, 2018). The outputs are added modulo 232 and XORed to produce the final 32-bit output (Asassfeh, Qatawneh, & AL-Azzeh, 2018). The procedure for a total of 16 rounds with successive components of the P-array. The output P' and F' are then XORed with the last two entries in the P-array and reunited to produce the 64-bit ciphertext.

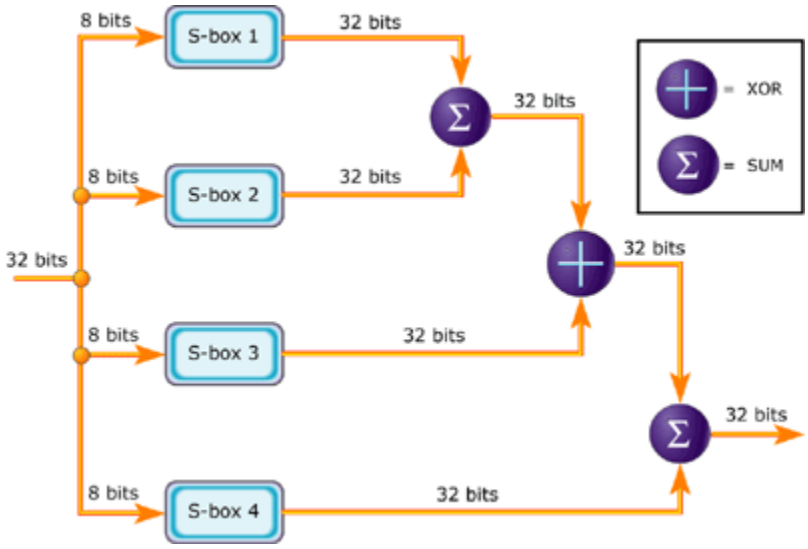

Figure 4: Blowfish Round Algorithm

Table 1: Summary of the Results

Metrics	DES	3 DES	AES	Blowfish
Key sizes	56 bits (+8 parity bits)	168 bits	128, 192 or 256 bits	32–448 bits
Score	*1*	*2*	*3*	*4*
Block sizes	64 bits	64 bits	128 bits	64 bits
Score	*3*	*3*	*4*	*3*

Rounds	16	48	10, 12, or 14	16
Score	*3*	*4*	*1*	*3*
Round complexity score	*1*	*2*	*3*	*4*
Total score	8	11	11	14

Each algorithm has been ranked according to the four metrics. Findings reveal that Blowfish is the most resistant algorithm among the four symmetric block ciphers, followed by AES and 3DES (which have equal resilience), and finally DES.

References

Abood, O. G., & Guirguis, S. K. (2018). A survey on cryptography algorithms. *International Journal of Scientific and Research Publications*, 8(7), 410-415.

Asassfeh, M. R., Qatawneh, M., & AL-Azzeh, F. M. (2018). Performance evaluation of blowfish algorithm on supercomputer iman1. Inte*rnational Journal of Computer Networks & Communications (IJCNC)*, 10(2).

Devi, S., & Kotha, H. D. (2019, May). AES encryption and decryption standards. *In Journal of Physics: Conference Series*, 1228(1).

Ratnadewi, R. P., Adhie, Y. H., Ahmar, A. S., & Setiawan, M. I. (2018). Implementation cryptography data encryption standard (DES) and triple data encryption standard (3DES) method in communication system based near field communication (NFC). *International Journal of Physics: Conference Series*, 954(1).

Wahid, M. N. A., Ali, A., Esparham, B., & Marwan, M. (2018). A comparison of cryptographic algorithms: DES, 3DES, AES, RSA and blowfish for guessing attacks prevention. *Journal Computer Science Applications and Information Technology*, 3(2), 1-7.