GROUP ASSIGNMENT

Encryption

Adriaan Pienaar (39399575)

Armin Pretorius (34739572)
Francois Hendrik Botha (34507965)

Michael van Niekerk (29580080)

Luigi Willemse (38887657)

Group Assignment submitted for CMPG 215 for the degree *Bachelor of Science* in *Information Technology* at the North-West University

Lecturer: Prof. Neels Kruger

Table of Contents:

Introduction

Cryptography is the study of securing communication. Encryption is the method used to conceal messages using algorithms. The main objective of cryptography is to protect the confidentiality, integrity, authentication, and non-repudiation of information (Singh *et al.*, 1165:2010).

Comparison of Encryption Algorithms

The following encryption algorithms will be compared: DES, 3DES, AES, Blowfish and RSA.

According to Patil *et al.* (620:2016) the parameters used to evaluate encryption algorithms against are:

1. Encryption time – The time it takes for the algorithm to convert plaintext to ciphertext.
2. Decryption time – The time it takes for the algorithm to recover plaintext from ciphertext.
3. Memory used – The memory required by the algorithm for its operations.
4. Avalanche effect - The desirable property of encryption algorithms wherein if an input is changed slightly, the output changes significantly. It reflects the cryptographic strength of an algorithm.
5. Entropy – The measure of randomness in the information. A higher value is desirable.
6. Number of bits required to encrypt optimally – The number of bits determine the storage size and bandwidth required for storing and transmitting encrypted bits and thus a smaller number of bits is desirable.

Encryption time

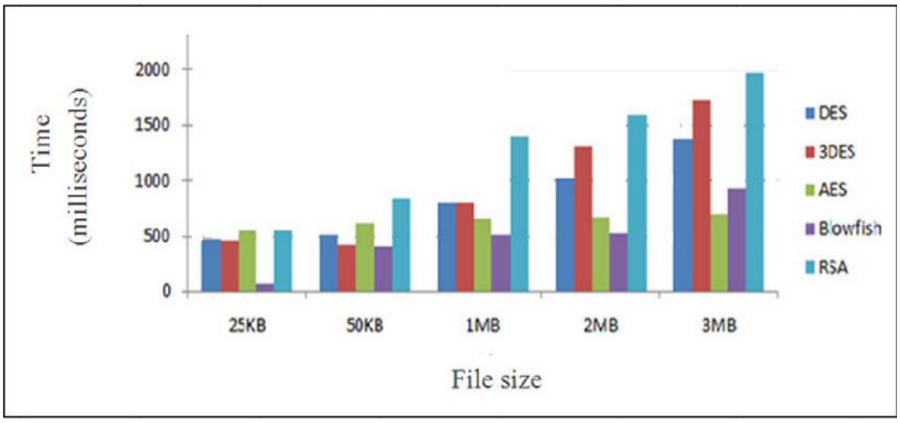

Fig. 1. Encryption time vs file size for DES, 3DES, AES, Blowfish and RSA. From "A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish," by Patil, et al.

Fig. 1 shows that Blowfish uses the least amount of time, but it increases significantly with file size. AES uses a large amount of time with small files, but it stays constant even as file size increases. DES, 3DES and RSA use more time than Blowfish and AES.

Decryption time

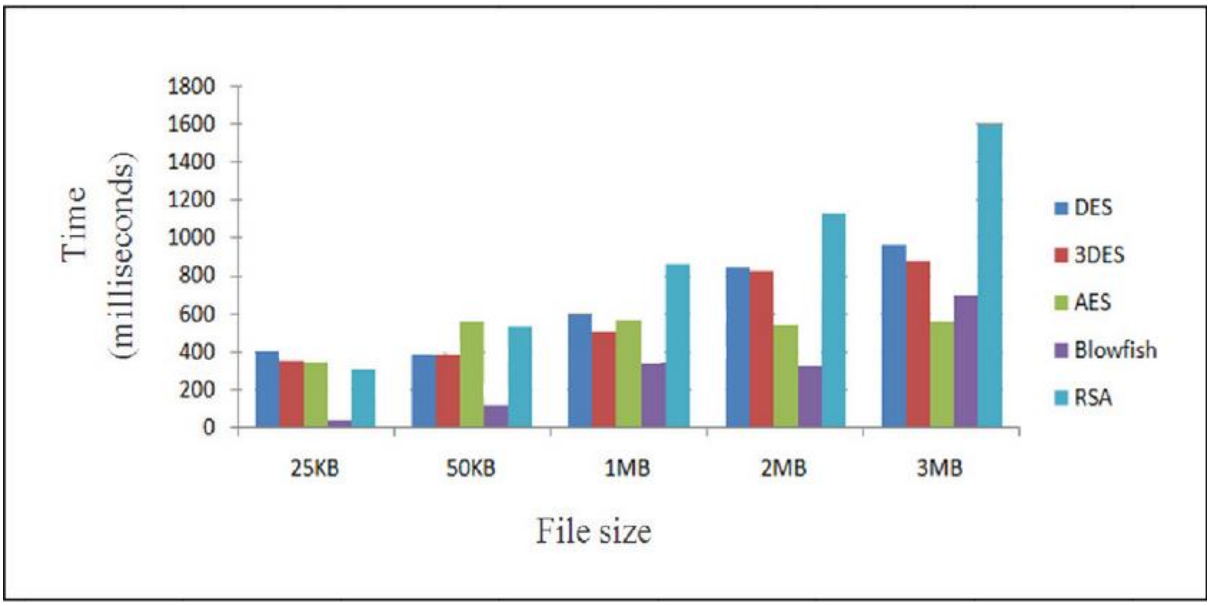

Fig. 2. Decryption time vs file size for DES, 3DES, AES, Blowfish and RSA. From "A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish," by Patil, et al.

Fig. 2 shows that Blowfish uses the least amount of time to decrypt the files, but the time increases significantly with file size. AES uses a large amount of time to decrypt small files, but it stays constant even as file size increases. DES, 3DES and RSA use more time than Blowfish and AES to decrypt files.

Memory used

Algorithm	Memory used (KB)
DES	18.2
3DES	20.7
AES	14.7
Blowfish	9.38
RSA	31.5

Table 1. Comparison between memory used by DES, 3DES, AES, Blowfish and RSA. Adapted from "A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish," by Patil, et al.

Table 1 shows that Blowfish uses the least of memory for its operations. AES takes second position for least memory used. DES, 3DES and RSA use more memory than Blowfish and AES.

Avalanche effect

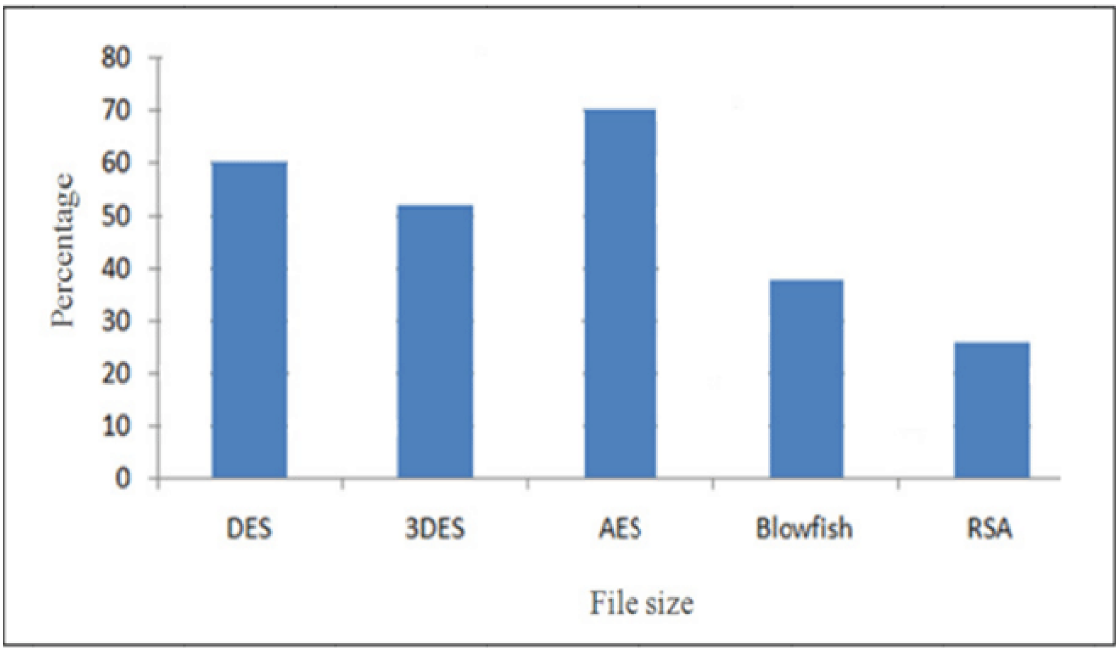

Fig. 3. Avalanche effect for DES, 3DES, AES, Blowfish and RSA. From "A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish," by Patil, et al.

Fig. 3 shows that AES has the highest Avalanche effect. Blowfish has the second lowest Avalanche effect.

Entropy

Algorithm	Average entropy per byte of encryption
DES	2.9477
3DES	2.9477
AES	3.84024
Blowfish	3.93891
RSA	3.0958

Table 2 shows the average entropy values for DES, 3DES, AES, Blowfish and RSA. Adapted from "A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish," by Patil, et al.

Table 2 shows that Blowfish scores the highest average entropy per byte of encryption with AES falling close behind. DES, 3DES and RSA have much lower scores than Blowfish and AES.

Number of bits required to encrypt optimally

Algorithm	Number of bits required to optimally encode a byte of encrypted data
DES	27
3DES	40
AES	256
Blowfish	128
RSA	44

Table 3 shows the number of bits required by DES, 3DES, AES, Blowfish and RSA to encrypt data optimally. Adapted from "A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish," by Patil, et al.

Table 3 shows that AES requires the highest number of bits to encode optimally. DES requires the lowest number of bits.

Our Choice: AES

Advance Encryption Standard (AES), also known as the Rijndael algorithm, is an encrypting algorithm developed in 1998 by Joan Daemen and Vincent Rijmen (Patil *et al.*, 619:2016) and recommended by the U.S. National Institute of Standards and Technology (NIST) to replace Data Encryption Standard (DES) in 2001 (Singh & Kinger, 2013:36).

AES is a block cipher that encrypts a 128-bit block in plaintext to a 128-bit block in ciphertext or decrypts a 128-bit block in ciphertext to a 128-bit block in plaintext (Singh *et al.*, 1186:2010). AES allows for a data length of 128 bits that can be split into four blocks (Patil *et al.*, 619:2016). AES supports key lengths of 128, 192, and 256 bits (Singh & Kinger, 2013:36). AES divides the data block into iterations, also known as rounds. Each round then uses permutation and substitution network, which is a series of linked mathematical operations used in block cipher algorithms to encrypt the data block, using the plaintext and key as input. Each round is then encrypted using a different round key (Patil *et al.*, 619:2016). The round keys are derived from the cipher key by using the AES key expansion algorithm (Singh *et al.*, 1186:2010).

Advantages of AES

- Uses the least amount of time to encrypt and decrypt bigger files.
- Uses less memory than most of the other algorithms.
- Exhibits the highest Avalanche effect which means it leads to high diffusion in information.

- Scores a high average entropy per byte of encryption.

Disadvantages of AES

- Uses more time than other algorithms to encrypt and decrypt smaller files.
- Requires the highest number of bits to encoded data optimally.

Conclusion

AES uses more time to encrypt and decrypt smaller files, but it is offset by maintaining the least amount of time to perform operations on increasingly bigger files. AES requires the highest number of bits to encoded data optimally, but this disadvantage is offset by having the highest Avalanche effect and having a very high entropy value which is the main objective of cryptography to protect the confidentiality, integrity, authentication, and non-repudiation of information.

References

Patil, P., Narayankar, P., Narayan, D.G. & Meena, S.M. 2016. A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish. *Procedia Computer Science,* 78:617-624. https://doi.org/10.1016/ j.procs.2016.02.108

Singh, A., Marwaha, M. & Singh, B. 2010. Comparative study of DES, 3DES, AES and RSA. *International Journal of Computers & Technology,* 9(3):1162-1170. doi: 10.24297/ijct.v9i3.3342

Singh, G. & Kinger, S. 2013. A study of encryption algorithms (RSA, DES, 3DES and AES) for information security. *International Research Journal of Engineering and Technology,* 67(19):33-38. doi: 10.5120/11507-7224