Zero : Jurnal Sains, Matematika, dan Terapan
E-ISSN : 2580-5754
P-ISSN : 2580-569X
Vol. 6, No. 2, Desember 2022
pp. 231-236

Implementation of Data Encryption Standard (DES) Algorithm for Data Security on PDF Documents

Arif Wijaya Panjaitan[1],Ilka Zufria[2], Yusuf Ramadhan Nasution[3]
[1,2,3]Department of Computer Science, Universitas Islam Negeri Sumatera Utara Medan, Indonesia

Article Info

Article history:

Received mm dd, yyyy
Revised mm dd, yyyy
Accepted mm dd, yyyy

Keywords:

Cryptography, Data encryption Standart, Portable Document Format

ABSTRACT

Misuse and theft of confidential PDF documents because documents can still be recognized and read by humans means, of course, these problems can harm those who have access to PDF document data. The act of tapping and stealing PDF documents can be minimized by the application of cryptographic encryption techniques. Cryptography is a science that studies mathematical techniques related to information security aspects such as confidentiality, data integrity and authentication. Cryptography requires an algorithm to perform the encryption process, one of the cryptographic algorithms that can be used is the Standard Data Encryption (DES) algorithm. The DES algorithm is a symmetric algorithm that works on the principle of a block cipher. The DES algorithm uses a 64-bit key to encrypt a 64-bit block. This thesis discusses the design of web-based cryptography using the Data Encryption Standard (DES) method. The application of this system is hiding pdf files using an 8-bit key without any errors or file damage and cannot be decrypted without the appropriate key. By using a data security application system using the DES method, it is useful to help hide the contents of important pdf files with a key so as to minimize digital theft by irresponsible parties.

Corresponding Author:

Arif Wijaya Panjaitan,
Department of Computer Science,
Universitas Islam Negeri Sumatera Utara, Medan, Indonesia
Email: arifpanjaitan70@gmail.com

1. INTRODUCTION

The use of PDF is usually identical in the world of work which leads to data processing. Data that has been created in Microsoft Office such as Word, Excel and others is usually saved in its original extension or in another extension, one of which is PDF. Many people choose to use this format because it is very practical and does not take long to open. So, some important and confidential data is also converted into PDF form.

Theft and misuse of PDF documents that are confidential because documents can still be recognized and read by humans, of course this is detrimental to those who have access to the PDF document data. By implementing cryptographic encryption techniques, interception and theft of PDF documents can be minimized. Cryptography is a science that studies mathematical techniques related to aspects of information security such as confidentiality, data integrity and authentication. Cryptography requires algorithms to perform encryption, one of the cryptographic algorithms that can be used is the Standard Data Encryption Algorithm (DES). Based on the description of the background above, the authors set the title of this research

as "Implementation of the Standard Data Encryption Algorithm (DES) for Data Security in PDF Documents".

2. RESEARCH METHODE

The place where researchers conducted research in this thesis is the UINSU Laboratory, IAIN No.1, Gaharu area Medan, North Sumatra the time used by researchers for this research was carried out from the date of issuance of research permits in the period from June to April 2022. The data collection method used in the discussion of this research is as follows:

1. Literature Study
   Is the data collection stage by collecting literature, journals, papers, and books related to the research title, as well as searching for information from various sources on the internet to find out the latest developments from the data taken as material in making the final project.
2. System analysis and design
   This stage will be carried out data analysis, system requirements described in the flowchart, and interface design.
3. System implementation
   Implementation is carried out based on the results of the analysis and design that has been done before. In this stage, coding is carried out using the PHP programming language.
4. System testing
   This test is carried out by testing the cryptographic process on the system that has been built. Includes pdf file input, encryption process, decryption process and also includes whether the system implementation is in accordance with the theory and design that has been done before.
5. System Test Results
   Make system test results, whether the system can produce PDF file security according to research objectives

2.1. Computer Data Security

Computer security is the prevention of computer-mediated crime. The security required includes physical security (server room and supporting infrastructure), access security (humans as users), data security (viruses and data theft), and computer operating system security ((Siregar, 2019) when developing computer security, aspects of confidentiality, integrity, authentication, non-repudiation, and availability must be considered The aspect of confidentiality aims to prevent data on the computer from falling into unauthorized hands so that it can be misused The aspect of integrity concerns the consistency of data information so that it cannot be changed or damaged by third parties another.In this case, the encryption method is often used for encoding [1].

2.2. Cryptography

Cryptography comes from the Greek words crypto and graphia. Crypto means secret and graphia means writing. Cryptography is a message encoding technique used so that messages can be sent and received safely. Cryptography aims to maintain the confidentiality of data and information so that it is not misused by unauthorized parties ((Yusfrizal, 2019)). For cryptography to work well there must be four main elements in it, which are most related to each other [2].

2.3. Cryptographic security aspects

Security has become an important aspect of an information system that is usually only shown to certain groups because it is important to protect an information system from falling into the hands of other people who are not interested. One of the efforts to protect information systems that can be done is cryptography which has several aspects of information security [3].

2.4. PHP

PHP (Hypertext Preprocessor) is a scripting language that can be embedded or inserted into HTML. PHP is widely used to create dynamic website programs. PHP can be used for free and is OpenSource. PHP is released under a PHP license. To make a PHP program we are required to install a web server first [4].

2.5. MYSQL

To describe an algorithm that is structured and easy to understand by others (especially programmers who are in charge of implementing the program), we need a tool in the form of a flowchart. The flowchart

describes the logical sequence of a problem-solving procedure, so that the flowchart is a problem solving steps written in certain symbols. This flowchart will show the flow in the program logically. Besides being needed as a communication tool, this flowchart is also needed as a documentation tool [5].

3. RESULT AND ANALYSIS

After designing and creating the system, testing is then carried out. The testing aims to see to what extent the system that has been built meets expectations, an example of the results of applying DES Cryptography in encrypting PDF files using a key with the DES algorithm, can be seen as follows:

1. Application Initial Display

   After designing and creating the system, testing is then carried out. Testing The display below is a display of the application of the DES Cryptography application in encrypting pdf files using the key.

Figure 1. Application Initial Display

2. Display input files, keys and output

   After that, enter the pdf file and key then select the type of hexa key according to the standard specified and carry out the encryption process then after that it appears to output it aiming to prove the manual results are the same as the results in the program, as shown below:

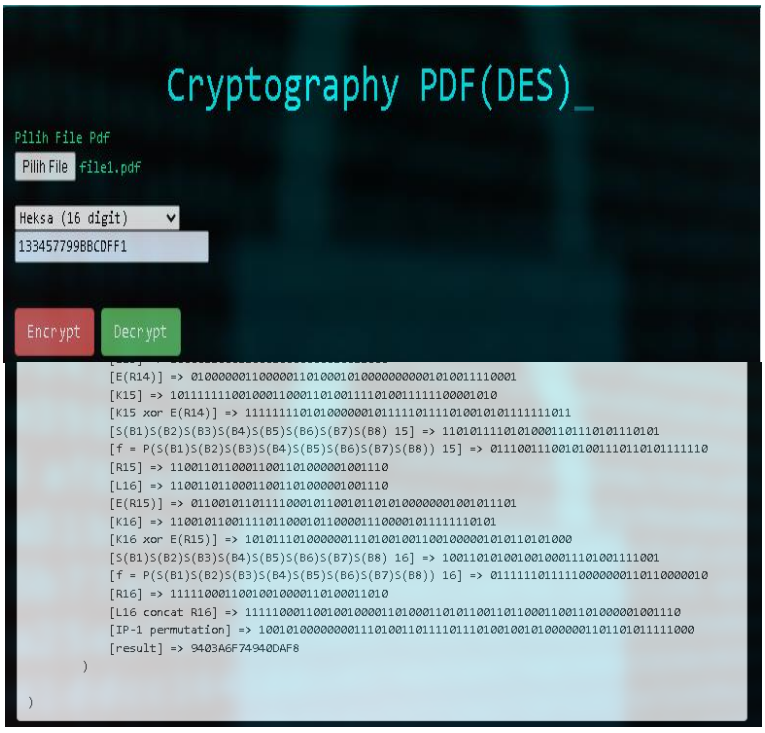

Figure 2. Input files, keys and output

3. View PDF files after encryption
   After clicking the decryption process button with the wrong key, the PDF file will be saved in the directory which has been specified and will create a new file, as shown below:

Figure 3. PDF files encryption result

4. Display the results of the pdf file after decryption with the wrong key
   After clicking the decryption process button with the wrong key, the PDF file will be saved in the directory which has been specified and will create a new file, as shown below:

Figure 4. pdf file after decryption with the wrong key

Based on the image above, the Decryption process with the wrong key will create an empty PDF file and not carry out the process correctly.

5. Display the results of the pdf file after it has been decrypted with the correct key
   After clicking the decryption process button with the correct key, the PDF file will be saved in the specified directory and will create a new file after which it appears to be output with the aim of proving that the manual results are the same as the results in the program, as in the image below:

Figure 5. Pdf file after decrypted with the correct key display

3.1. Encryption key Test Results and description

Based on cryptographic tests on the application, it was found that the pdf file is the data file object for carrying out the DES Algorithm. This of course makes the pdf file data not damaged, because there is no change to the original data object because it is encoded to base64 so that the pdf file does not change at all before being executed encryption. Therefore, the confidentiality of encrypted PDF files will not leak because the key can only be stored by the creator. The test results with 3 sample pdfs and keys are as follows:

Table 1. Test Results and description

Filename Pdf			Pdf Data Size			Key	Description
Original	Encryption	Decryption	Original	Encryption	Decryption		
file1.pdf	enk1.pdf	dek1.pdf	609KB	812KB	609 KB	133457799BB CDFF1	Berhasil
file2.pdf	Enk2.pdf	Dek2.pdf	430KB	574KB	430KB	5EAF 57799BBCDFe 1	Berhasil
File3.pdf	Enk3.pdf	Dek3.pdf	20KB	26KB	20KB	COMPUTER	Berhasil

4. CONCLUSIOON

Based on the results of research on protecting pdf files with keys using the DES method, several conclusions can be drawn from the descriptions described in the previous chapters. The results of this study draw the following conclusions:

1. PDF document files can be protected by DES encryption using a key, and cannot be decrypted without knowing the key.
2. The size and file contents of the PDF document encrypted with the key will change. The decrypted pdf data file is back to normal in terms of size and number of bytes in the file

REFERENCES

[1] Adhar, D. (2019). Implementasi Algoritma Des (Data Encryption Standard) Pada Enkripsi Dan Deskripsi Sms Berbasis Android. *JTIK (Jurnal Teknik Informatika Kaputama)*, *3*(2), 53–60.
[2] Agustina, E. R., & Kurniati, A. (2015). Pemanfaatan kriptografi dalam mewujudkan keamanan informasi pada e-voting di indonesia. Seminar Nasional Informatika (SEMNASIF), 1(3).
[3] Aleisa, N. (2015). A Comparison of the 3DES and AES Encryption Standards. International Journal of Security and Its Applications, 9(7), 241–246.
[4] Ariyus, D. (2008). Pengantar ilmu kriptografi: teori analisis & implementasi. Penerbit Andi.
[5] Gunawan, H. A., Arifin, Z., & Astuti, I. F. (2016). Keamanan Login Web Menggunakan Metode 3DES Berbasis Teknologi Quick Response Code. Informatika Mulawarman: Jurnal Ilmiah Ilmu Komputer, 9(2), 18–23.
[6] Hasugian, B. S. (2017). Peranan Kriptografi Sebagai Keamanan Sistem Informasi Pada Usaha Kecil Dan Menengah. Warta Dharmawangsa, 53.
[7] Nasution, Y. R., Furqan, M., & Sinaga, M. (2020). Implementasi Steganografi Menggunakan Metode Spread Spectrum Dalam Pengamanan Data Teks Pada Citra Digital. J-SAKTI (Jurnal Sains Komputer Dan Informatika), 4(2), 351–358.
[8] Nugroho, A. (2005). Analisis dan Perancangan Sistem Informasi dengan Metodologi Berorientasi Objek. Edisi Revisi.
[9] Pratiwi, P., & WP, D. A. (2016). Peningkatan Keamanan Data Dengan Metode Cropping Selection Pseudorandom. Jurnal TICOM, 4(3), 92394.
[10] Primartha, R. (2011). Penerapan enkripsi dan dekripsi file menggunakan algoritma Data Encryption Standard (DES). JSI: Jurnal Sistem Informasi (E-Journal), 3(2).
[11] Rohmanu, A. (2017). Implementasi kriptografi dan steganografi dengan metode algoritma DES dan metode End Of File. Jurnal Informatika SIMANTIK, 2(1), 1–11.
[12] Setyaningsih, E., Si, S., & Kom, M. (2015). Kriptografi & implementasinya menggunakan MATLAB. Yogyakarta: ANDI.
[13] Siregar, N. (2019). PERANCANGAN APLIKASI KEAMANAN PESAN TEKS DENGAN MENGGUNAKAN ALGORITMA TRIPLE DES. JTIK (Jurnal Teknik Informatika Kaputama), 3(2), 11–17
[14] Sulastri, S., & Putri, R. D. M. (2018). Implementasi Enkripsi Data Secure Hash Algorithm (SHA-256) dan Message Digest Algorithm (MD5) pada Proses Pengamanan Kata Sandi Sistem Penjadwalan Karyawan. Jurnal Teknik Elektro, 10(2), 70–74.
[15] Wibowo, G. T., Rumani, M., & Saputra, R. E. (2015). Analisis Dan Implementasi Enkripsi Dan Dekripsi Ganda Kombinasi Algoritma Blowfish Dan Algoritma Triple Des Untuk Sms Pada Smartphone Android. EProceedings of Engineering, 2(2).
[16] Winafil, M., Sinurat, S., & Zebua, T. (2018). Implementasi Algoritma Advanced Encryption Standard dan Triple Data Encryption Standard Untuk Mengamankan Citra Digital. KOMIK (Konferensi Nasional Teknologi Informasi Dan Komputer), 2(1).
[17] Yanti, N. R., Alimah, A., & Ritonga, D. A. (2018). Implementasi Algoritma Data Encryption Standard Pada Penyandian Record Database. J-SAKTI (Jurnal Sains Komputer Dan Informatika), 2(1), 23–32.
[18] Yusfrizal, Y. (2019). Rancang Bangun Aplikasi Kriptografi Pada Teks Menggunakan Metode Reverse Chiper Dan Rsa Berbasis Android. JTIK (Jurnal Teknik Informatika Kaputama), 3(2), 29–37.s