Digital Document Validation Using Cryptography With DES (Data Encryption Standard) METHODS

by Nenny Anggraini

Submission date: 27-Jun-2019 07:24PM (UTC+0700)
Submission ID: 1147451736
File name: sing_Cryptography_With_DES_Data_Encryption_Standard_Methods.docx (31.89K)
Word count: 1137
Character count: 6256

DIGITAL DOCUMENT VALIDATION USING CRYPTOGRAPHY WITH DES (Data Encryption Standard) METHODS

Nenny Anggraini, Feri Fahrianto***
nenny@yahoo.com, fahrianto@gmail.com
Lecturer Department of Information Engineering
Syarif Hidayatullah State Islamic University Jakarta

ABSTRACT

Validation of digital documents is one of the important issues in the era of information and communication technology, given the increasing use of digital documents in all aspects. Another thing that is important in a digital document is a matter of safety and capacity of the file of documents.

Data compression as a science exists to be a solution to the data requires a large storage capacity, the process of data compression is to reduce the number of bits used to store and transmit data. Compression of data covering a wide range of compression techniques implemented in software and hardware with a lot of advantages.

One alternative to maintain data security is by using cryptographic algorithms that implement DES (Data Encryption Standard). DES algorithm is a symmetric cryptographic algorithm that uses the same key for encryption and decryption. DES algorithm works on 64 bit data blocks and uses a key length of 56 bits. The processes contained in the DES algorithm include an internal key generation, initial permutation, enciphering, and the final permutation.

Key words: Cryptography, Data Compression, Validation, digital documents, DES Algorithm

I. INTRODUCTION

The document is an article containing information from one person to another or from one group to another group. Digital document is any electronic information is created, transmitted, sent, received, or stored in the form of analog, digital, electromagnetic, optical, or the like, which can be displayed and / or heard via computer or electronic system, including but not limited to text, sound or image, map, plan, photograph or the like that can be understood by people who are able to understand it. (Hartiyanto, 2009).

Digital documents highly flexible to be edited copied or distributed, it makes more and more people tend to work on a digital-based documents than working with documents conventional. Today, many digital documents are made via the computer because a lot of the benefits obtained by digital documents such as ease of storage and speed of distribution. However, the use of digital documents does not mean that the document is safe, there are a variety of attack techniques in digital documents so that those who are not responsible know and misusing confidential information contained in those documents, the security factor therefore becomes an important issue in document management digital (Rashid, 2009). Besides the safety factor, digital documents also tend to have large storage capacity; this will affect the speed of data transmission and storage waste on the media that required compression of digital data. On the other hand the standardization of digital documents is also a separate issue that affects validation and validity of digital Document sent or received.

Cryptography as a science exists to improve the security aspects in digital document, either in the form of text documents, images or audio. Crypto graphing text is

more familiar among the public at large. Applications that are already implementing cryptography on text data had already been developed. Data compression is an attempt to reduce the number of bits used to store and transmit data. Compression of data covering a wide range of compression techniques implemented in software or hardware, the benefits of data compression such as reducing the bottleneck in the I / O and data transmission, more efficient data storage space, complicate the reading of data by unauthorized parties, and facilitate the distribution of data with removable media like flash drives, CDs, DVDs, etc..

From the description above, the author tries to take a common thread of all the weaknesses of digital documents by doing cryptography in digital documents by performing a validation of such documents to be shown to the legality and validity by generating a file that has been compressed.

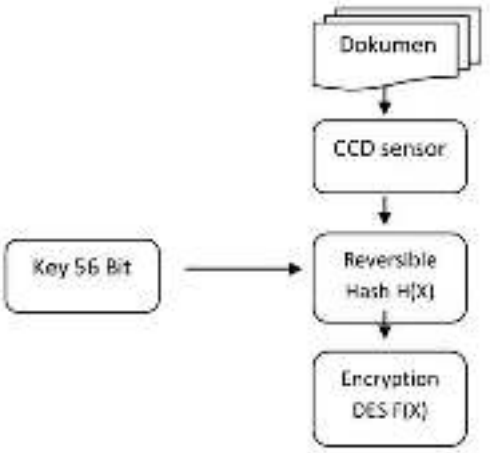
II. Similar research

Writing and research on digital documents with DES method of research has been done especially in the area of cryptography that uses the DES algorithm of DES Algorithm Simulation Application Data Transfer Money In Bank (Fitria, 2006), Simulation Privacy / Security Information By Using Algorithm DES (Data Encryption Standard) (Indra Syahputra, 2009) and Application Development Audio File Cryptographic algorithm data Encryption Standard (DES) (I WAYAN Dana Asmara, Made Windu Between Kasiman, Ketut Agustini, 2011).

III. Discussion of issues

Discussion of this paper is about the validation of digital documents using the DES cryptographic methods, in the process of validation required a kind of scanner devices, so the cryptographic process undertaken within the scanner, but the tool is only an intermediary that basically can be replaced with another.

The design tools developed through several steps that must be carried out with the purpose of facilitating the study. The flow of research conducted by the author begins with the observation whether there was a kind of device that has been created and analyzed the system to be created. After observation / analysis system next stage is literature and literary studies. Literature study done to find solutions to problems as well as the basic theory related to the research literature, while studies conducted in similar research to support the research. The next stage is to carry out the system development phase. Stages of system development through prototyping approach. And the last is the implementation of a system that includes the construction and testing. More clearly, the flow is described as shown below.



IV. CONCLUSION

The conclusion of this paper is that this tool as a tool that is able to validate the digital documents with a file that has been compressed output making it easier for companies and institutions in the process to obtain important documents. using the DES algorithm allows made pin with id 2 rank 56, while the user has many

benefits to doing the scan a document and the document can be sent directly to the intended recipient in the form of files that have been encrypted to guarantee the security of data and the data received has been given a recognized code validation. On Company or agency side, using this tool will help the process to obtain important documents which if submitted manually will take time and the security is not guaranteed.

V. REFERENCES

[1] Rasyid, Muhammad Fajri. 2009. "Kriptografi Audio dengan Teknik Interferensi Data Non Biner". http://www.digilib.itb.ac.id

[2] Arnyus, Dony, 2008. Pengantar Ilmu Kriptografi Teori, Analisis, dan Implementasi, Yogyakarta CV, Andi Offset

[2] Firna, Faiz Sungkar, 2006. "Simulasi Aplikasi Algoritma DES Pada Transfer Data Uang Bank", Jurnal Informatika, Vol.6, No.1. STMIK Damnajaya

[3] Indra Syahputra. 2009. Simulasi Kerahasiaan / Keamanan Informasi Dengan Menggunakan Algoritma DES (Data Encryption Standard). Skripsi (tidak diterbitkan). Universitas Sumatra Utara.

[4] I Wayan Dana Asmara, Made Windu, Ketut Agustini, 2011. "Pengembangan Aplikasi Kriptografi File Audio dengan Menggunakan Algoritma DES", Prosiding Seminar Nasional Pendidikan Teknik Informatika, SENAPATI Singaraja

Digital Document Validation Using Cryptography With DES (Data Encryption Standard) METHODS

ORIGINALITY REPORT

10%	8%	6%	0%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	toryhafizh.blogspot.com Internet Source	3%
2	Heiser, Jay, Steve Stanek, Sasan Hamidi, Ben Rothke, Paul Lambert, Ralph Spencer Poore, James Tiller, Ronald Gove, and Mark Edmead. "Methods of Attacking and Defending Cryptosystems", Information Security Management Handbook on CD-ROM 2006 Edition, 2006. Publication	1%
3	docplayer.info Internet Source	1%
4	zh.scribd.com Internet Source	1%
5	Dimas Riyan Hartadi, Nurhayati. "Development of web-based savings Kurban management application with YII framework case study: CV Almanna", 2014 International Conference on Cyber and IT Service Management (CITSM),	1%

2014
Publication

6	www.flevin.com Internet Source	1%
7	eprints.unm.ac.id Internet Source	1%

Exclude quotes	On	Exclude matches	< 3 words
Exclude bibliography	On		