# Welcome to JARDCS

Journal of Advanced Research in Dynamical and Control Systems presents peer-reviewed survey and original research articles.

ISSN: 1943-023X

Know More (about.php)

# Journal of Advanced Research in Dynamical and Control Systems - JARDCS

**Journal of Advanced Research in Dynamical and Control Systems** examines the entire spectrum of issues related to dynamical systems, focusing on the theory of smooth dynamical systems with analyses of measure-theoretical, topological, and bifurcational aspects. It covers all essential branches of the theory--local, semi local, and global--including the theory of foliations.

The journal also features in-depth papers devoted to control systems research that spotlight the geometric control theory, which unifies Lie-algebraic and differential-geometric methods of investigation in control and optimization, and ultimately relates to the general theory of dynamical systems.

**Journal of Advanced Research in Dynamical and Control Systems** presents peer-reviewed survey and original research articles. Accessible to a broad range of scholars, each survey paper contains all necessary definitions and explanations, a complete over-view of the problem discussed, and a description of its importance and relationship to basic research on the subject.

This publication also features authoritative contributions describing ongoing investigations and innovative solutions to unsolved problems as well as detailed reviews of newly published books relevant to future studies in the field.

## Publisher

Institute of Advanced Scientific Research

## Acceptance Ratio

2008 - 10%
2009 - 15%
2010 - 18%
2011 - 20%
2012 - 46%
2013 - 30%
2014 - 40%
2015 - 50%
2016 - 20%
2017 - 55%
2018 - 58%

## Key Dates

**Paper Submission Open:**
01 Jan 2019

**Final Date for Submission**
20 Feb 2019

**Acceptance Notification**
10 Mar 2019

Archives

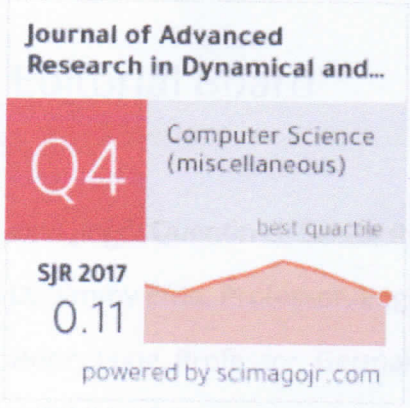
Current Issue (current-issue.php)

All Archives (archives.php)

Special Issues (special-issue.php)

Accepted Articles (accepted-articles.php)

Scopus SJR




(http://www.scimagojr.com/journalsearch.php?q=20500195215&tip=sid&exact=no)

# EDITORIAL BOARD

## Editorial Board



## More About Us

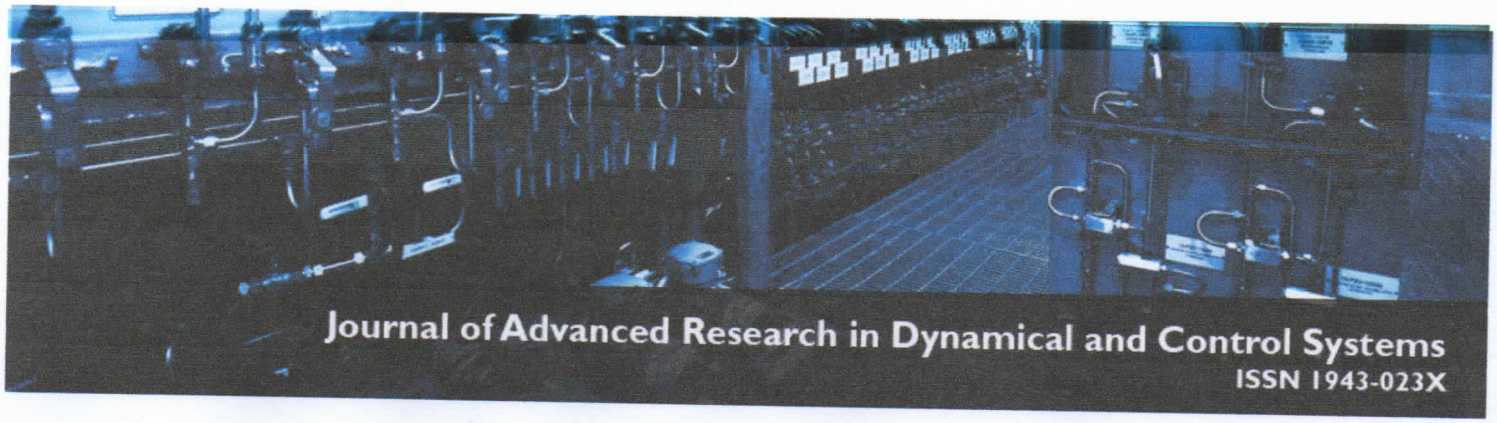
› About JARDCS (about.php)

› Scope of JARDCS (scope.php)

› Contact (contact.php)

JARDCS






## Special Issue

### 07-Special Issue, 2018

Guest Editor(s):

### Table of Contents

### Modeling and Analysis of the Characteristics of Ultraviolet Channels under Different Conditions of Radiation Propagation for the Organization of Wireless AD-HOC Network

Authors: I.S. Konstantinov, G.S. Vasilyev, O.R. Kuzichkin, I.A. Kurilov, S.A. Lazarev
Abstract Purchase this Article

Pages: 1853-1859

### Modeling Of the Mechanism of the Main Macroeconomic Categories' Interrelations of National Economies

Authors: L.M. Davletshina, L.G. Nabieva, A.E. Ustinov, R.I. Muhamadiyarova, A.I. Mingazova
Abstract Purchase this Article

Pages: 1860-1868

### Design of Expert System to Determine Stock Investment Using Forward Chaining Method

Authors: *Bakaruddin,Zul Azmi,B.Herawan Hayadi
Abstract Purchase this Article

Pages: 1869-1873

### IPv6 Modeling in E-ID Cards as Efficiency Efforts in the Population Registration Process

Authors: *A M H Pardede, Y Maulita, R Buaton, H Mawengkang,M Zarlis
Abstract Purchase this Article

Pages: 1874-1878

### Security Application using Data Encryption Standard Algorithm

Authors: *R Ratnadewi, Dadang Sudrajat, Ayu Esteka Sari, Sri Utami Ady, Dian Rianita
Abstract Purchase this Article

Pages: 1879-1882

Total Results : 249

previous 1 2 ... 17 18 19 20 21 22 23 24 25 next

# Security Application using Data Encryption Standard Algorithm

[1*]*R Ratnadewi*, Department of Electrical Engineering, Universitas Kristen Maranatha, Bandung, Indonesia
[2]*Dadang Sudrajat,* Department of Informatics, Sekolah Tinggi Manajemen Informatika dan Komputer IKMI Cirebon, Indonesia
[3]*Ayu Esteka Sari*, Department of Management, STIE Sakti Alam Kerinci, Jambi, Indonesia
[4]*Sri Utami Ady*, Faculty of Economics and Business, Universitas Dr. Soetomo, Surabaya, Indonesia
[5]*Dian Rianita*, Faculty of Administration, Universitas Lancang Kuning, Pekanbaru, Indonesia

**Abstract---** Security is an important factor in data communication, and cryptography is a process that can secure existing data communications. The Data Encryption Standard (DES) algorithm that is used as a data security process can be well done and the application that is made is given information in the form of a simulation process of the encryption and decryption process so that users know the cryptographic process with the DES algorithm.

**Keywords---** Cryptography, Simulation DES, Secure Text

## I. Introduction

In an era of increasingly sophisticated technology, data and information security is very important for the company and for personal needs[1]–[3]. Especially when it comes to data security in networks where everything can be accessed[4]–[7]. Various activities such as hackers, making viruses, electronic fraud and electronic sniffing that will cause problems in data security that cause data loss or data theft for use by irresponsible parties[8], [9]. The development of computer systems and their interconnection through the network has increased very sharply in recent years, of course this also requires reliable data security to avoid or minimize attacks on the network or outside the network, and one of the solutions that can be used is cryptography[10]–[12].

Cryptographic applications are applications that are most often used to secure information, secure information can be in the form of video, audio, image and text files[7], [13]. Security can be done in many ways and using many methods with different levels of security ranging from classical cryptography to cryptographic use modern like One Time Pad, Vigenere Cipher, Blowfish, AES, DES and RSA. For data security, cryptography is required with the encryption method. This study focuses on the use of cryptographic applications that follow the DES method to secure data.

## II. Methodology

Cryptography is a mathematical science that deals with the transformation of data to make its meaning incomprehensible (to hide its meaning), prevent it from changing without permission, or prevent it from unauthorized use. If the transformation can be restored, cryptography can also be interpreted as the process of converting encrypted data back into an understandable form. That is, cryptography can be interpreted as a process to protect data in the sense that it is[11], [14], [15].

Cryptography is a secret technique in writing, with special characters, using letters and characters outside their original form, or with other methods that can only be understood by those who process the keys, as well as all things written in this way. So, generally it can be interpreted as the art of writing or solving ciphers[16].

### *A. Cryptography Algorithm*

Cryptography is a form of algorithm for scrambling messages and returning scrambled messages, where the cryptographic algorithm is made using calculations and mathematical formulas. Cryptographic algorithm is a mathematical function used for encryption and decryption. To encrypt a plaintext message, apply the encryption algorithm to the plaintext message. To decrypt a ciphertext message, apply the decryption algorithm to the ciphertext message[8]

The algorithm is not reliable confidentiality. By using a published algorithm, the cryptographer is free to consult with a number of academic cryptologists who wish to penetrate the system so that they can publish writings that show how clever they are. If after the algorithm has been published for 5 years and no one has managed to solve it, then maybe the algorithm is quite solid[9].

*Corresponding Author: R Ratnadewi*
Article History: Received: Aug 15, 2018, Revised: Sep 10, 2018, Accepted: Oct 04, 2018

Secrecy actually lies in the key and the length of the key is an important issue in the design. Take a simple combination key. The general principle is where a person enters a digit in sequence. Everyone knows this, but the key is a secret. With a double digit key length means that there are a hundred possibilities. The three-digit key length has a thousand possibilities, and the six-digit key length has a million possibilities. The longer the key, the higher the work factor that the cryptanalyst must do. The work factor to penetrate the system with exhausting key searches is exponential to the key length. Confidentiality comes from the existence of powerful and published algorithms with long keys. The requirements of a good cryptographic algorithm include:

a. System security lies in the confidentiality of the key and not in the confidentiality of the algorithm used.
b. The algorithm has a large key space.
c. Generate random ciphertext in all statistical tests performed on it.
d. Able to withstand all previously known attacks.

However, it should be noted that if a cryptographic algorithm manages to fulfill all of the above characteristics it is not necessarily a good system. Many weak cryptographic algorithms that look good at first. Sometimes to show that a cryptographic algorithm is strong or good can be done using mathematical proof.

Until now there are still many who use Cryptographic algorithms that are relatively easy to open, the reason is that they do not know of other systems that are better and sometimes there is less motivation to invest all the effort needed to open a system

### *B. DES Algorithm*

The DES algorithm is the most widely used encryption algorithm in the world adopted by NIST (National Institute of Standards and Technology) as the US Federal information processing standard. The plaintext data is encrypted in 64-bit blocks into 64-bit ciphertext data using an internal key 56 key. DES transforms 64-bit input in several stages of encryption into 64-bit output. Thus, DES includes block ciphers.

In the DES algorithm, there are external keys and internal keys. Internal keys are generated from external keys provided by the user. Internal keys can be generated before the encryption process or together with the encryption process. External keys are 64 bits long or 8 characters long. Because there are 16 rounds, the required internal keys are 16, namely K1, K2, ..., K16.

The external key is 64 bits, compressed first to 54 bits using the PC-1 compression permutation matrix. In each permutation the 8th bit of the 8 bytes of the key will be ignored. So there will be an 8-bit use of the initial 64-bit external key[17].

## III. Result and Discussion

Cryptographic applications that are made require some software such as Microsoft Windows 10, Visual Basic.Net 2017 and some library functions for cryptographic algorithms, figure 1 until figure 3 are simulation result of DES Application.

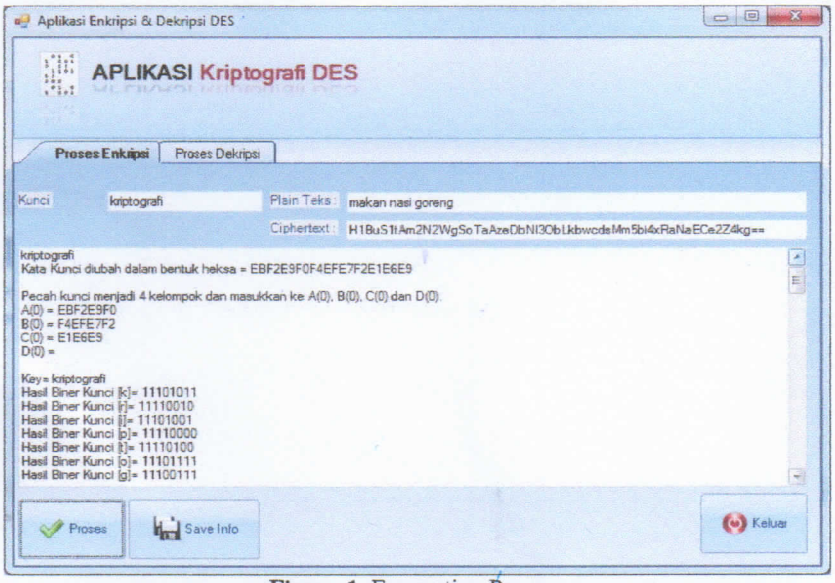



**Figure 1.** Encryption Process

Figure 1 describes the encryption process from plaintext = *makan nasi goreng*, key = *kriptografi*, the encryption process is made in the form of a simulation so that the DES algorithm process can be manually learned as part of the DES algorithm cryptographic learning process.

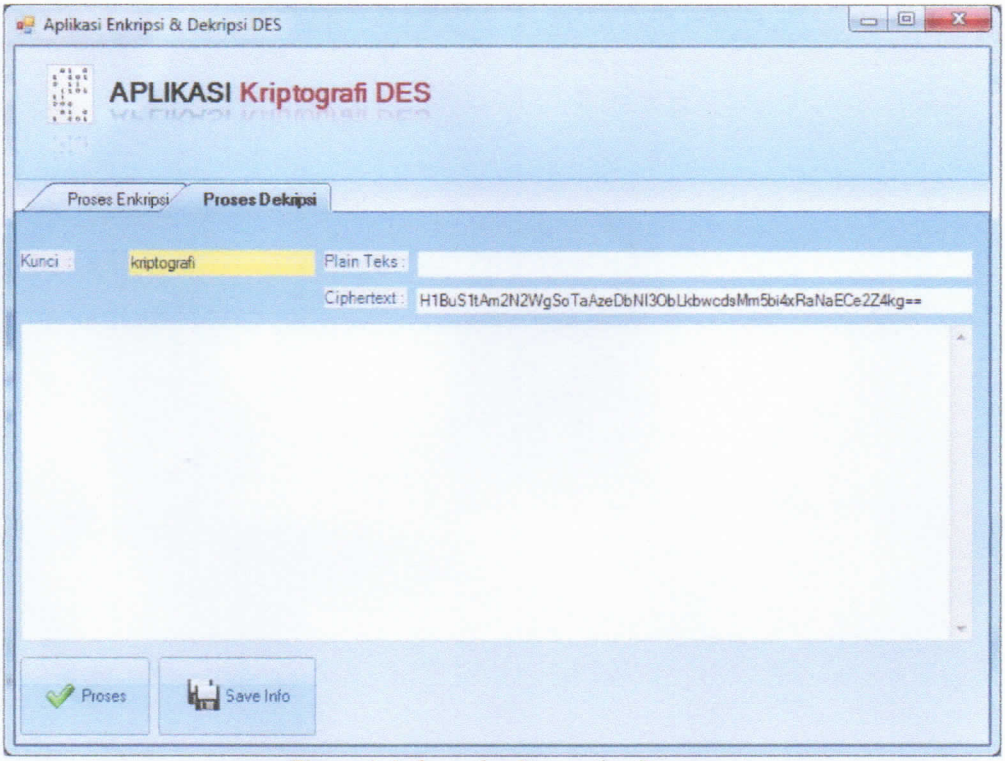



**Figure 2.** Information Decryption Process

Figure 2 displays information on the decryption process, to do the decryption process, the key and ciphertext *needed from the encryption process that has been done.*

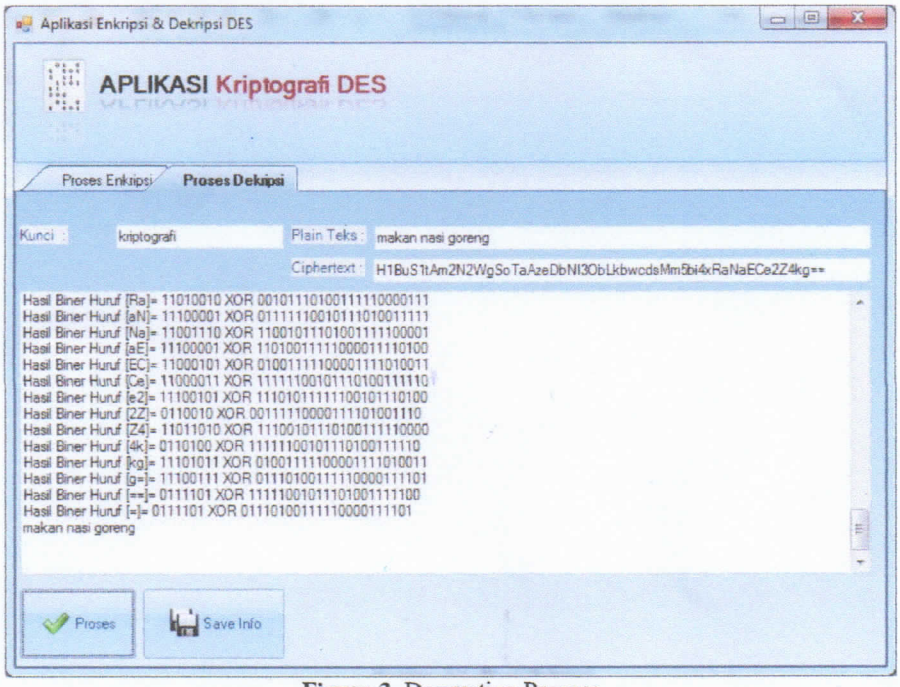



**Figure 3.** Decryption Process

Figure 3 is a decryption process carried out using the DES algorithm, the results of the simulation process are displayed in stages to facilitate the cryptographic education process.



*Corresponding Author: R Ratnadewi
Article History: Received: Aug 15, 2018, Revised: Sep 10, 2018, Accepted: Oct 04, 2018

## IV. Conclusion

DES algorithms that are applied to data security applications can run well without any errors, in addition to the application given the manual DES algorithm calculation process to make it easier for users to know the work process of the DES algorithm and calculations performed. This application is far from perfect, especially the DES algorithm, it also needs improvisation to be more strong in the future.

## References


[1] G. Singh and Supriya, "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security," *Int. J. Comput. Appl.*, vol. 6, no. 19, pp. 33–38, 2013.

[2] S. Maitra and G. Paul, "Analysis of RC4 and proposal of additional layers for better security margin," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2008, vol. 5365 LNCS, pp. 27–39.

[3] S. Hawkins, D. C. Yen, and D. C. Chou, "Awareness and challenges of Internet security," *Inf. Manag. Comput. Secur.*, vol. 8, no. 3, pp. 131–143, 2000.

[4] W. Stallings, *Network security essentials : applications and standards*. 2011.

[5] K. J. Fitzgerald, "Security and data integrity for LANs and WANs," *Inf. Manag. Comput. Secur.*, vol. 3, no. 4, pp. 27–33, 1995.

[6] T. Özyer, Z. Erdem, J. Rokne, and S. Khoury, *Mining Social Networks and Security Informatics*. 2013.

[7] B. Prema Sindhuri and M. Kameswara Rao, "IoT security through web application firewall," *Int. J. Eng. Technol.*, vol. 7, no. 2–7, p. 58, Mar. 2018.

[8] R. Rahim, "Man-in-the-middle-attack prevention using interlock protocol method," *ARPN J. Eng. Appl. Sci.*, vol. 12, no. 22, pp. 6483–6487, 2017.

[9] M. Mesran, M. Syahrizal, and R. Rahim, "Enhanced Security for Data Transaction with Public Key Schnorr Authentication and Digital Signature Protocol," *ARPN J. Eng. Appl. Sci.*, vol. 13, no. 11, pp. 3839–3846, 2018.

[10] J. Yuan, S. Yu, and L. Guo, "SEISA: Secure and efficient encrypted image search with access control," in *Proceedings - IEEE INFOCOM*, 2015, vol. 26, pp. 2083–2091.

[11] R. I. Al-Khalid, R. A. Al-Dallah, A. M. Al-Anani, R. M. Barham, and S. I. Hajir, "A Secure Visual Cryptography Scheme Using Private Key with Invariant Share Sizes," *J. Softw. Eng. Appl.*, vol. 10, no. 01, pp. 1–10, Jan. 2017.

[12] E. Koopahi and S. E. Borujeni, "Secure scan-based design using Blum Blum Shub algorithm," in *Proceedings of 2016 IEEE East-West Design and Test Symposium, EWDTS 2016*, 2017.

[13] R. Ratnadewi, R. P. Adhie, Y. Hutama, J. Christian, and D. Wijaya, "Implementation and performance analysis of AES-128 cryptography method in an NFC-based communication system," *World Trans. Eng. Technol. Educ.*, vol. 15, no. 2, pp. 178–183, 2017.

[14] A. G. D. Uchoa, M. E. Pellenz, A. O. Santin, and C. A. Maziero, "A Three-Pass Protocol for Cryptography Based on Padding for Wireless Networks," in *2007 4th IEEE Consumer Communications and Networking Conference*, 2007, pp. 287–291.

[15] S. Bruce, *Applied cryptography*. 1996.

[16] R. A. Mollin, *An introduction to cryptography*. Chapman & Hall/CRC, 2007.

[17] NIST, "Data Encryption Standard," *Fed. Inf. Process. Stand. Publ.*, 1999.