

PROCEEDINGS



The Second International Conference on Science,
Engineering and Technology

“Sustainable Development in Developing
Country for Facing Industrial Revolution 4.0”

September 5-7, 2019

SKA Convention & Exhibition Center, Pekanbaru, Riau, Indonesia

Editors:

Arbi Haza Nasution

Evizal Abdul Kadir

Luiz Moutinho

Organizer :



Co-Organizers :



UNIVERSITI
TEKNOLOGI
MARA



Infrastructure
University
Kuala Lumpur

ICoSET 2019

Proceedings of the
Second International Conference on
Science, Engineering and Technology

Riau - Indonesia

September 5 - 7, 2019

Copyright © 2020 by SCITEPRESS – Science and Technology Publications, Lda.
All rights reserved

Edited by Arbi Haza Nasution, Evizal Abdul Kadir and Luiz Moutinho

Printed in Portugal

ISBN: 978-989-758-463-3

Depósito Legal: 473348/20

<http://icoset.uir.ac.id>

BRIEF CONTENTS

INVITED SPEAKERS	IV
ORGANIZING COMMITTEES	V
PROGRAM COMMITTEE	VI
FOREWORD	VII
CONTENTS	IX

INVITED SPEAKERS

Prof. EE-Peng Lim
Singapore Management University
Singapore

Assoc. Prof. Yuichi Sugai
Kyushu University
Japan

Prof. Ir. Dr Sharul Kamal Abdul Rahim
Universiti Teknologi Malaysia
Malaysia

Assoc. Prof. Dr. Norma binti Alias
Universiti Teknologi Malaysia
Malaysia

ORGANIZING COMMITTEES

GENERAL CHAIR

Dr. Arbi Haza Nasution, M.IT, Universitas Islam Riau, Indonesia

TECHNICAL PROGRAM CHAIR

Dr. Evizal Abdul Kadir, ST., M.Eng, Universitas Islam Riau, Indonesia

GENERAL CO-CHAIR

Dr. Eng. Muslim, ST., MT, Universitas Islam Riau, Indonesia

EDITORIAL CHAIR

Yudhi Arta, S.Kom., M.Kom, Universitas Islam Riau, Indonesia

STEERING COMMITTEE

Prof. Josaphat Tetuko Sri Sumantyo, Ph.D, Chiba University, Japan
Prof. Ir. Dr. Sharul Kamal Abdul Rahim, Universiti Teknologi Malaysia, Malaysia
Prof. Toru Ishida, Kyoto University, Japan
Prof. Ee-Peng Lim, Singapore Management University, Singapore
Prof. Dr. H Syafrinaldi SH, MCL, Universitas Islam Riau, Indonesia

PUBLICATION AND RELATIONSHIP CHAIR

Dr. Syafriadi, S.H., M.H., Universitas Islam Riau, Indonesia

FINANCIAL CHAIR

Ause Labellapansa, ST., M.Cs., M.Kom., Universitas Islam Riau, Indonesia

EDITORIAL BOARD

Putra Efri Rahman, S.Kom, Universitas Islam Riau, Indonesia
Khairul Umam Syaliman, S.T., M.Kom., Politeknik Caltex Riau, Indonesia
Winda Monika, S.Pd., M.Sc., Universitas Lancang Kuning, Indonesia
Panji Rachmat Setiawan, S.Kom., M.M.S.I., Universitas Islam Riau, Indonesia
Rizdqi Akbar Ramadhan, S.Kom., M.Kom., Universitas Islam Riau, Indonesia
Anggiat, Universitas Islam Riau, Indonesia
Arif Lukman Hakim, Universitas Riau, Indonesia

PROGRAM COMMITTEE

- Prof. Dr. Tengku Dahril, M.Sc.**, Universitas Islam Riau, Indonesia
- Prof. Dr. Hasan Basri Jumin, M.Sc.**, Universitas Islam Riau, Indonesia
- Prof. Dr. Sugeng Wiyono, MMT**, Universitas Islam Riau, Indonesia
- Prof. Zainal A. Hasibuan, MLS., Ph.D.**, University of Indonesia, Indonesia
- Prof. Josaphat Tetuko Sri Sumantyo, Ph.D.**, Chiba University, Japan
- Prof. Dr. Eko Supriyanto**, Universiti Teknologi Malaysia, Malaysia
- Prof. Dr. Zailuddin Arifin**, Universiti Teknologi MARA, Malaysia
- Prof. Jhon Lee, B.Sc, M.Sc., Ph.D.**, Kyungdong University, Korea
- Prof. Ahmed A. Al Absi**, Kyungdong University, Korea
- Prof. Wisup Bae, Ph.D.**, Sejong University, Korea
- Prof. Kyuro Sasaki**, Kyushu University, Japan
- Prof. Adiwijaya**, Telkom University, Indonesia
- Prof. Ir. Asep Kurnia Permadi, M. Sc, Ph.D.**, Institut Teknologi Bandung, Indonesia
- Assoc. Prof. Dr. Azhan Hashim Ismail**, Universiti Teknologi MARA, Malaysia
- Assoc. Prof. Yuichi Sugai**, Kyushu University, Japan
- Assoc. Prof. Dr. Sonny Irawan**, Universiti Teknologi Petronas, Malaysia
- Assoc. Prof. Hussein Hoteit**, King Abdullah University of Science and Technology, Saudi Arabia
- Assoc. Prof. Dr. Anas Puri, ST., MT**, Universitas Islam Riau, Indonesia
- Kuen-Song Lin, Ph.D.**, Yuan Ze University, Taiwan
- Dr. Shukor Sanim Mohd Fauzi**, Universiti Teknologi MARA, Malaysia
- Dr. Inkyo Cheong**, Inha University, Korea
- Ahn, Young Mee, Ph.D.**, Inha University, Korea
- Hitoshi Irie, Ph.D.**, Chiba University, Japan
- Julie Yu-Chih Liu, Ph.D.**, Yuan Ze University, Taiwan
- Liang Chih Yu, Ph.D.**, Yuan Ze University, Taiwan
- Chia-Yu Hsu, Ph.D.**, Yuan Ze University, Taiwan
- Dr. Amit Pariyar**, University Malaysia Sarawak, Malaysia
- Dr. Madi Abdullah Naser**, Sebha University, Libya
- Dr. Nguyen Xuan Huy**, Ho Chi Minh City University of Technology, Vietnam
- Dr. Chunqiu Li**, Beijing Normal University, China
- Dr. Goh Thian Lai**, Universiti Kebangsaan Malaysia, Malaysia
- Dr. Syahrir Ridha**, Universiti Teknologi Petronas, Malaysia
- Dr. Kemas Muslim L.**, Telkom University, Indonesia
- Dr. Moch. Arif Bijaksana**, Telkom University, Indonesia
- Dr. Satria Mandala**, Telkom University, Indonesia
- Dr. Wahyudi Sutopo**, Solo State University, Indonesia
- Dr. Zulfatman**, University of Muhammadiyah Malang, Indonesia
- Dr. Suranto AM**, UPN Veteran Yogyakarta, Indonesia
- Dr. Eng. Husnul Kausarian, B.Sc (Hons)., M.Sc.**, Universitas Islam Riau, Indonesia

FOREWORD

In the name of Allah, Most Gracious, Most Merciful
Assalamu'alaikum Wr. Wb.,

Welcome to the Second International Conference on Science Engineering and Technology (ICoSET 2019). The advancement of today's computing technology, science, engineering and industrial revolution 4.0 play a big role in the sustainable development of social, economic, education, and humanity in developing countries. Institute of higher education is one of many parties that need to be involved in the process. Academicians and researchers should promote the concept of sustainable development. The Second International Conference on Science, Engineering and Technology (ICoSET 2019) is organized to gather researchers to disseminate their relevant work on science, engineering and technology. The conference is co-located with The Second International Conference on Social, Economy, Education, and Humanity (ICoSEEH 2019) at SKA Co-EX Pekanbaru Riau.

I would like to express my hearty gratitude to all participants for coming, sharing, and presenting your research at this joint conference. There is a total of 84 manuscripts submitted to ICoSET 2019. However only high-quality selected papers are accepted to be presented in this event, with the acceptance rates of ICoSET 2019 is 70%. We are very grateful to all steering committees and both international and local reviewers for their valuable work. I would like to give a compliment to all co-organizers, publisher, and sponsors for their incredible supports.

Organizing such prestigious conferences was very challenging and it would be impossible to be held without the hard work of the program committee and organizing committee members. I would like to express my sincere gratitude to all committees and volunteers from Singapore Management University, Kyoto University, Kyushu University, University of Tsukuba, Khon Kaen University, Ho Chi Minh City University of Technology, University of Suffolk, Universiti Teknologi Malaysia, Infrastructure University Kuala Lumpur, Universiti Malaya, Universiti Kebangsaan Malaysia, Universiti Utara Malaysia, Universiti Teknologi Mara, and Universiti Pendidikan Indonesia for providing us with so much support, advice, and assistance on all aspects of the conference. We do hope that this event will encourage collaboration among us now and in the future.

We wish you all find the opportunity to get rewarding technical programs, intellectual inspiration, and extended networking.

Pekanbaru, 27th August 2019
Dr. Arbi Haza Nasution, M.IT
Chair of ICoSET 2019

CONTENTS

PAPERS

FULL PAPERS

Design of Community-based Ecotourism at Cengkehan and Giriloyo, Wukirsari Village, Imogiri District, Bantul Regency, Special Region of Yogyakarta <i>Suhartono, Sri Mulyaningsih, Desi Kiswiranti, Sukirman, Nurwidi A. A. T. Heriyadi, Muchlis and Iva Mindhayani</i>	5
Prototype Storage Locker Security System based on Fingerprint and RFID Technology <i>Apri Siswanto, Hendra Gunawan and Rafiq Sanjaya</i>	11
Feasibility Study of CO ₂ Flooding under Gross-split Mechanism: Simulation Approach <i>Muslim Abdurrahman, Wisup Bae, Adi Novriansyah, Dadan Damayandri and Bop Duana Afrireksa</i>	15
Online Classroom Attendance System based on Cloud Computing <i>Sri Listia Rosa and Evizal Abdul Kadir</i>	20
Analysis of Porosity and Permeability on Channel Deposit Sandstone using Pore-gas Injection and Point Counting in Sarilamak Area, West Sumatra <i>Bayu Defitra, Tiggi Choanji and Yuniarti Yuskar</i>	26
A Simulation Study of Downhole Water Sink Guidelines Plot Application using Real Field Data <i>Praditya Nugraha</i>	31
Groundwater Exploration using 2D Electrical Resistivity Imaging (ERI) at Kulim, Kedah, Malaysia <i>Adi Suryadi, Muhammad Habibi, Batara, Dewandra Bagus Eka Putra and Husnul Kausarian</i>	35
Risk Identification in Management System Process Integration Which Have Impact on the Goal of Management System Components <i>Nastasia Ester Siahaan, Leni Sagita and Yusuf Latief</i>	41
The Performance of 3D Multi-slice Branched Surface Reconstruction on CPU-GPU Platform <i>Normi Abdul Hadi and Norma Alias</i>	49
Tile-based Game Plugin for Unity Engine <i>Salhazan Nasution, Arbi Haza Nasution and Arif Lukman Hakim</i>	55
Image Segmentation of Nucleus Breast Cancer using Digital Image Processing <i>Ana Yulianti, Ause Labellapansa, Evizal Abdul Kadir, Mohana Sundaram and Mahmud Othman</i>	64
An Integrated Framework for Social Contribution of Diabetes Self-care Management Application <i>Zul Indra, Liza Trisnawati and Luluk Elvitaria</i>	68
Spatiotemporal Analysis of Urban Land Cover: Case Study - Pekanbaru City, Indonesia <i>Idham Nugraha, Faizan Dalilla, Mira Hafizhah Tanjung, Rizky Ardiansyah and M. Iqbal Hisyam</i>	74
The Effectiveness of Rice Husk Biochar Application to Metsulfuron Methyl Persistence <i>Subhan Arridho, Saripah Ulpah and Tengku Edy Sabli</i>	80
Digital Forensics: Acquisition and Analysis on CCTV Digital Evidence using Static Forensic Method based on ISO /IEC 27037:2014 <i>Rizdqi Akbar Ramadhan, Desti Mualfah and Dedy Hariyadi</i>	85

Testing the Role of Fish Consumption Intention as Mediator <i>Junaidi, Desi Ilona, Zaitul and Harfiandri Damanhuri</i>	90
Segmentation of Palm Oil Leaf Disease using Zoning Feature Extraction <i>Ause Labellapansa, Ana Yulianti and Agus Yuliani</i>	98
Analysis of Economy in the Improvement of Oil Production using Hydraulic Pumping Unit in X Field <i>Muhammad Ariyon, Novia Rita and Tribowo Setiawan</i>	102
Construction Design and Performance of Dry Leaf Shredder with Vertical Rotation for Compost Fertilizer <i>Syawaldi</i>	109
The Impact of Additively Coal Fly Ash toward Compressive Strength and Shear Bond Strength in Drilling Cement G Class <i>Novrianti, Dori Winaldi and Muhammad Ridho Efras</i>	114
Impact of Vibration of Piling Hammer on Soil Deformation: Study Case in Highway Construction Section 5 Pekanbaru-Dumai <i>Firman Syarif, Husnul Kausarian and Dewandra Bagus Eka Putra</i>	120
Combination Playfair Cipher Algorithm and LSB Steganography for Data Text Protection <i>Apri Siswanto, Sri Wahyuni and Yudhi Arta</i>	125
Fire Detection System in Peatland Area using LoRa WAN Communication <i>Evizal Abdul Kadir, Hitoshi Irie and Sri Listia Rosa</i>	130
Forest Fire Monitoring System using WSNs Technology <i>Evizal Abdul Kadir, Sri Listia Rosa and Mahmud Othman</i>	135
Multi Parameter of WSNs Sensor Node for River Water Pollution Monitoring System (Siak River, Riau-Indonesia) <i>Evizal Abdul Kadir, Abdul Syukur, Bahruddin Saad and Sri Listia Rosa</i>	140
Analysis for Gerund Entity Anomalies in Data Modeling <i>Des Suryani, Yudhi Arta and Erdisna</i>	146
The Incidence of Rhinoceros Beetle Outbreak in Public Coconut Plantation in Tanjung Simpang Village, Indragiri Hilir, Riau Province <i>Saripah Ulpah, Nana Sutrisna, Fahroji, Suhendri Saputra and Sri Swastika</i>	151
Mobile Application of Religious Activities for the Great Mosque Islamic Center Rokan Hulu with Push Notification <i>Salhazan Nasution, Arbi Haza Nasution and Fitra Yamita</i>	155
An Augmented Reality Machine Translation Agent <i>Arbi Haza Nasution, Yoze Rizki, Salhazan Nasution and Rafi Muhammad</i>	163
The Community Perception of Traditional Market Services in Pekanbaru City, Riau Province <i>Puji Astuti, Syaifullah Rosadi, Febby Asteriani, Eka Surya Pratiwi and Thalia Amanda Putri</i>	169
Separation of Crude Oil and Its Derivatives Spilled in Seawater by using Cobalt Ferrite Oxide <i>Mohammed A, Samba, Ibrahim Ali Amar, Musa Abuadabba, Mohammed A. Alfroji, Zainab M. Salih and Tomi Erfando</i>	175

Study of Open Space Utilization in Pekanbaru City, Riau Province <i>Mira Hafizhah T., Febby Asteriani, Mardianto and Angelina Rulan S.</i>	182
Application of Augmented Reality as a Multimedia Learning Media: Case Study of Videography <i>Ahmad Zamsuri, Fadli Suandi and Rizki Novendra</i>	188
Green Building Performance Analysis in the Stimi Campus Building <i>Dian Febrianti and Samsunan</i>	194
Towing Service Ordering System based on Android: Study Case - Department of Transportation, Pekanbaru <i>Panji Rachmat Setiawan, Yudhi Arta and Rendi Sutisna</i>	200
Biosurvey of Mercury (Hg), Cadmium (Cd), and Lead (Pb) Contamination in Reclamation Island-Jakarta Bay <i>Salmi Salma, Achmad Sjarmidi and Salman</i>	205
Expert System to Detect Early Depression in Adolescents using DASS 42 <i>Nesi Syafitri, Yudhi Arta, Apri Siswanto and Sonya Parlina Rizki</i>	211
Geotechnics Analysis: Soil Hardness on Stability of Davit Kecil's Weir in Ulu Maras, Kepulauan Anambas, Kepulauan Riau <i>Miftahul Jannah, Dewandra Bagus Eka Putra, Firman Syarif, Joni Triparadi, Nopiyanto and Husnul Kausarian</i>	219
Support for Heritage Tourism Development: The Case of Ombilin Coal Mining Heritage of Sawahlunto, Indonesia <i>Jonny Wongso, Desi Ilona, Zaitul and Bahrul Anif</i>	229
Aerial Photogrammetry and Object-based Image Analysis for Bridge Mapping: A Case Study on Bintan Bridge, Riau Islands, Indonesia <i>Husnul Kausarian, Muhammad Zainuddin Lubis, Primawati, Dewandra Bagus Eka Putra, Adi Suryadi and Batara</i>	237
Monitoring Single Site Verification (SSV) System and Optimization BTS Network based on Android <i>Abdul Syukur, Siti Rahmadhani Sabri and Yudhi Arta</i>	243
Characterization of the Ethnobotany of Riau Province Mascot Flora (<i>Oncosperma tigillarum</i> (Jack) Ridl.) <i>Desti, Fitmawati, Putri Ade Rahma Yulis and Mayta Novaliza Isda</i>	250
Effect Stocking Density on Growth and Survival rate of Larval Selais Fish (<i>Kryptopterus lois</i>) Cultured in Recirculation System <i>Agusnimar Muchtar and Rosyadi</i>	254
Development of Safety Plan to Improve OHS (Occupational Health and Safety) Performance for Construction of Dam Supporting Infrastructure based on WBS (Work Breakdown Structure) <i>Aprilia Dhiya Ulhaq, Yusuf Latief and Rossy Army Machfudiyanto</i>	258
Design of Web Login Security System using ElGamal Cryptography <i>Yudhi Arta, Hendra Pratama, Apri Siswanto, Abdul Syukur and Panji Rachmat Setiawan</i>	268
Standard Operational Procedures Development for Government Building's Care and Maintenance Work of Outer Spatial and Housekeeping Component to Improve Work Effectiveness and Efficiency using Risk-based Approach <i>Lasita Khaerani, Yusuf Latief and Rossy Army Machfudiyanto</i>	274

A Novel Correlation on MMP Prediction in CO ₂ -LPG Injection System: A Case Study of Field X in Indonesia <i>Prasandi Abdul Aziz, Hendra Dwimax, Tutuka Ariadji, Steven Chandra, Wijoyo Niti Daton and Ressi Bonti</i>	285
Productivity Analysis of Frac-pack Completion in M Well with Sand Problem Indication and High Permeability Formation <i>Herianto, Prasandi Abdul Aziz, Wijoyo Niti Daton and Steven Chandra</i>	291
Emulsion Treatment using Local Demulsifier from Palm Oil <i>Tomri Erfando and Emre Fathan</i>	299
Designing an IoT Framework for High Valued Crops Farming <i>Domingo Junior P. Ngipol and Thelma D. Palaoag</i>	304
Consideration of the Different Pile Length Due to Soil Stress and Inner Forces of the Nailed-slab Pavement System under Concentric Load <i>Anas Puri, Roza Mildawati and Muhammad Solihin</i>	311
Utilization of Agricultural Waste to Be Bioethanol Sources as a Solvent on Paraffin Wax Crude Oil Issues <i>M. K. Afdhol, F. Hidayat, M. Abdurrahman, H. Z. Lubis, R. K. Wijaya and N. P. Sari</i>	315
The Effect of Regeneration Time of Biomass Activated Carbon using Low Temperature to Reduce Filtration Loss in Water-based Drilling Fluid <i>Nur Hadziqoh, Mursyidah, Arif Rahmadani, Idham Khalid and Hasnah Binti Mohd Zaid</i>	322
Improving the Accuracy of Features Weighted k-Nearest Neighbor using Distance Weight <i>K. U. Syaliman, Ause Labellapansa and Ana Yulianti</i>	326
Predicting of Oil Water Contact Level using Material Balance Modeling of a Multi-tank Reservoir <i>Muslim Abdurrahman, Bop Duana Afrireksa, Hyundon Shin and Adi Novriansyah</i>	331
Chip Formation and Shear Plane Angle Analysis on Carbon Steel Drilling using Solid Carbide Tools <i>Rieza Zulrian Aldio</i>	337
A Solution to Increase Natuna D Alpha's Resource Utilization by Cryogenic Distillation: Conceptual Design & Sensitivity Study <i>Wijoyo Niti Daton, Ezra Revolin, Siptian Nugrahawan, Prasandi Abdul Aziz, Tutuka Ariadji, Steven Chandra and J. A. Nainggolan</i>	342
Design of Volcanic Educational-based Natural Tourism at Giriloyo, Wukirsari Village, Imogiri District, Bantul Regency, Yogyakarta-Indonesia <i>Sri Mulyaningsih</i>	349
Four Types of Moral Holistic Values for Revolutionizing the Big Data Analytics in IoT-based Applications <i>Norma Alias</i>	357
AUTHOR INDEX	363

Design of Web Login Security System using ElGamal Cryptography

Yudhi Arta, Hendra Pratama, Apri Siswanto, Abdul Syukur and Panji Rachmat Setiawan

Department of Informatics Engineering, Universitas Islam Riau, Pekanbaru, Indonesia
{yudhiarta,aprisiswanto, abdulsyukur,panji.r.setiawan}@eng.uir.ac.id, hpratama1992@gmail.com

Keywords: Web Login, ElGamal, Cryptography.

Abstract: The login system is a process for accessing a computer by entering the identity of the user and the password to obtain permissions using the destination computer resources. In an information system security issues and maintaining data confidentiality is one important aspect. However, these security issues often get less attention from the owners and managers of information systems. If talking about security issues related to the use of computers, it is difficult to separate it with the login process. Login aims to provide security services on the system. In this research used ElGamal cryptography algorithm to secure username and password in web login. The security level of this algorithm is based on the problem of discrete logarithms in the multiplication group of prime modulo primes. This algorithm includes asymmetric cryptography algorithms that use two key types, namely public key and secret key. The data contained in the login is secured by using ElGamal algorithm, so the username and password entered into the database are already in the form of ciphertext.

1 INTRODUCTION

The login system is the process of accessing a computer by entering the identity of the user and password to get access rights using the destination computer resources. When logging in to enter the system, the user will be asked to enter a user identity such as user id and password in anticipation of system security. Passwords can be changed according to needs while user id is never changed because it is a unique identity that refers to a particular user.

Information system on security issues and maintaining data confidentiality is one important aspect. But this security problem often gets less attention from the owners and managers of information systems (Arta et al., 2018). Security issues are second or even last in the list of things that are considered important (Arta, 2017; Novendra et al., 2018).

Internet users, usually using internet facilities to carry out the process of changing information. Data security is very important. The need for information makes website developers present a variety of services for users (Dharmawan et al., 2013). But most of the website developers ignore system security on the website. The most widely used attack by these attackers is the SQL Injection attack. This study focused on securing the system using the Rijndael algorithm to encrypt data (Minier, 2017). The Rijndael algorithm was chosen as a cryptographic algorithm that

can protect information well and efficiently in its implementation and was named the Advanced Encryption Standard (Daemen and Rijmen, 1998; Daemen and Rijmen, 2013). This algorithm will be embedded in the system login to protect unauthorized access from the attacker (Dawood and Hammadi, 2017; Sajadieh et al., 2017). The results of using the Rijndael algorithm can protect the login system properly so that the system is declared safe from the attackers (Kuo and Verbauwhede, 2001).

Computer network security is part of a system that is very important to maintain data validity and integrity and ensure availability of services for its users (Arta et al., 2016). The current network intruder detection system is generally able to detect various attacks but is unable to take further action. But on the one hand, humans are very dependent on information systems. This has caused the statistics of network security incidents to continue to increase sharply from year to year (Namjoshi and Narlikar, 2014; Waisman et al., 2007). This is due to the people's lack of concern for network security systems. We need a system that can help network administrators to be used as a network traffic monitor with Intrusion Prevention System (IPS) which is a combination of blocking capabilities from Firewall (Giokas, 2016).

2 ElGamal ENCRYPTION

The process of key formation is the process of determining a number which will then be used as a key in the process of encryption and decryption of messages (Hashim, 2014). The key for encryption is generated from the p value, g , y while the decryption key consists of the value x , p (Makkaoui et al., 2016). Each value has requirements that must be met. Rare in making keys are as follows:

- Primes p , with p values > 255 .
- Select a random number g with the condition $g < p$.
- Select a random number x with the condition $1 < x < p-2$.
- Calculate $y = g^x \text{ mod } p$.

The public key is y , g , p while the private key is x . The value of y , g , and p is not save secret while the value of x must be kept secret because it is a private key to describe plaintext (Kiltz and Pietrzak, 2010; Tsiounis and Yung, 1998; Weinberger et al., 2006).

3 RESULT AND DISCUSSION

3.1 Username Encryption Process with ElGamal Algorithm

In this section a comparison will be made between the ElGamal login username and the standard login on the web login system using ElGamal cryptography, the results of the comparison can be seen in table 1.

The process in table 1 above, is the result of the encryption process using the ElGamal method. Below this is the process of an ElGamal method at work.

- If the testing system uses a username: 23081990, Number of characters: 59, Uppercase: 0, Small letters: 0, Numbers: 8, special character: 0, Other: 15, Results: 8.81.
- If the testing system uses username: abcd1234, Number of characters: 58, Uppercase: 0, Small letters: 4, Numbers: 8 special character: 0, Other: 15, Result: 4,058.
- If the testing system uses username: AbCd1234, Number of characters: 56, Upper-case: 2, Small letters: 2, Numbers: 4, special character: 0, Other: 15, Result: 4,058.
- If the test system uses a username: Ac54\$h, Number of characters: 50, Uppercase: 1, Small letter: 2, Numbers: 2, Special character: 2, Other: 13, Result: 23,941.

- If the testing system uses a username: 6\$ Ab788, Number of characters: 50, Uppercase: 1, Small letter: 1, Number: 3, Special character: 1, Other: 13, Result: 19.981.
- If the test system uses username: aaD#6754, Number of characters: 57, Uppercase: 1, Small letter: 2, Number: 4, special character: 1, Other: 15, Result: 4,995.
- If the testing system uses username: &*\$# 9764, Number of characters: 59, Uppercase: 0, Small letters: 0, Number: 4, Special character: 4, Other: 15, Result: 9,313.

The process in table 2 above, is the result of the encryption process using the standart character. Below this is the process of standard login process testing

- If the test system uses a username: 23081990, Number of characters: 8, Large letters: 0, Lower case letters: 0, Numbers: 8, character specials: 0, Other: 0 Result: 0.
- If the testing system uses username: abcd1234, Number of characters: 8, Large letters: 0, Lowercase letters: 4, Numbers: 8, Special characters: 0, Other: 0, Results: 0.13.
- If the testing system uses username: AbCd1234, Number of characters: 8, Large letters: 2, Lowercase letters: 2, Numbers: 4, Special characters: 0, Other: 0, Results: 0.13.
- If the testing system uses a username: Ac54\$h, Number of characters: 7, Large letters: 1, Lowercase: 2, numbers: 2, special character: 2, Other: 0, Results: 0.5.
- If the testing system uses a username: 6\$Ab788, Number of characters: 7, Large letters: 1, Lowercase: 1, Number: 3, Special characters: 1, Other: 0, Result: 0.2.
- If the testing system uses username: aaD#6754, Number of characters: 8, Large letters: 1, Lowercase: 2, Number: 4, Special character: 1, Other: 0, Results: 0.16.
- If the testing system uses username: &*\$# 9764, Number of characters: 8, Large letters: 0, Lower case letters: 0, Numbers: 4, special character: 4, Other: 0, Results: 0.31.

In table 1 and 2 above can be seen the comparison between the ElGamal login username and the standart login that has been done. Then the comparison results will be accumulated into a graph and can be seen in figure 1.

In Figure 1, the average time of the encryption and decryption results of each username gets an ElGamal

Table 1: Username for ElGamal Login Testing.

ElGamal								
Exam	Username	Char Encryp	char(U)	Char(L)	Number	Special(A)	Other	Result
1	23081990	59	0	0	8	0	15	8.81
2	abcd1234	58		4	4	0	15	4.05
3	AbCd1234	56	2	2	4	0	15	4.05
4	Ac54\$h	50	2	1	2	2	13	23.9
5	6\$Ab788	50	1	2	3	1	13	19.9
6	aaD#6754	57	1	2	4	1	15	4.99
7	&*\$#9764	59	0	0	4	4	15	9.31

Table 2: Username for Standard Login Testing.

Standard								
Exam	Username	Char Encryp	char(U)	Char(L)	Number	Special(A)	Other	Result
1	23081990	8		0	8		0	0
2	abcd1234	8		4	4		0	0.13
3	AbCd1234	8	2	2	4		0	0.13
4	Ac54\$h	7	2	1	2	2	0	0.5
5	6\$Ab788	7	1	2	3	1	0	0.2
6	aaD#6754	8	1	2	4	1	0	0.16
7	&*\$#9764	8	0	0	4	4	0	0.31

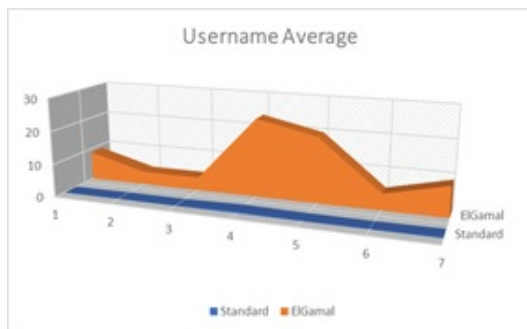


Figure 1: Username Average (Second).

value: 27, 87 and standard: 0.2. Processing requires a longer span of time than the standard username because each process from ElGamal requires the insertion of a value before entering the username.

3.2 Password Encryption Process With ElGamal Algorithm

In this section a comparison will be made between the ElGamal login password and the standard login on the web login system using ElGamal cryptography, the results of the comparison can be seen in table 3.

When a password is given a character using standard letters, the time required does not take a long process of about 13 seconds. For ElGamal use using ASCII numbers, it will take quite a long time. The combination of standard letters and also ASCII numbers is a safe step.

Password ElGamal Process Testing

- If the testing system uses a username: kauy984, number of characters: 51, uppercase: 3, lowercase: 1, number: 3, special characters: 0, other: 13, Result: 16,235.
- If the test system uses username: abdx*&#, number of characters: 53, uppercase: 2, lowercase: 2, numbers: 0, special characters: 3, other: 13, Results: 53.99.
- If the testing system uses username: abcd1234, number of characters: 56, uppercase: 2, lowercase: 2, numbers: 4, character specials: 0, other: 15, Results: 4,058.
- If the testing system uses a username: 65*&%k, number of characters: 53, uppercase: 0, lowercase: 1, number: 2, special characters :4, other: 13, Results: 63,941.
- If the test system uses username: 6\$ab788, number of characters: 50, uppercase: 1, lowercase: 1, number: 3, special characters: 1, other: 13, results: 19.981.
- If the test system uses username: aad#6754, number of characters: 57, uppercase: 1, lowercase :2, number: 4, special characters: 1, other: 15, Results: 4.995.
- If the test system uses username: &*\$# 9764, number of characters: 59, uppercase: 0, lowercase: 0, number: 4, special characters: 4, other: 15, Results: 9,313.

Table 3: Password for ElGamal Login Testing.

ElGamal								
Exam	Password	Char Encryp	char(U)	Char(L)	Number	Special(A)	Other	Result
1	kAUY984	51	3	1	3		13	16.2
2	abDX* & #	53	2	2	0	3	15	53.9
3	AbCd1234	56	2	2	4		15	4.05
4	65* & ^ % k	53	0	1	2	4	13	63.9
5	6\$Ab788	50	1	2	3	1	13	19.9
6	aaD#6754	57	1	2	4	1	15	4.99
7	& * \$ # 9764	59	0	0	4	4	15	9.31

The results from table 4 that use standard numbers, are not much different from previous experiments. And for the average results of the above test is 0.23 seconds.

Standart Password Process Testing

- If the test system uses username: kauy984, number of characters: 7, uppercase letters: 4, lowercase letters: 0, numbers: 3, character specials: 0, other: 0, Results: 0.01.
- If the testing system uses username: abdx* & #, number of characters: 7, uppercase: 2, lowercase: 2, numbers: 0, special characters: 3, other: 0, Results: 0.44.
- If the test system uses username: abcd1234, number of characters: 8, uppercase: 2, lowercase: 2, numbers: 4, special characters: 0, other: 0, Results: 0.13.
- If the test system uses a username: 65* & ^ % k, number of characters: 7, uppercase: 0, lowercase: 1, number: 2, special characters: 4, other: 0, results: 0.4.
- If the testing system uses a username: 6\$ ab788, number of characters: 8, uppercase: 1, lowercase: 1, number: 3, special characters: 1, other: 0, Result: 0.2.
- If the test system uses username: aad#6754, number of characters: 8, uppercase: 1, lowercase: 2, number: 4, special characters: 1, other: 0, Result: 0.16.
- If the test system uses username: & * \$ # 9764, number of characters: 8, uppercase letters: 0, lowercase letters: 0, numbers: 4, character specials: 4, other: 0, Results: 0.31.

In table 2 above can be seen the comparison between the ElGamal login username and the standard login that has been done. Then the comparison results will be accumulated into a graph and can be seen in figure 2.

In Figure 2, it can be seen that the process of inserting a value into a password takes time. This value

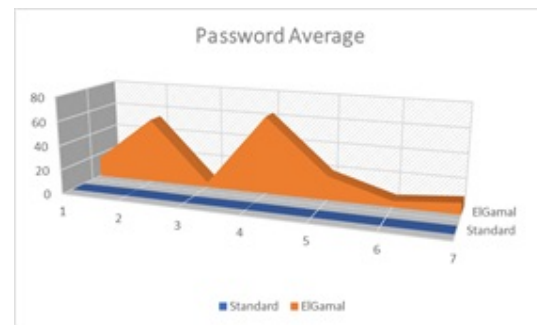


Figure 2: Password Average (Second).

is used for comparison when a password is to be tested if it is security, it will take a longer time than just using a password that does not use ElGamal. This is a subjective assessment for a password security trial. for the average process of a password using the ElGamal method and ASCII numbers, it takes 24.64 seconds.

The following is the comparative result of calculations based on ElGamal and Standard login. To increase the security of the username and password on the ElGamal encryption login, it should be added to the length of the character, because the more the length of characters, the more difficult the hackers intend to break into ElGamal encryption login system. The graph of these methods are shown in figure 3.

4 CONCLUSIONS

From the comparison test results above, it can be concluded that the level of security and average hourly for comparison testing Elgamal login username: 10.73 and for testing the comparison of standard login username: 0.20. Then for testing the comparison of Elgamal login passwords: 24.64 and for testing the comparison of standard login passwords: 0.23.

Table 4: Password for Standart Login Testing.

Standard								
Exam	Password	Char Encryp	char(U)	Char(L)	Number	Special(A)	Other	Result
1	kAUY984	7	3	1	3		0	0.01
2	abDX* & #	7	2	2	0	3	0	0.44
3	AbCd1234	8	2	2	4		0	0.13
4	65* & ^ % k	7	0	1	2	4	0	0.4
5	6\$Ab788	7	1	2	3	1	0	0.2
6	aaD#6754	8	1	2	4	1	0	0.16
7	& * \$ # 9764	8	0	0	4	4	0	0.31

Table 5: Comparison of Username Password.

USERNAME	EIGamal	Standard	PASSWORD	EIGamal	Standard
23081990	8.81	0	kAUY984	16.235	0.01
abcd1234	4.058	0.13	abDX* & #	531.99	0.44
AbCd1234	4.058	0.13	AbCd1234	4.058	0.13
Ac54\$h	63.941	0.5	65* & ^ % k	63.941	0.4
6\$Ab788	19.981	0.2	6\$Ab788	19.981	0.2
aaD#6754	4.995	0.16	aaD#6754	4.995	0.16
& * \$ # 9764	9.313	0.31	& * \$ # 9764	9.313	0.31
Average	10.73	0.20	Average	24.64	0.23

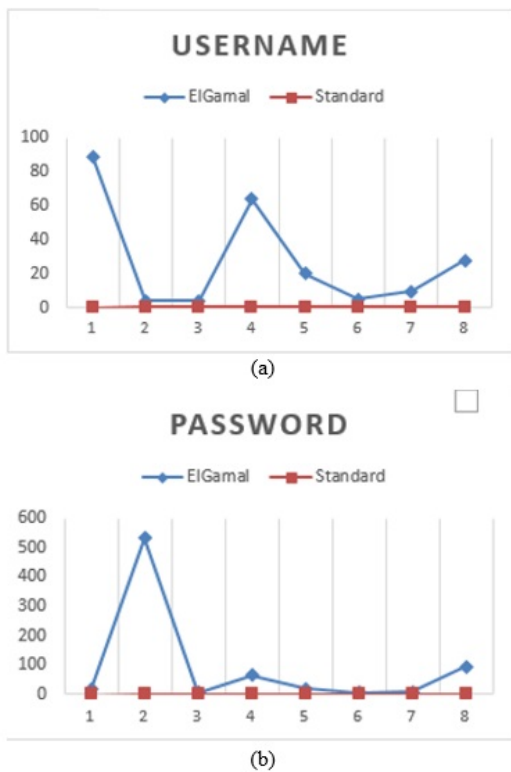


Figure 3: Graph Comparison ElGamal And Standard Login (a) Top and (b) bottom views.

ACKNOWLEDGEMENTS

We would like to express our gratitude to the Universitas Islam Riau for the fund this project.

REFERENCES

Arta, Y. (2017). Implementasi intrusion detection system pada rule based system menggunakan sniffer mode pada jaringan lokal. *IT Journal Research and Development*, 2(1):43–50.

Arta, Y., Kadir, E. A., and Suryani, D. (2016). Knopix: Parallel computer design and results comparison speed analysis used amdahl theory. In *2016 4th International Conference on Information and Communication Technology (ICoICT)*, pages 1–5. IEEE.

Arta, Y., Syukur, A., and Kharisma, R. (2018). Simulasi implementasi intrusion prevention system (ips) pada router mikrotik. *IT JOURNAL RESEARCH AND DEVELOPMENT*, 3(1):104–114.

Daemen, J. and Rijmen, V. (1998). The block cipher Rijndael. In *International Conference on Smart Card Research and Advanced Applications*, pages 277–284.

Daemen, J. and Rijmen, V. (2013). *The design of Rijndael: AES-the advanced encryption standard*. Springer Science & Business Media.

Dawood, O. A. and Hammadi, O. I. (2017). An analytical study for some drawbacks and weakness points of the AES cipher (rijndael algorithm). In *The 1st International Conference on Information Technology (ICoIT17)*, page 126.

- Dharmawan, E. A., Yudaningtyas, E., and Sarosa, M. (2013). Perlindungan Web pada Login Sistem Menggunakan Algoritma Rijndael. *Jurnal EECCIS*, 7(1):77–84.
- Giokas, I. (2016). *April 19*). Systems and methods for self-tuning network intrusion detection and prevention.
- Kiltz, E. and Pietrzak, K. (2010). Leakage resilient elgamal encryption. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 595–612.
- Kuo, H. and Verbauwhede, I. (2001). *Architectural optimization for a 1*. 82 Gbits/sec VLSI implementation of the AES Rijndael algorithm.
- Makkaoui, E., K., B.-H., A., and Ezzati, A. (2016). Cloud-ElGamal: An efficient homomorphic encryption scheme. In *2016 International Conference on Wireless Networks and Mobile Communications (WINCOM)*, pages 63–66.
- Minier, M. (2017). Improving impossible-differential attacks against Rijndael-160 and Rijndael-224. *Designs, Codes and Cryptography*, pages 117–129.
- Namjoshi, K. S. and Narlikar, G. J. (2014). *March 25*). Method and apparatus for pattern matching for intrusion detection/prevention systems.
- Novendra, Y., Arta, Y., and Siswanto, A. (2018). Analisis perbandingan kinerja routing ospf dan eigrp. *IT JOURNAL RESEARCH AND DEVELOPMENT*, 2(2):97–106.
- Sajadieh, M., Mirzaei, A., Mala, H., and Rijmen, V. (2017). A new counting method to bound the number of active S-boxes in Rijndael and 3D. *Designs, Codes and Cryptography*, 83(2):327–343.
- Tsiounis, Y. and Yung, M. (1998). On the security of ElGamal based encryption. In *International Workshop on Public Key Cryptography*, pages 117–134.
- Waisman, N., Paterno, H. A., Mata, C. L., and Tamaroff, A. R. (2007). *May 29*). Methods and apparatus for computer network security using intrusion detection and prevention.
- Weinberger, K. Q., Blitzer, J., and Saul, L. K. (2006). Distance metric learning for large margin nearest neighbor classification. In *Advances in neural information processing systems*, pages 1473–1480.