BUKTI KORESPONDENSI
ARTIKEL JURNAL INTERNASIONAL BEREPUTASI

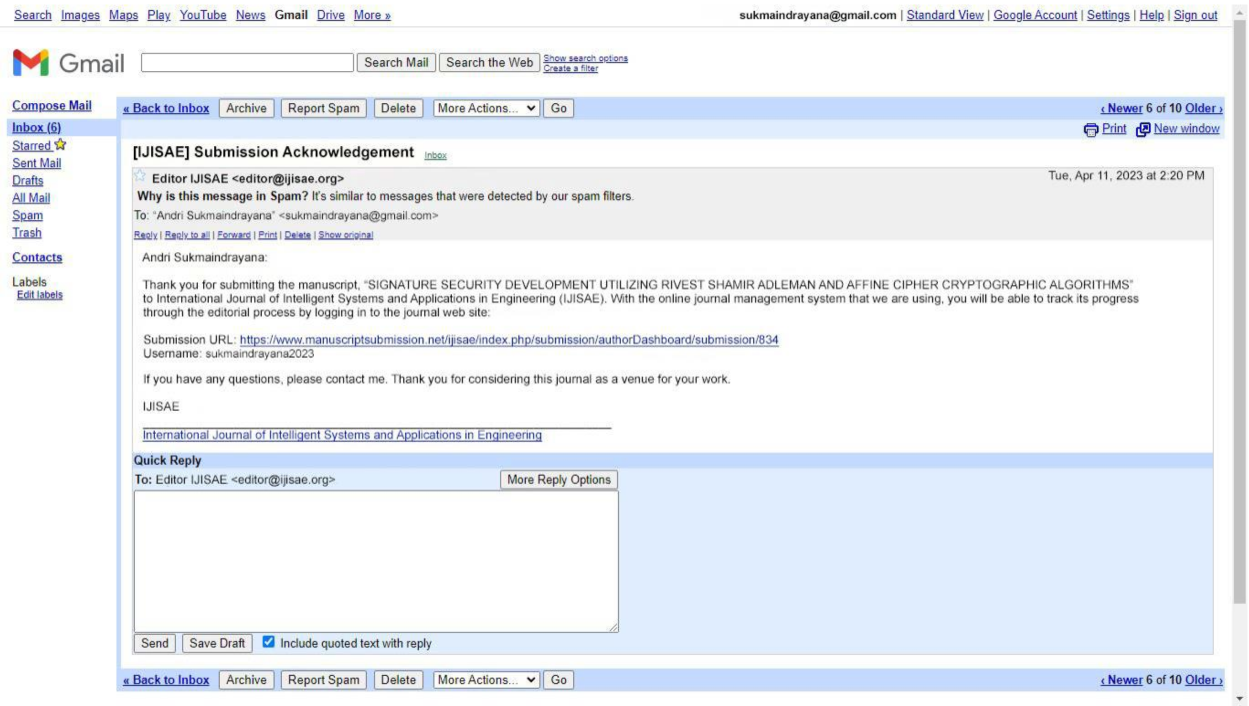
Judul Artikel : SIGNATURE SECURITY DEVELOPMENT UTILIZING RIVEST SHAMIR ADLEMAN AND AFFINE CIPHER CRYPTOGRAPHIC ALGORITHMS

Jurnal : International Journal of Intelligent Systems and Applications in Engineering (IJISAE)

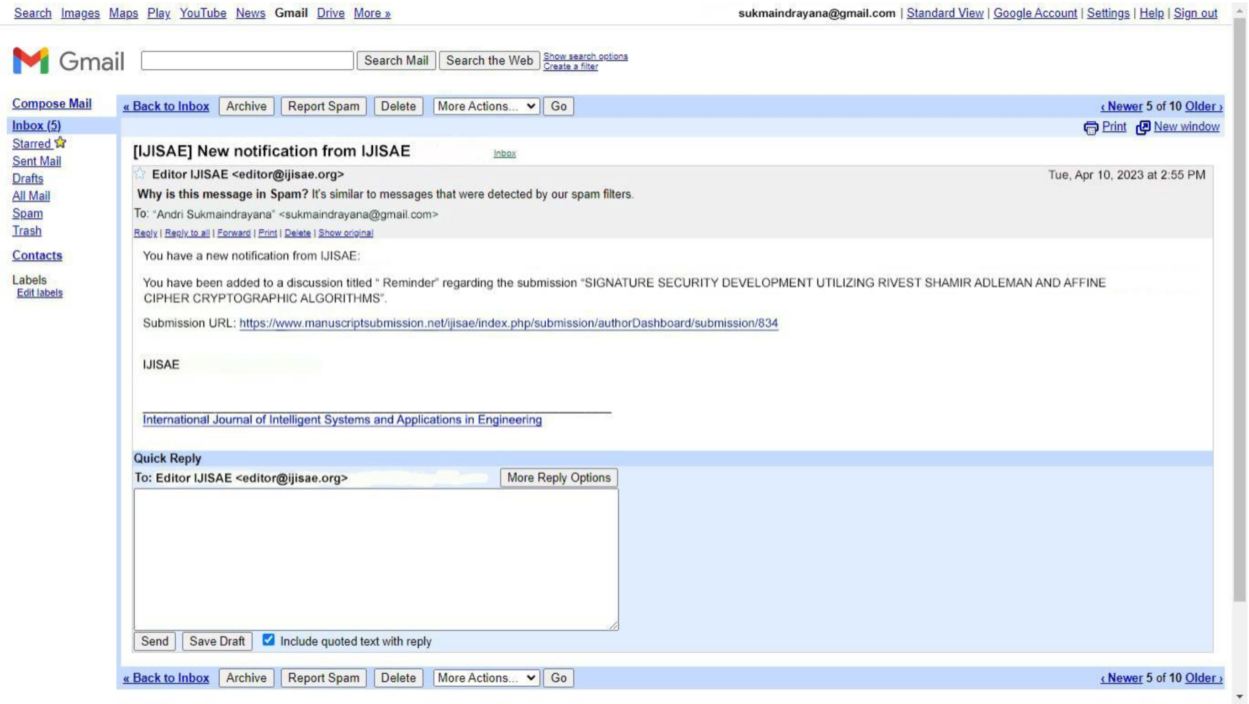
Penulisa : Andri Sukmaindrayana, Aneu Yulianeu

No	Perihal	Tanggal
1	Bukti konfirmasi submit artikel	11 April 2023, 2:20 PM
2	Bukti konfirmasi artikel yang di submit	11 April 2023, 2:55 PM
3	Bukti konfirmasi submit revisi pertama, respon kepada reviewer, dan artikel yang diresubmit	2 Mei 2023, 3:10 PM
4	Bukti konfirmasi review dan hasil review kedua	19 Juni 2023, 2:29 PM
5	Bukti konfirmasi artikel accepted	20 Juni 2023, 11:44 AM
6	Bukti pembayaran jurnal	20 Juni 2023
7	Bukti jurnal sudah berada di bagian produksi	20 Juni 2023, 4:49 PM
8	Bukti publish	22 Juni 2023

1. BUKTI KONFIRMASI SUBMIT ARTIKEL
(11 April 2023, 2:20 PM)



2. BUKTI KONFIRMASI ARTIKEL YANG DISUBMIT (11 April 2023, 2:55 PM)



Search Images Maps Play YouTube News Gmail Drive More »
sukmaindrayana@gmail.com | Standard View | Google Account | Settings | Help | Sign out

Gmail
Search Mail | Search the Web | Show search options | Create a filter

Compose Mail
Inbox (5)
Starred
Sent Mail
Drafts
All Mail
Spam
Trash
Contacts
Labels
Edit labels

« Back to Inbox | Archive | Report Spam | Delete | More Actions... | Go
‹ Newer 5 of 10 Older ›
Print | New window

[IJISAE] New notification from IJISAE
Inbox

Editor IJISAE <editor@ijisae.org>
Tue, Apr 10, 2023 at 2:55 PM

Why is this message in Spam? It's similar to messages that were detected by our spam filters.

To: "Andri Sukmaindrayana" <sukmaindrayana@gmail.com>

Reply | Reply to all | Forward | Print | Delete | Show original

You have a new notification from IJISAE:

You have been added to a discussion titled " Reminder" regarding the submission "SIGNATURE SECURITY DEVELOPMENT UTILIZING RIVEST SHAMIR ADLEMAN AND AFFINE CIPHER CRYPTOGRAPHIC ALGORITHMS".

Submission URL: https://www.manuscriptsubmission.net/ijisae/index.php/submission/authorDashboard/submission/834

IJISAE

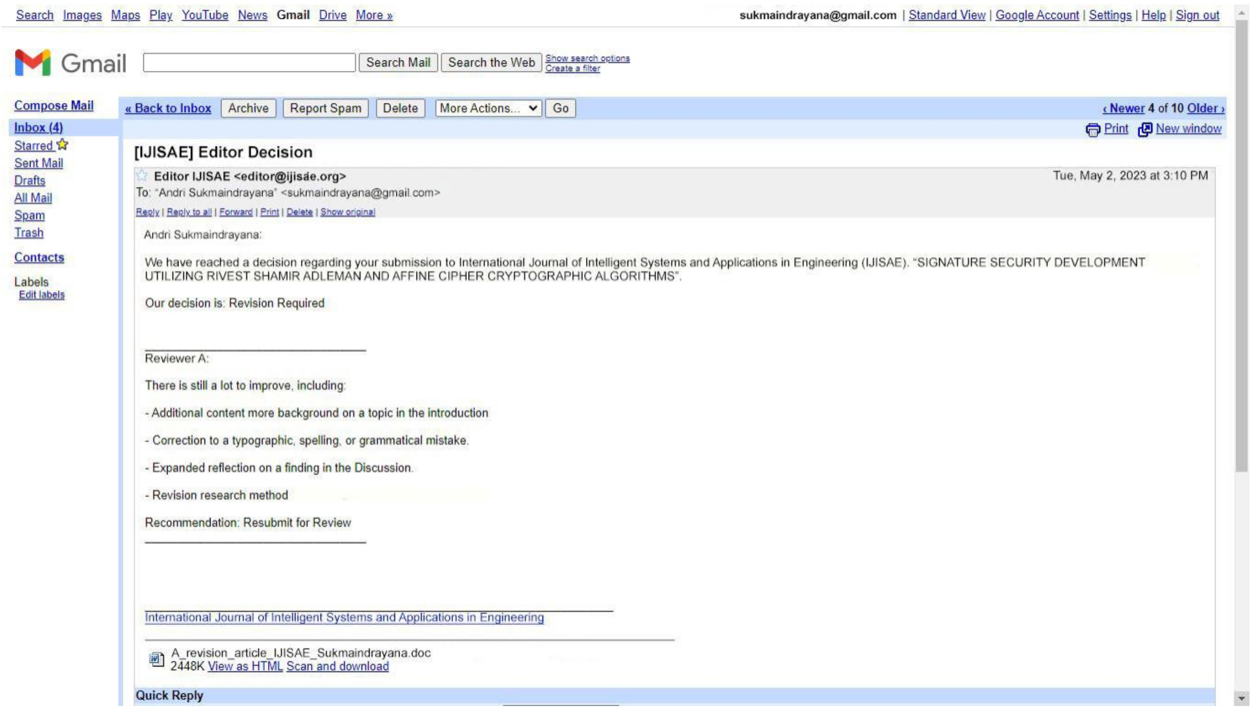
International Journal of Intelligent Systems and Applications in Engineering

Quick Reply
To: Editor IJISAE <editor@ijisae.org>
More Reply Options

Send | Save Draft | Include quoted text with reply

« Back to Inbox | Archive | Report Spam | Delete | More Actions... | Go
‹ Newer 5 of 10 Older ›

3. BUKTI KONFIRMASI SUBMIT REVISI PERTAMA, RESPON KEPADA REVIEWER, DAN ARTIKEL YANG DIRESUBMIT
(2 Mei 2023, 3:10 PM)



Search Images Maps Play YouTube News Gmail Drive More »   sukmaindrayana@gmail.com | Standard View | Google Account | Settings | Help | Sign out

Gmail   Search Mail   Search the Web   Show search options   Create a filter

Compose Mail
Inbox (4)
Starred
Sent Mail
Drafts
All Mail
Spam
Trash
Contacts
Labels
Edit labels

« Back to Inbox   Archive   Report Spam   Delete   More Actions...   Go   ‹ Newer 4 of 10 Older ›

Print   New window

[IJISAE] Editor Decision

Editor IJISAE <editor@ijisae.org>   Tue, May 2, 2023 at 3:10 PM

To: "Andri Sukmaindrayana" <sukmaindrayana@gmail.com>

Reply | Reply to all | Forward | Print | Delete | Show original

Andri Sukmaindrayana:

We have reached a decision regarding your submission to International Journal of Intelligent Systems and Applications in Engineering (IJISAE), "SIGNATURE SECURITY DEVELOPMENT UTILIZING RIVEST SHAMIR ADLEMAN AND AFFINE CIPHER CRYPTOGRAPHIC ALGORITHMS".

Our decision is: Revision Required

Reviewer A:

There is still a lot to improve, including:

- Additional content more background on a topic in the introduction
- Correction to a typographic, spelling, or grammatical mistake.
- Expanded reflection on a finding in the Discussion.
- Revision research method

Recommendation: Resubmit for Review

International Journal of Intelligent Systems and Applications in Engineering

A_revision_article_IJISAE_Sukmaindrayana.doc
2448K View as HTML Scan and download

Quick Reply

DEVELOPMENT OF SIGNATURE SECURITY USING RIVEST SHAMIR ADLEMAN AND AFFINE CIPHER CRYPTOGRAPHIC ALGORITHMS

Andri Sukmaindrayana
Informatics Engineering, STMIK DCI, Tasikmalaya, Indonesia
E-mail: sukmaindrayana@gmail.com

Abstract

The purpose of this research was to secure images using only Base64 security and combining Affine Cipher and Rivest Shamir Adleman cryptography in image security. The research used a qualitative descriptive method, using document study procedures, natural observations and interviews to obtain and collect data. Meanwhile, software development techniques use the Rapid Application Development (RAD) method. The results of the study, hybrid cryptography which is a combination of Affine Cipher and Rivest Shamir Adleman cryptography methods are able to overcome weaknesses in securing Base64 encoding according to the tests that have been carried out. Weaknesses in Affine Cipher cryptography can be covered with Rivest Shamir Adleman cryptography so that the value of confidentiality is better maintained and the value of integrity is also better maintained because the use of asymmetric keys in RSA cryptography is difficult to solve. In comparison, hybrid cryptography is able to disguise signature image data well, but in terms of speed it takes longer and data memory usage becomes larger compared to using only Base64 encoding.

Keywords: Signature, Affine Cipher, Rivest Shamir Adleman, Cryptography, Algorithm.

INTRODUCTION

Security in information technology is one of the most important things to protect data and information from interference and threats from hackers (Ienca & Haselager, 2016; McLeod & Dolezel, 2018; Whitman & Mattord, 2021). An important component in information technology security is data or information. Security can be interpreted as a condition free from danger and threat. Security is an effort to maintain confidentiality, integrity, and availability of data and information (Aloraini & Hammoudeh, 2017; Cains et al., 2022; L. Kim, 2022; Yang et al., 2019). Data or information can be in the form of documents, text, images, sounds, or video files. The process of exchanging data and information between the recipient and the sender must be maintained so that there is no loss to each other. One of the techniques that can be used in securing data exchange to maintain the confidentiality, integrity, and availability of data is cryptography, where the data exchanged will be encrypted using certain techniques (Panigrahi et al., 2021; Tchernykh et al., 2019; Varshney et al., 2019).

Cryptography is the art and science of securing data, information, and messages. Cryptography is a security method for protecting data or information by using a password that can only be understood by people who have the right to access the data or information (Abel et al., 2022; Rani & Kaur, 2017; Sethi & Kapoor, 2016; Taha et al., 2019). In cryptography, there is an encryption process that can be done using an algorithm with several parameters. Usually, the algorithm is not kept secret, even encryption that relies on the secrecy of the algorithm is considered something that is not good. The secret lies in several parameters that determine the decryption key that must be kept secret, parameters being equivalent to the key. One of the cryptography to secure data is the affine cipher technique. The affine cipher cryptographic algorithm is one of the classic cryptographic techniques with a type of substitution which is the development of the Caesar cipher. Affine cipher is a symmetric cryptographic algorithm, where the key for encryption is the same as the key for decryption, because this cryptography is a development of the Caesar cipher, affine cipher has a weakness in the small key size (Masya et al., 2020; Qowi & Hudallah, 2021; Tan et al., 2021). Thus, this cryptography can be solved with a brute force attack (Lone et al., 2022).

Another cryptographic algorithm is Rivest Shamir Adleman (RSA). RSA is public or asymmetric key cryptography, where this cryptography has different keys for encryption and decryption (Mallouli et al., 2019; Obaid, 2020). In the key generation process with RSA cryptography, two keys will be generated. First, the public key is not secret and can be published and known freely. The public key is only used for the encryption process. The second key is a private key that is highly confidential, and may not be shared, and only the recipient of the message may know this key. The private key is only used for the decryption process. If the private key is known by an unauthorized party, then that party can easily decrypt the cipher text into plain text. The use of cryptography is not only used on data in the form of text, documents, or communication messages but can be applied to images. An image is a form of multimedia that presents information visually (Taher et al., 2022).

Commented [A1]: Please check Spelling and grammar

One example of an image that must be secured is a digital signature or what is called a digital signature. Digital signature security can usually be secured using Base64 security. However, digital signatures that use Base64 security have weaknesses in the confidentiality of the data so they are very vulnerable to abuse or illegal operations that can eliminate the confidentiality of the data itself, such as modification, duplication, or fabrication. Digital Signature images can be secured using affine cipher cryptographic algorithms. However, affine cipher cryptography requires other cryptography to make data security strong (Masya et al., 2020). To overcome these weaknesses, affine cipher cryptography can be combined with the RSA algorithm. RSA cryptography has a very good level of security. This is because the security level of RSA cryptography lies in the difficulty of factoring integers into two prime numbers. By combining digital signature image security using affine cipher cryptography with asymmetric RSA cryptography, image data security can be disguised and prevent unauthorized parties from breaking the digital signature (Gunawan et al., 2019).

Related to some understanding of signature image security using the affine cipher and Rivest Shamir Adleman cryptographic algorithms, this research was conducted to secure images that only use Base64 security and combine Affine Cipher and Rivest Shamir Adleman cryptography in image security.

Commented [A2]: Please add More content background

LITERATURE REVIEW

Affine Cipher Cryptographic Algorithm

Affine Cipher is a cryptographic algorithm developed from the Caesar Cipher method. This algorithm is monoalphabetic exchange cryptography (Masya et al., 2020). Affine Cipher performs the encryption process by shifting characters in a mathematically substantial way. The fundamental difference from this algorithm is that shifting is done by multiplying a number that is relatively prime with the number used during the decryption process. The whole process depends on the working lock and modulus. The keys used in this algorithm are two prime numbers and one integer as a shift. The result obtained is the use of the Affine Cipher algorithm in carrying out the encryption and decryption process (Lone et al., 2021). The use of this method is very helpful in securing text that will be sent to other people or on a computer network. Affine Cipher is the development of Caesar Cipher which multiplies plain text with a value and adds it with a character shift value. To encryption plaintext (P) and ciphertext decryption (C) is stated by the formula in table 1.

Commented [A3]: Please check Typographi

Commented [A4]: Please check spelling and grammar

Table 1. The Formula for PlainText Encryption (P) and CipherText Decryption (C)

Encryption PlainText (P)	Decryption CipherText (C)
Ci = mPi + b (mod n) Where: C = CipherText P = PlainText n = Character range m = Multiplier key is a number that is relatively prime with n b = Character Shift Key i = Character sequence	**Pi = m-1 (Ci – b) (mod n)** Where: C = CipherText P = PlainText n = Character range m-1 = Key Inverse Multiplier of m b = Character Shift Key i = Character sequence

Rivest Shamir Adleman (RSA) Cryptographic Algorithm

Cryptography uses two numbers a public key and a private key. RSA cryptography was created by Ron Rivest, Adi Shamir, and Leonard Adleman, after the name of the inventor, in the 1970s (Purnomo Sidik et al., 2019). This design relies on the complexity of factoring integers which is different from solving discrete algorithms (Kallam, 2011). RSA cryptography is often used in short

Commented [A5]: Please check Spelling and grammar

messages. Because RSA cryptography uses two keys for encryption and decryption, RSA cryptography is considered an example of asymmetric key cryptography (Mezher, 2018). The process in RSA cryptography consists of three processes, namely as follows.

1) RSA cryptographic key generation, namely choosing two large random prime numbers, p and q. Calculate the system modulus n = p * q. Choose encryption key e randomly, where $1 < e < \phi(n)$, PBB (e, $\phi(n)$) = 1 (where $\phi(n)$ is the total value = $\phi(n) = (p - 1)(q - 1)$). Solve the following formula to determine the decryption key d, $e * d = 1 \pmod{\phi(n)}$ and $0 \leq d \leq n$. Then each user provides a public encryption key: public key = {e, n} and stores the decryption key: private key = {d, n}. If p is the message to be sent, then the encryption formula is public key = {e, n}, c = pe (mod n), where $0 \leq p \leq n$, and to decrypt it use the formula private key = {d, n}, p = cd (mod n).
2) The encryption process can be done using a public key based on the following equation.

$$Ci = Pie \bmod n$$

Where:
C = CipherText
P = PlainText
e = PublicKey
n = Product of the two prime numbers p and q
i = Character sequence

3) The decryption process can be done using the private key based on the following equation.

$$Pi = Cid \bmod n$$

Where:
C = CipherText
P = PlainText
d = Private Key
n = Product of the two prime numbers p and q
i = Character sequence

RESEARCH METHODS

The research was conducted using qualitative descriptive methods used to understand phenomena with a complete description of the phenomena studied (H. Kim et al., 2017). This study uses document study procedures, natural observation, and interviews to obtain and collect data. While software development techniques use the Rapid Application Development (RAD) method because the developed software requires feedback from users (Rizwan & Iqbal, 2011). Data analysis techniques use qualitative data analysis techniques which are based on the existence of a symmetrical relationship between the variables studied which aims to answer the problems formulated in the research. Data analysis activities include collecting, reducing, presenting, and drawing conclusions (Rahayu et al., 2021).

RESULTS AND DISCUSSION

Image Security Testing Results

Security testing will be carried out using the cryptanalysis method. Cryptanalysis is a study of ciphertexts that aims to find weaknesses in the encoding system, so that it is possible to obtain plaintext from existing ciphertexts, without the need to know the key or the ciphertext-building algorithm (Sarkar & Ghosh, 2020). This method is also known as breaking ciphertext. There are several techniques for performing cryptanalysis, depending on the access the cryptanalyst has, whether through ciphertext, plaintext, or other aspects of the cryptographic system. Several types of attacks that are commonly used to crack ciphers are Known-Plaintext Analysis, Chosen-Plaintext Analysis, Ciphertext-Only Analysis, Man-in-the-middle Attack, Timing/differential power analysis, Correlation, and Rubber-hose cryptoanalysis (Singh et al., 2021; Tuasikal et al., 2020; Wei et al., 2019). The author will test the security of the image using Ciphertext-Only Analysis. The Ciphertext-Only Analysis method is used because the image data that can be retrieved by hackers is only a ciphertext contained in the database so the method can be used as a test.

Commented [A6]: Please check Spelling and grammar

Commented [A7]: Revision research method

Commented [A8]: Expanded reflection

Commented [A9]: Please check Spelling and grammar

In the direct image processing process, the user will write his signature first and then save it by clicking the save button. The system will process signatures in this form without going throught Base64 encoding and Affine Cipher and RSA cryptography. After the system processes the image processing, the image results obtained are shown in figure 1.

Figure 1. Image Processing Results

If you look at the contents of the file in the image, the results obtained are shown in figure 2.

Figure 2. Image File Contents

The contents of the file in image processing immediately show that there is one of the texts indicating that the content is an image, namely PNG is one of the formats that comply with the provisions, so the signature image can be read directly by the user. Image processing through Base64 encoding, after the user writes and then saves the signature the system will process the signature via Base64 encoding, but without going through the Affine Cipher and RSA cryptographic proceses. The processing results cannot be seen directly, because the signature image has been disguised. The contents of the signature image file that has gone through the Base64 encoding process can be seen in figure 3.

Commented [A10]: Please check Typographi

Commented [A11]: Please check Typographi

iVBORw0KGgoAAAANSUhEUgAAASwAAACWCAYAAABk
W7XSAAAYMklEQVR4Xu1decxeQxefamxF0RApVUTt
a0soqvhD_K3wNmqnCCKEKk_sRCOl0hJiaymR2PdK
Y0la1VRbUbRF_KVqb6yVWiJ4v/zu983znXc6z/ve
+zwzc+/M/U3SWHqfe8/8zrm/e+bMOWd6dXZ2dioO
IkAEiEAECPQiYUWgJYpIBIhAhgAJi4ZABIhANAiQ
sKJRFQUlAkSAhEUbIAJEIBoESFjRqIqCEgEiQMKi
DRABIhANAiSsaFRFQYkAESBh0QaIABGIBgESVjSq
oqBEgAiQsGgDRIAIRIMACSsaVVFQIkAESFi0ASJA
BKJBgIQVjaooKBEgAiQs2gARIA_RIEDCikZVFJQI
EAESFm2ACBCBaBAgYUWjKgpKBIgACYs2QASIQDQI
k_CiURUFJQJEgIRFGyACRCAaBEhY0aiKghIBIkDC
og0QASIQDQIkrGhURUGJABEgYdEGiAARiAYBElY0
qqKgRIAIk_BoA0SACESDAAkrGlVRUCJABEhYtAEi
QASiQYCEFY2qKCgRIAIk_NoAESAC0SBAwopGVRSU
CBABEhZtgAgQgWgQIGFFoyoKSgSIQBKENX78ePXb
b7+pyy+/XG200UbUKhEgAokiED1hXX_JJWrSpEmZ
em699VaF/+YgAkDgl19+UQ899FAGxpgxY/gxS8As
oiYsGOSWW26pVq1alanixhtvVFdffXUCauEUXCAw
bNgwNXfu3OxW1113nbr++utd3Jb3KBGBqAnr9NNP
b3xBhwwZohYuXFgilHx0lRC47bbb1_hx4xoiwcN6
8MEHqyQiZWkBgWgJ67XXXlOHHHJIY8rPPvusOuaY
Y1qAgD9JDYF3331XDR48uMu05s2bp4YOHZraVGs3
n2gJ6+CDD1azZ89uxCf49ayd7VonjDABPmQg_T1g
K7NmzSJACSAQJWFJd3/DDTfMjHPrrbdOQB2cQrsI
XHTRRer2229v3KZPnz5q5syZat9992331vx9BRCI
jrDwBd1mm22yHSAMBlMrYEUVEcG2FBw9erR64okn
KiIhxWgXgegISwbat9pqq8y7Yu5Vu2aQxu9lmEDP
q_OzM43JcRYZAlERlvkFnTZtmgKBcRCB5557TnV0
dHQBAsvDyZMnE5yEEIiKsPbcc0+1aNGiDP6DDjpI
YaeQgwgAAXjZK1eu7A_GJ598ogYNGkSAEkIgGsIy
82qW_VvGQHtChtjOVJAQesMNN3S5xSmnnKIefvjh
dm7_31YQgSgIywy0jx07VoHAOIjA559/nuVc6U0Y
I__rrruqOXPmM_aZoHlEQVhICH3++ecz+JHGACON
_dCu84KwrK3j0ITiWm/SNoDr2muvrebPn6/qinPq
tlV5wjKDqQiiIpgay8C_evbZZ6unnnoqE/mdd96p
xcsEvSHeiI8_SqaW_FmSzf/nn3929rF57_HH1Ikn
ntjFFG666SZ1xRVXxGIel_MgApUm__zscPdh9Bix
pTFA/iOOOC_74usRkrCw_M_ze/fuvVpAuqCd5_4c
niR267TOzB+6JKwBAwaor7/+uvGIbbfdVi1dujS3

Figure 3. Base64 Encoding Image File Contents

As seen in figure 3, the contents of the image file have changed to a Base64 encoding pattern which has the characteristics of uppercase and lowercase letters of the alphabet, numbers, '+' and '/' symbols. As a result, the user is no longer able to read the signature directly and requires decoding first to read the signature. When the user presses the "Save" button, the signature is processed first into Base64 encoding, then it will be encrypted using cryptographic techniques using the code shown in figure 4.

```
$ttd    = $_POST['img_data'];
$enc    = encrypt($sign, $primeOne, $primeTwo, $publicKey, $keyAffine, $sftAffine);
```

Figure 4. Encryption Source Code

As seen in figure 4 the user's direct signature image which is in Base64 encoding form will be stored in $sign. After that, $sign will go through the encryption process with the name of the encrypt function and take six parameters, namely $sign for Base64 formatted images, $primeOne for the first prime number in RSA, $primeTwo for the second prime number in RSA, $publicKey for the public key. on RSA, $keyAffine for the multiplier key on Affine Cipher, and $sftAffine for the character shift key on Affine Cipher. The way the "encrypt" function works is that the encrypted image will first be checked for the size of the image data. Then each bit in the image data will be converted first to ASCII code to facilitate the encryption process. Each bit of the ASCII code will go through an encryption process using RSA cryptography with a public key and two predetermined prime numbers.

```
function encrypt($data,$prime1,$prime2,$publickey,$multiplierkey,$shiftkey) {
        $length = strlen ($data);
        $cipher = "";
        for ($i=0; $i<$length; $i++) {
                $convert        = ord($data[$i]);
                $encrypt0       = encryptor0($convert,$publickey,$prime1*$prime2,$multiplierkey,$shiftkey);
                $encrypt1       = encryptor1($convert,$publickey,$prime1*$prime2,$multiplierkey,$shiftkey);
                $replace0       = substr_replace($cipher, chr($encrypt0), 2*$i+0, 1);
                $replace1       = substr_replace($replace0, chr($encrypt1), 2*$i+0, 1);
                $cipher         = $replace1;
        }
        return $cipher;
};
```

Figure 5. Encryption Source Code (RSA and Affine Cipher)

Commented [A12]: Please check Spelling and grammar

The results of encryption in RSA cryptography are of great value, so the value of RSA encryption is divided into two parts, namely Most Significant Bit (MSB) and Least Significant Bit (LSB). The MSB resulting from RSA encryption will be entered as the first character and the LSB resulting from RSA encryption will be entered as the last character. After the MSB and LSB on the RSA encryption results have been obtained, then the encryption process is carried out using an Affine Cipher with a multiplier key and a predtermined character shift key. After the Affine Cipher encryption process has been carried out, all ASCII codes are converted back into characters and collected into one text to form an image that turns into ciphertext. The results of images that have been changed to ciphertext become cryptic or unreadable when viewed by the user. The following is an example of the encrypted result of the signature when viewed in the contents of the file in figure 6.

Commented [A13]: Please check Typographi

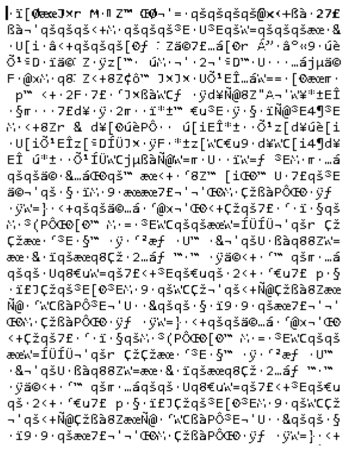


Figure 6. Fill in the Image Processing Results File with Affine Cipher and RSA

It can be seen in figure 6 that the user's signature which was previously written directly has changed to ciphertext.

Security Testing Results

The results of implementing cryptography on image data will be tested using a security technique, namely cryptanalysis techniques. One of the cryptanalysis techniques used is the Ciphertext-Only Analysis method. This method is taken as an example of a case when a hacker has succeeded in retrieving image data in a database, but the image data taken is only in the form of ciphertext which needs to be broken down into plaintext, the hacker does not know what cryptographic algorithm is implemented in the system and also does not know which key is used. Must be searched to open the ciphertext. The application used to test uses CrypTool which contains a cryptanalysis method to solve a cryptographic technique.

In using the Ciphertext-Only Analysis method, several tools are used to test whether cryptographic security is safe. The tools used include Caesar Analysis using character frequencies, ADFGVX heuristic analysis, M-138 Ciphertext only attack, Vigenere analysis, Homophonic Substitution Analysis, Transposition Hill Climbing Analysis, Solitaire Brute-force Analysis, RC4 Analysis, Enigma Analyzer, RSA Decryption. Based on the results of the tests that have been carried out, it can be concluded that the implementation of Affine Cipher and RSA cryptography is difficult to solve so that the image data is still maintained its authenticity.

Commented [A14]: Please check Spelling and grammar

After Affine Cipher and RSA cryptography is implemented on the image data in the system, a comparison is obtained between before implementation and after implementation. The aspects that are considered in the comparison of the old and new systems include data processing speed, memory usage, and data security. The details of the comparison of the old and new systems, namely that the old system was better in terms of data processing speed and data memory usage, but in terms of data security it was still quite weak. In contrast, the new system in terms of data processing speed and data memory usage is not good, but the data security aspect is better than the old system.

CONCLUSION

Based on data analysis and discussion of research problems, and testing, several conclusions can be drawn, namely, the use of the Affine Cipher and Rivest Shamir Adleman (RSA) cryptographic algorithms is able to overcome weaknesses in Base64 encoding security according to the results of tests that have been carried out. Weaknesses in Affine Cipher cryptography can be covered with Rivest Shamir Adleman (RSA) cryptography so that the values of confidentiality, integrity, and availability are better maintained due to the use of asymmetric keys in RSA cryptography which are difficult to solve. Comparatively, the use of the Affine Cipher and Rivest Shamir Adleman (RSA) cryptographic algorithms is able to disguise signature image data well, but in terms of speed it takes longer and data memory usage becomes larger compared to using only Base64 encoding. In further research, cryptographic techniques can be found that have faster processing and use smaller file memory, but still, pay attention to the strength of securing stored data.

REFERENCES

Abel, K. D., Misra, S., Agrawal, A., Maskeliunas, R., & Damasevicius, R. (2022). Data Security Using Cryptography and Steganography Technique on the Cloud. *Lecture Notes in Electrical Engineering*, *834*(6), 475–481. https://doi.org/10.1007/978-981-16-8484-5_46

Aloraini, A., & Hammoudeh, M. (2017). A Survey on Data Confidentiality and Privacy in Cloud Computing. *Proceedings of the International Conference on Future Networks and Distributed Systems*. https://doi.org/10.1145/3102304.3102314

Cains, M. G., Flora, L., Taber, D., King, Z., & Henshel, D. S. (2022). Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context using Expert Elicitation. *Risk Analysis*, *42*(8), 1643–1669. https://doi.org/https://doi.org/10.1111/risa.13687

Gunawan, I., Sumarno, Tambunan, H. S., Irawan, E., Qurniawan, H., & Hartama, D. (2019). Combination of Caesar Cipher Algorithm and Rivest Shamir Adleman Algorithm for Securing Document Files and Text Messages. *Journal of Physics: Conference Series*, *1255*(1), 12077. https://doi.org/10.1088/1742-6596/1255/1/012077

Ienca, M., & Haselager, P. (2016). Hacking the brain: brain–computer interfacing technology and the ethics of neurosecurity. *Ethics and Information Technology*, *18*(2), 117–129. https://doi.org/10.1007/s10676-016-9398-9

Kim, H., Sefcik, J. S., & Bradway, C. (2017). Characteristics of Qualitative Descriptive Studies: A Systematic Review. *Research in Nursing & Health*, *40*(1), 23–42. https://doi.org/https://doi.org/10.1002/nur.21768

Kim, L. (2022). *Cybersecurity: Ensuring Confidentiality, Integrity, and Availability of Information BT - Nursing Informatics : A Health Informatics, Interprofessional and Global Perspective* (U. H. Hübner, G. Mustata Wilson, T. S. Morawski, & M. J. Ball (eds.); pp. 391–410). Springer International Publishing. https://doi.org/10.1007/978-3-030-91237-6_26

Lone, P. N., Singh, D., & Mir, U. H. (2021). A novel image encryption using random matrix affine cipher and the chaotic maps. *Journal of Modern Optics*, *68*(10), 507–521. https://doi.org/10.1080/09500340.2021.1924885

Lone, P. N., Singh, D., Stoffová, V., Mishra, D. C., Mir, U. H., & Kumar, N. (2022). Cryptanalysis and Improved Image Encryption Scheme Using Elliptic Curve and Affine Hill Cipher. In *Mathematics* (Vol. 10, Issue 20). https://doi.org/10.3390/math10203878

Mallouli, F., Hellal, A., Saeed, N. S., & Alzahrani, F. A. (2019). A Survey on Cryptography: Comparative Study between RSA vs ECC Algorithms, and RSA vs El-Gamal Algorithms. *2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/ 2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)*, 173–176. https://doi.org/10.1109/CSCloud/EdgeCom.2019.00022

Masya, R. I., Aji, R. F., & Yazid, S. (2020). Comparison of Vigenere Cipher and Affine Cipher in Three-pass Protocol for Securing Image. *2020 6th International Conference on Science and Technology (ICST)*, *1*, 1–5. https://doi.org/10.1109/ICST50505.2020.9732873

McLeod, A., & Dolezel, D. (2018). Cyber-analytics: Modeling factors associated with healthcare data breaches. *Decision Support Systems*, *108*, 57–68. https://doi.org/https://doi.org/10.1016/j.dss.2018.02.007

Mezher, A. E. (2018). Enhanced RSA cryptosystem based on multiplicity of public and private keys. *International Journal of Electrical and Computer Engineering*, *8*(5), 3949–3953. https://doi.org/10.11591/ijece.v8i5.pp3949-3953

Obaid, T. S. (2020). Study A Public Key in RSA Algorithm. *European Journal of Engineering and Technology Research*, *5*(4 SE-Articles), 395–398. https://doi.org/10.24018/ejeng.2020.5.4.1843

Panigrahi, A., Nayak, A. K., & Paul, R. (2021). Issues and Challenges of Classical Cryptography in Cloud Computing. In *Machine Learning Approach for Cloud Data Analytics in IoT* (pp. 143–165). https://doi.org/https://doi.org/10.1002/9781119785873.ch7

Purnomo Sidik, A., Efendi, S., & Suherman, S. (2019). Improving One-Time Pad Algorithm on Shamir's Three-Pass Protocol Scheme by Using RSA and ElGamal Algorithms. *Journal of Physics: Conference Series*, *1235*(1), 12007. https://doi.org/10.1088/1742-6596/1235/1/012007

Qowi, Z., & Hudallah, N. (2021). Combining caesar cipher and hill cipher in the generating encryption key on the vigenere cipher algorithm. *Journal of Physics: Conference Series*, *1918*(4), 42009. https://doi.org/10.1088/1742-6596/1918/4/042009

Rahayu, R., Abbas, E. W., & Jumriani, J. (2021). Social Studies Lesson Planning for Children with Intellectual Disabilities in the Pembina State Special School of South Kalimantan Province. *The Kalimantan Social Studies Journal*, *2*(2), 160–169.

Rani, S., & Kaur, H. (2017). Technical Review on Symmetric and Asymmetric Cryptography Algorithms. *International Journal of Advanced Research in Computer*, *8*(4), 182–186.

Rizwan, M., & Iqbal, M. (2011). *Application of 80/20 Rule in Software Engineering Rapid Application Development (RAD) Model BT - Software Engineering and Computer Systems* (J. M. Zain, W. M. bt Wan Mohd, & E. El-Qawasmeh (eds.); pp. 518–532). Springer Berlin Heidelberg.

Sarkar, M., & Ghosh, S. (2020). Development of a secured optical code-division multiple access system by implementing hybrid 2D-modified Walsh code. *Optical Engineering*, *59*(10), 106107. https://doi.org/10.1117/1.OE.59.10.106107

Sethi, P., & Kapoor, V. (2016). A Proposed Novel Architecture for Information Hiding in Image Steganography by Using Genetic Algorithm and Cryptography. *Procedia Computer Science*, *87*, 61–66. https://doi.org/https://doi.org/10.1016/j.procs.2016.05.127

Singh, P., Kumar, R., Yadav, A. K., & Singh, K. (2021). Security analysis and modified attack algorithms for a nonlinear optical cryptosystem based on DRPE. *Optics and Lasers in Engineering*, *139*, 106501. https://doi.org/https://doi.org/10.1016/j.optlaseng.2020.106501

Taha, M. S., Mohd Rahim, M. S., Lafta, S. A., Hashim, M. M., & Alzuabidi, H. M. (2019). Combination of Steganography and Cryptography: A short Survey. *IOP Conference Series: Materials Science and Engineering*, *518*(5), 52003. https://doi.org/10.1088/1757-899X/518/5/052003

Taher, M. M., Ahmad, A. R. B. H. J., Hameed, R. S., & Mokri, S. S. (2022). a Literature Review of Various Steganography Methods. *Journal of Theoretical and Applied Information Technology*, *100*(5), 1412–1427.

Tan, C. M. S., Arada, G. P., Abad, A. C., & Magsino, E. R. (2021). A Hybrid Encryption and Decryption Algorithm using Caesar and Vigenere Cipher. *Journal of Physics: Conference Series*, *1997*(1), 12021. https://doi.org/10.1088/1742-6596/1997/1/012021

Tchernykh, A., Schwiegelsohn, U., Talbi, E., & Babenko, M. (2019). Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability. *Journal of Computational Science*, *36*, 100581. https://doi.org/https://doi.org/10.1016/j.jocs.2016.11.011

Tuasikal, A. R., Indra, D., & Fattah, F. (2020). Analisis Perbandingan Known Plaintext dan Chosen Plaintext Pada Metode Hill Chiper. *Buletin Sistem Informasi Dan Teknologi Islam (BUSITI); Vol 1, No 1 (2020)DO - 10.33096/Busiti.V1i1.514* .

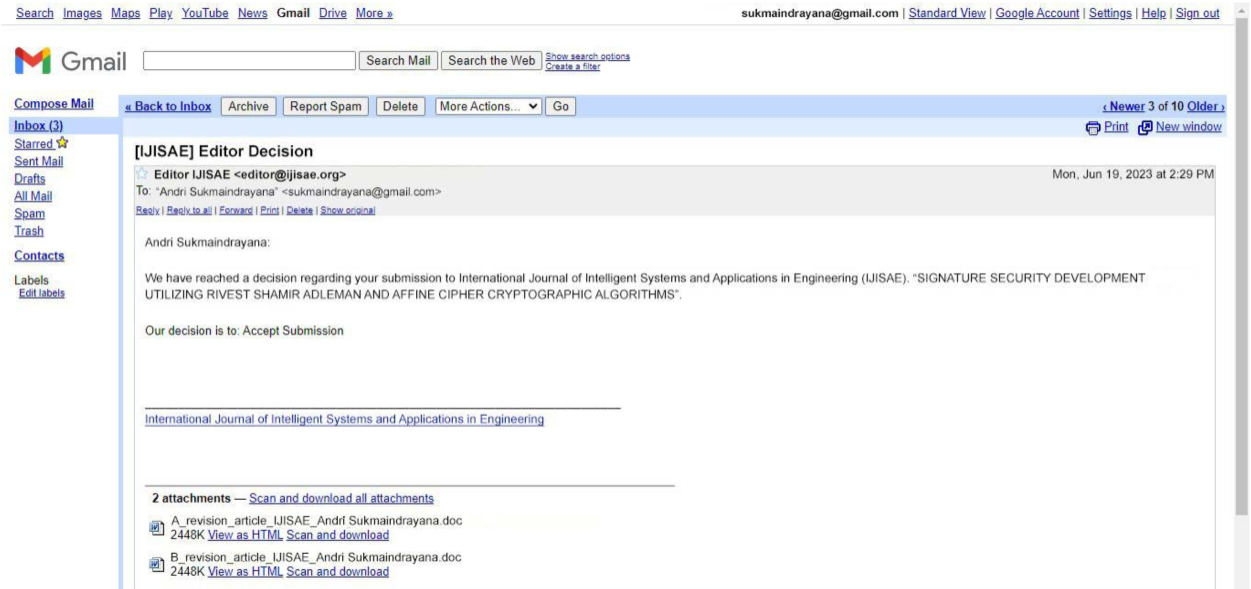
https://jurnal.fikom.umi.ac.id/index.php/BUSITI/article/view/514
Varshney, T., Sharma, N., Kaushik, I., & Bhushan, B. (2019). Authentication & Encryption Based Security Services in Blockchain Technology. *2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*, 63–68. https://doi.org/10.1109/ICCCIS48478.2019.8974500

Wei, W., Woźniak, M., Damaševičius, R., Fan, X., & Li, Y. (2019). Algorithm Research of Known-plaintext Attack on Double Random Phase Mask Based on WSNs. *Journal of Internet Technology; Vol 20, No 1 (2019)*. https://jit.ndhu.edu.tw/article/view/1972

Whitman, M. E., & Mattord, H. J. (2021). *Principles of Information Security*. Cengage Learning.

Yang, L., Elisa, N., & Eliot, N. (2019). *Chapter 7 - Privacy and Security Aspects of E-Government in Smart Cities* (D. B. Rawat & K. Z. B. T.-S. C. C. and P. Ghafoor (eds.); pp. 89–102). Elsevier. https://doi.org/https://doi.org/10.1016/B978-0-12-815032-0.00007-X

4. BUKTI KONFIRMASI REVIEW DAN HASIL REVIEW KEDUA
(19 Juni 2023, 2:29 PM)



Search Images Maps Play YouTube News Gmail Drive More »

sukmaindrayana@gmail.com | Standard View | Google Account | Settings | Help | Sign out

Gmail [Search Mail] [Search the Web] Show search options Create a filter

Compose Mail
Inbox (3)
Starred
Sent Mail
Drafts
All Mail
Spam
Trash
Contacts
Labels
Edit labels

« Back to Inbox [Archive] [Report Spam] [Delete] [More Actions...] [Go] ‹ Newer 3 of 10 Older ›

Print New window

[IJISAE] Editor Decision

Editor IJISAE <editor@ijisae.org> Mon, Jun 19, 2023 at 2:29 PM
To: "Andri Sukmaindrayana" <sukmaindrayana@gmail.com>
Reply | Reply to all | Forward | Print | Delete | Show original

Andri Sukmaindrayana:

We have reached a decision regarding your submission to International Journal of Intelligent Systems and Applications in Engineering (IJISAE). "SIGNATURE SECURITY DEVELOPMENT UTILIZING RIVEST SHAMIR ADLEMAN AND AFFINE CIPHER CRYPTOGRAPHIC ALGORITHMS".

Our decision is to: Accept Submission

____
International Journal of Intelligent Systems and Applications in Engineering

2 attachments — Scan and download all attachments

A_revision_article_IJISAE_Andri Sukmaindrayana.doc
2448K View as HTML Scan and download

B_revision_article_IJISAE_Andri Sukmaindrayana.doc
2448K View as HTML Scan and download

5. BUKTI KONFIRMASI ARTIKEL ACCEPTED
(20 Juni 2023, 11:44 AM)

Andri Sukmaindrayana <sukmaindrayana@gmail.com> Tue, Jun 20, 2023 at 11:44 PM
To: **Editor IJISAE** <editor@ijisae.org>

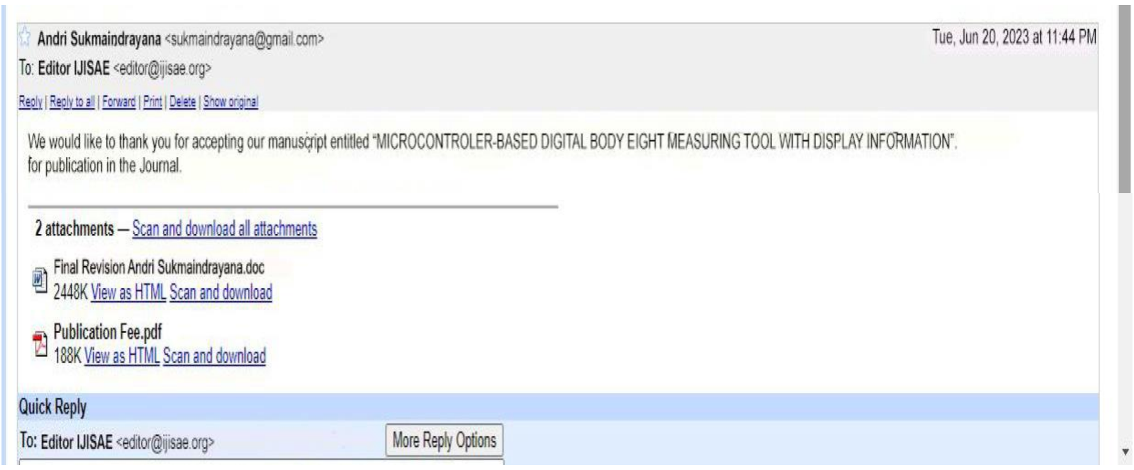
Reply | Reply to all | Forward | Print | Delete | Show original

We would like to thank you for accepting our manuscript entitled "MICROCONTROLER-BASED DIGITAL BODY EIGHT MEASURING TOOL WITH DISPLAY INFORMATION".
for publication in the Journal.

Final version of our article and proof of payment for our publication is attached below.

- Show quoted text -

6. BUKTI PEMBAYARAN JURNAL



Andri Sukmaindrayana <sukmaindrayana@gmail.com> Tue, Jun 20, 2023 at 11:44 PM

To: Editor IJISAE <editor@ijisae.org>

Reply | Reply to all | Forward | Print | Delete | Show original

We would like to thank you for accepting our manuscript entitled "MICROCONTROLER-BASED DIGITAL BODY EIGHT MEASURING TOOL WITH DISPLAY INFORMATION".
for publication in the Journal.

2 attachments — Scan and download all attachments

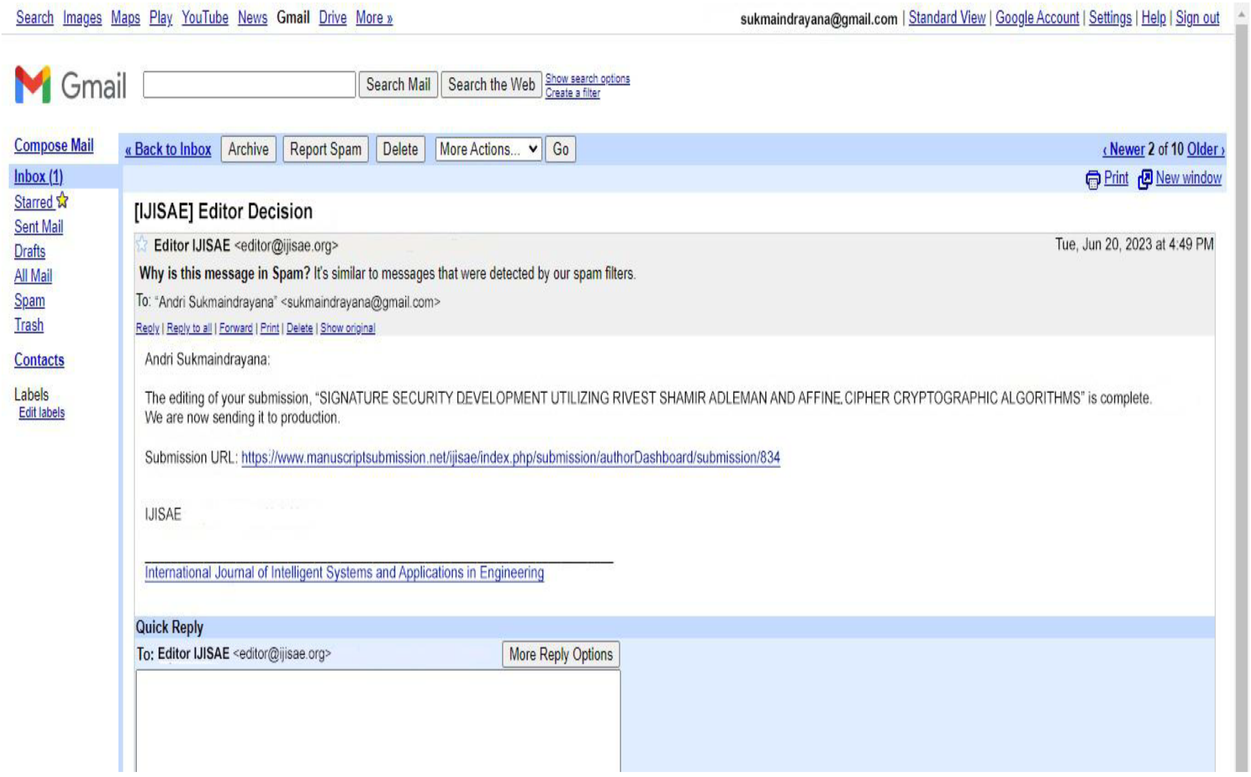
Final Revision Andri Sukmaindrayana.doc
2448K View as HTML Scan and download

Publication Fee.pdf
188K View as HTML Scan and download

Quick Reply

To: Editor IJISAE <editor@ijisae.org> More Reply Options

7. BUKTI JURNAL SUDAH BERADA DI BAGIAN PRODUKSI (20 Juni 2023, 4:49 AM)



Search Images Maps Play YouTube News Gmail Drive More »

sukmaindrayana@gmail.com | Standard View | Google Account | Settings | Help | Sign out

Gmail

Search Mail | Search the Web | Show search options | Create a filter

Compose Mail

Inbox (1)

Starred

Sent Mail

Drafts

All Mail

Spam

Trash

Contacts

Labels

Edit labels

« Back to Inbox | Archive | Report Spam | Delete | More Actions... | Go

‹ Newer 2 of 10 Older ›

Print | New window

[IJISAE] Editor Decision

Editor IJISAE <editor@ijisae.org>

Tue, Jun 20, 2023 at 4:49 PM

Why is this message in Spam? It's similar to messages that were detected by our spam filters.

To: "Andri Sukmaindrayana" <sukmaindrayana@gmail.com>

Reply | Reply to all | Forward | Print | Delete | Show original

Andri Sukmaindrayana:

The editing of your submission, "SIGNATURE SECURITY DEVELOPMENT UTILIZING RIVEST SHAMIR ADLEMAN AND AFFINE CIPHER CRYPTOGRAPHIC ALGORITHMS" is complete. We are now sending it to production.

Submission URL: https://www.manuscriptsubmission.net/ijisae/index.php/submission/authorDashboard/submission/834

IJISAE

International Journal of Intelligent Systems and Applications in Engineering

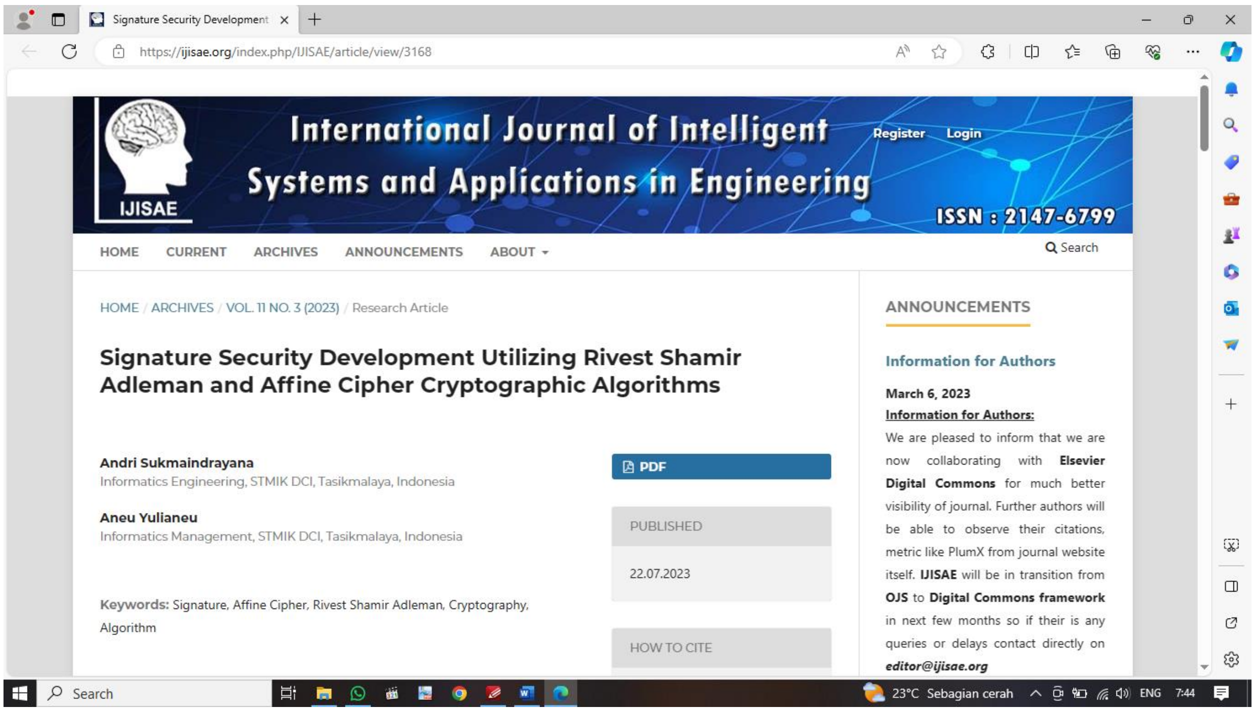
Quick Reply

To: Editor IJISAE <editor@ijisae.org>

More Reply Options

8. BUKTI JURNAL SUDAH PUBLISH
(22 Juni 2023)

Link Jurnal :
https://ijisae.org/index.php/IJISAE/article/view/3168


International Journal of Intelligent Systems and Applications in Engineering
IJISAE
Register Login
ISSN : 2147-6799

HOME CURRENT ARCHIVES ANNOUNCEMENTS ABOUT

HOME / ARCHIVES / VOL. 11 NO. 3 (2023) / Research Article

Signature Security Development Utilizing Rivest Shamir Adleman and Affine Cipher Cryptographic Algorithms

Andri Sukmaindrayana
Informatics Engineering, STMIK DCI, Tasikmalaya, Indonesia

Aneu Yulianeu
Informatics Management, STMIK DCI, Tasikmalaya, Indonesia

Keywords: Signature, Affine Cipher, Rivest Shamir Adleman, Cryptography, Algorithm

PDF

PUBLISHED
22.07.2023

HOW TO CITE

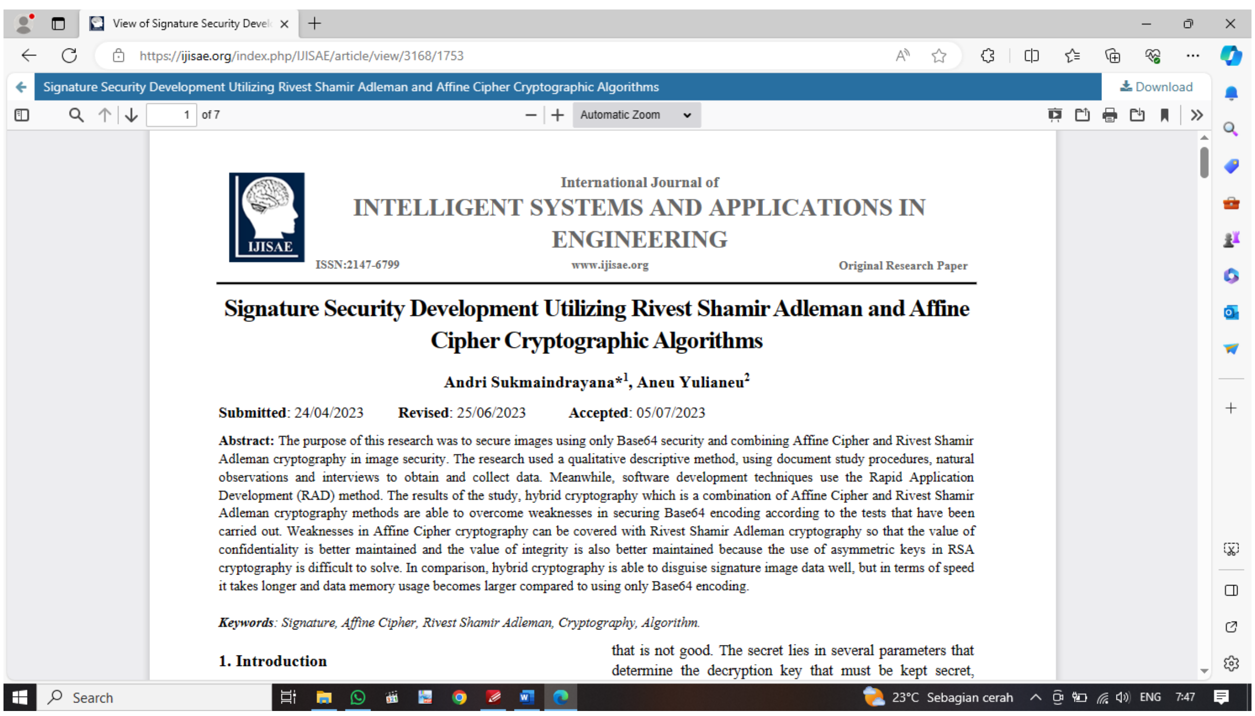
ANNOUNCEMENTS

Information for Authors

March 6, 2023

Information for Authors:

We are pleased to inform that we are now collaborating with **Elsevier Digital Commons** for much better visibility of journal. Further authors will be able to observe their citations, metric like PlumX from journal website itself. **IJISAE** will be in transition from **OJS** to **Digital Commons framework** in next few months so if their is any queries or delays contact directly on ***editor@ijisae.org***


Signature Security Development Utilizing Rivest Shamir Adleman and Affine Cipher Cryptographic Algorithms

International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
IJISAE
ISSN:2147-6799 www.ijisae.org Original Research Paper

Signature Security Development Utilizing Rivest Shamir Adleman and Affine Cipher Cryptographic Algorithms

Andri Sukmaindrayana*[1], Aneu Yulianeu[2]

Submitted: 24/04/2023 **Revised**: 25/06/2023 **Accepted**: 05/07/2023

Abstract: The purpose of this research was to secure images using only Base64 security and combining Affine Cipher and Rivest Shamir Adleman cryptography in image security. The research used a qualitative descriptive method, using document study procedures, natural observations and interviews to obtain and collect data. Meanwhile, software development techniques use the Rapid Application Development (RAD) method. The results of the study, hybrid cryptography which is a combination of Affine Cipher and Rivest Shamir Adleman cryptography methods are able to overcome weaknesses in securing Base64 encoding according to the tests that have been carried out. Weaknesses in Affine Cipher cryptography can be covered with Rivest Shamir Adleman cryptography so that the value of confidentiality is better maintained and the value of integrity is also better maintained because the use of asymmetric keys in RSA cryptography is difficult to solve. In comparison, hybrid cryptography is able to disguise signature image data well, but in terms of speed it takes longer and data memory usage becomes larger compared to using only Base64 encoding.

Keywords: *Signature, Affine Cipher, Rivest Shamir Adleman, Cryptography, Algorithm.*

1. Introduction

that is not good. The secret lies in several parameters that determine the decryption key that must be kept secret,