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

Security in information technology is one of the most important things to protect data and information from interference and threats from hackers [1]–[3]. 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 [4]–[7]. 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 [8]–[10].

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 [11]–[14]. 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 [15]–[17]. Thus, this cryptography can be solved with a brute force attack [18].

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 [19], [20]. 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 [21].

One example of an image that must be secured is a digital signature or what is called a digital signature. Digital

1 Informatics Engineering, STMIK DCI, Tasikmalaya, Indonesia
ORCID ID : 0000-0001-5684-2811
2 Informatics Management, STMIK DCI, Tasikmalaya, Indonesia
ORCID ID : 0000-0002-5566-6446
** Corresponding Author Email: sukmaindrayana@gmail.com*

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 [17]. 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 [22].

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.

2. Literature Review

2.1. Affine Cipher Cryptographic Algorithm

Affine Cipher is a cryptographic algorithm developed from the Caesar Cipher method. This algorithm is monoalphabetic exchange cryptography [17]. 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 [23]. 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.

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

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

2.2. 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 [24]. 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 messages. Because RSA cryptography uses two keys for encryption and decryption, RSA cryptography is considered an example of asymmetric key cryptography [25]. The process in RSA cryptography consists of three processes, namely as follows.

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, $e * d = 1 \ (\mathrm{mod}\ \phi(n))$ and $0 \le d \le n$. 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 $0 \le p \le n$, and to decrypt it use the formula private key = {d, n}, p = cd (mod n).

The encryption process can be done using a public key based on the following equation.

$$Ci = Pie \bmod n \tag{1}$$

Where:

C = CipherText

P = PlainText

e = PublicKey

n = Product of the two prime numbers p and q

i = Character sequence

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

Pi = Cid mod n (2)

Where:

C = CipherText

P = PlainText

d = Private Key

n = Product of the two prime numbers p and q

i = Character sequence

3. Research Methods

The research was conducted using qualitative descriptive methods used to understand phenomena with a complete description of the phenomena studied [26]. 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 [27]. 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 [28].

4. Results and Discussion

4.1. 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 [29]. 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 [30]–[32]. 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.

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 through Base64 encoding and Affine Cipher and RSA cryptography. After the system processes the image processing, the image results obtained are shown in figure 1.

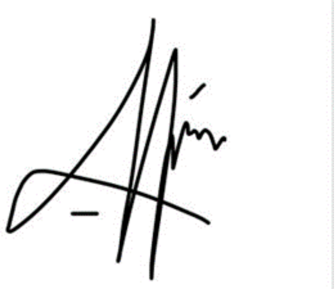
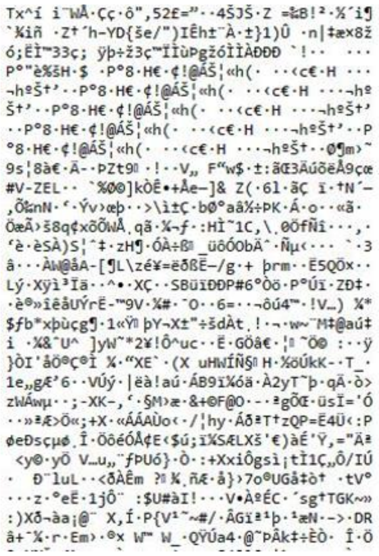


Fig. 1. Image Processing Results

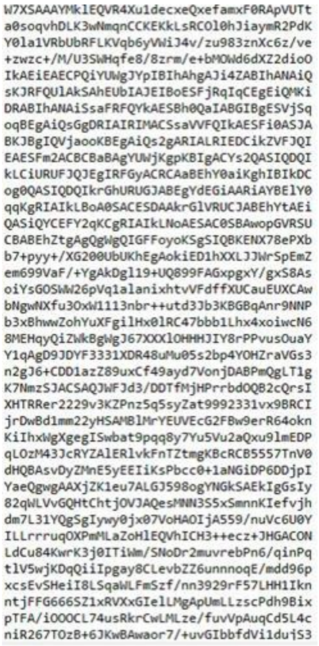
If you look at the contents of the file in the image, the results obtained are shown in figure 2.



```
Tx^í i¯WÅ·Çç·ô",52£="··4ŠJŠ·Z =‰B!²·%´i¶
`‰iñ ·Z†´h-YD{še/")IÊh±¨À·±}1)Û ·n|‡æx8ž
ó;ËÌ™33ç; ÿþ÷ž3ç™ÏÌùÞgžóÌÌÀÐÐÐ `!··  ···
P°"è%šH·$ ·P°8·H€·¢!@ÁŠ¦«h(· ··‹c€·H ···
¬hºŠ†’··P°8·H€·¢!@ÁŠ¦«h(· ··‹c€·H ···¬hº
Š†’··P°8·H€·¢!@ÁŠ¦«h(· ··‹c€·H ···¬hºŠ†’
··P°8·H€·¢!@ÁŠ¦«h(· ··‹c€·H ···¬hºŠ†’··P
°8·H€·¢!@ÁŠ¦«h(· ··‹c€·H ···¬hºŠ†··Ø¶m›˜
9s¦8à€·Ā--·ÞZt9 ·!··V„ F“w$·±:ãŒ3ÃúõëÅ9çœ
#V-ZEL·· `%Ø©]kÒÊ•+Åe—]& Z(·6l·ãÇ ï·†N´—
,Õ‰nN·ʻ·Ýv›œþ··>\ì±Ç·bØ°aå½÷ÞK·Á·o··«ã·
ÖæÃ›š8q¢xõÕWÅ,qã·%¬ƒ·:HÌ˜1C,\,0ÖfÑî···,·
ʻè·èSÀ)S¦ˆ‡·zH¶·ÓÀ÷ß _üôÓObÄˆ·Ñµ‹···  `·3
â···ÀW@åA-[¶L\zé¥=ëðßĒ—/g·+ þrm··Ē5QŌx··
Lý·Xÿì³Īä··^•·XÇ··SBüīÐÐP#6°Òö·P°Úī·ZÐ‡·
·è®»îêåUÝrË-™9V·%#·¯O··6=··¬ôú4™·!V…) %*
$ƒb*xþùçg¶·1«Ÿ þY¬X±"÷šdÀt,!·¬·w~¯M‡@aú‡
i ·%&¯U^ ]yW˜*2¥!Ô^uc··Ë·GÖâ€·¦ ˜Ö© :··ÿ
}ÒI'åÖ®Ç®Î %·“XEˋ·(X uHWÍÑ§ H·%öÚkK-·T_·
1e„gÆ’6··VÚý·|ëà!aú·ÁB9ï%óä·À2yT˜þ·qĀ·ō>
zWÁwµ··;-XK-,ʻ·§M›æ·&+©F@O·--ªgÕŒ·üsÏ='Ó
··»ªÆ>Ō«;+X·«ÁÁAÙo‹·/¦hy·Áðªт†zQP=Ē4Ū‹:P
ǿeÐsçµǿ,Î·ÖôéÓÅ¢E‹$ú;ï%SÆLXš'€)àÉ'Ÿ,="Äª
 <y©·yŌ V…u„¨ƒÞUó}·Ò·:+XxiÔgsì¡tÌ1Ç„Ô/IÚ
·  Ð¨luL··<ðÀÊm ? %,ñÆ·å}›7o®UGå‡ò† ·tV°
···z·°eË·1jÔ¨ :$U#àI!···V•ÀºÉC·´sg†TGK~»
:)Xð¬àa¡@¯ X,Í·P{V¹˜~#/·ÂGïª¹þ·¹æN·–>·DR
â+¯%·r·Em›·®x W™ W_·QŸÚa4·@˜ÞÂk‡÷ÈÒ· Î·Ö
```

Fig. 2. Image File Contents

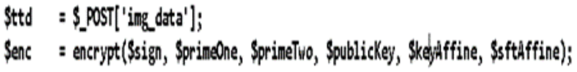
The contents of the file in image processing immediately show that there is one of the texts indicating that the content is an image, namely PNG is one of the formats that comply with the provisions, so the signature image can be read directly by the user. Image processing through Base64 encoding, after 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 processes. 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.



W7XSAAAYMklEQVR4Xu1decxeQxefamxF0RApVUTt
a0soqvhDLK3wNmqnCCKEKkLsRCOl0hJiaymR2PdK
Y0la1VRbUbRFLKVqb6yVWiJ4v/zu983znXc6z/ve
+zwzc+/M/U3SWHqfe8/8zrm/e+bMOWd6dXZ2dioO
IkAEiEAECPQiYUWgJYpIBIhAhgAJi4ZABIhANAiQ
sKJRFQUlAkSAhEUbIAJEIBoESFjRqIqCEgEiQMKi
DRABIhANAiSsaFRFQYkAESBh0QaIABGIBgESVjSq
oqBEgAiQsGgDRIAIRIMACSsaVVFQIkAESFi0ASJA
BKJBgIQVjaooKBEgAiQs2gARIALRIEDCikZVFJQI
EAESFm2ACBCBaBAgYUWjKgpKBIgACYs2QASIQDQI
kLCiURUFJQJEgIRFGyACRCAaBEhY0aiKghIBIkDC
og0QASIQDQIkrGhURUGJABEgYdEGiAARiAYBElY0
qqKgRIAIkLBoA0SACESDAAkrGlVRUCJABEhYtAEi
QASiQYCEFY2qKCgRIAIkLNoAESAC0SBAwopGVRSU
CBABEhZtgAgQgWgQIGFFoyoKSgSIQBKENX78ePXb
b7+pyy+/XG200UbUKhEgAokiED1hXXLJJWrSpEmZ
em699VaF/+YgAkDgl19+UQ899FAGxpgxY/gxS/As
oiYsGOSWW26pbzbNb62VqlalanXCauuEUXCauEUXCAw
bNgwNXfu3OxW1113nbr++nbr++utd3Jb3KBGBqAnr9NNP
b3xBhwwZohYuXFgilHx0lRC47bbb1bb1Lhx4xoiwcN6
8MEHqyQiZWkBgWgJ67XXXl0OHHHJIY8rPPvusOuaY
Y1qAgD9JDYF3331XDR48uMu05s2bp2bp4YOHZraVGs3
n2gJ6+CDD1azZ89uxCf49ayd7VonjDABPmQgLT1g
K7NmzSJACSAQJWFJd3/DDTfMfjMiHPrrrbd0QB2cQrsI
XHTRRer2229v3KZZnz5q5syZat9992992331vx9BRCI
jrDwBd8d1mm22YEUVEcG2FFBw9erR64okn
KiIhxWgXgXgISYbl9pqq8y7Yu5Vu2aQxu9lmEDP
qLOzM43JcRYZAlERlvkFnTZtmgKBcRCB5557T3nP
dHQBAsvDyZMnE5yEIiKsPbc0+1aNGDP6DDjpI
YaeQgwgAtGAAXjZK1eu7aH59LlaoLGJG4uRq9kgwHpI
82qWLVVvGQHtChtjOV0xgMPmNNKTxSmnnnKIefvhv
dm7L31YQgSgyw0w0fY/nuVc6U0Y
ILLrrruqOXPmMLaZoHlEQxVhICH3++ec+ecz+JHGACON
LdCu84KwrK3j0ITiWm/SNoDr2muvrebPn6/qinPq
tlV5wjKDqQiipgay8CLevbZZ6unnnoqE/mdd96p
xcsEvSHeiI8LSqaWLFmSzf/nn3929f7LHH1Ikn
ntjFFG666SZ1xRVXGIelLMgApUmLLLzscPdh9Bix
pTFA/iOOOCL74usRkrCwLMLze/fuvVpAuqCd5L4c
niR267TOzB+6JKwBAwaor7/+uvGIbbfdVi1ldujS3

Fig. 3. Base64 Encoding Image File Contents

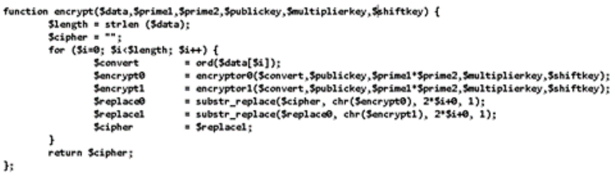
As seen in figure 3, the contents of the image file have changed to a Base64 encoding pattern which has the characteristics of uppercase and lowercase letters of the alphabet, numbers, '+' and '/' symbols. As a result, the user is no longer able to read the signature directly and requires decoding first 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);
```

Fig. 4. Encryption Source Code

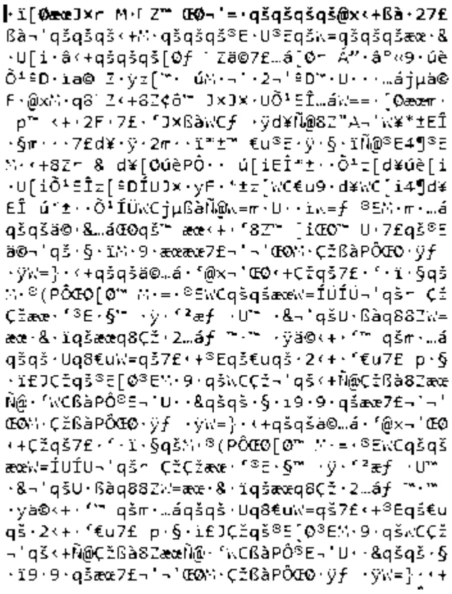
As seen in figure 4 the user's direct signature image which is in Base64 encoding form will be stored in $sign. After that, $sign will go through the encryption process with the name of the encrypt function and take six parameters, namely $sign for Base64 formatted images, $primeOne for the first prime 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;
};
```

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

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 predetermined 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.



```
|·ï[ØææJ×r M·Γ Z™ ŒØ¬'=·qšqšqšqš@x‹+ßà·27£
ßà¬'qšqšqš‹+M·qšqšqš³E·U³Eqš=qšqšqšææ·&
·U[i·â‹+qšqšqš[Øƒ ˙Zä©7£…á¸Ø¬ Á”·â°«9·úè
Ò¹ªD·ia© Z·ÿz[™· úM·¬˙·2¬'ªD™·U···…ájµà©
F·@xM·q8˙Z‹+8Z¢ô™ J×J×·UÕ¹EÎ…áW==·¸Øææπ·
 p™ ‹+·2F·7£·ʻJ×ßàWCƒ ·ÿd¥Ñ@8Z"A¬'W¥*±EÎ
·§π···7£d¥·ÿ·2π··ï"±™ €u³E·ÿ·§·ïÑ@³E4¶³E
M·‹+8Z¬ & d¥[ØúèPÔ·· ú[iEÎ"±··Ò¹z[d¥úè[i
·U[iÒ¹EÎz[ªDÍUJ×·yF·ʻ±z¸WC€u9·d¥WC¸i4¶d¥
EÎ ú˙±··Ò¹ÍÜWCjµßàÑ@W=π·U··iW=ƒ ³EM·π·…á
qšqšä©·&…áŒØqš™ ææ‹+·ʻ8Z™ ¸iŒØ™ U·7£qš³E
ä©¬'qš·§·ïM·9·æææææ7£¬'¬'ŒØM·ÇžßàPÔŒØ·ÿƒ
·ÿW=}·‹+qšqšä©…á·ʻ@x¬'ŒØ‹+Çžqš7£·ʻ·ï·§qš
M·³(PÔŒØ[Ø™ M·=·³EWCqšqšææW=ÍUÍU¬'qš¬ Çž
Çžææ·ʻ³E·§™ ·ÿ·ʻ²æƒ ·U™ ·&¬'qšU·ßàq88ZW=
ææ·&·ïqšææq8Çž·2…áƒ ™·™ ·ÿä©‹+·ʻ™ qšπ·…á
qšqš·Uq8€uW=qš7£‹+³Eqš€uqš·2‹+·ʻ€u7£ p·§
·ï£JÇžqš³E[Ø³EM·9·qšWCÇž¬'qš‹+Ñ@Çžßà8Zææ
Ñ@·ʻWCßàPÔ³E¬'U··&qšqš·§·ı9·9·qšææ7£¬'¬'
ŒØM·ÇžßàPÔŒØ·ÿƒ ·ÿW=}·‹+qšqšä©…á·ʻ@x¬'ŒØ
‹+Çžqš7£·ʻ·ï·§qšM·³(PÔŒØ[Ø™ M·=·³EWCqšqš
ææW=ÍUÍU¬'qš¬ ÇžÇžææ·ʻ³E·§™ ·ÿ·ʻ²æƒ ·U™
·&¬'qšU·ßàq88ZW=ææ·&·ïqšææq8Çž·2…áƒ ™·™
·yä©‹+·ʻ™ qšπ·…áqšqš·Uq8€uW=qš7£‹+³Eqš€u
qš·2‹+·ʻ€u7£ p·§·i£JÇžqš³E¸Ø³EM·9·qšWCÇž
¬'qš‹+Ñ@ÇžßàßZææÑ@·ʻWCßàPÔ³E¬'U··&qšqš·§
·ï9·9·qšææ7£¬'¬'ŒØM·ÇžßàPÔŒØ·ÿƒ ·ÿW=}·‹+
```

Fig. 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.

4.2. 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.

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.

5. 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.

Acknowledgements

This research was supported/partially supported by [Name of Foundation, Grant maker, Donor]. We thank our colleagues from [Name of the supporting institution] who provided insight and expertise that greatly assisted the research, although they may not agree with all of the interpretations/conclusions of this paper. We thank [Name Surname, title] for assistance with [particular technique, methodology], and [Name Surname, position, institution name] for comments that greatly improved the manuscript.

Author contributions

Andri Sukmaindrayana: Conceptualization, Methodology, Software, Data curation, Writing-Original draft preparation, Software, Validation., Field study **Aneu Yulianeu:** Visualization, Investigation, Writing-Reviewing and Editing.

Conflicts of interest

We confirm that there is no conflict of interest associated with this manuscript and there has been no significant financial support fit toward this work that could have influenced its outcome. We also authorize that the manuscript has been read and approved by all authors, including its order of authors list. We declare that this manuscript has not been published before and is not currently being considered for publication elsewhere.

References

[1] M. Ienca and P. Haselager, "Hacking the brain: brain–computer interfacing technology and the ethics of neurosecurity," *Ethics Inf. Technol.*, vol. 18, no. 2, pp. 117–129, 2016.

[2] M. E. Whitman and H. J. Mattord, *Principles of Information Security*. Cengage Learning, 2021.

[3] A. McLeod and D. Dolezel, "Cyber-analytics: Modeling factors associated with healthcare data breaches," *Decis. Support Syst.*, vol. 108, pp. 57–68, 2018.

[4] M. G. Cains, L. Flora, D. Taber, Z. King, and D. S. Henshel, "Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context using Expert Elicitation," *Risk Anal.*, vol. 42, no. 8, pp. 1643–1669, Aug. 2022.

[5] A. Aloraini and M. Hammoudeh, "A Survey on Data Confidentiality and Privacy in Cloud Computing," in *Proceedings of the International Conference on Future Networks and Distributed Systems*, 2017.

[6] L. Yang, N. Elisa, and N. Eliot, "Chapter 7 - Privacy and Security Aspects of E-Government in Smart Cities," D. B. Rawat and K. Z. B. T.-S. C. C. and P. Ghafoor, Eds. Elsevier, 2019, pp. 89–102.

[7] L. Kim, "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, and M. J. Ball, Eds. Cham: Springer International Publishing, 2022, pp. 391–410.

[8] A. Panigrahi, A. K. Nayak, and R. Paul, "Issues and Challenges of Classical Cryptography in Cloud Computing," in *Machine Learning Approach for Cloud Data Analytics in IoT*, 2021, pp. 143–165.

[9] T. Varshney, N. Sharma, I. Kaushik, and B. Bhushan, "Authentication & Encryption Based Security Services in Blockchain Technology," in *2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*, 2019, pp. 63–68.

[10] A. Tchernykh, U. Schwiegelsohn, E. Talbi, and M. Babenko, "Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability," *J. Comput. Sci.*, vol. 36, p. 100581, 2019.

[11] S. Rani and H. Kaur, "Technical Review on Symmetric and Asymmetric Cryptography Algorithms," *Int. J. Adv. Res. Comput.*, vol. 8, no. 4, pp. 182–186, 2017.

[12] P. Sethi and V. Kapoor, "A Proposed Novel Architecture for Information Hiding in Image Steganography by Using Genetic Algorithm and Cryptography," *Procedia Comput. Sci.*, vol. 87, pp. 61–66, 2016.

[13] K. D. Abel, S. Misra, A. Agrawal, R. Maskeliunas, and R. Damasevicius, "Data Security Using Cryptography and Steganography Technique on the Cloud," *Lect. Notes Electr. Eng.*, vol. 834, no. 6, pp. 475–481, 2022.

[14] M. S. Taha, M. S. Mohd Rahim, S. A. Lafta, M. M. Hashim, and H. M. Alzuabidi, "Combination of Steganography and Cryptography: A short Survey," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 518, no. 5, p. 52003, 2019.

[15] C. M. S. Tan, G. P. Arada, A. C. Abad, and E. R. Magsino, "A Hybrid Encryption and Decryption Algorithm using Caesar and Vigenere Cipher," *J. Phys. Conf. Ser.*, vol. 1997, no. 1, p. 12021, 2021.

[16] Z. Qowi and N. Hudallah, "Combining caesar cipher and hill cipher in the generating encryption key on the vigenere cipher algorithm," *J. Phys. Conf. Ser.*, vol. 1918, no. 4, p. 42009, 2021.

[17] R. I. Masya, R. F. Aji, and S. Yazid, "Comparison of Vigenere Cipher and Affine Cipher in Three-pass Protocol for Securing Image," in *2020 6th International Conference on Science and Technology (ICST)*, 2020, vol. 1, pp. 1–5.

[18] P. N. Lone, D. Singh, V. Stoffová, D. C. Mishra, U. H. Mir, and N. Kumar, "Cryptanalysis and Improved Image Encryption Scheme Using Elliptic Curve and Affine Hill Cipher," *Mathematics*, vol. 10, no. 20. 2022.

[19] F. Mallouli, A. Hellal, N. S. Saeed, and F. A. Alzahrani, "A Survey on Cryptography: Comparative Study between RSA vs ECC Algorithms, and RSA vs El-Gamal Algorithms," in *2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/ 2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)*, 2019, pp. 173–176.

[20] T. S. Obaid, "Study A Public Key in RSA Algorithm," *Eur. J. Eng. Technol. Res.*, vol. 5, no. 4 SE-Articles, pp. 395–398, Apr. 2020.

[21] M. M. Taher, A. R. B. H. J. Ahmad, R. S. Hameed, and S. S. Mokri, "a Literature Review of Various Steganography Methods," *J. Theor. Appl. Inf. Technol.*, vol. 100, no. 5, pp. 1412–1427, 2022.

[22] I. Gunawan, Sumarno, H. S. Tambunan, E. Irawan, H. Qurniawan, and D. Hartama, "Combination of Caesar Cipher Algorithm and Rivest Shamir Adleman Algorithm for Securing Document Files and Text Messages," *J. Phys. Conf. Ser.*, vol. 1255, no. 1, p. 12077, 2019.

[23] P. N. Lone, D. Singh, and U. H. Mir, "A novel image encryption using random matrix affine cipher and the chaotic maps," *J. Mod. Opt.*, vol. 68, no. 10, pp. 507–521, Jun. 2021.

[24] A. Purnomo Sidik, S. Efendi, and S. Suherman, "Improving One-Time Pad Algorithm on Shamir's Three-Pass Protocol Scheme by Using RSA and ElGamal Algorithms," *J. Phys. Conf. Ser.*, vol. 1235, no. 1, p. 12007, 2019.

[25] A. E. Mezher, "Enhanced RSA cryptosystem based on multiplicity of public and private keys," *Int. J. Electr. Comput. Eng.*, vol. 8, no. 5, pp. 3949–3953, 2018.

[26] H. Kim, J. S. Sefcik, and C. Bradway, "Characteristics of Qualitative Descriptive Studies: A Systematic Review," *Res. Nurs. Health*, vol. 40, no. 1, pp. 23–42, Feb. 2017.

[27] M. Rizwan and M. Iqbal, "Application of 80/20 Rule in Software Engineering Rapid Application Development (RAD) Model BT - Software Engineering and Computer Systems," 2011, pp. 518–532.

[28] R. Rahayu, E. W. Abbas, and J. Jumriani, "Social Studies Lesson Planning for Children with Intellectual Disabilities in the Pembina State Special School of South Kalimantan Province," *Kalimantan Soc. Stud. J.*, vol. 2, no. 2, pp. 160–169, 2021.

[29] M. Sarkar and S. Ghosh, "Development of a secured optical code-division multiple access system by implementing hybrid 2D-modified Walsh code," *Opt. Eng.*, vol. 59, no. 10, p. 106107, Oct. 2020.

[30] P. Singh, R. Kumar, A. K. Yadav, and K. Singh,

"Security analysis and modified attack algorithms for a nonlinear optical cryptosystem based on DRPE," *Opt. Lasers Eng.*, vol. 139, p. 106501, 2021.

[31] A. R. Tuasikal, D. Indra, and F. Fattah, "Analisis Perbandingan Known Plaintext dan Chosen Plaintext Pada Metode Hill Chiper," *Bul. Sist. Inf. dan Teknol. Islam (BUSITI); Vol 1, No 1 (2020)DO - 10.33096/busiti.v1i1.514* , Feb. 2020.

[32] W. Wei, M. Woźniak, R. Damaševičius, X. Fan, and Y. Li, "Algorithm Research of Known-plaintext Attack on Double Random Phase Mask Based on WSNs," J. Internet Technol. Vol 20, No 1, Jan. 2019.

[33] Latha, S. ., Gundavarapu, M. R. ., Kumar, N. P. ., Parameswari, D. V. L. ., & Reddy, B. R. K. . (2023). Technology for Kisan Samanvayam: Nutrition Intelligibility of Groundnut Plant using IoT-ML Framework. International Journal on Recent and Innovation Trends in Computing and Communication, 11(3), 273–282. https://doi.org/10.17762/ijritcc.v11i3.6345

[34] Prof. Naveen Jain. (2013). FPGA Implementation of Hardware Architecture for H264/AV Codec Standards. International Journal of New Practices in Management and Engineering, 2(01), 01 - 07. Retrieved from http://ijnpme.org/index.php/IJNPME/article/view/11