Volume: 7 Issues: 47 [September, 2022] pp. 132 - 141
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.jised.com
DOI: 10.55573/JISED.074714

REDUCTION-BY-PERCENTAGE COMPRESSION TECHNIQUE FOR REDUCING SIZES OF PLAINTEXT PRIOR TO ENCRYPTION ALGORITHM

Arif Mandangan[1]
Che Haziqah Che Hussin[2*]
Darmesah Gabda[3]
Suriana Lasairaya[4]

[1]Faculty of Science and Natural Resources, Universiti Malaysia Sabah (UMS), Malaysia,
(E-mail: arifman@ums.edu.my)
[2]Preparatory Centre for Science and Technology, Universiti Malaysia Sabah (UMS), Malaysia,
(Email: haziqah@ums.edu.my)
[3]Faculty of Science and Natural Resources, Universiti Malaysia Sabah (UMS), Malaysia,
(E-mail: [3]darmesah@ums.edu.my)
[4]Preparatory Centre for Science and Technology, Universiti Malaysia Sabah (UMS), Malaysia,
(Email: [4]suriana@ums.edu.my)
* Corresponding Author

Article history
Received date : 25-6-2022
Revised date : 1-8-2022
Accepted date : 15-8-2022
Published date : 7-9-2022

To cite this document:
Mandangan, A., Che Hussin, C. H., Gabda, D., & Lasairaya, S. (2022). Reduction-By-Percentage Compression Technique for Reducing Sizes of Plaintext Prior To Encryption Algorithm. *Journal of Islamic, Social, Economics and Development (JISED)*, 7(47), 132 - 141.

Abstract: *Other than security, another major concern in cryptography is efficiency to ensure cryptosystem could be embedded and deployed in various communication devices. Encrypting high numbers of data would consume high computational and storage capacity costs. These issues could affect the efficiency of cryptosystem. One of the approaches to overcome these issues is by integrating data compression technique into cryptosystem. To avoid any encryption and decryption error, lossless compression techniques are deployed in cryptography. The compression techniques are deployed to reduce either the size or number of plaintexts prior to encryption algorithm. Nevertheless, the sizes of the compressed plaintext are still large. To deal with this issue, we proposed a simple technique with ability for reducing the sizes of the compressed plaintext. The inverse of this technique is able to recover the original value of the data without any loss or difference compared to the original data. With smaller sizes, the encryption algorithm would process inputs with smaller sizes, and these could potentially make the encryption algorithm be executed in cheaper computational and storage capacity costs.*

Keywords: *Cryptography, data compression, lossless compression, continued fraction, Euclidean algorithm.*

Volume: 7 Issues: 47 [September, 2022] pp. 132 - 141
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.jised.com
DOI: 10.55573/JISED.074714

Introduction

The role of cryptography in network security becomes more crucial during this pandemic era since most of our daily tasks are done through the Internet. Using cryptography, main security goals such as confidentiality, data integrity, authentication and non-repudiation could be achieved (Abbasi & Singh, 2021). To provide confidentiality, readable data known as plaintext are transformed becomes unreadable data known as ciphertext via encryption algorithm. Then, an authorized sender known as Bob sends the ciphertext to an authorised recipient, known as Alice. In order to read the data, Alice retransforms the ciphertext to become plaintext via decryption algorithm. Both the encryption and decryption algorithms are executed using keys, known as encryption and decryption keys respectively. Other than security, another major concern in cryptography is efficiency to ensure cryptosystem could be embedded and deployed in various communication devices. Encryption of high numbers of data would consume high computational and storage capacity costs, for example in Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA) cryptosystems (Al-Ahdal, 2021). This issue would affect the efficiency of cryptosystem. One of the approaches to overcome this issue is by applying the data compression technique prior to the encryption algorithm (Wahab, et al., 2021; Hameed, et al., 2020; Brindhashree & Prakash, 2020).

Basically, data compression is used to encode data using fewer bits compared to its original bits. Data compression can be categorized as lossy and lossless compressions. Lossy compression techniques are widely used for image, audio and video where lostness of a few bits from the original data after decompression step is acceptable. On the contrary, lossless compression techniques are more suitable to be used in cryptography to ensure the original message could be recovered after decompression stage without any lostness even a single bit of the message. There are several lossless compression techniques have been applied in cryptography. Recently, Huffman coding is applied by Bouguessa et. al (2021) and Abdel Wahab et. al (2021), Lempel-Ziv-Welch (LZW) compression is applied by Rahim et. al (2018) and Novamizanti et. al (2015) while Run Length Encoding (RLE) algorithm is applied by Hasugian et. al (2020) and Elsayed (2014). Using these techniques, the size of original data can be significantly reduced.

Other than reducing the size of data, another approach that worth to be explored is by reducing the numbers of data as done by the Continued Fraction and Euclidean Algorithm (CFEA) compression technique. The CFEA-technique was first applied to the RSA cryptosystem in (Chang & Mandangan, 2013). The CFEA-technique has two stages, namely the compression and decompression stages. In the compression stage, the continued fraction is used to reduce the number of k-plaintext $m_1, m_2, \dots m_k \in \mathbb{Z}^+$, where $k \in N$ and $k > 2$, become only two plaintexts $M_1, M_2 \in \mathbb{Z}^+$ regardless how large is the k. Then, Euclidean algorithm is deployed in the decompression stage to recover the original k-plaintext from the compressed 2-plaintext M_1, M_2. Then, Mandangan et. al (2015) integrated the CFEA-technique on other asymmetric cryptosystems such as the El-Gamal and Elliptic-Curve Cryptography (ECC) cryptosystems. Recently, the CFEA-technique is employed by Siriboonpipattana et al. (2020) and Daud et. al (2020) to improve the efficiency of RSA and Baptista Symmetric Chaotic cryptosystems respectively.

Although the number of plaintexts could be compressed from k-plaintext to only 2-plaintext, the sizes of the compressed 2-plaintext M_1, M_2 are much larger than each of the k-plaintext $m_1, m_2, \dots m_k$. The larger the k is, the larger the sizes of the compressed 2-plaintext M_1 and M_2 (Mandangan, et al., 2014). Although the numbers of the plaintext can be drastically reduced to

Volume: 7 Issues: 47 [September, 2022] pp. 132 - 141
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.jised.com
DOI: 10.55573/JISED.074714

only 2, the large sizes of these compressed-plaintext M_1, M_2 would affect the efficiency of the public-key cryptosystems. Clearly, new effort for reducing the sizes of this compressed plaintext M_1, M_2 is demanded. By reducing the sizes of the compressed 2-plaintext M_1, M_2, there is a prospect for further improving the efficiency of the public-key cryptosystems.

In this paper, we proposed a simple technique for making the size of the compressed 2-plaintext M_1, M_2 smaller than before. The proposed technique, named as Reduction-by-Percentage (RbP) technique, is expected to be able to reduce the sizes of the M_1, M_2 more than 90% than the original sizes. The size reduction is expected would give a significant improvement in terms of computational and storage capacity costs in asymmetric cryptosystems.

Methodology

The idea behind the proposed technique is to reduce the size of the compressed-plaintext prior to the encryption algorithm. In cryptography, it is crucial to ensure that the decrypted ciphertext is exactly the same as the original message without any single difference. That means, lossless compression must be used instead of lossy compression. In this technique, the reduction of the compressed-plaintext is done by reducing its value based on certain percentage. By adding the outcome to the same percentage value, then the original value can be reobtained without losing any single bit of it. The formation of the technique and how its working is discussed in the following sections.

Reduction-by-Percentage Technique

Basically, percentage is a ratio or fraction with denominator that is fixed as 100. The percentage is normally used to represent value of certain portion from the whole amount. The percentage also can be used to make an increment on the whole amount or decrement from the whole amount. Consider the following definition:

Definition 1: *Let* $A, B, p \in \mathbb{R}^+$ *where* $p \in (0,99]$**.** *If* $A - B = \left(\frac{p}{100}\right) B$*, then* A *is larger* $p\%$ *than* B*. If* $A - B = -\left(\frac{p}{100}\right) B$*, then* A *is smaller* $p\%$ *than* B*.*

Based on Definition 1, $p\%$ from B can be added to A to make A larger $p\%$ than B. On the contrary, $p\%$ from B also can be deducted from A to make A smaller $p\%$ than B. From this fact, the Reduction-by-Percentage (RbP) technique is developed. It has two stages, named as reduction stage and recovery stage.

Definition 2: *Let* $M, p \in \mathbb{Z}^+$ *where* $p \in (0,99]$*. The reduction stage in the Reduced-by-Percentage technique is defined as follows,*

$$\widehat{M} = M\left(1 - \frac{p}{100}\right) \in \mathbb{R}^+.$$

Now, consider the following proposition:

Proposition 1: *Let* $M, p \in \mathbb{Z}^+$ *and* $\widehat{M} \in \mathbb{R}^+$ *where* $p \in (0,99]$*. If*

$$\widehat{M} = M\left(1 - \frac{p}{100}\right) > 0,$$

then, $\widehat{M} < M$ *in* $p\%$*.*
Proof

Volume: 7 Issues: 47 [September, 2022] pp. 132 - 141
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.jised.com
DOI: 10.55573/JISED.074714

Note that,

$$\begin{aligned}\widehat{M} - M &= M\left(1 - \frac{p}{100}\right) - M \\ &= M - \frac{Mp}{100} - M \\ &= -\frac{Mp}{100}.\end{aligned}$$

Based on Definition 1, $\widehat{M} < M$ in $p\%$.

Example 1: *Let* $M = 12345$ *and* $p = 75$. *Then,*

$$\widehat{M} = M\left(1 - \frac{p}{100}\right) = 12345\left(1 - \frac{75}{100}\right) = 3086.25$$

Note that,

$$\widehat{M} - M = 12345 - 3086.25 = -9258.75$$

and

$$-\left(\frac{p}{100}\right)M = -\left(\frac{75}{100}\right)12345 = -9258.75.$$

Therefore, $\widehat{M} < M$ *in* 75%.

To recover the original value M, recovery stage in the RbP-technique is required.

Proposition 2: *Let* $p \in \mathbb{Z}^+$ *where* $p \in (0,99]$ *and* $\widehat{M} \in \mathbb{R}^+$ *where*

$$\widehat{M} = M\left(1 - \frac{p}{100}\right).$$

Then, the recovery stage in the Reduced-by-Percentage technique is done as follows,

$$M = \widehat{M}\left(\frac{100}{100 - p}\right).$$

Proof
Since

$$\widehat{M} = M\left(1 - \frac{p}{100}\right),$$

then

$$M = \frac{\widehat{M}}{\left(1 - \frac{p}{100}\right)} = \frac{\widehat{M}}{\left(\frac{100 - p}{100}\right)} = \widehat{M}\left(\frac{100}{100 - p}\right).$$

Example 2: *Let* $\widehat{M} = 3086.25$ *and* $p = 75$. *Then,*

$$M = \widehat{M}\left(\frac{100}{100 - p}\right) = 3086.25\left(\frac{100}{100 - 75}\right) = 12345.$$

Volume: 7 Issues: 47 [September, 2022] pp. 132 - 141
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.jised.com
DOI: 10.55573/JISED.074714

Reducing Sizes of the Compressed Plaintext

As shown in the previous section, the Reduction-by-Percentage (RbP) technique could reduce the value of a number based on a particular percentage in its' reduction stage. By reversing the reduction stage, the actual value of the reduced number could be recovered. This process is done in the recovery stage of the RbP-technique. The recovery stage yields exactly the original number without any change or difference even a single digit. That means, the RbP-technique can be considered as a lossless compression technique. The only issue to be addressed is the reduction stage of the RbP-technique yields a non-integer value, $\widehat{M} \in \mathbb{R}^+$. This issue could limit the application of the RbP-technique in cryptography since the input of the encryption and decryption algorithms are normally in integer forms. Nevertheless, the non-integer $\widehat{M}$ could be ensured as having at most two digits after its decimal point. Consider the following lemma:

Lemma 1: Let $M, p \in \mathbb{Z}^+$ and $\widehat{M} \in \mathbb{R}^+$ such that

$$\widehat{M} = M\left(1 - \frac{p}{100}\right)$$

$p \in (0,99]$. If $M > 100$, then $\widehat{M} = q + s$ where $q \in \mathbb{Z}^+$, $s \in [0,1)$ and s has at most 2 digits after the decimal point.

Proof

Given that,

$$\widehat{M} = M\left(1 - \frac{p}{100}\right).$$

Thus,

$$\widehat{M} = M\left(\frac{100 - p}{100}\right) = \frac{100M - Mp}{100}.$$

Since $p \in \mathbb{Z}^+$ and $p \in (0,99]$, then $100M - Mp > 0$. Denote $100M - Mp = u$ where $u \in \mathbb{Z}^+$.

The smallest value for p is $p = 1$. By letting $p = 1$, we have

$$100M - Mp = M(100 - p) = M(99)$$

Let $M > 100$. Then, $99M > 100$. Thus,

$$\frac{99M}{100} = q_1 + \frac{r_1}{100}$$

where $q_1 \in \mathbb{Z}^+$, $r_1 \in \mathbb{Z}$ and $r_1 \in [0,100)$.

The biggest value for $p = 99$. By letting $p = 99$, we have

$$100M - Mt = M(100 - 99) = M$$

Volume: 7 Issues: 47 [September, 2022] pp. 132 - 141
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.jised.com
DOI: 10.55573/JISED.074714

Since $M > 100$, then

$$\frac{M}{100} = q_2 + \frac{r_2}{100}$$

where $q_2 \in \mathbb{Z}^+$, $r_2 \in \mathbb{Z}$ and $r_2 \in [0,100)$. Note that, $q_1, q_2 \in \mathbb{Z}^+$ and $r_1, r_2 \in [0,100)$.

Therefore,

$$\widehat{M} = q + s$$

where $q \in \mathbb{Z}^+$, $s \in \mathbb{Q}$ and $s \in [0,1)$. Since

$$s = \frac{r}{100}$$

where $r \in \mathbb{Z}$ and $r \in [0,100)$, then s has at most 2 digits after the decimal point.

As proven in Lemma 1, the reduced number $\widehat{M}$ can be guaranteed as having only 2 digits after its decimal point by ensuring that the value of M is larger than 100.

By considering the results from Lemma 1, we proposed a strategy to combine the RbP-technique with the CFEA-technique. The idea is to use the CFEA-technique to compress the numbers of plaintext from k-plaintext, $m_1, m_2, \dots, m_k \in \mathbb{Z}^+$ where $k \in N$ and $k > 2$, to only 2-plaintext $M_1, M_2 \in \mathbb{Z}^+$. Then, the RbP-technique is deployed to reduce the size of the compressed 2-plaintext M_1, M_2 based on certain percentages, for instance, $p\%$. Thus, the reduction stage reduces the plaintext M_1 becomes $\widehat{M}_1 \in \mathbb{R}^+$ where $\widehat{M}_1$ is $p\%$ smaller than M_1. Similarly, the reduction stage reduces the plaintext M_2 becomes $\widehat{M}_2 \in \mathbb{R}^+$ where $\widehat{M}_2$ is $p\%$ smaller than M_2. Note that, $\widehat{M}_1, \widehat{M}_2 \in \mathbb{R}^+$ with at most 2 digits after the decimal points of these numbers. A shown in Lemma 1, both plaintext $\widehat{M}_1$ and $\widehat{M}_2$ can be represented as,

$$\widehat{M}_1 = q_1.s_1, \text{ and } \widehat{M}_2 = q_2.s_2$$

where $q_1, q_2 \in \mathbb{Z}^+$ are quotient parts of $\widehat{M}_1$ and $\widehat{M}_2$ respectively, while $s_1, s_2 \in \mathbb{Z}^+$ are the digits in the decimal parts of $\widehat{M}_1$ and $\widehat{M}_2$ respectively. Note that, each s_1 and s_2 has at most two digits. By separating the quotient part and the decimal part of the reduced 2-plaintext $\widehat{M}_1, \widehat{M}_2$ and putting these values as ordered pair, then we have the following smaller plaintext,

$$\widehat{M}_1' = (q_1, s_1), \text{ and } \widehat{M}_2' = (q_2, s_2).$$

To demonstrate the encryption and decryption algorithm, let e_k as an encryption function with encryption key k and $d_{k'}$ as a decryption function with decryption key k'. Thus, encryption on $\widehat{M}_1'$ yields 2-ciphertext $(C_{1,1}, C_{1,2})$ as,

$$e_k(q_1) = C_{1,1} \text{ and } e_k(s_1) = C_{1,2}.$$

Similarly, encryption on $\widehat{M}_2'$ yield 2-ciphertext $(C_{2,1}, C_{2,2})$ as,

$$e_k(q_1) = C_{1,1} \text{ and } e_k(s_2) = C_{1,2}.$$

Volume: 7 Issues: 47 [September, 2022] pp. 132 - 141
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.jised.com
DOI: 10.55573/JISED.074714

To read the message, the ciphertext pairs $(C_{1,1}, C_{1,2})$ and $(C_{2,1}, C_{2,2})$ are decrypted as,

$$d_{k'}(C_{1,1}) = q_1, d_{k'}(C_{1,2}) = s_1,$$
$$d_{k'}(C_{2,1}) = q_2, d_{k'}(C_{2,2}) = s_2.$$

Then, the reduced 2-plaintext can be reformed as $\widehat{M}_1' = (q_1, s_1)$ and $\widehat{M}_2' = (q_2, s_2)$. Then, recovery stage of the RbP-technique is used to recover the compressed 2-plaintext M_1, M_2. Finally, decompression stage of the CFEA-technique is used to recover all the original messages $m_1, m_2, \dots, m_k$. The proposed strategy can be illustrated in the following table:

Table 1: A Strategy to Combine the CFEA and RbP Techniques in an Asymmetric Cryptosystem

Suppose that Bob wants to send k-plaintext $m_1, m_2, \dots, m_k \in \mathbb{Z}^+$ to Alice. They agree to use an asymmetric cryptosystem with integrated CFEA and RbP techniques.	
Alice (authorized recipient)	**Bob (authorized sender)**
Perform key generation algorithm	
Sends encryption key k to Bob and keeps decryption key k' privately.	Deploys the compression stage of the CFEA-technique to compresses the k-plaintext $m_1, m_2, \dots, m_k$ and obtain the compressed 2-plaintext M_1, M_2.
	Deploys the reduction stage of the RbP-technique to reduce the compressed 2-plaintext M_1, M_2 and obtain the reduced 2-plaintext $\widehat{M}_1, \widehat{M}_2$.
	Represent the reduced 2-plaintext $\widehat{M}_1, \widehat{M}_2$ as $\widehat{M}_1' = (q_1, s_1)$ and $\widehat{M}_2' = (q_2, s_2)$.
	Encrypts the plaintext $\widehat{M}_1'$ and $\widehat{M}_2'$ as follows; $e_k(q_1) = C_{1,1}, e_k(s_1) = C_{1,2}$, $e_k(q_1) = C_{1,1}, e_k(s_2) = C_{1,2}$ and forms the ordered pairs of ciphertext $(C_{1,1}, C_{1,2})$ and $(C_{2,1}, C_{2,2})$.
	Sends $(C_{1,1}, C_{1,2})$ and $(C_{2,1}, C_{2,2})$ to Alice
Decrypts the ciphertext pairs $(C_{1,1}, C_{1,2})$ and $(C_{2,1}, C_{2,2})$ as follows, $d_{k'}(C_{1,1}) = q_1, d_{k'}(C_{1,2}) = s_1$, $d_{k'}(C_{2,1}) = q_2, d_{k'}(C_{2,2}) = s_2$.	
Reform the plaintext $\widehat{M}_1' = (q_1, s_1)$ and $\widehat{M}_2' = (q_2, s_2)$. Then, reform the reduced 2-plaintext $\widehat{M}_1 = q_1.s_1$ and $\widehat{M}_2 = q_2.s_2$.	
Deploys the recovery stage of the RbP-technique to recover the compressed 2-plaintext M_1, M_2.	
Deploys the decompression stage of the CFEA-technique to obtain all the k-plaintext, $m_1, m_2, \dots, m_k$.	

Volume: 7 Issues: 47 [September, 2022] pp. 132 - 141
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.jised.com
DOI: 10.55573/JISED.074714

Example 3: For $k = 10$, suppose that $21, 34, 78, 16, 23, 77, 54, 29, 12, 73 \in \mathbb{Z}^+$ be the 10-plaintext. Compression stage of the CFEA-technique yields,

$$21 + \cfrac{1}{34 + \cfrac{1}{78 + \cfrac{1}{16 + \cfrac{1}{23 + \cfrac{1}{77 + \cfrac{1}{54 + \cfrac{1}{29 + \cfrac{1}{12 + \frac{1}{73}}}}}}}}} = \frac{2188211927177063}{104054887712319} = \frac{M_1}{M_2}.$$

Then, reduce the compressed 2-plaintext M_1, M_2 by 95% in the reduction stage of the RbP-technique yields,

$$\widehat{M}_1 = M_1\left(1 - \frac{p}{100}\right) = 2188211927177063\left(1 - \frac{95}{100}\right) = 109410596358853.15$$

$$\widehat{M}_2 = M_2\left(1 - \frac{p}{100}\right) = 104054887712319\left(1 - \frac{95}{100}\right) = 5202744385615.95$$

Now, represent the reduced 2-plaintext $\widehat{M}_1$ and $\widehat{M}_2$ as follows,

$$\widehat{M}_1' = (q_1, s_1) = (109410596358853, 15), \widehat{M}_2' = (q_2, s_2) = (5202744385615, 95).$$

Encryption on $\widehat{M}_1'$ yield 2-ciphertext $(C_{1,1}, C_{1,2})$ as follows,

$$e_k(109410596358853) = C_{1,1}, e_k(15) = C_{1,2}.$$

Similarly, encryption on $\widehat{M}_2'$ yields 2-ciphertext $(C_{2,1}, C_{2,2})$ as follows,

$$e_k(5202744385615) = C_{1,1}, e_k(95) = C_{1,2}.$$

To read the message, the ciphertext $(C_{1,1}, C_{1,2})$ and $(C_{2,1}, C_{2,2})$ are decrypted as follows,

$$d_{k'}(C_{1,1}) = 109410596358853, d_{k'}(C_{1,2}) = 15,$$

$$d_{k'}(C_{2,1}) = 5202744385615, d_{k'}(C_{2,2}) = 95.$$

Thus, the reduced 2-plaintext can be reformed as $\widehat{M}_1 = 109410596358853.15$ and $\widehat{M}_2 = 5202744385615.95$. Then, recovery stage of the RbP-technique is used to recover the compressed 2-plaintext $M_1 = 2188211927177063, M_2 = 104054887712319$. Finally, decompression stage of the CFEA-technique recovers all the original messages as follows,

$$\begin{aligned}
2188211927177063 &= 104054887712319(21) + 3059285218364, && m_1 = 21\\
104054887712319 &= 3059285218364(34) + 39190287943, && m_2 = 34\\
3059285218364 &= 39190287943(78) + 2442758810, && m_3 = 78
\end{aligned}$$

Volume: 7 Issues: 47 [September, 2022] pp. 132 - 141
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.jised.com
DOI: 10.55573/JISED.074714

$$39190287943 = 2442758810(16) + 106146983, \quad m_4 = 16$$
$$2442758810 = 106146983(23) + 1378201, \quad m_5 = 23$$
$$106146983 = 1378201(77) + 25506, \quad m_6 = 77$$
$$1378201 = 25506(54) + 877, \quad m_7 = 54$$
$$25506 = 877(29) + 73, \quad m_8 = 29$$
$$877 = 73(12) + 1, \quad m_9 = 12.$$
$$73 = 1(73) + 0, \quad m_{10} = 73.$$

Observe that, $m_1, m_2, m_3, m_4, m_5, m_6, m_7, m_8, m_9, m_{10} = 21,34,78,16,23,77,54,29,12,73$, exactly similar to the original 10-plaintext.

Conclusion

In this paper, we proposed a Reduction-by-Percentage (RbP) technique with the ability for reducing the value and size of any number based on the fixed percentage value. By reversing the process, the original value of the reduced number could be reobtained without any changes compared to its original value. It means that the RbP-technique could be considered as a lossless compression technique. Hence, this technique is potentially applicable in cryptography for reducing the sizes of plaintext prior to the encryption algorithm. Moreover, we suggested a strategy for combining the RbP-techniques with the Continued-Fraction-Euclidean-Algorithm (CFEA)-technique to reduce not only the number of the plaintext from k-plaintext to only 2-plaintext, but also to reduce the size of the compressed 2-plaintext to make it smaller before performance of the deployed cryptosystem. To verify this claim, thorough efficiency analysis on asymmetric cryptosystems with integrated RbP and CFEA techniques is suggested as future work. Moreover, other strategy for embedding the CFEA and RbP techniques in cryptosystem also would be interesting to be explored.

Acknowledgement

The authors would like to send gratitude to anonymous reviewers for constructive comments for the betterment of this paper. This research is supported by Universiti Malaysia Sabah under the research grant SBK0508-2021 and XXXXX-2021.

References

Abbasi, F. & Singh, P. (2021). Cryptography: Security and Integrity of Data. *Journal of Management and Service Science*, *1*(2), p.4.

AbdelWahab, O.F., Hussein, A.I., Hamed, H.F., Kelash, H.M. & Khalaf, A.A. (2021). Efficient Combination of RSA Cryptography, Lossy, and Lossless Compression Steganography Techniques to Hide Data. *Procedia Computer Science*, *182*, pp.5-12.

Al-Ahdal, A.H. (2021). Security Analysis of a Robust Lightweight Algorithm for Securing Data in Internet of Things Networks. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(12), pp.133-143.

Bouguessa, A., Said, N.H. & Pacha, A.A. (2021). Proposition of new secure data communication technique based on Huffman coding, chaos and LSB. *International Journal of Biometrics*, *13*(2-3), pp.343-365.

Brindhashree, K. & Prakash, S.J. (2020). Data security based on cryptography steganography combined with OTP algorithm and Huffman coding in the cloud environment. *International Research Journal of Modernization in Engineering Technology and Science*, *2*(10).

Daud, M. A., Mahad, Z, Rasit, M. R. A. & Asbullah, M. A. (2020), Nov. Use of the CFEA Lossless Data Compression Method in Transmitting Encrypted Modified Baptista

Volume: 7 Issues: 47 [September, 2022] pp. 132 - 141
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.jised.com
DOI: 10.55573/JISED.074714

Symmetric Chaotic Cryptosystem Data. *ASM Sc. J.*, 13. https://doi.org/10.32802/asmscj.2020.sm26(4.29)

Elsayed, H.A. (2014). Burrows-Wheeler Transform and combination of Move-to-Front coding and Run Length Encoding for lossless audio coding. In *2014 9th International Conference on Computer Engineering & Systems (ICCES)* (pp. 354-359). IEEE.

Hameed, M.E., Ibrahim, M.M., Manap, N.A. & Mohammed, A.A. (2020). An enhanced lossless compression with cryptography hybrid mechanism for ECG biomedical signal monitoring. *International Journal of Electrical & Computer Engineering (2088-8708)*, *10*(3).

Hasugian, P.M., Simangunsong, P.B.N., Panjaitan, M.I., Wahyuni, D. & Rezky, S.F. (2020). Combination of Cryptography Algorithm Knapsack and Run Length Enconding (RLE) Compression in Treatment of Text File. In *Journal of Physics: Conference Series* (Vol. 1573, No. 1, p. 012017). IOP Publishing.

Chang E. H. & Mandangan, A. (2013). Compression-RSA: New approach of encryption and decryption method. In *AIP Conference Proceedings* (Vol. 1522, No. 1, pp. 50-54). American Institute of Physics.

Mandangan, A., Loh, C.M., Chang, E. H. & Che Hussin, C.H. (2014). Compression-RSA technique: A more efficient encryption-decryption procedure. In *AIP Conference Proceedings* (Vol. 1602, No. 1, pp. 50-55). American Institute of Physics.

Mandangan, A., Loh, C.M., Chang, E.H. & Che Hussin, C.H.C. (2015). CFEA-Technique: Smaller Size of the Compressed Plaintext. *International Journal of Cryptology Research*, *5*(1), pp.1-10.

Novamizanti, L., Budiman, G. & Tritoasmoro, I.I. (2015). Designing secured data using a combination of LZW compression, RSA encryption, and DCT steganography. In *2015 1st International Conference on Wireless and Telematics (ICWT)* (pp. 1-6). IEEE.

Rahim, R., Adyaraka, D., Sallu, S., Sarimanah, E., Hidayat, A., Sewang, A. & Hartinah, S. (2018). An application data security with lempel-ziv welch and blowfish. *Int. J. Eng. Technol*, *7*(9), pp.71-73.

Singh, S., Sharma, P.K., Moon, S.Y. & Park, J.H. (2017). Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions. *Journal of Ambient Intelligence and Humanized Computing*, pp.1-18.

Siriboonpipattana, W., Soomlek, C. & Seresangtakul, P. (2020). Increasing the input data length of RSA cryptosystem by applying a hybrid lossless data compression algorithm. In *Journal of Physics: Conference Series* (Vol. 1502, No. 1, p. 012036). IOP Publishing.

Wahab, O.F.A., Khalaf, A.A., Hussein, A.I. & Hamed, H.F. (2021). Hiding Data Using Efficient Combination of RSA Cryptography, and Compression Steganography Techniques. *IEEE Access*, *9*, pp.31805-31815.