CRYPTOGRAPH RSA AND COMPRESSION SHANNON FANO TEXT FILE SERVICES AT MOBILE DEVICES

Dwi Kuswanto
Jurusan Teknik Informatika, Universitas Trunojoyo Madura

Jl. Raya Telang, PO BOX 2, Kamal, Bangkalan-69192

E-mail: dwi.kuswanto@trunojoyo.ac.id

Abstract. Text File Services is still an option for sending a message, the visible difference between Text File Services and other services besides the file size of sending messages is the security level. In Instant Messenger there are features to secure conversations with various Cryptograph methods, while Text File Services does not have that feature. Therefore made Text File Services with additional features Cryptograph. Cryptograph method used is the RSA algorithm. The RSA algorithm makes the plaintext increase in the number of characters, so the Compression feature needs to be added to suppress the increase in the number of characters. Shannon Fano is a Compression symbol wise algorithm where each character that is compressed is converted into a new binary code. This compression is intended to reduce the number of Encryption result characters. The results of this study obtained information that the RSA and Shannon Fano methods can be implemented in the text file service, with the longer key being used the longer the process of decryption of messages with the average value of the avalanche effect ciphertext and the result of Compression is relatively the same. The key length used for the possibility of Brute Force is positively correlated with an average Test Compression Ratio of 1.41 and space-saving of 29.37%.

Kata kunci: Cryptograph, RSA, Compression, Shannon Fano, Layanan text file

1. Introduction
Communication is an activity to convey information to others. Along with the development of the times along with the development of ways of delivering information. Text File Services is one way to convey information.

The development of mobile devices today also develops to adjust the development of the internet network. Mobile devices are very supportive for text file service applications, but on mobile devices with various operating systems there must be a built-in feature to deliver messages with text file services.

The difference between Text File Services and other services besides the file size of sending messages is the level of security in sending messages. In the Text File Services still have shortcomings, one of which is the lack of security in the delivery of messages because the message sent will be sent whatever in accordance with what has been typed by the sender. This can cause information to be leaked.

Researchers conducted this research to overcome the two problems that have been mentioned namely: security and message compression, so messages sent cannot be read directly by unauthorized persons without security keys, and messages to be sent are compressed so as to reduce the size of service delivery files text file.
Cryptograph method used is the RSA method. This method has two key combinations for Encryption namely public key and decryption namely private key, the complexity of this method lies in factoring large numbers into prime number factors.

With the RSA method the message delivered is converted into number values so that what should be 1 character will be several number characters so that it will multiply the number of characters to send a message, that is the need to add the Compression method in this study by testing the use of key bit lengths that are most appropriate, the level of avalanche effect, brute force, compression ratio and space-saving.

2. Related Work

2.1. Cryptograph

According to Estik Lestari in Erick Ruliyanto Sardju, Encryption is the process of securing data or information. In other words randomize data or information so that it cannot be read by other parties [3].

RSA is an Asymmetric Encryption method using two keys, public key and private key. These keys are in the form of prime numbers which are the security points of the RSA method. The security of the RSA method lies in factoring large numbers into prime number factors.

Some variables in the RSA algorithm:
- \( p \) = prime number of private key generator. Confidential.
- \( q \) = prime number of private key generator. Confidential.
- \( e \) = prime number for the public key (Encryption key). Are not confidential.
- \( n \) = combination of public and private keys. Are not confidential.
- \( \varphi \) (euler) = private key generator. Confidential.
- \( d \) = private key (decryption key). Confidential.

The public key is a combination of values (e and n), whereas the private key is a combination (d and n) with the RSA algorithm:

\[
\text{encrypt} = \text{plaintext}^e \mod n \tag{1}
\]
\[
\text{decrypt} = \text{ciphertext}^d \mod n \tag{2}
\]

Information:
- \( e \) = public key.
- \( d \) = private key.
- \( n \) = combination of public and private keys.

2.2. Compression

Shannon Fano is a lossless algorithm. This algorithm uses the occurrence frequency to form the binary tree that is used for Compression, the way to form the binary tree for the Shannon Fano algorithm starting from the root to the node.

Formation of the Shannon Fano binary tree algorithm as follows:
- Count the number of characters used in the data.
- Sorting large data to small.
- The total is divided into two.
- Repeated until getting the final knot.

3. Design Model

3.1. Design System
Figure 1. Design system Sender and Receiver

Message sending (left) starts from entering the destination number and the message to be sent, if both have been filled then enter the public key (the key for Encryption), then the Encryption and Compression process will be carried out and the message has been encrypted and Compression obtained.

Receiving messages (right), recipients will receive messages that have been Encrypted and Compression, then enter the private key (the key for decryption), the message will be processed so that it can produce the plaintext that is sent.

3.2. Flowchart Generate Key RSA
Generate key for the RSA algorithm, is done by first filling in the values of p, q, e, then checking, if p, q, e are prime numbers, the process will proceed by finding the values of n and e, u, the value of n is obtained from p * q, if e, u is obtained from (p-1) * (q-1), then a calculation is made where the first value d is 1, this process looks for new e and d values, when e! = 1 the calculation will continue, until e = 1, and the last d value is the private key value. A public key (e and n) and private key (d and n) are obtained.

3.3 Pengujian
- Avalanche Effect

Avalanche effect is the ratio of ciphertext bits that change due to changes in character in the plaintext or key used [12].

\[
\text{avalanche effect} = \frac{\text{No. of flipped bits in the chippered text}}{\text{No. of bits in the chippered text}} \times 100\% 
\] (3)

- Brute Force

Brute Force is one way crackers use to guess certain keywords. The process is done by guessing in the order of a combination of passwords.

\[
\text{brute force} = \frac{0.5 \times \text{enkripsi} \times \text{x} \times \text{sum} \times \text{x} \times \text{maximal bit key}}{365 \times 24 \times 3600} 
\] (4)

- Ratio Compression

Ratio Compression is the ratio between compressed and uncompressed data.

\[
\text{ratio compression} = \frac{\text{bit size before compression}}{\text{bit size compression}} 
\] (5)

- Space-saving

Space-saving is how much space can be saved after Compression.
\[
\text{space saving} = \left(1 - \frac{\text{bit size compression}}{\text{bit size before compression}}\right) \times 100\% \tag{6}
\]

4. Result and Discussion

4.1. Test Encryption, Compression and Transferring.
The plaintext used is "Trunojoyo University located on Madura Island, located in Kamal District, Bangkalan District. Existing faculties of Law, Economics, Agriculture, Engineering, ISIB, Teacher Training. "With a character length of 169 characters, all messages can be sent.

![Test Diagram result Encryption and Compression](image)

Figure 3. Test Diagram result Encryption and Compression

Figure 3 can be seen from the results of Encryption and Compression using the same plaintext length.

4.2. Test Avalanche Effect
The results obtained from the Encryption (ciphertext) process and the operating results of ciphertext, the results are converted into bits and then compared using XOR logic, calculated how many changes occur and divided by the total number of bits (avalanche effect formula).

![Avalanche Effect Tests](image)

Figure 4. Test Diagram Avalanche Effect

In Figure 4, the avalanche effect for ciphertext (result Encryption) is explained between 4.62\% - 29.36\%, as for the Compression result of ciphertext ranges from 8.53\% -27.18\%.
In Figure 5 it is explained that the longer the key bits used, the longer the time needed to try all possible keys by brute force. Test Ratio and *Space-saving*.

Figure 6 shows the ratio of each test between 1.37-1.45.

Figure 7 shows the value of space-saving for each test between 27.29% -31.45%.
5. Conclusion
From the research it can be concluded that the following RSA and Shannon Fano methods can be implemented in the text file service, with the longer key being used the longer the process of message decryption with the average value of the avalanche effect ciphertext and the result of Compression is relatively the same. The key length used for the possibility of Brute Force is positively correlated with an average Test Compression Ratio of 1.41 and space-saving of 29.37%.

6. References
[1] Lamorahan, Christine., Pinontoan, Benny. and Nainggolan, Nelson. 2013. Data Compression Using Shannon Fano Algorithm. FMIPA UNSRAT.
[2] Adhitama, Gagarin. PERBANDINGAN ALGORITMA HUFFMAN DENGAN ALGORITMA SHANNON FANO. Institut Teknologi Bandung.
[3] Sardju, Erick Ruliyanto., Magdalena, Rita. and Atmaja, Ratri. IMPLEMENTASI ALGORITMA RSA UNTUK ENCRYPTION AND DEKRIPSI SMS (SHORT MESSAGE SERVICE) PADA PERANGKAT MOBILE BERBASIS ANDROID. Universitas Telkom.
[4] Alamanda, Chlara., Cahyani, Niken Dwi. and Abdurohman, Maman. 2008. IMPLEMENTASI ALGORITMA RSA DALAM ENCRYPTION AND DEKRIPSI SMS DI HANDPHONE BERBASIS JAVA. Universitas Telkom.
[5] Ardiyan, Muhammad., Barmawi, Ari Moesrami. and Sudiharto, Dodi Wisaksono. 2012. IMPLEMENTASI ALGORITMA COMPRESSION HUFFMAN PADA BERKAS DIGITAL RESULT SYSTEM CRYPTOGRAPH RSA. Universitas Telkom.
[6] Haryanto, Heri., Wiryadinata, Romi. and Afif, Muhammad. 2014. Implementasi Kombinasi Algoritma Encryption Aes 128 And Algoritma Compression Shannon Fano. Universitas Tirta Ageng Tirtayasa Cilegon.
[7] Utama, Febrian Budi. 2014. APLIKASI SMS CRYPTOGRAPH DENGAN METODE RSA PADA PERANGKAT MOBILE ANDROID. STMIK AMIKOM Yogyakarta.
[8] Hendry. “Menegenal Euler Phi Function”. 2009. http://hendrydext.blogspot.co.id/2009/09/menegenal-euler-phi-function.html. Diakses pada: 21 Juli 2016, 13.00 WIB.
[9] Wikipedia. “Extended Euclidean Algorithm”. 2016. https://en.wikipedia.org/wiki/Extended_Euclidean_algorithm. Diakses pada: 6 Juli 2016, 12.44 WIB.
[10] P, Dessyanto Boedi. Rustamaji, Heru Cahya. and Nugraha, Muhammad Arif. 2009. APLIKASI COMPRESSION SMS BERASIS JAVA ME DENGAN METODE COMPRESSION LZW-HUFFMAN. UPN “Veteran” Yogyakarta.
[11] Ayuningtyas, Nadhira. IMPLEMENTASI KODE HUFFMAN DALAM APLIKASI COMPRESSION TEKS PADA LAYANAN SMS. Institut Teknologi Bandung.
[12] http://paper.ijcsns.org/07_book/201101/20110116.pdf diakses pada 1 Agustus 2019 pukul 13.59 WIB.