APPLICATION OF GOST ALGORITHM FOR THE SAFETY OF DATA SENDING OF GENERAL ELECTION

Novan Wijaya

Department of Informatics Management, AMIK Multi Data Palembang, Palembang, Indonesia, novan.wijaya@mdp.ac.id

Email Correspondence: novan.wijaya@mdp.ac.id

Received: January 20, 2020 Accepted: June 6, 2020 Published: June 30, 2020

Abstract : The rapid development of the internet has an impact on the security of data sent using internet media. One government agency that uses the internet as data transmission includes the KPU. Data transmission becomes very risky especially the data sent is very important and even confidential. In the internet world, there are many threats and ways to change or retrieve data sent via the internet. Indonesia in particular has conducted direct elections but the data that are in the regions which are the results of recapitulation of the elections will be sent via the internet with a system provided by the KPU. Data from the recapitulation of regional elections becomes very important because it can be changed by intruders. Secure the data sent, methods such as cryptographic techniques that can minimize interference from intruders are needed. One algorithm that can be applied as data security is the GOST algorithm. The GOST algorithm is designed to take a balance between data efficiency and security. Cryptographic techniques that use the GOST algorithm are expected to be able to increase the security of sending election results from various threats without reducing the performance of sending data. The rapid development of the internet has the impact of the security of data sent using internet media. One government agency that uses the internet as data transmission includes the KPU. Data transmission becomes very risky especially the data sent is very important and even confidential. In the internet world, there are many threats and ways to change or retrieve data sent through internet media. Indonesia in particular has conducted direct elections but the data that are in the regions which are the results of recapitulation of the elections will be sent via the internet with a system provided by the KPU. Data from the recapitulation of regional elections becomes very important because it can be changed by intruders. Secure the data sent, methods such as cryptographic techniques that can minimize interference from intruders are needed. One algorithm that can be applied as data security is the GOST algorithm. The GOST algorithm is designed to take a balance between data efficiency and security. Cryptographic techniques that use GOST algorithm can improve the security of sending election results from various threats without reducing the performance of sending data. Election result data that was conducted during the testing was the Ogan Ilir regional election recap data. Tests that have been carried out using the GOST algorithm using WireShark produce stream files sent over the network are not easily identified because they are converted into random strings, so it takes a long time to analyze them.

Keywords : Cryptography, GOST Algorithm, Intruder, Election, Wireshark

Abstrak : Perkembangan internet yang sangat cepat mempunyai dampak diantranya keamanan data yang dikirim menggunakan media internet. Salah satu instansi pemerintahan yang menggunakan internet sebagai pengiriman data diantaranya KPU. Pengiriman data menjadi sangat beresiko terlebih data yang dikirimkan sangat penting bahkan bersifat rahasia. Didunia internet terdapat banyak ancaman serta cara dalam mengubah atau mengambil data yang dikirimkan melalui media internet. Indonesia pada khususnya telah melakukan pemilu secara langsung tetapi data-data yang berada pada daerah yang merupakan hasil rekapitulasi dari pemilu akan dikirimkan melalui internet dengan sistem yang telah disediakan oleh KPU. Data hasil rekapitulasi pemilu suatu daerah menjadi sangat penting dikarenakan bisa diubah oleh *intruder*. Untuk mengamankan data yang dikirimkan diperlukan metode seperti teknik kriptografi yang bisa meminimalisir gangguan dari para *intruder*. Salah satu algoritma yang bisa diterapkan sebagai keamanan data yaitu algoritma *GOST*. Algoritma *GOST* dirancang agar mengambil keseimbangan antara efisiensi dan keamanan data. Teknik kriptografi yang menggunakan algoritma *GOST* mampu meningkatkan keamanan pengiriman data hasil pemilu dari berbagai ancaman tanpa mengurangi performansi dari pengiriman data. Data hasil pemilu yang dilakukan saat pengujian ialah data rekap pilkada Ogan Ilir. Pengujian yang telah dilakukan menggunakan algoritma *GOST* menggunakan *wireshark* menghasilkan *stream file* yang dikirim melalui jaringan tidak mudah diidentifikasi dikarenakan diubah menjadi *string* acak sehingga membutuhkan waktu yang lama untuk menganalisanya.
Kata kunci : Kriptografi, Algoritma *GOST*, *Intruder*, Pemilu, *Wireshark*

Introduction

Internet is a collection of several giant computer networks that enables people to find information. And it is important to keep safe the information sent through the internet especially the data of the result of a general election. Once a certain general election is done, the result will immediately be sent from municipal KPU to provincial KPU or national KPU through internet network (Purwati, 2005). According to UU KPU RI that the result of the general election is recapitulated consecutively from TPS, regency, municipality, province and national (Umum, 2008). Two methods are used in the process of recapitulation: manual and KPU system entry. In the former method, all files are manually sent level by level, while in the latter, the data are input in a special system in KPU. The process of inputting the data is subject to intruders, so it is tightly monitored by both parties (Yasa, 2015).

In Islamic law, ownership of an object or data prevents other people from taking or doing anything to them. Rafi' bin Khadij RA said, "The prophet said: anyone who grows plant on other person's land without permission has no right for the crops, even a little, regardless of his cultivation expense (HR. Abu Dawud)". In other words, an intruder is categorized as *ghasb*, which in Islamic law means taking something from other people by force, and a *ghasb* has no right and authority to see or change anything.

Regional result of the general election is national classified which means that only the authorized people can have access to process the data. Therefore,

high-level security is required. If sent through the internet network, the data are susceptible to attack (Hendrawan, 2016). For safety reason, the sending of the data within the internet network requires a system that can protect the data and confidentiality (Muharyanto & Fatimah, 2018).

Cryptography is a method for keeping the safety and confidentiality of data or messages by using a certain algorithm (Pabokory, Astuti, & Kridalaksana, 2015). for safety and confidentiality reasons, a rapid algorithm is required in sending the result of the general election, so that it can prevent the unauthorized parties (intruders) from accessing the data. A strong algorithm that needs a long time is not suitable to be implemented here, such as asymmetric algorithm (Arrijal, Efendi, & Susilo, 2016). GOST algorithm is designed so that there is a balance between efficiency and data safety. GOST designer modifies the previous basic algorithm (DES) to create a better algorithm in implementing the software (Simatupang & Hasibuan, 2018). GOST has an easier algorithm procedure compared to the DES algorithm. GOST algorithm does not use permutation expansion used in DES, and it uses rotation (cyclic shift rotation) of 11 bits. The implementation of cryptography using GOST algorithm is expected to increase the safety in sending the data of the result of the general election from various threats without reducing the significant performance of data sending (Udoyono & Saepudin, 2018).

Research Methods

Cryptography Definition

Cryptography comes from Greek *cryptos* and *graphien* meaning secret writing. Terminologically, cryptography works by changing and manipulating the data or information into a different form so that it is not understood by unauthorized parties, which makes the data safer (Mukhtar, 2018). The data or information which is readable is called plaintext, and the data or information which has been manipulated using cryptography is called ciphertext. In cryptography, there is a process called encryption, a process of changing the plaintext data or information into ciphertext. And the process of changing ciphertext back to plaintext is called description (Munir, 2019).

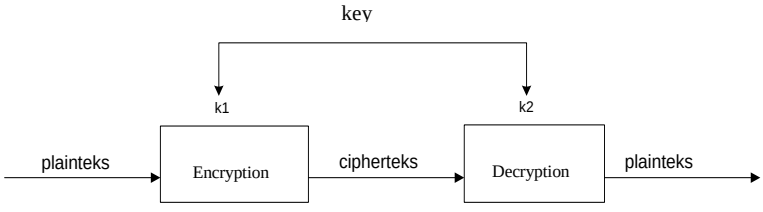

Figure 1. The Encryption and Decryption Progress

Cipher Category Symetrical Keys

Symmetrical Key Algorithm operates in bit mode and is grouped into 2 categories (Sari, Rachmawanto, Utomo, & Sani, 2016):

1. **Stream Chiper**

   Cryptography algorithm operates in plaintext/ciphertext in a single bit, in which the series of bits are encrypted/decrypted bit per bit.
   Examples : RC4, A2, Seal, Wake, etc.

2. **Block Chiper**

   Cryptography algorithm operates in plaintext/ciphertext in the form of blocks, in which the bits are divided into blocks of bits at a certain length.
   Examples: Blowfish, DES, GOST, IDEA, RC6, Safer, Twofish.

GOST Algorithm

GOST Algorithm is a symmetrical algorithm categorized cipher block. GOST stands for 'Gosudarstvennyi Standard" or Government Standard. This algorithm is modified from the earlier basic algorithm design for a better implementation process of algorithm and the bigger microprocessor (32 bits above with big data cache) (Benedict, Budiman, & Rachmawati, 2017).

Rational Unified Process (RUP)

RUP is a good method in software manipulation because RUP assigns anyone responsible for that manipulation. RUP uses the object-oriented concept, in which the steps focus more on the model development process using Unified Model Language (UML) (Wijaya, Irsyad, & Taqwiym, 2017). The design is done using the model development process, that is by making use case diagram to see the interaction between user and system. In figure 2 explain phases of architecture RUP.

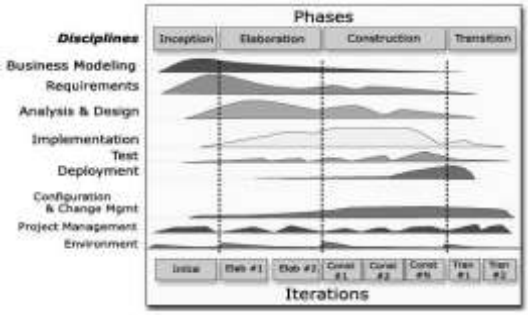

Figure 2. Architecture Rational Unified Process

System Design and Analysis

GOST Algorithm Usage Analysis

GOST Algorithm is used for coding the data of the result of the general election so that the data sent by the network is safe. The application set up

consists of 2 parts: Client and server. The process of coding or encryption is done by the client before the data is sent. This way the data sent is in the form of ciphertext or coded data (Anas, Nanda, & Hidayat, 2019). Then the server decrypts the ciphertext data received to make it plaintext (readable data) (figure 3).

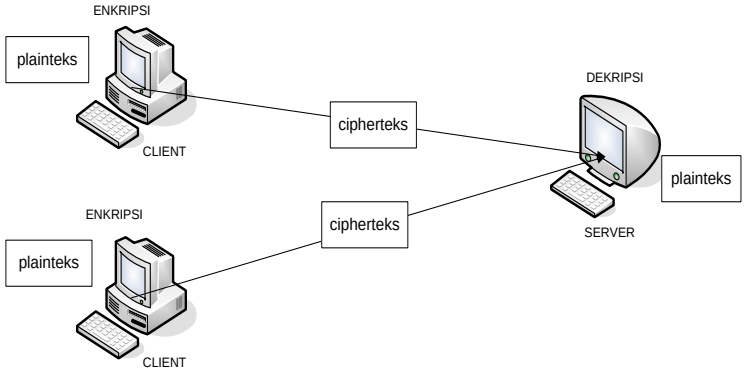

Figure 3. Encryption and Decryption Process on Client and Server

Use Case Diagram

Use case diagram depicts the interaction done by the actor to the set-up system (Wijaya, 2017). Figure 4 shows that the actor "server user" can interact with the system by activating the process, sending messages, receiving data, processing files and deactivating the process. Meanwhile, the system client actor can only send and receive data.

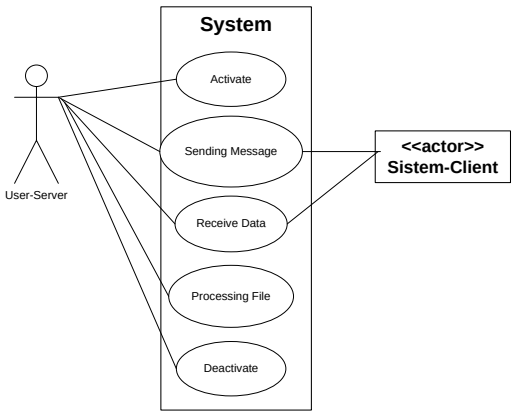

Figure 4. Client-System Use Case Diagram

Use case diagram server system (figure 5) describes the interaction between "client user" actor and 'system server" actor. Both actors can interact with the system, such as: connecting, sending messages, sending files, and disconnecting.

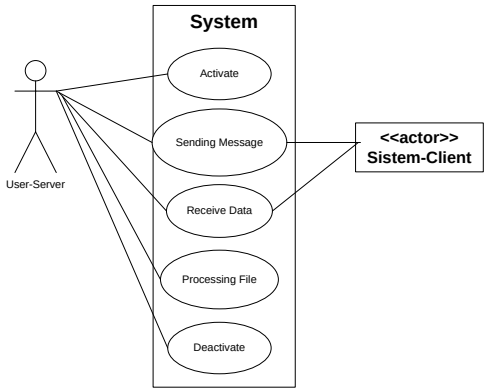

Figure 5. Server-System Use Case Diagram

Result and Discussion

Implementation between Server and Client Faces

Figure 6. Server and Client User Interface Implementation

System Testing

Testing Plan

The system testing is done by using the black-box testing method which tests only the unit and faces of the system (Mustaqbal, Firdaus, & Rahmadi, 2015). The result of the system testing shows that the system runs well. The tested data is limited to the "recap of Pilkada Ogan Ilir.xlsx" because it is not easy to get the data since it is a top-secret data. The testing is done in a certain place agreed before. This is meant to directly witness the process of securing the data of the general election with the data from the recap of the general election in Ogan Ilir.

The testing consists of 2: Performance Testing and Comparison Testing. In performance testing, 8 units of computers comprising 1 server computer and 7 client computers are used, while in comparison testing, 2 sets of client-server software are used. The first client-server software uses cryptography in securing the data by encryption and decryption. Meanwhile, the second software does not use cryptography for securing the data.

The server computer runs the PPSP-Server application while the client computers run the PPDP-Client application. The testing of the process of files in client and server applications can be seen in the following display:

Figure 7. Activating Connecting on Server

Figure 7 shows that the server connection status is active (ready) and it can be seen in the column '*sambungan*' that there are some connected clients: *client*-PC1 192.168.1.6, *client*-PC2 192.168.1.22, *client*-PC4 192.168.1.24, *client*-PC5 192.168.1.25, *client*-PC6 192.168.1.26, *client*-PC7 192.168.1.27, and *client*-PC8 192.168.1.28.

Figure 8. Client Connection to The Server

Figure 8 shows that client-PC1 is connected to the server. In order to get connected to the server, the client user must enter the name KPU and correct target IP server address. In that figure, Client-PC1 uses the name KPUD Ogan Ilir with the target IP server 192.168.1.5. Once it is connected, the client user can select the file: the recap of the result of the general election in the file column to be sent to the server securely.

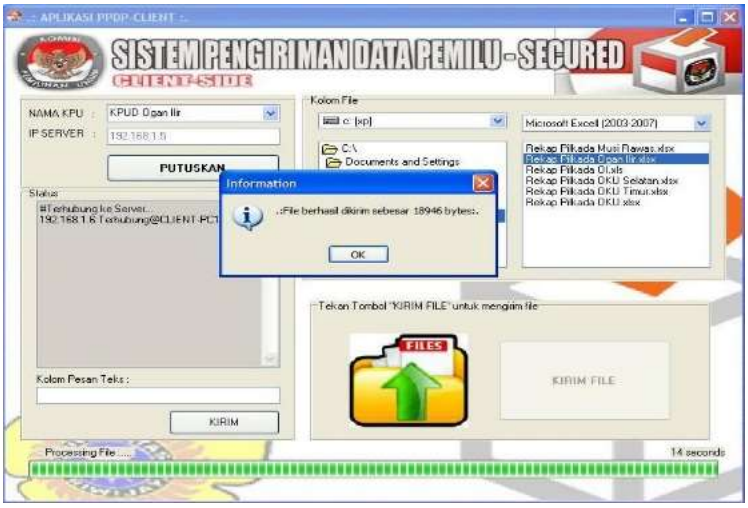

Figure 9. The Process of Sending a File From Client to Server

Figure 9 shows the process of sending the file "recap of Pilkada Ogan Ilir.xlsx" from the client to the server. The message in the dialogue box says that the file is successfully sent. The sent file has been encrypted using GOST Algorithm so that the data transition from the client to the server is secure. Once the file is received by the server, confirmation in the form of sound will pop up in the server-side, and the file will be located in the column of the list of the file as shown in figure 10. The different file name must be used. If the file name is not changed, the server will automatically reject and give a warning message to the client saying that there are files that have the same names. The received files of the recap of the result of the general election from all clients connected to the server can be seen in figure 10.

Figure 10. The Reception of a File From The Client Beside The Server

Figure 10 shows the file received from the clients in the column of file list along with the information from KPU and the IP address and the time the data is received. In order to process the received files, the server user must double-click the selected files. Then the process of encryption is done. Once it is finished, the file can be saved.

Sniffing Process using Wireshark

There are 2 sets of software in the testing for data tapping using Wireshark (Susianto & Rachmawati, 2018). The first client-server software uses cryptography in securing the data by encryption. Meanwhile the second software does no use cryptography in securing the data. The Capture testing of sending the files using encryption (secure):

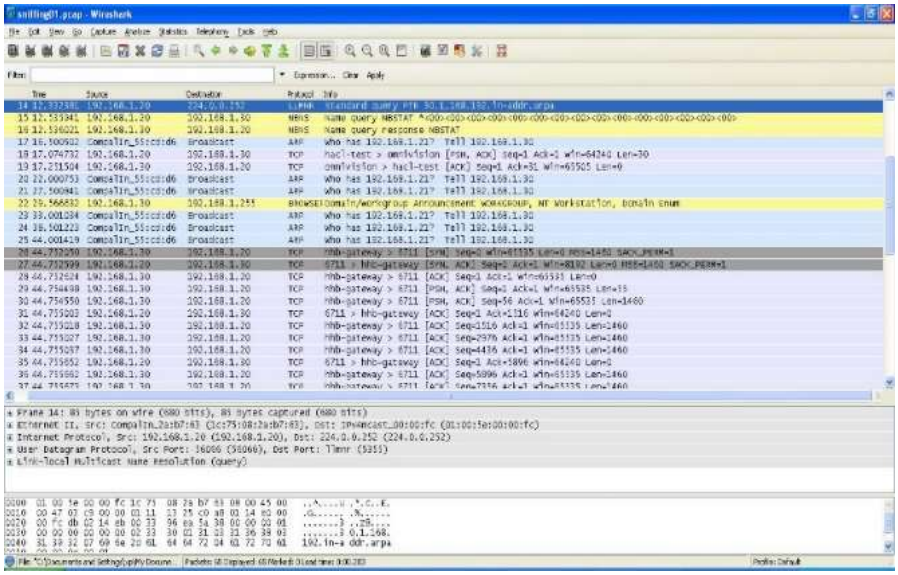

Figure 11. The capture of Encrypted File Sending

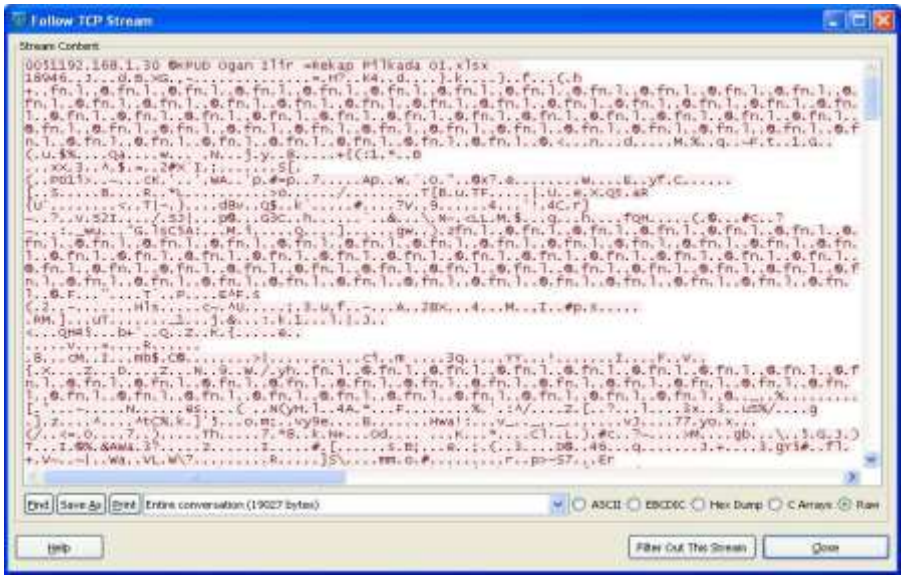

Figure 12. The capture of Encrypted Stream file

The capture of unencrypted file sending (not secure).

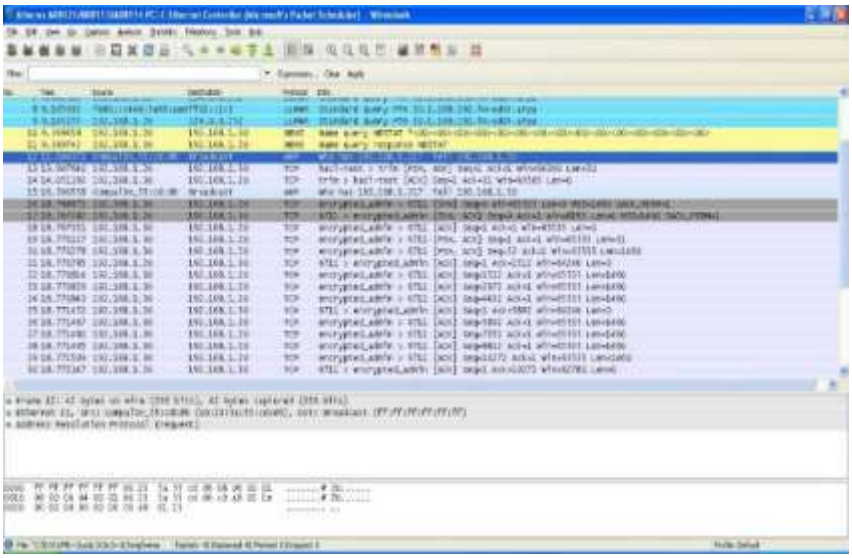

Figure 13. The capture of Unencrypted File Sending

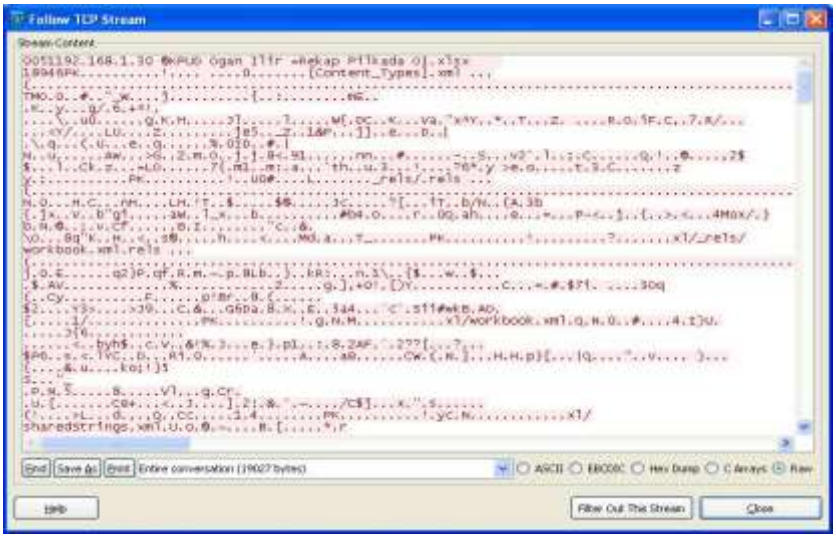

Figure 14. The capture of Unencrypted Stream file

From the test using Wireshark, it can be concluded that the stream files sent through the network from the client to the server between secured and not secured application are very different. In secured application, the stream file sent is in the form of chipper that must be encrypted in order to know its content (figure 12). Meanwhile in not secured application, the stream file is in the form of plaintext (not encrypted yet) (figure 14). Figure 14 shows that the data sent is still in the form of plaintext (not encrypted yet) and is susceptible to intruders. However, figure 12 shows the encrypted data in which the bits have been manipulated by GOST algorithm. So, it can be concluded that the manipulation of the data/bits in the encrypted stream file is successful. The manipulation of the

stream file makes it difficult for the intruders to change the result of the general election.

Conclusions

The system for securing and sending the data of the result of the general election has been successfully developed by using GOST algorithm without affecting the performance of the data sending significantly. The system set up gives a good solution for overcoming the stealing of the data in the network. The stream file sent through the network is not easily identified because it appears in the form of manipulated string which cannot be directly reconstructed into a file. It will take a lot of time to analyze it.

Acknowledgement

The writer would like to express his gratitude to all of the people, who have given their kind contribution, until this article completed, especially LPPM AMIK MDP.

References

Anas, I., Nanda, P. A., & Hidayat, A. (2019). Implementasi Algoritma Vigeneere Cipher dan GOST dalam Keamanan Data. *SinkrOn*, *2*(2), 18–22.

Arrijal, I. M., Efendi, R., & Susilo, B. (2016). Vigenere Cipher Dalam Aplikasi. *Pseudocode*, *III*(1), 69–82. https://doi.org/https://doi.org/10.33369/pseudocode.3.1.69-82

Benedict, M., Budiman, M. A., & Rachmawati, D. (2017). Perbandingan Algoritma Message Digest-5 (MD5) dan Gosudarstvennyi Standard (GOST) pada Hashing File Dokumen. *Jurnal Teknik Informatika Kaputama (JTIK)*, *1*(1), 50–61.

Hendrawan, A. H. (2016). Analisis Serangan Flooding Data Pada Router Mikrotik. *Krea-TIF*, *4*(1), 12–20. https://doi.org/http://dx.doi.org/10.32832/kreatif.v4i1.894

Muharyanto, A. S., & Fatimah, T. (2018). Keamanan Database Dengan Metode Rivest Code 4 (RC4) dan Caesar Cipher Berbasis Desktop. *SKANIKA*, *1*(2), 508–513.

Mukhtar, H. (2018). *Kriptografi Untuk Keamanan Data* (Ed.1). Yogyakarta: Deepublish.

Munir, R. (2019). *Kriptografi Edisi Kedua*. Bandung: Informatika.

Mustaqbal, M. Si., Firdaus, R. F., & Rahmadi, H. (2015). Pengujian Aplikasi Menggunakan Black Box Testing Boundary Value Analysis. *Jurnal Ilmiah Teknologi Informasi Terapan (JITTER)*, *1*(3), 31–36.

Pabokory, F. N., Astuti, I. F., & Kridalaksana, A. H. (2015). Implementasi Kriptografi Pengamanan Data Pada Pesan Teks , Isi File Dokumen , dan File Dokumen Menggunakan Algoritma Advanced Encryption. *Informatika Mulawarman: Jurnal Ilmiah Ilmu Komputer*, *10*(1), 20–31. https://doi.org/http://dx.doi.org/10.30872/jim.v10i1.23

Sari, C. A., Rachmawanto, E. H., Utomo, D. W., & Sani, R. R. (2016).

Penyembunyian Data Untuk Seluruh Ekstensi File Menggunakan Kriptografi Vernam Cipher dan Bit Shiffting. *Journal of Applied Intelligent System*, *1*(3), 179–190. https://doi.org/https://doi.org/10.33633/jais.v1i3.1252

Simatupang, N. A., & Hasibuan, N. A. (2018). Keamanan File Teks Menggunakan Algoritma Government Standard (GOST). *Pelita Informatika*, *17*(4), 490–494.

Susianto, D., & Rachmawati, A. (2018). Implementasi dan Analisis Jaringan Menggunakan Wireshark , Cain and Abels , Network Minner (Studi Kasus : AMIK Dian Cipta Cendikia). *Jurnal Cendikia*, *16*(2), 120–125.

Udoyono, K., & Saepudin, Ah. (2018). Pengamanan Basis Data Sistem Penjualan Dengan Menggunakan Teknik Enkripsi Kriptografi GOST. *Jurnal Teknologi Informasi Dan Komunikasi STMIK Subang*, *13*(1), 1–18.

Umum, K. P. *Perubahan Terhadap Peraturan Komisi Pemilihan Umum Nomor 09 Tahun 2009 Tentang Tahapan, Program, dan Jadwal Penyelenggaraan Pemilihan Anggota DPR, DPD, dan DPRD Tahun 2009*. , (2008).

Wijaya, N. (2017). Perancangan Aplikasi Promosi Songket Palembang Berbasis Android. *JUSIM*, *2*(2), 10–22.

Wijaya, N., Irsyad, H., & Taqwiym, A. (2017). Design Verification Using Palmprint. *TEKNOMATIKA*, *07*(02), 36–46.

Yasa, G. I. (2015). Keamanan pada Grid Computing~Survey Paper. *Elkawnie: Journal of Islamic Science and Technology*, *1*(2), 199–212. https://doi.org/10.22373/ekw.v1i2.539