IMPLEMENTASI ALGORITMA CAESAR CIPHER PADA KEAMANAN DATA SISTEM E-VOTING PEMILIHAN KETUA ORGANISASI KEMAHASISWAAN

Husni Angriani[1], Yeni Saharaeni[2]
Sistem Informasi, STMIK KHARISMA Makassar [1]
husniangriani@kharisma.ac.id[1], yenisaharaeni@kharisma.ac.id[2]

ABSTRAK

Kemanan data peserta dan hasil pemilihan pada proses pemilihan ketua organisasi pada STMIK KHARISMA Makassar, merupakan hal yang sangat penting dan bersifat rahasia. Untuk menjaga keamanan data maka dapat digunakan algoritma kriptografi, salah satu satunya adalah algoritma caesar cipher. Algoritma tersebut diterapkan pada sistem e-voting pemilihan ketua unit kegiatan mahasiswa (UKM) pada STMIK KHARISMA Makassar dengan metode pergeseran 3 pada proses enkripsi dan dekripsinya. Proses enkripsi dilakukan sebelum penyimpanan data pada database dilakukan, proses dekripsi dilakukan pada saat sistem melakukan proses pembacaan data hasil pemilihan. Dengan menerapkan algoritma tersebut, diperlihatkan bahwa data yang tersimpan kedalam database dalam bentuk enkripsi tidak dapat dibaca dengan mudah oleh administrator sistem. Sehingga dapat meminimalisir penyalah gunaan data hasil pemilihan maupun seluruh informasi yang ada dalam sistem. Penerapan algoritma caesar chipper pada sistem e-voting pemilihan ketua UKM pada STMIK KHARISMA Makassar, cukup aman dalam menjaga kerahasiaan data. Diharapkan penelitian ini dapat dikembangkan dengan menggabungkan dua algoritma untuk memberikan hasil yang lebih baik atau menggabungkan dua buah pola pergeseran yang berbeda, sehingga sulit untuk menemukan pola dekripsi oleh orang-orang yang ingin menyalah gunakan data tersebut.

Kata Kunci: ***E-Voting, Kriptografi, Caesar Cipher, Kriptografi.***

ABSTRACT

The safety of participant data and the results of the election in the process of selecting the chair of the organization at STMIK KHARISMA Makassar is very important and confidential. To maintain data security, cryptographic algorithms can be used. one of them is the caesarean cipher algorithm. The algorithm is applied to the e-voting system for the election of the head of the student activity unit *(UKM) at STMIK KHARISMA Makassar with the shift 3 method in the encryption and decryption process. The encryption process is carried out before storing data in the database, the decryption process is carried out when the system reads the results of the selection. By applying the algorithm, it is shown that data stored in the database in the form of encryption cannot be read easily by the system administrator. So as to minimize the misuse of election data and all information contained in the system. The application of the caesar cipher algorithm in the e-voting system for the election of the UKM chairperson at the STMIK KHARISMA Makassar is quite safe in maintaining data confidentiality. It is hoped that this research can be developed by combining two algorithms to provide better results or combining two different shift patterns, making it difficult to find decryption patterns by people who want to misuse the data.*

Keywords: e-voting, cryptography, caesar cipher.

1. PENDAHULUAN

Perkembangan teknologi yang semakin pesat membawa dampak perubahan pada gaya hidup manusia, salah satu perubahan tersebut adalah cara manusia memberikan hak suara (Saputri, Sudarsono, & Yuliana, 2017). Voting merupakan salah satu cara yang paling umum dilakukan untuk memilih pemimpin dalam suatu organisasi (Juniawan, 2016). Proses pemilihan ketua unit kegiatan kemahasiswaan, bahkan proses pemilihan ketua Badan Eksekutif Mahasiswa pun menggunakan metode voting. Penggunaan istilah e-voting merujuk pada kebebasan pemilih untuk memberikan suara secara aman dan rahasia melalui jalur elektronik (Abba, Awad, Al-qudah, & Jallad, 2017). Prosedur untuk menjaga keamanan data dan kerahasiaan data dapat dilakukan dengan menerapkan algoritma kriptografi. Pada Algoritma kriptografi dilakukan dengan dua fungsi yaitu enkripsi dan dekripsi. Salah satu algoritma kriptografi yang dapat digunakan untuk menjaga keamanan dan kerahasiaan data adalah caesar cipher. Metode yang digunakan dalam caesar cipher ini adalah dengan menukarkan atau mengganti setiap huruf dari plaintext dengan huruf lain dengan interval tertentu (Rohmi & Insannudin, 2016). Dengan menerapkan algoritma caesar cipher pada sistem e-voting, dapat menjaga keamanan dan kerahasiaan seluruh data pada sistem e-voting.

2. LANDASAN TEORI

Sebelum adanya komputer, pensil dan kertas merupakan media untuk menerapkan algoritma kriptografi. Algoritma kriptografi *(cipher)* yang digunakan dinamakan algoritma klasik. Algoritma klasik merupakan algoritma yang berbasis karakter. Dimana proses enkripsi dan dekripsi dilakukan pada setiap karakter pesan (Pradipta, 2016).

Enkripsi adalah sebuah proses yang melakukan perubahan sebuah kode dari yang bisa dimengerti menjadi sebuah kode yang tidak bisa dimengerti (tidak terbaca). Enkripsi dapat diartikan sebagai kode atau cipher. Sebuah cipher menggunakan suatu algoritma yang dapat mengkodekan semua aliran data (stream) bit dari sebuah pesan menjadi cryptogram yang tidak dimengerti (unitelligible). Karena teknik cipher merupakan suatu sistem yang telah siap untuk di automasi, maka teknik ini digunakan dalam sistem keamanan komputer dan network (Indriyono, 2016).

Algoritma kriptografi *Caesar Cipher* sangat mudah untuk digunakan. Inti dari algoritma kriptografi ini adalah melakukan pergeseran terhadap semua karakter pada plainteks dengan nilai pergeseran yang sama. Adapun langkahlangkah yang dilakukan untuk membentuk cipherteks dengan *Caesar Cipher* adalah menentukan besarnya pergeseran karakter yang digunakan dalam membentuk cipherteks ke plainteks, Menukarkan karakter pada plainteks menjadi cipherteks dengan berdasarkan pada pergeseran yang telah ditentukan sebelumnya (Priyono, 2016).

Beberapa Penelitian yang telah dilakukan dalam penerapan algoritma kriptografi antara lain Seperti penelitian yang dilakukan oleh priyono pada tahun 2016 yang menggunakan metode caesar chiper dan algoritma vigenere chiper untuk mengamankan pesan teks. Penelitian tersebut berjudul “Penerapan Algoritma Caesar Cipher Dan Algoritma Vigenere Chiper Dalam Pengamanan Pesan Teks”. Pada penelitian tersebut dilakukan proses

enkripsi dan dekripsi menggunakan caesar chiper atau vigenere chiper terhadap pesan yang dikirimkan sesuai karakter yang ada pada tabel ASCII 256 dengan panjang karakter maksimal 14 karakter. Kedua algoritma tidak digabungkan pada saat proses enkripsi dan dekripsi pesan. (Priyono, 2016).

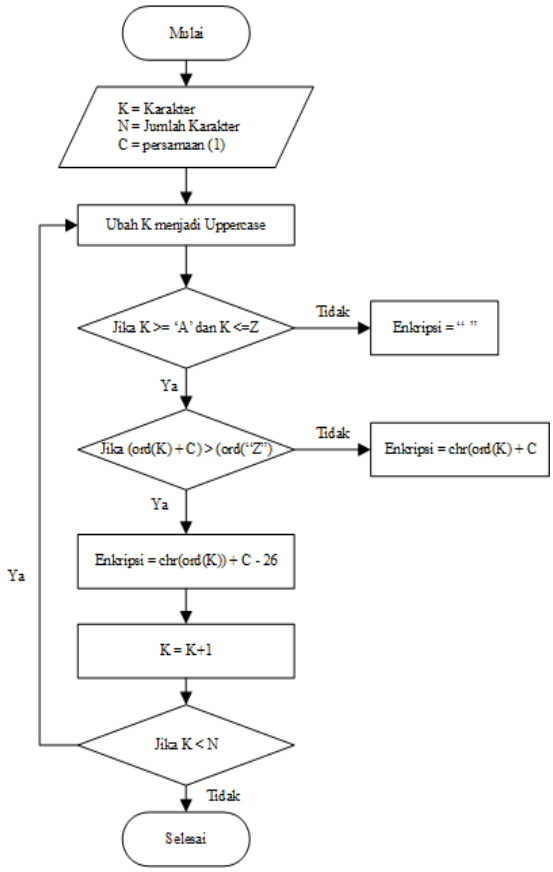
3. METODE PENELITIAN

Dalam menerapkan algoritma caesar cipher dibutuhkan proses enkripsi dan dekripsi. Proses enkripsi dilakukan sebelum data disimpan kedalam database. Untuk menerapkan algoritma caesar cipher digunakan persamaan (1).

$$C = C \bmod 26 \quad (1)$$

dimana C adalah nilai pergeseran karakter, dalam penelitian ini digunakan pergeseran 3 sehingga nilai awal C adalah 3. Selanjutnya dilakukan proses enkripsi dengan melakukan konversi setiap karakter ke kode ASCII. Perintah ord digunakan untuk mengambil nilai ASCII dari karakter, perintah chr digunakan untuk mengubah kode ASCII ke karakter. Untuk memudahkan perhitungan nilai ASCII maka setiap karakter akan diubah menjadi huruf besar atau uppercase. Kemudian dilakukan perulangan hingga seluruh karakter dikonversi. Seluruh proses tersebut dapat dilihat pada Gambar 1.

Proses dekripsi terhadap data dilakukan pada saat pembacaan hasil voting oleh sistem. Alur proses dekripsi memiliki kesamaan dengan proses enkripsi yang membedakan adalah pada proses dekripsi dilakukan pengurangan nilai C.



Gambar 1. Flowchart Proses Enkripsi

4. HASIL DAN PEMBAHASAN

Proses enkripsi dilakukan sebelum data disimpan kedalam database. Salah satu contoh hasil penerapan proses enkripsi pada Gambar 1 dapat dilihat pada Gambar 2.

id_user	fullname	prodi	jk	angkatan	pemilih
12096087	IDFKUXO EXGL	X - TI	L	2017	Y
12098760	SHUPDQD	X - TI	L	2007	Y
12345678	KXVQL DQJULDQL	X - SI	P	2017	Y

Gambar 2. Hasil Enkripsi data Mahasiswa

Hasil enkripsi data mahasiswa pada Gambar 2 merupakan data yang tersimpan dalam database. Proses dekripsi dilakukan pada saat sistem membaca data mahasiswa melalui sistem. Penerapan proses dekripsi pada diperlihatkan pada Gambar 3.

Gambar 3. Hasil dekripsi data Mahasiswa

Pada Gambar 3 diperlihatkan data mahasiswa yang dapat dilihat melalui sistem. Sedangkan pada Gambar 2 diperlihatkan data mahasiswa yang berada dalam database yang telah terenkripsi. Salah satu contoh proses enkripsi nama mahasiswa PERMANA menjadi SHUPDQD dengan menerapkan algoritma caesar cipher pergeseran 3.

5. SIMPULAN DAN SARAN

Penerapan algoritma caesar chipper pada sistem e-voting pemilihan ketua UKM pada STMIK KHARISMA Makassar, cukup aman dalam menjaga kerahasiaan data. Diharapkan penelitian ini dapat dikembangkan dengan menggabungkan dua algoritma untuk memberikan hasil yang lebih baik atau menggabungkan dua buah pola pergeseran yang berbeda, sehingga sulit untuk menemukan pola dekripsi oleh orang-orang yang ingin menyalah gunakan data tersebut.

6. UCAPAN TERIMA KASIH

Penelitian ini disponsori oleh Kementrian Riset dan Teknologi Pendidikan Tinggi dalam program hibah Penelitian Dosen Pemula Tahun 2019, untuk itu peneliti mengucapkan Terima Kasih Sebesar-besarnya kepada Kemenristek Dikti. Dan juga STMIK KHARISMA Makassar yang telah memberikan fasilitas pendukung dalam melakukan penelitian.

DAFTAR PUSTAKA

Abba, A. L., Awad, M., Al-qudah, Z., & Jallad, A. H. (2017). Security Analysis of Current Voting Systems. In *International Conference on Electrical and Computing Technologies and Applications (ICECTA)*.

Indriyono, B. V. (2016). Implementasi Sistem Keamanan File dengan Metode Steganografi EOF dan Enkripsi Caesar Cipher. *Junal Sisfo*, *06*(01), 1–16. https://doi.org/10.24089/j.sisfo.2016.09.001

Juniawan, F. P. (2016). RSA implementation for data transmission security in BEM chairman E-voting Android based application. *Proceedings - 2016 1st International Conference on Information Technology, Information Systems and Electrical Engineering, ICITISEE 2016*, 93–98. https://doi.org/10.1109/ICITISEE.2016.7803054

Pradipta, A. (2016). Implementasi Metode Caesar Chiper Alphabet Majemuk Dalam Kriptografi Untuk Pengamanan Informasi. *Indonesian Journal on Networking and Security*, *5*(3), 3–6.

Priyono. (2016). Penerapan Algoritma Caesar Cipher Dan Algoritma Vigenere Cipher Dalam Pengamanan Pesan Teks. *Jurnal Riset Komputer (JURIKOM)*, *3*(5), 351–356.

Rohmi, G. F., & Insannudin, E. (2016). Implementasi Algoritma Cipher caesar untuk Enkripsi dan Dekripsi pada Tabel ASCII menggunakan Bahasa Java, (May).

Saputri, Z. A., Sudarsono, A., & Yuliana, M. (2017). E-voting security system for the election of EEPIS BEM president. *Proceedings - International Electronics Symposium on Knowledge Creation and Intelligent Computing, IES-KCIC 2017*, *2017-Janua*, 147–152. https://doi.org/10.1109/KCIC.2017.8228578