

IMPLEMENTASI METODE CAESAR CIPHER DALAM PENERAPAN SISTEM E-VOTING BERBASIS WEB PADA PEMILIHAN ABANG NONE JAKARTA

Radithya Pramuditha Yenadi¹, Fauziah², Deny Hidayatullah³
Fakultas Teknologi Komunikasi dan Informatika – Sistem Informasi, Universitas Nasional
radith239@gmail.com¹, fauziah@civitas.unas.ac.id.²

Submitted January 17, 2020; Revised January 14, 2020; Accepted March 14, 2020

Abstrak

Semakin majunya zaman sekarang ini, teknologi menjadi hal keharusan dalam memajukan performa pada setiap organisasi dan berbagai macam kegiatan lainnya. Salah satu contoh penerapan teknologi yang akan dijelaskan pada penelitian kali ini adalah perancangan sistem berbasis *web e-voting* dalam pemilihan Abang None Jakarta dengan cara memasukkan nomor E-KTP untuk dapat melakukan pemilihan. Sebelumnya dalam menentukan pemilihan Abang None Jakarta, masih menerapkan sistem voting SMS terbanyak dimana pada sistem ini dianggap kurang efektif karena penggunaan pulsa dianggap lebih boros dari pada penggunaan kuota internet. Dalam mengembangkan sistem e-voting berbasis web ini, penulis menggunakan metode SDLC (*System Development Life Cycle*) dan metode algoritma *Caesar Cipher* untuk keamanan data pemilih. Selain itu digunakan system SMS Gateway sehingga dapat mencegah adanya pemilih yang menggunakan E-KTP orang lain sebelum melakukan pemilihan. Sistem *e-voting* yang dibuat menggunakan bahasa pemrograman PHP dan Xampp sebagai databasenya. Tujuan dari sistem *e-voting* ini dapat digunakan sebagai pengambilan keputusan secara transparan, mempercepat proses penghitungan voting menghemat biaya dan mencegah terjadinya kecurangan pada saat pelaksanaan *e-voting* terkait pemilihan Abang None Jakarta. Hasil penelitian yang dilakukan terbukti berhasil baik dari segi penggunaan *web* untuk melakukan pemilihan dan keamanan yang digunakan berhasil melakukan enkripsi dan dekripsi data penggunaanya.

Kata Kunci : E-Voting, sistem berbasis web, Abang None Jakarta, SDLC, algoritma Caesar Cipher.

Abstract

In this increasingly modern era, technology has become a must in improving performance in every organization and various other activities. One example of the application of technology that will be explained in this research is the design of a web-based e-voting system in the election of Abang None Jakarta by inserting an E-KTP numbers to be able to cast a vote in the election. Previously, the selection of Abang None Jakarta still uses SMS voting system that is considered to be less effective because the use of credits is considered more wasteful than the use of internet quota. In developing this web-based e-voting system, the researcher uses the SDLC (System Development Life Cycle) method and the Caesar Cipher algorithm method for voter data security. Besides that, the Gateway SMS system is used to prevent any voter who uses someone else's E-KTP before casting a vote in an election. The e-voting system is made using the PHP and Xampp programming languages as its database. The e-voting system is expected to be used in making a transparent decision, speeding up the voting counting process, saving costs and preventing fraud when implementing e-voting in the election of Abang None Jakarta. The results of research is proven successful in terms of both the use of the web to conduct the election and the use of security in encryption and decryption of user data.

Keywords: E-Voting, web-based system, Abang None Jakarta, SDLC, Caesar Cipher algorithm

1. PENDAHULUAN

Dengan semakin majunya zaman, teknologi yang berkembang kian meningkat pula. Salah satunya teknologi

yang ingin dikembangkan saat ini yaitu sistem informasi *e-voting* berbasis *web* dalam menentukan pemilihan Abang None Jakarta. Voting merupakan suatu metode

proses pengambilan keputusan dalam masyarakat.

Fungsi lain voting dapat digunakan untuk mengumpulkan aspirasi masyarakat dan sebagai jalan keluar untuk menyelesaikan suatu masalah [1]. Alasan penggunaan sistem informasi *e-voting* berbasis *web* ini yaitu dapat mengatasi hal-hal atau masalah yang sering terjadi pada sistem pemilihan berbasis konvensional terkait proses penghitungan yang lambat, biaya yang cukup besar dan adanya pemilih ganda. Dengan adanya *e-voting* berbasis *web* ini nantinya dapat mengatasi masalah tersebut dan dapat memberikan kemudahan kepada pemilih dalam melakukan pemilihan terkait Abang None Jakarta. Demokrasi yang dilakukan di Indonesia masih konvensional sehingga menjadi kurang efektif dan memiliki berbagai macam masalah lainnya yang diakibatkan oleh kesalahan masyarakat itu sendiri sehingga dibutuhkan suatu solusi untuk mengatasi permasalahan tersebut [2]. Pada *e-voting* yang akan dirancang dibutuhkan sistem keamanan agar terjamin kerahasiaan data pemilihnya salah satunya enkripsi [3]. Enkripsi yang digunakan yaitu algoritma Caesar Cipher dan menggunakan fitur foto wajah sebelum masuk ke tahap pemilihan.

Dengan aplikasi *e-voting* yang dibuat dapat memudahkan pemilih dalam memilih pilihannya tanpa harus mendatangi tempat pemungutan suara dan dapat membantu panitia dalam menghitung suara pemilih dengan cepat [4]. Pada penelitian ini digunakan teknik pengumpulan data melalui studi dokumentasi untuk mengumpulkan data primer dan data

sekunder serta menggunakan teknik analisis data yang dimulai dengan reduksi data, penyajian data dan penarikan kesimpulan [5]. Sistem informasi *e-voting* berbasis web yang akan dibuat tidak hanya digunakan pada pemilihan Abang None Jakarta saja tetapi dapat juga digunakan sebagai rancangan untuk pemilihan ketua

RT, ketua RW, Kepala Desa, Bupati/Wali Kota, Gubernur, DPR, DPD, DPRD bahkan pemilihan Presiden. Dalam perancangan pembuatan sistem informasi *e-voting* berbasis *web*, diperlukannya suatu data yang pasti seperti E-KTP. E-KTP merupakan nomor unik yang memuat isi data valid dari pemilih tersebut sehingga dapat dikenali datanya pada database kependudukan.

Tujuan dari penelitian ini diharapkan dapat menciptakan proses pemilihan yang cepat, efektif dan efisien serta dapat dijadikan sebagai alternatif atau solusi untuk mengatasi berbagai macam kegiatan voting lainnya seperti pemilihan umum presiden dan wakilnya, pemilihan ketua OSIS dan pemilihan-pemilihan dalam bentuk lainnya yang dibarengi dengan adanya keamanan enkripsi algoritma Caesar Cipher yang membuat data dari setiap penggunaanya dapat menjadi lebih aman dan membuat penggunaanya tidak perlu khawatir lagi dengan masalah data dari penggunaanya dapat dilihat oleh orang lain.

2. METODE PENELITIAN

Metode penelitian yang digunakan adalah metode pengembangan SDLC dan penggunaan algoritma Caesar Cipher untuk pengamanan data *e-voting* untuk keamanan data.

Metode SDLC (*System Development Life Cycle*)

Metode SDLC yaitu metode pengembangan sistem perangkat lunak atau software yang melalui beberapa tahapan:

1. Analysis

Analysis merupakan tahapan pertama kali pada SDLC di mana mengumpulkan informasi sebanyak mungkin untuk kebutuhan pengembangan sistem dengan memanfaatkan sistem yang sudah usang lalu dikembangkan lagi dengan data masukan *user*.

2. Desain

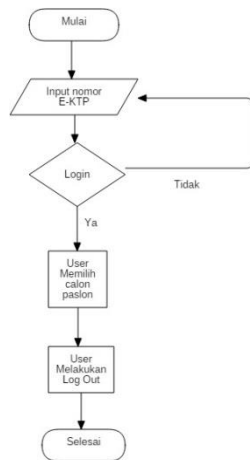
Desain merupakan tahapan dalam membuat alur atau proses dan tampilan pada sistem yang akan dibuat berdasarkan data dari tahapan analysis yang sudah dilakukan pada tahapan sebelumnya yang nantinya akan diteruskan pada tahapan implementasi selanjutnya seperti pada gambar disamping.

3. Implementasi

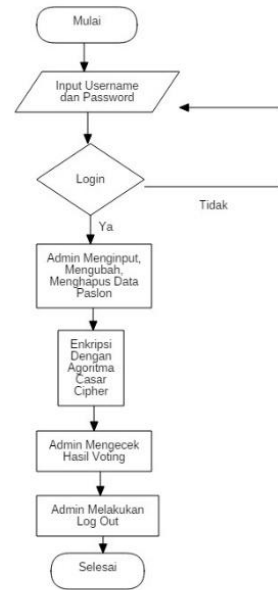
Implementasi merupakan tahapan penulisan kode program untuk membuat desain tampilan antar muka atau *interface* berdasarkan tahapan desain yang sudah dibuat sesuai dengan alur proses yang dilakukan

4. Testing

Testing merupakan tahapan pengujian dari sistem yang telah dibuat apakah sistem sudah berjalan dengan baik atau belum dan apakah sudah sesuai dengan keinginan *user*.



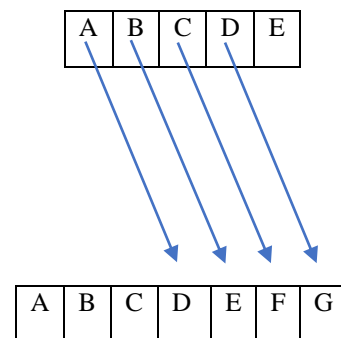
Gambar 1. Flowchart Alur Proses Sistem dari Sisi User atau Pemilih



Gambar 2. Flowchart Alur Proses Sistem dari Sisi Admin

Metode Algoritma Caesar Cipher

Metode algoritma Caesar Cipher merupakan salah satu algoritma kriptografi pengamanan data dan informasi dengan cara teknik substitusi pada pesan yang dapat dibaca (*plaintext*) menjadi pesan yang tidak dapat dibaca (*ciphertext*) yang disebut dengan enkripsi atau mengubah pesan yang tidak dibaca (*ciphertext*) menjadi pesan yang dapat dibaca (*plaintext*) yang disebut dengan deskripsi.



Gambar 3. Proses Substitusi Huruf dengan Menggunakan Algoritma Caesar Cipher

Pada gambar di atas terjadi pergeseran 3 buah karakter yaitu A menjadi D, B menjadi E, C menjadi F dan D menjadi G

sehingga kata-kata yang semula dapat dibaca menjadi tidak dapat dibaca. Jika operasi di atas ditulis secara matematis maka rumus enkripsi:

$$C_i = (P_i + K) \text{ mod } 26 \quad (1)$$

Sedangkan rumus dekripsi:

$$P_i = (C_i - K) \text{ mod } 26 \quad (2)$$

Alasan adanya mod 26 dikarenakan total jumlah seluruh huruf alphabet ada 26 buah.

Keterangan:

C_i = nilai urutan karakter *ciphertext* ke- i .

P_i = nilai urutan karakter *plaintext* ke- i .

K = nilai kunci.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Gambar 4. Tabel Huruf Alphabet

D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Gambar 5. Tabel Huruf Alphabet setelah pergeseran

3. HASIL DAN PEMBAHASAN

Tampilan Antar Muka User

Berikut merupakan tahapan *user* dalam melakukan *e-voting* adalah sebagai berikut:

1. Tampilan Login User



Gambar 6. Tampilan Login User

Agar user dapat melakukan pemilihan *e-voting*, *user* diharuskan *login* terlebih dahulu dengan memasukkan nomor E-KTP yang dimilikinya dan apabila sudah diinput maka *user* mengklik tombol *login* untuk melanjutkan ke tahapan selanjutnya.

2. Tampilan Pemilihan



Gambar 7. Tampilan Pemilihan

Pada halaman ini *user* dapat melakukan pemilihan terkait calon Abang None mana yang akan dipilihnya. *User* dapat mengklik tombol visi misi terlebih dahulu sebelum melakukan pemilihan.

3. Tampilan Visi dan Misi Calon Kandidat Abang None Jakarta



Gambar 8. Tampilan Profil Kandidat.

Gambar di atas merupakan tampilan dari halaman visi dan misi calon kandidat Abang None Jakarta yang isinya terdiri dari nama kandidat, visi dan misi, jumlah

perolehan suara saat ini dan periode pencalonan. Apabila user sudah melihat visi dan misi dari setiap pasangan calon Abang None Jakarta maka *user* dapat melakukan pemilihan dengan mengklik tombol beri suara tetapi jika user ingin melihat visi dan misi calon kandidat Abang None lainnya maka user dapat mengklik tombol kembali.

4. Tampilan Setelah Melakukan Pemilihan



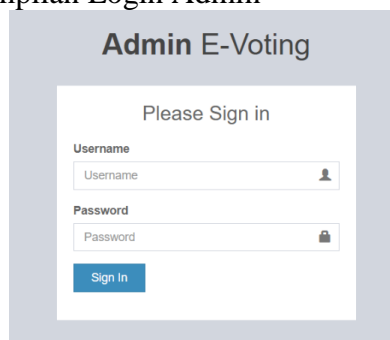
Gambar 9. Tampilan Setelah Melakukan Pemilihan

Jika *user* sudah melakukan pemilihan akan muncul tampilan di atas yang menandakan user sudah melakukan pemilihan. Untuk keluar dari halaman tersebut *user* dapat mengklik tombol kembali agar kembali halaman *login*.

Tampilan Antar Muka Admin

Berikut merupakan tahapan admin untuk melakukan pengaturan terkait *e-voting* sebagai berikut:

1. Tampilan Login Admin



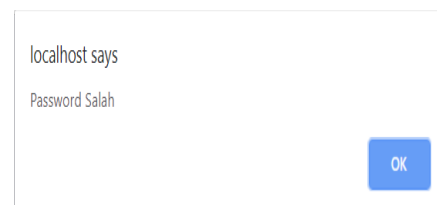
Gambar 10. Tampilan Login Admin

Agar admin dapat menginput, mengedit dan menghapus data calon kandidat Abang None Jakarta, admin diharuskan *login* terlebih dahulu dan apabila admin sudah masuk akan muncul tampilan seperti gambar di bawah ini.



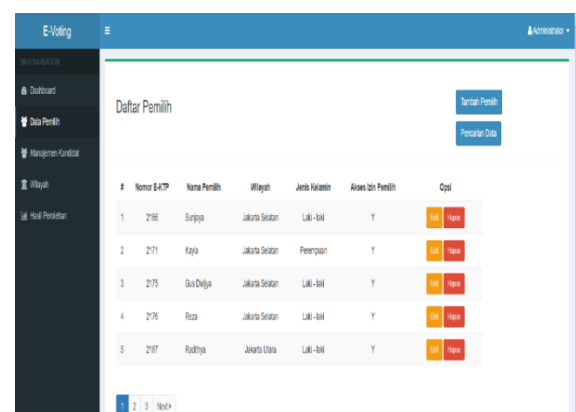
Gambar 11. Tampilan Setelah Login Admin

Apabila admin salah memasukkan *username* atau *password* maka akan muncul tampilan seperti di bawah ini.



Gambar 12. Tampilan Apabila Salah Memasukkan Username Atau Password

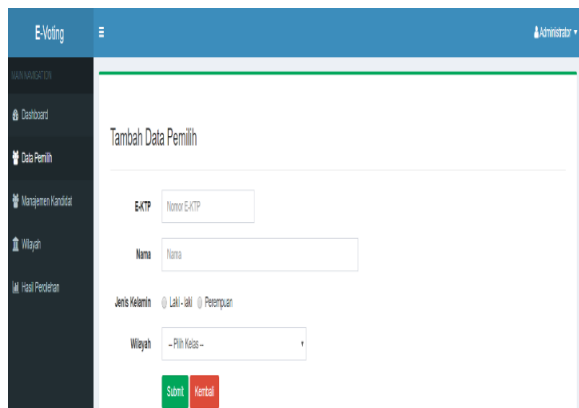
2. Tampilan Data Pemilih



Gambar 13. Tampilan Menu Data Pemilih

Pada menu tampilan data pemilih berisikan data user yang terdaftar sebagai peserta *e-voting* terdapat informasi terkait nomor E-KTP, nama pemilih, nama wilayah, jenis kelamin dan akses izin dalam melakukan pemilihan. Di dalam menu data pemilih, terdapat fitur lainnya seperti:

a. Tampilan Penambahan Data User

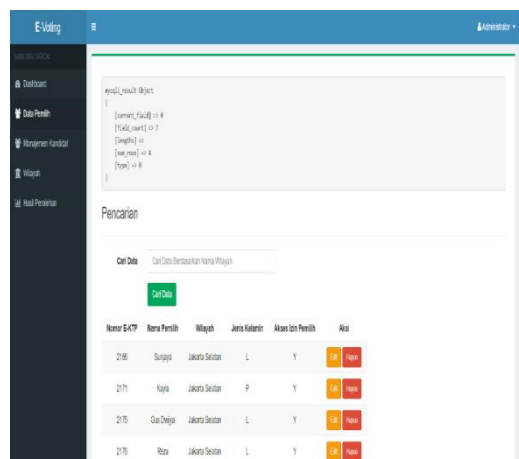


Gambar 14. Tampilan input data pemilih

Pada tampilan ini admin dapat melakukan penginputan atau penambahan data *user* dengan mengklik tombol tambah pemilih pada tampilan utama data pemilih.

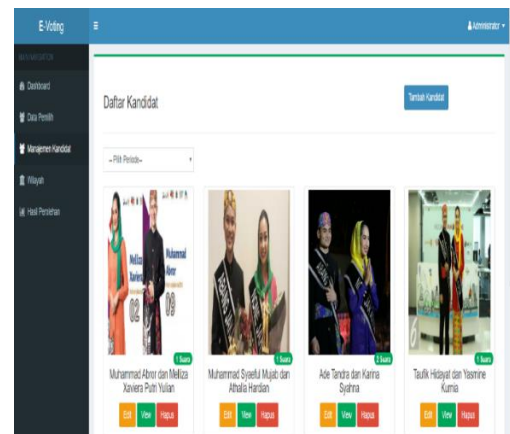
b. Tampilan Pencarian Data

Tampilan ini digunakan untuk melakukan pencarian data *user* dengan cepat. Admin hanya perlu memasukkan wilayah mana user yang ingin dicari datanya.



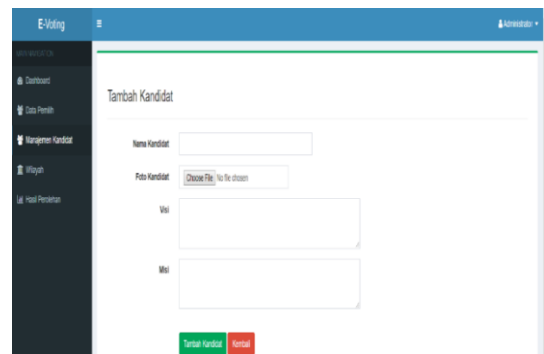
Gambar 15. Tampilan Pencarian Data Pemilih

3. Tampilan Manajemen Kandidat



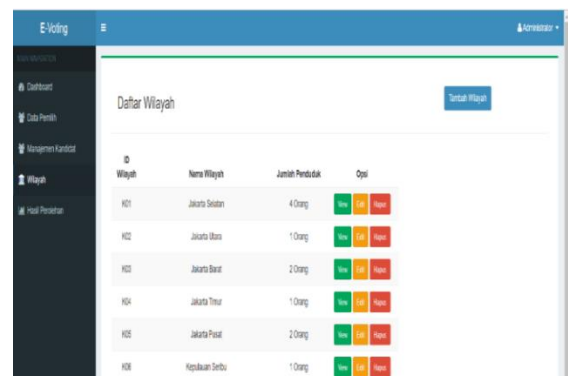
Gambar 16. Tampilan Menu Manajemen Kandidat

Tampilan ini menampilkan daftar kandidat yang telah diinput. Jika ingin melakukan penambahan kandidat, dapat mengklik tombol tambah kandidat dan admin dapat menginputkan data kandidat yang ingin diinput seperti gambar di bawah ini.



Gambar 17. Tampilan Input Data Kandidat

4. Tampilan Wilayah



Gambar 18. Tampilan Menu Wilayah

Pada tampilan menu ini, admin dapat melihat daftar wilayah yang sudah ditambahkan datanya melalui fitur tambah wilayah seperti gambar di atas. Selain itu admin dapat mengklik tombol *view* untuk melihat *user* siapa saja yang terdaftar pada setiap wilayah, tombol *edit* untuk mengedit nama wilayah serta tombol hapus untuk menghapus nama wilayah.

5. Tampilan Hasil Perolehan



Gambar 19. Tampilan Menu Hasil Perolehan

Ini merupakan tampilan menu terakhir yang menunjukkan berapa jumlah total suara dari tiap pasangan calon Abang None Jakarta.

Metode Algoritma Caesar Cipher

Untuk melakukan enkripsi dan dekripsi menggunakan algoritma Caesar Cipher dapat menggunakan 2 cara yaitu manual dan matematis. Cara menghitung manual yaitu dengan menentukan berapa pergeseran yang diinginkan seperti contoh dibawah ini.

1. Enkripsi

Contoh kalimat : Sunjaya
Kunci geser : 3
Jawab :

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Setelah dilakukan pergeseran menjadi gambar seperti dibawah ini.

D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Jika sudah disesuaikan antara tabel Alphabet dengan tabel Alphabet setelah pergeseran maka dapat ditentukan enkripsinya yaitu S menjadi V, U menjadi X, N menjadi Q, J menjadi M, A menjadi D, Y menjadi B dan A menjadi D dengan mengikuti tabel Alphabet awal dan tabel Alphabet setelah adanya pergeseran. Hasil enkripsi yaitu dari Sunjaya menjadi VXQMDBD. Untuk mengembalikan bentuk enkripsi menjadi kalimat semula dapat dilakukan dekripsi yang dapat dilihat di bawah ini.

2. Dekripsi

Contoh kalimat : VXQMDBD
Kunci geser : 3
Jawab :

D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Dibandingkan dengan tabel Alphabet semula dibawah ini

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Maka apabila dilakukan dekripsi didapat V menjadi S, X menjadi U, Q menjadi N, M menjadi J, D menjadi A, B menjadi Y dan D menjadi A. Hasil dekripsi yaitu dari VXQMDBD menjadi kata semula yaitu SUNJAYA.

Untuk melakukan perhitungan secara matematis sama perhitungan manual yaitu dengan menentukan jumlah pergeseran yang diinginkan seperti dibawah ini.

1. Enkripsi

Contoh kalimat : Sunjaya
Kunci geser : 3
Jawab :

$$C_i = (P_i + K) \bmod 26 \quad (1)$$

Keterangan:

- C_i = nilai urutan karakter *ciphertext* ke-i.
- P_i = nilai urutan karakter *plaintext* ke-i.
- K = nilai kunci.

Untuk menentukan P_i dapat ditentukan dengan melihat tabel Alphabet di bawah ini.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Jika contoh kalimat adalah Sunjaya berarti S diurutkan nomor 18, U diurutkan nomor 20, N diurutkan nomor 13, J diurutkan nomor 9, A diurutkan nomor 0, Y diurutkan nomor 24 dan A diurutkan nomor 0.

Huruf U:

$$C_i = (20 + K) \bmod 26$$

$$= (20 + 3) \bmod 26$$

$$C_i = (23) \bmod 26$$

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Jika dilihat ditabel maka nomor 23 itu yaitu X.

Huruf N:

$$C_i = (13 + K) \bmod 26$$

$$= (13 + 3) \bmod 26$$

$$C_i = (16) \bmod 26$$

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Jika dilihat ditabel maka nomor 16 itu yaitu Q.

Masukkan nomor yang sudah didapat ke dalam rumus dengan menghitung secara satu per satu dari mulai huruf S seperti di bawah ini.

Huruf S:

$$C_i = (18 + K) \bmod 26$$

$$= (18 + 3) \bmod 26$$

$$C_i = (21) \bmod 26$$

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Jika dilihat ditabel maka nomor 21 itu yaitu V. Mod 26 hanya menunjukkan bahwa ada 26 huruf Alphabet total.

Huruf J:

$$C_i = (9 + K) \bmod 26$$

$$= (9 + 3) \bmod 26$$

$$C_i = (12) \bmod 26$$

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Jika dilihat ditabel maka nomor 12 itu yaitu M.

Huruf A:

$$C_i = (0 + K) \bmod 26$$

$$= (0 + 3) \bmod 26$$

$$C_i = (3) \bmod 26$$

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Jika dilihat ditabel maka nomor 3 itu yaitu D.

Huruf Y:

$$C_i = (24 + K) \bmod 26$$

$$= (24 + 3) \bmod 26$$

$$C_i = (27) \bmod 26$$

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Jika dilihat ditabel maka nomor 27 itu melebihi jumlah Alphabet total maka $27 - 25 = 2$. Sisanya dihitung dari awal maka akan didapat enkripsinya adalah B.

Huruf A:

$$C_i = (0 + K) \bmod 26$$

$$= (0 + 3) \bmod 26$$

$$C_i = (3) \bmod 26$$

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Jika dilihat ditabel maka nomor 3 itu yaitu D.

Di dapat hasil enkripsinya yaitu VXQMDBD. Untuk mengembalikan ke kalimat semula maka dilakukan deskripsi secara matematis yang akan dijelaskan di bawah ini.

2. Dekripsi

Contoh kalimat : VXQMDBD
Kunci geser : 3

Jawab :

$$P_i = (C_i - K) \text{ mod } 26$$

Keterangan:

C_i = nilai urutan karakter *ciphertext* ke-i.

P_i = nilai urutan karakter *plaintext* ke-i.

K = nilai kunci.

Untuk menentukan C_i dapat ditentukan dengan melihat table Alphabet di bawah ini.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Jika contoh kalimat adalah VXQMDBD berarti V diurutan nomor 21, X diurutan nomor 23, Q diurutan nomor 16, M diurutan nomor 12, D diurutan nomor 3, B diurutan nomor 1 dan D diurutan nomor 3.

Masukkan nomor yang sudah didapat ke dalam rumus dengan menghitung secara satu per satu dari mulai huruf V seperti di bawah ini.

Huruf V:

$$P_i = (21 - K) \text{ mod } 26$$

$$= (21 - 3) \text{ mod } 26$$

$$P_i = (18) \text{ mod } 26$$

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Jika dilihat ditabel maka nomor 18 itu yaitu S. Mod 26 hanya menunjukkan bahwa ada 26 huruf Alphabet total.

Huruf X:

$$P_i = (23 - K) \text{ mod } 26$$

$$= (23 - 3) \text{ mod } 26$$

$$P_i = (20) \text{ mod } 26$$

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Jika dilihat ditabel maka nomor 20 itu yaitu U.

Huruf Q:

$$P_i = (16 - K) \text{ mod } 26$$

$$= (16 - 3) \text{ mod } 26$$

$$P_i = (13) \text{ mod } 26$$

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Jika dilihat ditabel maka nomor 13 itu yaitu N.

Huruf M:

$$P_i = (12 - K) \text{ mod } 26$$

$$= (12 - 3) \text{ mod } 26$$

$$P_i = (9) \text{ mod } 26$$

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Jika dilihat ditabel maka nomor 9 itu yaitu J.

Huruf D:

$$P_i = (3 - K) \text{ mod } 26$$

$$= (3 - 3) \text{ mod } 26$$

$$P_i = (0) \text{ mod } 26$$

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Jika dilihat ditabel maka nomor 0 itu yaitu A.

Huruf B:

$$P_i = (1 - K) \text{ mod } 26$$

$$= (1 - 3) \text{ mod } 26$$

$$P_i = (-2) \text{ mod } 26$$

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Jika dilihat ditabel maka nomor -2 itu lebih dari 0 sehingga $0 - (-2) = 2$. 2 Sisanya dihitung dari akhir Alphabet sehingga didapat dekripsinya adalah Y.

Huruf D:

$$P_i = (3 - K) \text{ mod } 26$$

$$= (3 - 3) \text{ mod } 26$$

$$P_i = (0) \text{ mod } 26$$

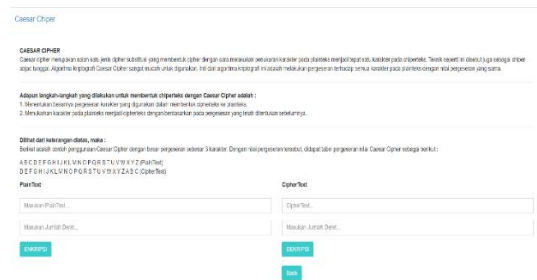
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Jika dilihat ditabel maka nomor 0 itu yaitu A.

Di dapat hasil dekripsinya yaitu SUNJAYA yang menunjukkan kembali ke kalimat semula.

3. Perhitungan Algoritma Caesar Cipher dengan Menggunakan Aplikasi

Berikut ini adalah penggunaan algoritma Caesar Cipher melalui aplikasi:



Gambar 20. Tampilan Menu Algoritma Caesar Cipher

Pada gambar di atas merupakan tampilan dari algoritma Caesar Cipher. Untuk menggunakannya admin hanya perlu memasukkan nama yang akan dienkripsi pada kolom *plaintext* yang sudah disediakan. Jika sudah diinput, tentukan jumlah kunci geser yang akan ditentukan dan klik tombol enkripsi untuk melihat hasilnya. Berikut gambar di bawah ini dalam mengenkripsi dan mendekripsi dengan contoh kata sunjaya seperti soal perhitungan manual algoritma Caesar Cipher dalam enkripsi dan dekripsi.

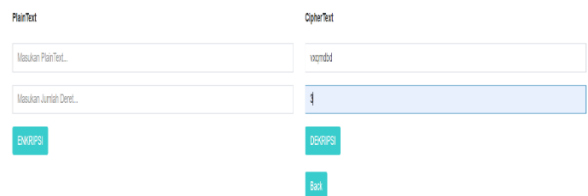


Gambar 21. Menginput Contoh Kalimat dan Jumlah Kuncinya



Gambar 22. Hasil Enkripsi dari Kalimat yang diinput

Dapat dilihat hasil enkripsi terbukti sama dengan perhitungan manual yaitu VXQMDBD. Berikut dekripsi dari kalimat VXQMDBD.



Gambar 23. Menginput Contoh Kalimat Enkripsi dan Jumlah Kuncinya



Gambar 24. Hasil Dekripsi dari Contoh Kalimat Enkripsi

Dapat dilihat juga bahwa contoh enkripsi VXQMDBD apabila didekripsi menghasilkan kalimat *plaintext* yaitu SUNJAYA yang menandakan bahwa hasil perhitungan manual yang sudah dilakukan yaitu benar.

4. Performace Security

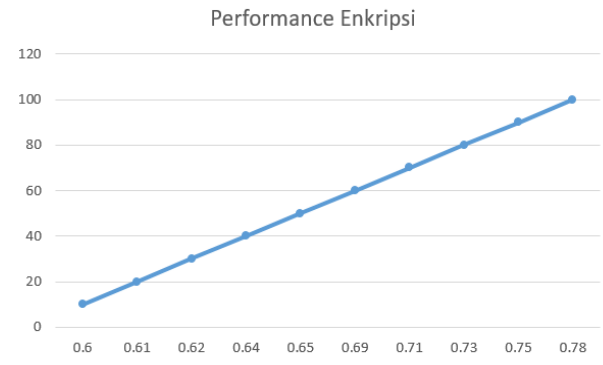
Berikut ini untuk menentukan *performance* yang dibutuhkan CPU dalam melakukan pemrosesan:

$$V_j = \frac{j}{t} \quad (3)$$

Keterangan:

- V_j = Kecepatan pemrosesan.
- j = jumlah kata.
- t = waktu enkripsi atau dekripsi.

Untuk menggunakan rumus tersebut dibutuhkan waktu yang diproses pada saat system dijalankan. Berikut merupakan *table performance security*:



Gambar 25. Grafik Kecepatan Enkripsi Yang Dibutuhkan CPU

Perhitungan Performance Enkripsi:

$$V_{10} = \frac{10}{0.6} = 16.67 \text{ m/s}$$

$$V_{20} = \frac{20}{0.61} = 32.79 \text{ m/s}$$

$$V_{30} = \frac{30}{0.62} = 48.38 \text{ m/s}$$

$$V_{40} = \frac{40}{0.64} = 62.5 \text{ m/s}$$

$$V_{50} = \frac{50}{0.65} = 76.92 \text{ m/s}$$

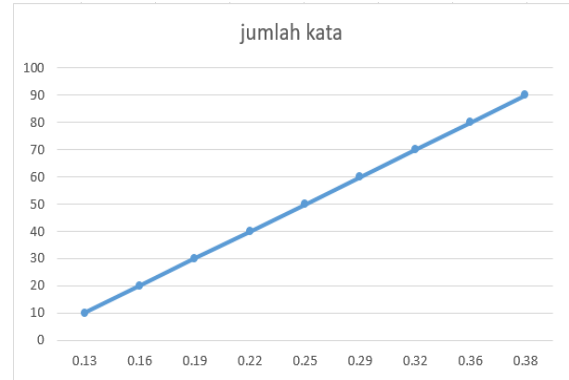
$$V_{60} = \frac{60}{0.69} = 86.96 \text{ m/s}$$

$$V_{70} = \frac{70}{0.71} = 98.59 \text{ m/s}$$

$$V_{80} = \frac{80}{0.73} = 109.59 \text{ m/s}$$

$$V_{90} = \frac{90}{0.75} = 120 \text{ m/s}$$

$$V_{100} = \frac{100}{0.78} = 128.2 \text{ m/s}$$



Gambar 26. Grafik kecepatan dekripsi yang dibutuhkan CPU

Perhitungan Performance Deskripsi:

$$V_{10} = \frac{10}{0.13} = 76.92 \text{ m/s}$$

$$V_{20} = \frac{20}{0.16} = 125 \text{ m/s}$$

$$V_{30} = \frac{30}{0.19} = 157.89 \text{ m/s}$$

$$V_{40} = \frac{40}{0.22} = 181.82 \text{ m/s}$$

$$V_{50} = \frac{50}{0.25} = 200 \text{ m/s}$$

$$V_{60} = \frac{60}{0.29} = 206.89 \text{ m/s}$$

$$V_{70} = \frac{70}{0.32} = 218.75 \text{ m/s}$$

$$V_{80} = \frac{80}{0.36} = 235.29 \text{ m/s}$$

$$V_{90} = \frac{90}{0.38} = 236.84 \text{ m/s}$$

$$V_{100} = \frac{100}{0.41} = 243.9 \text{ m/s}$$

4. SIMPULAN

Dari hasil penelitian yang telah dilakukan, pembuatan aplikasi *e-voting* berbasis *web* dapat disimpulkan:

- 1) Hasil perhitungan algoritma yang digunakan dalam mengamankan data user berhasil dilakukan.
- 2) Didapatkan hasil percepatan yang dilakukan pada enkripsi dan deskripsi sehingga dapat dilihat seberapa cepat

proses yang dilakukan enkripsi maupun dekripsi.

- 3) Tujuan yang dicapai yaitu mempercepat proses penghitungan voting, menghemat biaya operasional, mendukung program *Go green*, mencegah terjadinya kecurangan pada saat melakukan e-voting dan memberikan hasil suara yang lebih akurat serta transparan.
- 4) Manfaat langsung bagi masyarakat adalah memberikan kemudahan bagi masyarakat dalam menyalurkan aspirasinya, yaitu cukup dengan mengklik tombol beri suara.
- 5) Dengan menggunakan algoritma Caesar Cipher diharapkan dapat menjaga keamanan data pada setiap user dengan melakukan enkripsi nama pada database data pemilih.

DAFTAR PUSTAKA

- [1] Muid, A., Sholihin, M., & Wardhani, R. (2017). “*Aplikasi E-Voting Terhadap Pemilihan Presiden Badan Eksekutif Mahasiswa Universitas Islam Lamongan*”. J-TIIS. Vol. 1 No. 1, 39–46.
- [2] Prasetyawan, P., Rusliyawati, & Sari, D. (2018). “*Pengembangan Aplikasi Mobile E-Voting Pilkada*”. Seminar Nasional Teknologi. 2001, 750–756.
- [3] Anggoro, N. D., Suhery, C., & Ruslianto, I. (2019). “*Penerapan Algoritma Knapsack Dan Fungsi Hash Pada Sistem E-Voting (Studi Kasus: Pemilihan Raya Mahasiswa Universitas Tanjungpura Pontianak)*”. Coding : Jurnal Komputer dan Aplikasi. Vol. 07 No. 01, 85–96.
- [4] Huda, O. N., Putra, F. P., & Jaroji (2018). “*Aplikasi E-Voting Berbasis Mobile Menggunakan Optical Character Recognition*”. Jurnal Informatika Polinema. Vol. 4 Edisi 3, 235–239.
- [5] Nisa, K., & Adnan. M. F. (2019). “*Implementasi Elektronik Voting (E-Voting) Dalam Pemilihan Walinagari Di Nagari Salareh Aia Kabupaten Agam Tahun 2017*”. Journal of Residu, Vol. 3 Issue 16, 39–48.
- [6] Singh, A., P, R. K., & Cholli, N. G. (2018). “*Empowering E-governance with E-voting*”. Indonesian Journal of Electrical Engineering and Computer Science. Vol. 12 No. 3, 1081–1086. <https://doi.org/10.11591/ijeecs.v12.i3.pp1081-1086>
- [7] Arun, V., Dutta, A., Rajeev, S., & Mathew, R. V. (2019). “*E-Voting Using a Decentralized Ethereum Application*”. International Journal of Engineering and Advanced Technology (IJEAT), Vol. 8 Issue 4, 830–833.
- [8] Apriani, T., Hamudy, M. I. A., Rifki, M. S., Hadi, A. S. (2018). “*E-Voting in The Village Head Election in Batanghari and Kabupaten Bogor Regencies*”. Jurnal Bina Praja. Vol. 10 Issue 2, 317–326. <https://doi.org/10.21787/jbp.10.2018.317-326>
- [9] B, V. N. R., Akshay, S., Arun, M., & A, I. K. M. (2019). “*Decentralized E-Voting System*”. International Research Journal of Engineering and Technology (IRJET). Vol. 06 Issue 03, 8040–8050.
- [10] Bhuvanesh, E., Purushothaman, B., Shyam, K., & Vanitha, V. (2017). “*Secure E-Voting System*”, International Research Journal of Engineering and Technology (IRJET), Vol. 04 Issue 04, 1–7.