IMPELEMENTASI ALGORITMA KRIPTOGRAFI KLASIK CAESAR UNTUK RANCANG BANGUN APLIKASI E-VOTING BERBASIS WEB (STUDI KASUS : SMAN 10 TANGERANG)

Nurul Chafid[1], Herlina Soffiana[2]
Program Teknik Informatika, Universitas Satya Negara Indonesia
Email: chafid09@gmail.com[1], herlinasoffiana04@gmail.com[2]

ABSTRACT

Elections or we are familiar with the term voting are not only carried out in the election of the legislative council of political parties in a country, the election is also carried out in a school and university organization in the election of candidates for the chairman of the organization or student president. The voting system is always carried out by voting if political opponents or opponents of potential leaders experience the same vote. Voting is an activity carried out to choose a candidate for a predetermined election. In today's modern era, a lot of work is done automatically, including voting, which was previously done manually. Voting that is done manually is done by voting on paper, and the results are calculated on each paper which makes the calculation process take longer. Created a system that can facilitate the voting process. E-Voting is a candidate selection system and the most votes are made and processed in a digital system. System In this voting process there is a process for nominating candidates, selecting candidates, and voting results. With the existence of e-voting to conduct candidate selection with clear and not manipulated data. The data security process is carried out by encrypting data from an existing database using Caesar's Classical Cryptography Algorithm.

Kata Kunci : *e-voting, security, algoritma kriptografi klasik Caesar.*

PENDAHULUAN

Di era modern saat ini sangat banyak pengetahuan dan ilmu-ilmu yang berkembang, termasuk perkembangan dalam bidang teknologi. Teknologi merupakan penerapan ilmu sistem,alat maupun mesin yang digunakan oleh manusia dalam melakukan suatu hal ataupun suatu pekerjaan dengan lebih mempersingkat waktu dan lebih mudah. Selain itu teknologi juga berkembang dalam hal informasi dan komunikasi. Manusia dengan sangat mudah bertukar informasi dan dapat berkomunikasi jarak dekat maupun jarak jauh dengan sangat efisien. Penyebaran informasi bisa dijangkau dari yang lingkup kecil sampai dengan lingkup besar sekaligus. Contoh studi kasus yang diambil adalah teknologi informasi dan komunikasi dalam melakukan pemungutan suara atau voting.

Voting merupakan suatu proses kegiatan pemungutan suara yang dilakukan untuk memilih beberapa kandidat yang sudah dicalonkan, setelah beberapa calon kandidat terpilih maka akan dilakukan pemilihan untuk mendapatkan suara terbanyak agar dapat menemukan hasil kandidat yang sesungguhnya dengan memperlihatkan grafik penilaian hasil pemungutan suara. Voting yang dilakukan secara manual dengan menggunakan kertas bergambar calon kandidat dan pemilih calon kandidat melakukan pemilihan dengan melingkari , mencentang atau melubangi kertas sesuai dengan gambar calon kandidat yang dipilih. Namun dalam pelaksanaan kegiatan pemilihan secara manual sering terjadi kecurangan yang seharusnya tidak terjadi dalam suatu kegiatan voting seperti yang ada di SMAN 10 Tangerang. Dari adanya kecurangan hasil kandidat banyak pihak yang tidak setuju dan menimbulkan konflik. Hasil yang tidak sesuai membuat banyak orang yang enggan untuk melakukan kegiatan pemilihan kandidat calon. Di SMAN 10 Tangerang melakukan voting masih dengan cara manual. Maka dari itu dengan berkembangnya

era teknologi dibuatlah suatu sistem yang dapat melakukan kegiatan voting secara otomatis, Selain dibuatnya suatu sistem, juga terdapat keamanan untuk melindungi data-data dan hasil voting yang kemungkinan dapat tercurangi, dengan adanya keamanan dalam suatu sistem.

Sistem voting yang dirancang adalah e-voting dengan menggunakan algoritma kriptografi Caesar . sistem e-votig yang dirancang berfungsi untuk mengotomatisasi kegiatan voting secara manual, yaitu melakukan pendataan,pemilihan calon kandidat, serta menampilkan grafik hasil suara secara otomatis tanpa harus dihitung satu per-satu hasil suara dari masing-masing calon. Aplikasi e-voting ini dilengkapi dengan keamanan data menggunakan algoritma kriptografi klasik Caesar. Algoritma kriptografi Caesar berfungsi untuk membuat kode akses sebelum melakukan voting dan dari data-data pemilih yang masuk data selain diperhitungkan maka, data juga akan di amankan dengan cara mengenkripsi atau dekripsi angka maupun huruf menjadi teks-kode. Pada enkripsi dekripsi kriptografi data di enkripsi menjadi.

Kriptogram dengan menggunakan Caesar Chiper huruf-huruf dalam plainteks digantikan oleh huruf lainnya dalam posisi tertentu dalam susunan alphabet yang menggeser sebanyak 3 huruf Jadi huruf chiper pada algoritma Caesar adalah hasil pergeseran sekian huruf dari huruf asli. Berdasarkan latar belakang diatas dapat dirumuskan beberapa masalah yang ada, tentang bagaimana mengimpelementasikan Algoritma Kriptografi Caesar untuk rancang bangun aplikasi e-voting berbasis web (Studi Kasus: SMAN 10 Tangerang). Berdasarkan permasalahan yang sudah dijelaskan diatas, tujuan dalam penelitian ini, untuk mempermudah admin dalam melakukan kegiatan dan mengontrol data hasil voting, dapat mempermudah pihak sekolah dalam hal penyimpanan data histori pemilihan osis, mpk, kepala sekolah.

Manfaat dari penelitian tersebut adalah sebagai berikut, terutama bagi penulis menjadikan sebagai penambah wawasan ilmu pengetahuan dalam segi teori maupun praktek dan menambah pengalaman dalam melakukan penelitian khususnya dalam pembuatan aplikasi *e-voting*, enkripsi data dan keamanan data. Adapun manfaat bagi sekolah dari hasil penelitian yang dibuat dapat meningkatkan akreditasi, meningkatkan anttusiasme bagi siswa-siswi dalam melakukan pemilihan suara dengan cara voting serta dapat mengevisiensi dana pengeluaran dalam organisasi. Pada penelitian terdahulu oleh (Husni Angriani & Yeni Saharaeni, 2019) yang berjudul "Implementasi Algoritma Caesar Cipher Pada Keamanan Data Sistem E-Voting Pemilihan Ketua Organisasi Kemahasiswaan". Dalam penelitian tersebut melakukan perlindungan data hanya untuk data mahasiswa, sistem pada penelitian ini tidak bisa melakukan voting dengan kategori lebih dari satu kategori.

Pada penelitian yang telah di teliti oleh (Dadang Amirudin, Irma Ruhiawati, & Murnati, 2021, Jurnal SIMIKA;Vol 4 No.1) dalam jurnalnya yang berjudul "Rancang Bangun Aplikasi E-Voting Ketua Osis di SMA PGRI 1 Kota Serang". penelitian yang sudah dilakukan oleh Dadang Amirudin,Ruhiawati dan Murnati bahwa rancang bangun E-voting yang telah dibuat tanpa menggunakan metode keamanan untuk melindungi data ataupun hasil voting, yang akan kemungkinan dapat dicurangi oleh pihak lain.

Selanjutnya pada peneltian yang diteliti oleh (Siswanto & Ferdiansyah, 2020) yang berjudul "Pengamanan Transfer Data pada API Untuk Aplikasi E-Voting Menggunakan Algoritma RSA". Dalam penelitian tersebut menggunakan Algoritma RSA untuk mengacak hasil pilihan pemilih menggunakan enkripsi RSA. Aplikasi yang dibangun untuk aplikasi e-voting sebagai pengamanan transfer data pad API.

Saya selaku penulis menyimpulkan dari ketiga penelitian diatas bahwa pada penelitian yang sudah dianalisa tentang perancangan aplikasi e-voting ternyata masih ada beberapa kelemahan dan masih butuh pengembangan selanjutnya, dengan kata lain saya selaku penulis dapat menambahkan dengan metode algoritma yang berbeda, maka dari itu selaku penulis mencoba membuat sebuah kebaruan dari sebuah metode yang akan diterapkan pada rancangan aplikasi e-vooting tersebut, adapun algoritma yang akan diterapkan dari rancangan ini harus dapat melakukan enkripsi dengan cara yang berbeda

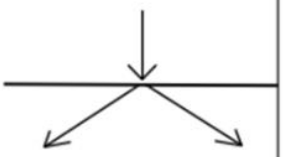
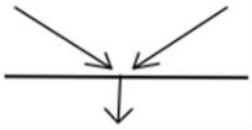
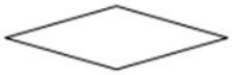
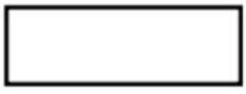
dari yang sebelumnya, dan dengan kasus yang berbeda. Sehingga pada penelitian ini peneliti menggunakan Algoritma Kriptografi Klasik Caesar untuk pengamanan data dan hasil voting sehingga sistem yang dijalankan berjalan sesuai dengan koridor serta tidak terjadi pengulangan atau penyalah gunaan identitas pengguna suara yang memilih calon pasangan dalam suatu organisassi sekolah dimana sistem yang sedang berjalan menghasilkan luaran yang diharapkan serta tidak terjadi kecurangan suara.

UML (*Unified Modeling Language)*

Untuk mempermudah pemahaman tata cara kerja modul, dibuatlah gambaran atau visualisasi interaksi aktor pemilih dan admin dari penelitian yang sedang dibuat. UML merupakan bahasa yang spesifik untuk digunakan dalam mendokumentasikan dalam pembuatan perangkat lunak. Cari ini juga merupakan pengembangan sistem yang berorientasi pada objek untuk adanya perkembangan suatu sistem (Sholiq, 2006)

Usecase Diagram

Usecase diagram adalah visualisasi atau gambaran untuk menggambarkan interaksi aktor pada sistem yang dibuat. Di dalam usecase diagram berisikan fungsi kebutuhan perangkat atau sistem secara ringkas, didalam fungsi tersebut di gambarkan atau dijelaskan dengan simbol-simbol dalam *usecase* diagram sebagai berikut:

Gambar	Keterangan
	*Start point*, diletakkan pada pojok kiri atas dan merupakan awal aktifitas.
	*End point*, akhir aktifitas.
	*Activites*, menggambarkan suatu proses/kegiatan bisnis.
	Fork (Percabangan) digunakan untuk menunjukkan kegiatan yang dilakukan secara parallel atau untuk menggabungkan dua kegiatan pararel menjadi satu.
	*Join* (penggabungan) atau rake, digunakan untuk menunjukkan adanya dekomposisi.
	*Decision Points*, menggambarkan pilihan untuk pengambilan keputusan, *true, false.*
	*Swimlane*, pembagian *activity* diagram untuk menunjukkan siapa melakukan apa.

Gambar 1. Simbol *Usecase*

Kriptografi

Kata kriptografi atau *cryptography* diketahui berasal dari bahasa Yunani, kripto dan graphia. Dimana kripto memiliki arti menyembunyikan, sementar graphia berarti tulisan. Sehingga bisa dijabarkan kriptografi merupakan ilmu yang mempelajari teknik-teknik matematika yang berkaitan dengan aspek keamanan informasi. Contohnya seperti keabsahan data, kerahasiaan data, kredibilitas data, integritas data, dan autentikasi data. Akan tetapi, tidak semua aspek keamanan informasi bisa diatasi dengan kriptografi. Kriptografi merupakan suatu ilmu yang mempelajari teknik dalam pengenkripsian data acak yang yang diubah kedalam sesuatu bacaan yang sulit dipahami atau sulit dibaca menggunakan suatu kunci, dimana bacaan yang sulit dipahami dan sulit dibaca tidak akan terbaca oleh *user* yang tidak memiliki kunci dekripsi. (Kromodimoeljo, 2009). Keamanan sebuah data menjadi hal terpenting untuk selalu dijaga kerahasiaannya. Karena sebuah informasi yang terbuka atau bocor tanpa ada kontrol yang jelas, dapat dimanfaatkan oleh pihak tertentu dengan tujuan yang membahayakan. Untuk itulah saat ini telah dikembangkan berbasis sistem keamanan pada jaringan komputer (*cyber security*). Dimana, salah satu tools yang banyak digunakan sekarang adalah kriptografi. Untuk itulah, kali ini kita akan membahas lebih dalam mengenai penggunaan dari kriptografi dan teknik implementasinya dalam dunia *cyber security*. Sehingga, anda mendapatkan *insight* baru dan lebih memperhatikan kesehatan komputer anda dari sisi sistem keamanan data secara berkala.

Kriptografi berasal dari kata bahasa Yunani, yang berarti kryptos dan graphein. Kryptos berarti rahasia atau tersembunyi, sedangkan graphein artinya menulis. Jadi, secara umum kriptografi merupakan proses menulis atau menyampaikan pesan secara rahasia dan tersembunyi. Namun, jika kita kaitkan dengan penggunaan teknologi digital, maka kriptografi adalah disiplin ilmu yang mempelajari teknik enkripsi naskah asli (*plaintext*) yang tersusun acak, dengan memanfaatkan kunci enkripsi sehingga naskah tersebut berubah menjadi teks yang sulit terbaca (*ciphertext*) oleh user yang tidak memiliki kunci dekripsi. Selanjutnya, ada istilah kriptografi klasik merupakan teknik cryptography yang pembuatannya tidak memerlukan bantuan komputer dan biasanya menggunakan alat bantu pena, batu, kertas, dan alat tradisional lainnya.

Enkripsi

Enkripsi data adalah proses pengamanan data informasi. Bagaimana tentang cara pengamanan enkripsi data dan enkripsi data mengamankan data informasi kamu dengan cara membuat data informasi tersebut nggak bisa dibaca tanpa bantuan khusus. Maksudnya, hanya kamu dan pihak yang terlibat aja yang bisa membaca pesan tersebut. Jadi, kamu nggak perlu takut chat kamu akan disadap atau semacamnya.

Enkripsi adalah bentuk pengamanan data yang sudah ada sejak dulu. Enkripsi data adalah proses yang biasanya diterapkan untuk menjaga keamanan data milik negara atau perusahaan. Enkripsi data menjaga keamanan informasi yang disampaikan dalam komunikasi antara satu negara dengan negara lainnya. Dengan enkripsi, informasi krusial yang dibicarakan dan dikirimkan bisa lebih terjaga kerahasiaannya.

Enkripsi adalah suatu proses perubahan kode dalam suatu pesan yang diubah menjadi kode lain. Kode tersebut diubah dari kode yang mudah dipahami (*plaintext*) dan diubah menjadi kode yang tidak bisa dipahami (*chipertext).* Kode pesan yang di ubah agar terjaga keamanan dan rahasia. (Amin, 2016).

Cara kerja Enkripsi

Cara kerja enkripsi data adalah mengubah data informasi yang asli menjadi data yang telah diubah menjadi kode yang tidak dapat dibaca oleh pihak luar. Contohnya gini, Sob. Misalnya kamu mengirim pesan berisi "Mimin, aku mau pakai layanan *Cloud Hosting* Indonesia". Nah,

pesan ini disebut dengan *plaintext*. Ketika menggunakan sistem keamanan enkripsi, *plaintext* itu akan diubah menjadi *chipertext*. *Ciphertext* adalah *plaintext* yang sudah diubah menjadi kode tertentu yang hanya bisa dibaca oleh pengguna atau pemilik aslinya. Orang lain yang berusaha membuka informasi tersebut tidak akan bisa membaca *plaintext* tersebut. Untuk melakukan enkripsi, bisa menggunakan *public key* atau *private key*. Kedua jenis kunci ini hanya dapat diketahui oleh pihak yang terlibat. Jadi, kamu bisa mengatur siapa yang bisa mengetahui kunci akses tersebut.

Enkripsi data ini juga dibutuhkan oleh kamu para pemilik bisnis online atau pelaku digitalisasi. Untuk mengoptimalkan keamanan, kamu tetap memerlukan server yang oke yang tangguh dan terjamin keamanannya. Seperti layanan *Cloud Hosting* Indonesia dan VPS Indonesia dari Jagoan *Hosting* yang sudah dilengkapi dengan teknologi keamanan terkini.

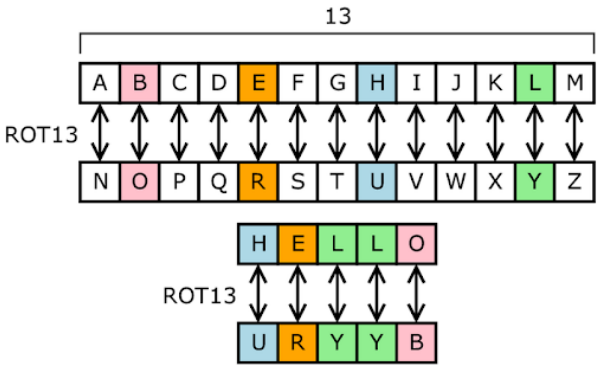
Algoritma Caesar

Dalam buku Kriptografi Teknik Keamanan Data dan Informasi dikatakan bahwa Algoritma kriptografi Caesar adalah algoritma yang mengenkripsi suatu kode sebagai sandi shift atau kode Caesar. Sandi atau kode tersebut diubah dari masing-masing huruf plaintext diubah menjadi huruf yang telah mengalami pergeseran dalam urutannya terhadap suatu angka. (Simarmata, Sriadhi, & Rahim, 2020) Menurut buku (Ariyus, Pengantar Ilmu Kriptografi, 2008) terdapat tiga bagian metode klasik Caesar yaitu :

- Blok
- Karakter
- Zig-zag

Jika belajar mengenai ilmu kriptografi, algoritma populer yang harus diketahui adalah Caesar Cipher. Konon, diberi nama demikian karena digunakan oleh kaisar Romawi, Julius Caesar untuk menyandikan pesan yang ia kirim ke para gubenurnya. Penggunaan Caesar Cipher pada masa Romawi menunjukkan kemajuan peradabannya. Padahal di masa itu, pengubahan plainteks menjadi cipherteks maupun sebaliknya, amatlah rumit. Semua serba manual. Jangankan komputer, lisrik saja belum ditemukan. Itulah sebabnya jika dibandingkan demgan algoritma lain di zaman modern ini, Caesar Cipher dianggap sebagai metode kriptografi paling sederhana, paling lemah dan paling mudah dibobol dengan *brute force attack*.

Caesar Cipher tergolong cipher substitusi, maksudnya setiap unit *plainteks* diganti dengan satu unit *cipherteks*. Satu unit bisa berupa huruf, pasangan huruf, atau kelompok huruf. Contohnya begini, tiap huruf *plainteks* disubstitusi dengan huruf ke tiga belas berikutnya dari susunan *alphabet*. Aturan subsitusi tertuang pada Gambar berikut ini:



Gambar 2. Susunan *Alphabet*

Maka, jika *plainteks* adalah HELLO, maka tiap huruf pada *plainteks* digeser sesuai aturan subsitusi sehingga membentuk cipherteks URYYB. Persegeran sejauh 13 ini bisa dianggap sebagai kunci k untuk enkripsi maupun dekripsi. Dengan demikin. fungsi enkripsi Caesar Cipher dapat dirumuskan sebagai berikut:

$C = E(P) = (P+k) \bmod 26$

dan fungsi dekripsi menjadi

$P=D(C) = (C-k) \bmod 26$

Tentu fungsi tersebut bisa dikembangkan lagi. Jika hanya terbatas mod 26, tentu kompleksitas kriptografi menjadi sangat rendah. Karena mod 26 menunjukkan jumlah alphabet. Bisa saja mod 26 ini diganti sesuai karakter yang terpampang pada keyboard komputer kekinian. Karakter modern ini mengacu ke ASCII (*American Standart Code for Information Interchange*). Sebanyak 256 karakter. Dari karakter ke 0 hingga ke 255. Jadi mod-nya akan berubah dari 26 ke 256. Sehingga kompleksitas terangkat, walau sedikit. Kalau zaman romawi menerapkan mod 26 ya wajar banget. Sesuai dengan teknologi zaman itu. Mod 26 pada Caesar Cipher dapat digunakan sebagai latihan untuk menerapkan algoritma kriptografi dalam bahasa pemrograman.

Database

Pengertian *database* adalah sekumpulan data yang dikelola berdasarkan ketentuan tertentu yang saling berkaitan sehingga memudahkan dalam pengelolaannya. Dihimpun dari berbagai sumber, secara sederhana, database atau basis data merupakan sekumpulan data atau informasi yang tersimpan secara sistematis. Database memiliki peran penting dalam perangkat untuk mengumpulkan informasi, data, atau file secara terintegrasi. (Janner Simarmata, 2007) sedangkan menurut (Enterprise, 2015), *Database* merupakan perkumpulan data yang terhubung secara terstruktur yang dibuat berdasarkan struktur data tertentu. *Database* dapat disimpan untuk kegunaan data dari sistem tertentu

Dihimpun dari berbagai sumber, secara sederhana, *database* atau basis data merupakan sekumpulan data atau informasi yang tersimpan secara sistematis. Database memiliki peran penting dalam perangkat untuk mengumpulkan informasi, data, atau file secara terintegrasi. Database membuat penyimpanan dan pengelolaan data menjadi lebih efisien. Adapun contoh *database* dapat dilihat dari pengembangan situs web. *Database* berwujud tabel yang terdiri dari kolom dan baris yang memuat atribut dan nilai tertentu. Adapun jumlah kolom dan baris dalam suatu *database* tergantung pada jumlah kategori atau jenis informasi yang perlu disimpan.

JavaScript

Pada tahun 1994 *JavaScript* mulai dikenal, pada saat itu web dan internet sudah mulai berkembang. JavaScript didesain oleh Brendan Eich yang merupakan karyawan Netscape. Transformasi nama *JavaScript,* dimulai dari Mocha, Mona, *LiveScript*, hingga akhirnya resmi bernama *JavaScript*. Versi awal bahasa JS hanya dipakai di kalangan Netscape beserta dengan fungsionalitas pun yang masih terbatas. Singkat cerita pada tahun 1996 *JavaScript* secara resmi dinamakan sebagai *ECMAScript*. *ECMAScript* 2 dikembangkan pada tahun 1998 yang dilanjutkan dengan *ECMAScript* 3 setahun kemudian. *ECMAScript* terus dikembangkan sampai akhirnya menjadi *JavaScript* atau JS hingga saat ini. Pada tahun 2016, 92% web diketahui telah menggunakan *JavaScript*. Itulah mengapa *JavaScript* atau JS terus berkembang. JavaScript adalah bahasa pemrograman yang banyak digunakan dalam pengembangan *website,* aplikasi, dan game seperti yang kita sudah ketahui bahwa keunggulan dari *JavaScript* memiliki beberapa ciri khas dalam setiap *source code* yang ada pada *JavaScript*. Jadi *JavaScript* adalah bahasa pemrograman populer yang digunakan untuk membuat situs dengan konten website yang dinamis. *JavaScript* merupakan bahasa pemrograman yang berbentuk skrip. Javascript berguna untuk menjalankan suatu dokumen HTML yang disisi *Client/Browser* untuk mengeksekusi perintah-perintah dari user ataupun untuk manipulasi element-element HTML dan menambahkan *Style* secara sederhana dan otomatis. Yang berarti perintah tersebut dari browser yang dijalankan oleh *user* (Ariona, Belajar HTML dan CSS, 2013).

Electronic Voting (E-Voting)

E-voting merupakan sistem yang melakukan pencatatan dalam kegiatan pemungutan suara atau pemilihan suarayang menggunakan teknologi informasi dan komunikasi. (Absari, 2011) Fitur umum yang terdapat pada sistem e-voting yaitu :

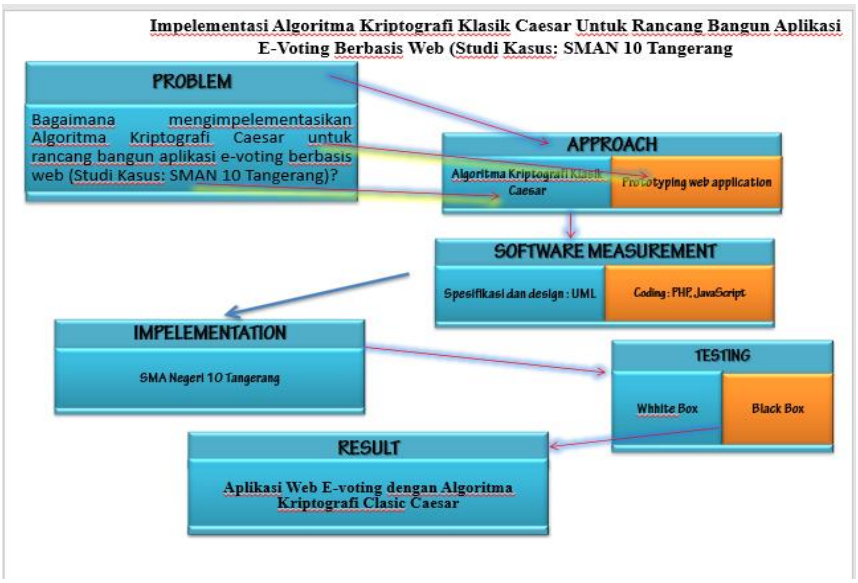
- Daftar user sebagai pemilih serta validasi (autentikasi) pemilih.
- Halaman untuk panitia (atau yang mengatur pemilu)
- Halaman untuk pemilihan voting

Menurut jurnal (Ridwan, Arifin & Yulianto, 2016). *E-voting* merupakan sistem pemilihan yang dilakukan dengan cara mencatat,menyimpan dan memproses dalam bentuk teknologi digital. *E-voting* memiliki sistem keamanan untuk menjamin suatu rahasia ataupun privasi hasil suara ataupun data pemilih, beberapa kriteria tersebut :

1) *Eligibility*, *User* pemilih yang melakukan pemilihan hanya yang telah terdaftar.
2) *Unreusability*, Pemilihan hanya bisa dilakukan satu kali.
3) *Anonymity*, Identitas user pemilih dirahasiakan
4) *Accuracy*, Pilihan yang telah dilakukan tidak bisa diubah selama pemilihan ataupun sesudah pemilihan.
5) *Fairness*, Hasil suara diperhitungkan sebelum selesai pemilihan tidak bisa dilakukan.
6) *Vote and Go*, *User* pemilih hanya bisa melakukan pemilihan saja
7) *Public Verifiability*, Hasil suara dipublikasi jumlahnya.

ANALISA SISTEM YANG BERJALAN

Penelitian ini dilaksanakan di sekolah SMAN 10 Tangerang. Penelitian ini dilaksanakan sesuai ruang lingkup yang telah dibatasi, ruang lingkup yang dibahas tentang voting dan penilaian hasil akhir dari perhitungan suara yang telah dipilih, serta keamanan data menggunakan algoritma yang telah ditentukan. Sedangkan waktu yang dilaksanakan untuk melakukan penilitian pada bulan Maret sampai dengan bulan April 2021. Adapun kerangka berpikir untuk memecahkan permasalahan pada penelitian algoritma kriptografi caesar dengan melalui tahapan-tahapan yang dimulai dari perumusan masalah sampai kesimpulan, yang membentuk sebuah alur yang sistematis. Kerangka ini digunakan sebagai pedoman dalam pelaksanaan penelitian agar hasil



yang dicapai tidak menyimpang dari tujuan yang telah ditentukan sebelumnya. Adapun diagram yang menjelaskan alur kerangka pemikiran seperti pada gambar dibawah ini:

Gambar 3. Kerangka Berfikir

Analisa Sistem

Di dalam analisa penelitian terhadap E-Voting dengan menggunakan model Algoritma Kriptografi caesar, dibutuhkan analisa terhadap sistem yang sedang berjalan beserta permasalahan pada tempat penelitian, yaitu di SMAN 10 Tangerang dengan permasalahan data pada pemilihan suara.

Analisa Masalah

Analisa masalah sangat diperlukan dalam perancangan suatu sistem agar kebutuhan sistem tersebut lebih jelas dan dapat dispesifikasi sehingga kriteria yang harus dipenuhi sistem dapat ditentukan, agar analisa yang dihasilkan nantinya dapat menjadi solusi atau usulan pemecahan masalah. Masalah yang dihadapi adalah adanya konflik siswa-siswi sekolah yang melakukan voting pemilihan calon kandidat calon ketua OSIS dengan cara curang, dengan demikian perlu dibuatnya sistem pemilihan yang dapat mengunci dari setiap pemilih dan suara hanya keluar satu kali dan tidak bisa diulang.

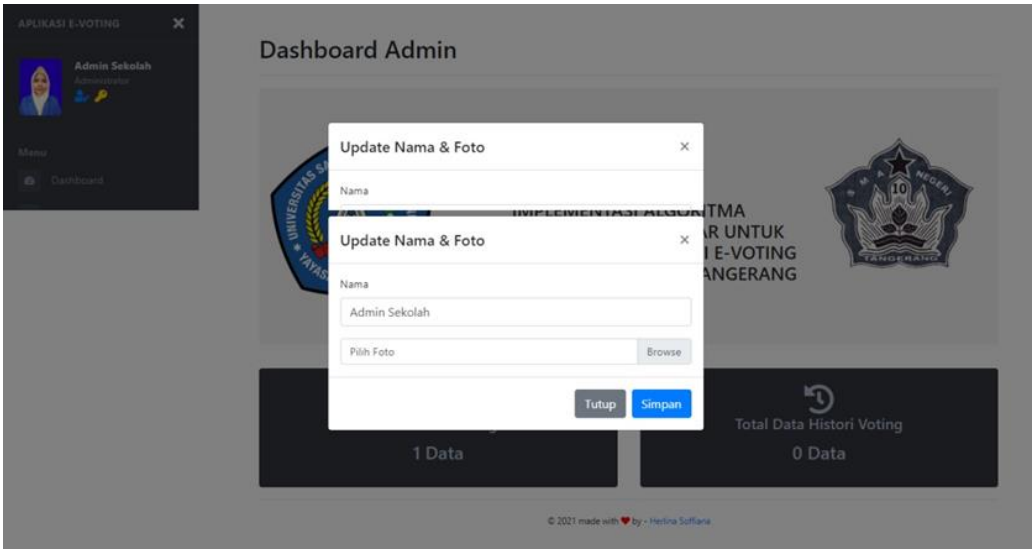
Usulan Pemecahan Masalah

Dari analisa masalah di atas maka dapat diusulkan pemecahan masalah yaitu dengan merancang aplikasi *e-voting* dengan Algoritma Kriptofgrafi Caesar secara online. Perancangan Aplikasi berisi Rancangan Input pemilih, Rancangan Proses menggunakan UML, dan Rancangan Sistem Aplikasi *e-voting.*

ANALISA DAN PEMBAHASAN

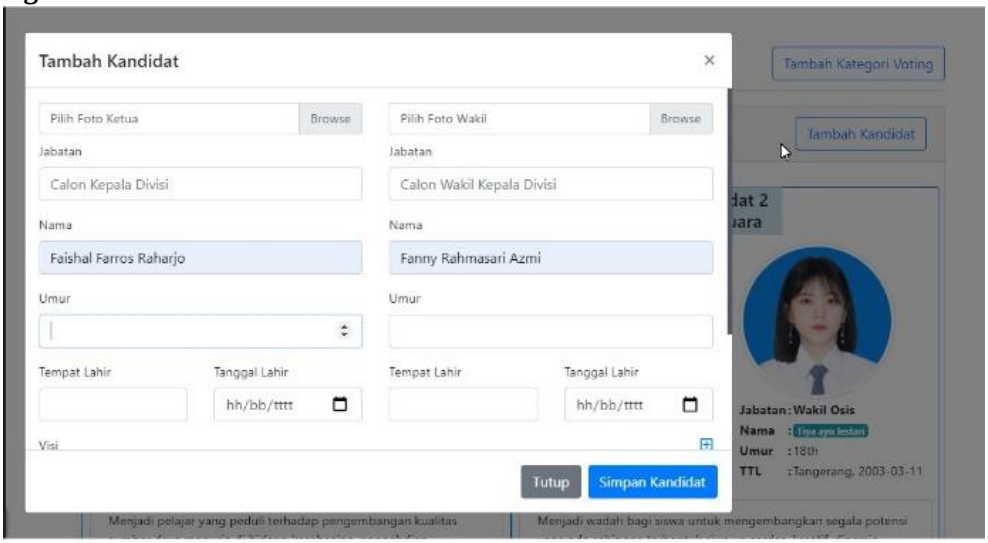
Rancagan Sistem Admin

Rancangan Sistem Admin adalah perancangan yang dirancang untuk menyediakan layanan seluruh pengguna dalam melakukan pemilihan suara sekaligus menyediakan atau mengekrips sistem pemilih. Dalam hal ini mengenai tampilan dari Sistem Aplikasi e-voting yang dibuat tampilan output secara umum terdiri :



Gambar 4. Rancangan Tampilan Menu Admin

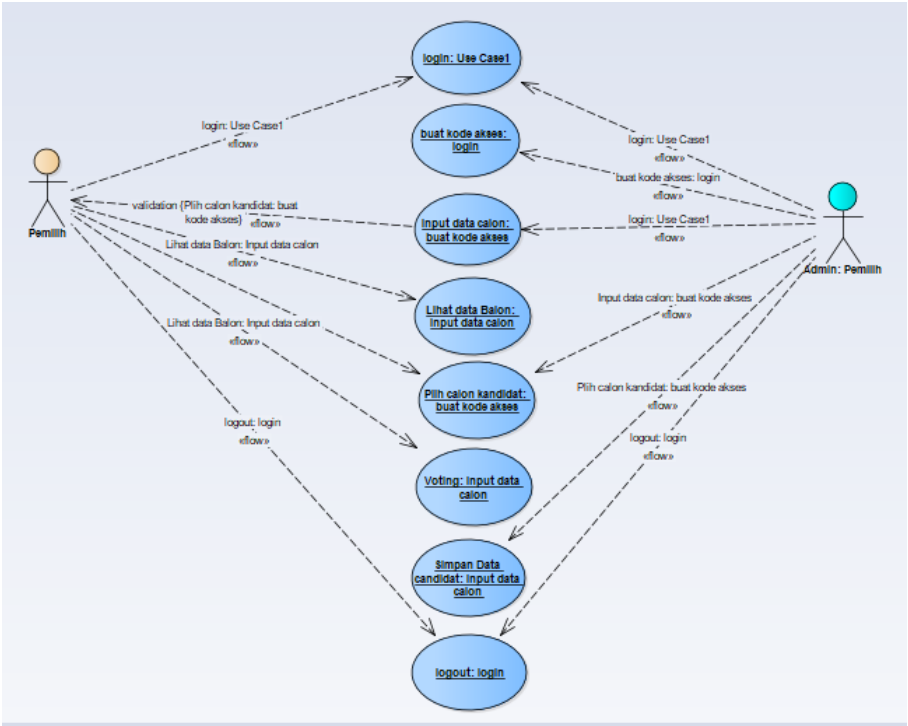
Rancangan Menu Kandidat



Gambar 5. Rancangan Menu Admin

Desain Modul

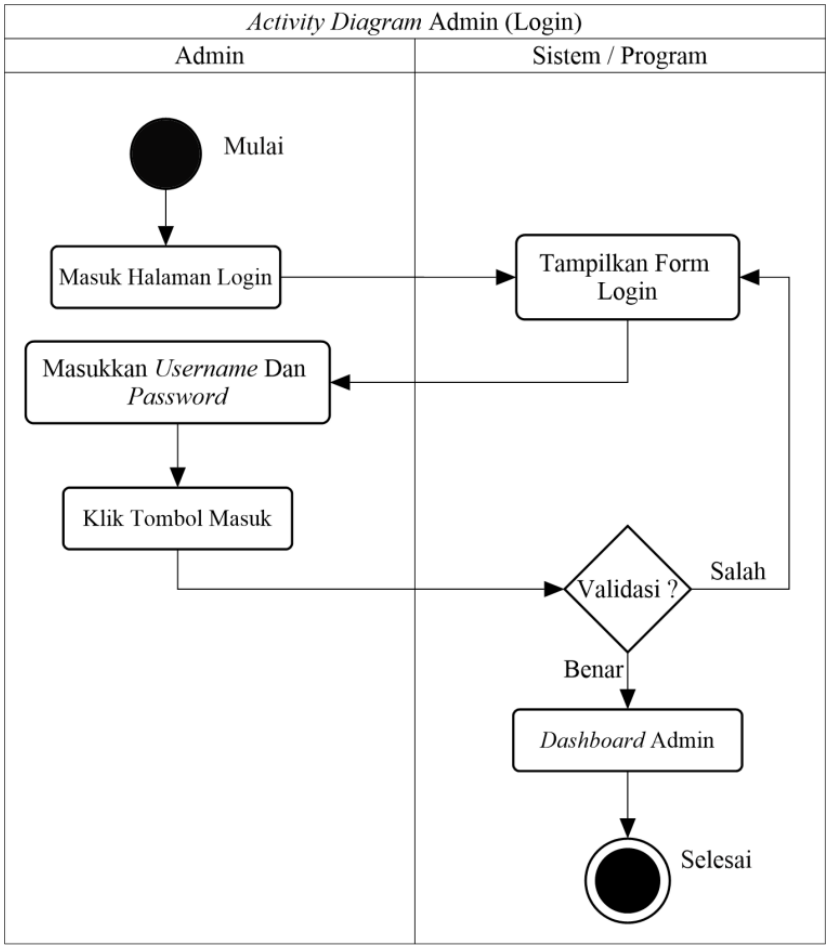
Pada pembahasan ini membahasa tentang Desain bagaiman modul program aplikasi e-voting dibuat dan ini merupakan hasil dokumentasi rancangan yang tertuang dalam sebuah *use case diagram*, yang menjelaskan dan mendeskripsikan tentang bagaimana interaksi sistem terhadap aktor sebagai pengguna, penjelasan tersebut dapat dijelaskan dengan diagram sebagai berikut:



Gambar 6. *Use case* pengguna

Activity Diagram Login

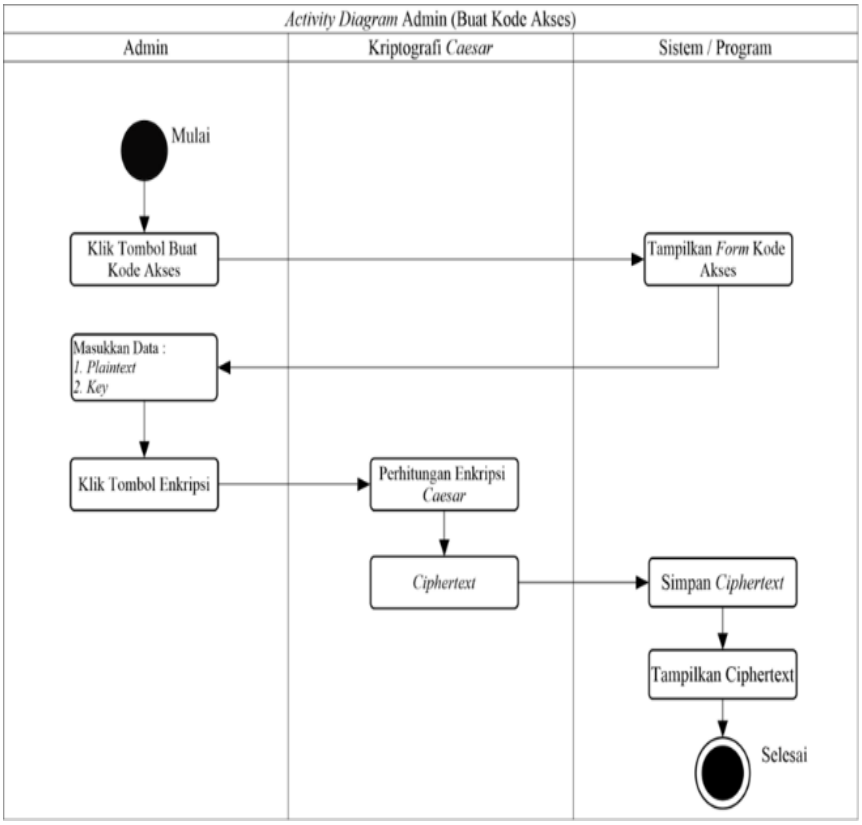
Dalam activity diagram ini menjelaskan tentang bagaimana suatu logika kerja procedural dengan keterangan bagaimana aktor bekerja dalam sebuah sistem, Ketika admin login, terdapat username dan password yang harus di masukkan untuk dapat login ke sistem e-voting.dengan demikian dapat dijelaskan pada gambar berikut:



Gambar 7. *Activity Diagram Login*

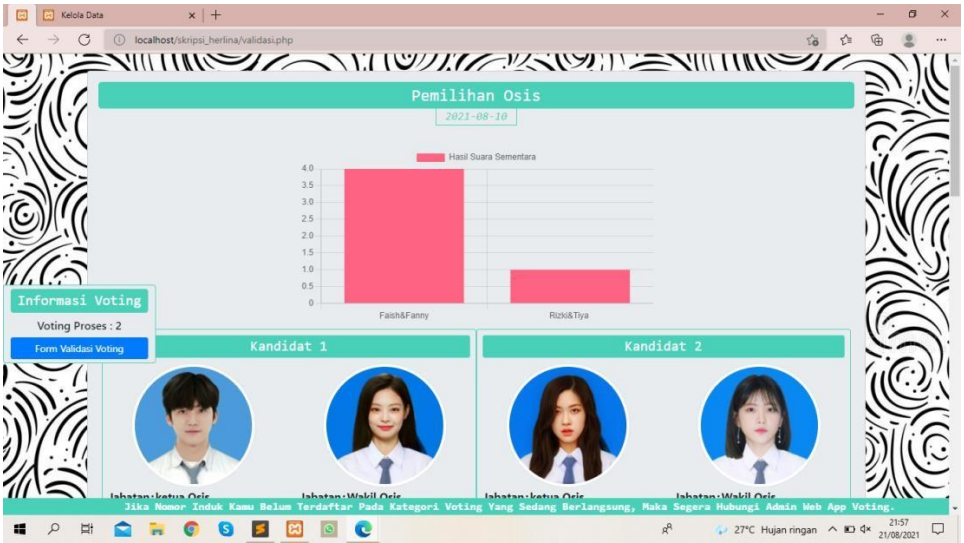
Activity Diagram Buat Kode Akses

Sebelum admin melakukan penginputan calon kandidat yang nantinya akan dipilih. Yang harus di input oleh admin adalah nomor induk,nama,foto,dan nomor kandidat balon (bakal calon), yang kemudian peserta atau pemilih yang sudah login akan mendapat kan kode akses untuk masuk ke dalam aplikasi dan bisa memilih baka calon lalu data tersebut ditampilkan diform dan nantinya akan di simpan di *database.*



Gambar 8. Activity Diagram Kode Akses

Halaman Grafik Bakal Calon



Gambar 9. Tampilan Hasil Bakal Calon

KESIMPULAN

Telah berhasil mengimpelentasikan dan merancang aplikasi e-voting dengan menggunakan Algoritma Kriptografi Caesar dengan baik walaupun dari segi tingkat error sebatas

kawajaran karena ini sebuah penelitian yang perlu terus dikembangkan, selaku peneliti menyadari bahwa dalam penelitian ini jauh dari kata sempurna dimana Rancangannya hanya sebatas berupa luaran bagaiman pada saat login di enkripsi dengan Bahasa yang bisa mengurangi kecurangan dalam sebuah suara, menu halaman utama yang memungkinkan para pemilih tetapa dapat menampilkan menu yang seharusnya, Rancangan Menu Admin, Rancangan Proses dengan menggunakan UML, sehingga ke depannya akan dikembangkan ke arah yang lebih baik lagi. Sebaiknya untuk pengembangan aplikasi selanjutnya yaitu dengan adanya penambahan fitur untuk mengekspor data dengan PDF maupun dengan excel untuk memudahkan admin atau pihak sekolah untuk merekap data hasil voting. Dan untuk bukti fisik hasil dari voting yang sudah dilakukan

DAFTAR PUSTAKA

Kromodimoeljo, S. (2009). Teori dan Aplikasi Kriptograf. SPK IT Consulting.

Simarmata, J., Sriadhi, & Rahim, R. (2020). Kriptografi, Teknik Keamanan Data Dan Informasi.

Absari, Y. (2011). Memperkenalkan Pemilihan Elektronik. Program Asia dan Pasifik Intrnationa IDEA.

Amin, M. M. (2016). IMPLEMENTASI KRIPTOGRAFI KLASIK PADA. Jurnal Pseudocode, 130.

Amirudin, D., Ruhiawati, I. Y., & Murnati. (2021). Rancang Bangun Aplikasi E- Voting Ketua Osis di SMA PGRI 1 Kota Serang. Jurnal Sistem Informasi dan Informatika.

Angriani, H., & Saharaeni, Y. (2019). IMPLEMENTASI ALGORITMA CAESAR CIPHER PADA IMPLEMENTASI ALGORITMA CAESAR

CIPHER PADA . Jurnal Teknologi Informasi dan Komunikasi.

Ariona, R. (2013). Belajar HTML dan CSS. Ariona, R. (2013). Belajar HTML dan CSS.

Ariyus, D. (2008). Pengantar Ilmu Kriptografi. Yogyakarta: C>V ANDI OFFSET.

Ariyus, D. (2008). Pengantar Ilmu Kriptografi. Yogyakarta: C.V Andi Offset.

Christian, A., Hesinto, S., & Agustina. (2018). Rancang Bangun Website Sekolah Dengan Menggunakan Framework Bootstrap (Studi Kasus SMP Negeri 6 Prabumulih). Jurnal Sisfokom, 22.

Enterprise, J. (2015). Mengenal Java dan Database dengan NetBeans. Jakarta: PT Elex Media Komputindo.

Ridwan , M., Arifin, Z., & Yulianto. (2016). RANCANG BANGUN E-VOTING DENGAN MENGGUNAKAN KEAMANAN ALGORITMA RIVEST

SHAMIR ADLEMAN (RSA) . Informatika Mulawarman, 2.

Sholiq. (2006). Pemodelan Sistem Informasi Berorientasi Obyek Dengan UML. yogyakarta: Graha Ilmu.

Siswanto, A., & Ferdiansyah. (2020). Pengamanan Transfer Data Pada API untuk Aplikasi E_Voting Menggunakan Algoritma RSA.

Yuliano, T. (2007). Pengenalan PHP. IlmuKomputer, 1-2.