`

Volume 20 Nomor 2 (2025) 1-11
E – Link P-ISSN 1858-2109 E-ISSN 2656-5676
Jurnal Teknik Elektro dan Informatika

IMPLEMENTASI KOMBINASI CAESAR CIPHER DAN POLYALPHABETIC CIPHER UNTUK KEAMANAN DATA PRIBADI PADA E-VOTING DALAM PEMILIHAN KETUA HUMANIKA

Yoshdianto Raka Akhdan Pratama[1)] , Arif Faizin[2)] , Ahmad Zulham Fahamsyah Havy[3)]
[1,2,3)] Jurusan Teknik Informatika, Fakultas Teknik, Universitas Yudharta Pasuruan
Jl. Yudharta No.7, Kembangkuning, Sengonagun, Kec. Purwosari, Pasuruan, Jawa Timur
E-mail : [1)]pratamaraka029@gmail.com, [2)]Arifusan@yudharta.ac.id, [3)]zulham92@yudharta.ac.id

ABSTRAK

Perkembangan teknologi digital yang pesat menuntut peningkatan keamanan data, terutama pada sistem e-voting yang rentan terhadap serangan siber. Penelitian ini mengimplementasikan kombinasi algoritma kriptografi Caesar Cipher (mod 10) dan Polyalphabetic Cipher (mod 26 berbasis Tabula Recta) untuk mengamankan data pribadi mahasiswa seperti nama dan NIM dalam pemilihan Ketua Himpunan Mahasiswa Teknik Informatika (HUMANIKA) di Universitas Yudharta Pasuruan. Metode ini dirancang untuk melindungi data dari kebocoran dan manipulasi melalui proses enkripsi dan dekripsi berlapis.Hasil penelitian menunjukkan bahwa kombinasi kedua algoritma ini menghasilkan sistem enkripsi yang efisien dan efektif dalam meminimalkan risiko serangan brute force serta analisis frekuensi. Caesar Cipher digunakan untuk mengenkripsi data numerik (NIM), sementara Polyalphabetic Cipher diterapkan pada data teks (nama). Pengujian keamanan dengan berbagai skenario kunci membuktikan bahwa sistem ini mampu menjaga kerahasiaan dan integritas data pemilih. Implementasi pada sistem e-voting berbasis web juga menunjukkan kemudahan penggunaan dan kecepatan proses tanpa mengorbankan keamanan.
Kata kunci: Kriptografi, *Caesar cipher*, *Polyalphabetic cipher*, *E-Voting*, *Tabula Recta*, Keamanan data

ABSTRACT

The rapid advancement of digital technology necessitates enhanced data security, particularly in e-voting systems vulnerable to cyber threats. This study implements a combination of Caesar Cipher (mod 10) and Polyalphabetic Cipher (mod 26 based on Tabula Recta) cryptographic algorithms to secure students' personal data, such as names and student ID numbers, during the election of the Head of the Informatics Engineering Student Association (HUMANIKA) at Yudharta Pasuruan University. This method is designed to protect data from leakage and manipulation through layered encryption and decryption processes. The results demonstrate that the combination of these algorithms produces an efficient and effective encryption system, minimizing the risk of brute force attacks and frequency analysis. Caesar Cipher is used to encrypt numerical data (student ID numbers), while Polyalphabetic Cipher is applied to textual data (names). Security testing with various key scenarios proves that the system successfully maintains voter data confidentiality and integrity. Implementation in a web-based e-voting system also highlights ease of use and processing speed without compromising security.
Keywords*: Cryptography, Caesar Cipher, Polyalphabetic Cipher, E-Voting, Tabula Recta, Data Security.*

1. PENDAHULUAN

Di era digital, keamanan data merupakan aspek kritis akibat tingginya aktivitas online, terutama dalam pengiriman data sensitif melalui jaringan publik. Risiko penyadapan dan akses ilegal dapat mengancam kerahasiaan dan integritas informasi, seperti yang terjadi pada sistem e-voting organisasi mahasiswa[1] Sebagai contoh, Himpunan Mahasiswa Teknik Informatika (HUMANIKA) Yudharta Pasuruan menggunakan sistem *e-voting* untuk pemilihan ketua organisasi, namun sistem ini rentan terhadap pencurian data, manipulasi suara, dan kecurangan. Oleh karena itu, diperlukan mekanisme keamanan yang kuat, seperti kombinasi algoritma *Caesar Cipher* dan *Polyalphabetic Cipher*, untuk memastikan kerahasiaan dan keabsahan proses pemilihan[2].

Bedasarkan permasalahan yang terjadi untuk itu di perlukan suatu metode untuk mengatasi permasalahan tersebut menggunakan Penerapan kombinasi *Caesar Cipher* dan *Polyalphabetic Cipher* dalam sistem *e-voting* pemilihan Ketua Humanika bedasarkan pada pertimbangan sistem keamanan berlapis dan efisiensi komputasi. *Caesar Cipher* sebagai algoritma kriptografi klasik menerapkan pergeseran karakter dengan nilai shift tertentu, namun memiliki kelemahan terhadap serangan *brute force* akibat terbatasnya variasi kunci[3]. Untuk mengatasi keterbatasan ini, dikombinasikan dengan *Polyalphabetic Cipher* yang menggunakan kunci lebih panjang dan multiple substitusi *alfabet* melalui mekanisme *Tabula Recta* dengan rumus matematis tertentu. Pendekatan ini mampu meningkatkan keamanan enkripsi dengan meminimalisir celah analisis frekuensi dan menghilangkan pola statistik pada teks terenkripsi[4].Kombinasi dua algoritma tersebut menghasilkan sistem enkripsi berlapis yang cocok untuk diterapkan pada sistem *e-voting* berbasis web atau aplikasi sederhana dengan kebutuhan skala pemilu internal[5]. Dalam pemilihan Ketua HUMANIKA, kerahasiaan suara merupakan prioritas, sehingga mekanisme enkripsi ganda ini dapat melindungi data pemilih dari kebocoran atau manipulasi. Solusi ini memberikan keseimbangan optimal antara tingkat keamanan dan kemudahan penerapan, khususnya untuk pemilihan dalam lingkup organisasi kemahasiswaan. Studi terdahulu menunjukkan bahwa algoritma kriptografi klasik seperti *Caesar Cipher* efektif dalam melindungi data numerik seperti NIM dengan menerapkan operasi modulo untuk mempertahankan konsistensi (Purnomo & Sembiring, 2022). Dengan penelitian yang berjudul ”Modifikasi Algoritma *Caesar Cipher* pada Kode *ASCII* dalam Meningkatkan Keamanan Pesan Teks”[6]. Penelitian lain juga pernah dilakukan oleh Qowi And Hudallah,2021 yang berjudul ”*Combining caesar cipher and hill cipher in the generating encryption key on the vigenere cipher algorithm*”[7]. Sementara itu, Polyalphabetic Cipher menawarkan keamanan lebih tinggi melalui substitusi alfabet multi-kunci, meminimalkan kerentanan terhadap analisis frekuensi[8]. Kombinasi kedua algoritma ini dianggap mampu menciptakan sistem enkripsi berlapis yang *robust* untuk aplikasi *e-voting*.

2. METODE PENELITIAN

Pada bagian ini membahas mengenai jenis data,metode dalam pengumpulan data yang akan di terapkan dalam metode kombinasi algoritma *caesar cipher* mod 10 dan *polyalphabetic cipher* mod 26 dan tahapan pengimplementasi.

2.1 Jenis Data

1. Data Primer

   Pada penelitian ini menggunakan data primer yang diperoleh secara langsung melalui organisasi internal mahasiswa teknik informatika (HUMANIKA) Dengan hasil wawancara ke teman teman mahaiswa informatika yudarttha dan mengambil sample keseluruhan mahasiswa teknik informatika yudartha pasuruan sebanyak 300 nama dan nim mahasiswa. [9].

2.2 Metode Pengumpulan Data

Pada penelitian ini menggunakan data sekunder, dimana data diperoleh dari sumber sumber yang sudah ada. Peneliti mendapatkan data nama mahasiswa dan nim

mahasiswa teknik informatika dari ketua program studi teknik informatika universitas yudharta pasuruan. Dengan data tentang presentase jumlah mahasiswa dan nim pribadi mahasiswa yang digunakan sampling pada penelitian ini.

2.3 Metode algoritma *Caesar Cipher* Mod 10

Caesar cipher merupakan metode enkripsi sederhana yang menerapkan teknik substitusi, di mana setiap huruf dalam pesan digeser sejumlah tertentu dalam alfabet[10].

Langkah-langkah dalam melakukan proses enkripsi dan dekripsi mod 10 dalam sistem e-voting. pada proses ini menggunakan mod 10 dikarenakan algoritma ini digunakan untuk proses enkripsi dan dekripsi pada angka (numerik) sebagai berikut :

a) masukan contoh sample nim mahasiswa seperti (0123456789)
b) penjelasan rumus enkripsi dan dekripsi :
   C : angka terdekripsi
   P : Angka asli
   Shift : jumlah pergeseran
   Mod 10 : operasi modulus untuk memastikan hasil tetap dalam rentang 0-9
c) lakukan proses enkripsi dengan menggunakan pergeseran shift 2 dengan menggunakan rumus :
   [C = (P + SHIFT) MOD 10]
d) Pada proses dekripsi ini teks yang terenkripsi dilakukan pergeseran shift 2 dengan menggunakan rumus :
   [P = (C – SHIFT) MOD 10]
e) dengan hasil proses enkripsi (2345678901) dan dekripsinya seperti ini : (0123456789)

2.4 Metode algoritma *Polyalphabetic Cipher* Mod 26 menggunakan *Tabula Recta*

Polyalphabetic Cipher merupakan teknik enkripsi yang memanfaatkan beberapa alfabet cipher, bukan hanya satu, untuk mengenkripsi teks. Metode ini dirancang untuk meningkatkan tingkat keamanan dibandingkan dengan *cipher* klasik seperti *Caesar Cipher* Dalam polyalphabetic cipher, setiap karakter pada teks asli *(plaintext*) dapat dienkripsi dengan alfabet *cipher* yang berbeda bergantung pada posisi karakter atau kunci yang digunakan. Hal ini menyebabkan pola frekuensi karakter dalam teks terenkripsi *(ciphertext*) menjadi lebih rumit, sehingga lebih sulit untuk dipecahkan[11].

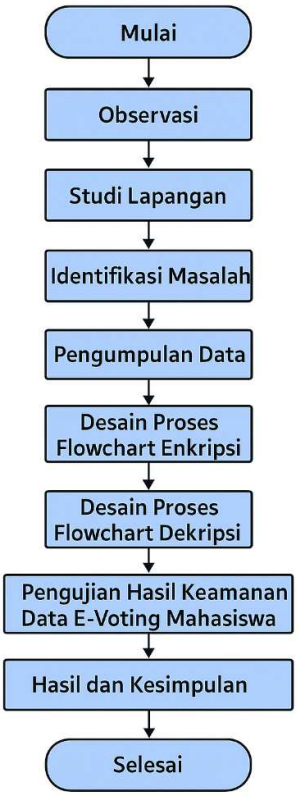
Langkah-langkah dalam melakukan proses enkripsi dan dekripsi mod 26 dalam sistem *e-voting.* pada proses ini menggunakan mod 26 dikarenakan algoritma ini digunakan untuk proses enkripsi dan dekripsi pada huruf (*alfabet*) sebagai berikut :

a) masukan contoh sample nim mahasiswa seperti (raka pratama)
b) penjelasan rumus enkripsi dan dekripsi :
   - C : Huruf *cipherteks* ke-1 (hasil enkripsi)
   - P : Huruf *plainteks* ke-1 yang dikonfersikan ke angka (A=0,B=1,...Z=25)
   - K : huruf kunci yang ke-1 dikonfersikan menjadi angka(kunci akan di ulang jika lebih pendek dari plainteks,contoh kunci "KEY" untuk plainteks nya HELLO menjadi "keyke")
   - mod 26 : operasi modulus 26 (karena alphabet latin memiliki 26 huruf) jika hasil p + k lebih besar dari 26 maka dikurangi 26 agar tetap rentang 0-25.
c) lakukan proses enkripsi dengan menggunakan kunci KEY dengan menggunakan rumus :
   [C = (P + K) MOD 26]
d) Pada proses dekripsi ini teks yang terenkripsi dilakukan kunci KEY dengan menggunakan rumus :
   [P = (C - K) MOD 26]
e) dengan hasil proses enkripsi :
   (beik tpkxywe) dan ketika nanti didekripsikan kembali menjadi teks seperti semula : (raka pratama)

2.5 Tahpan Alir Penelitian

pada Diagram ini mencakup proses mulai dari observasi hingga penyimpulan hasil, dengan pendekatan sistematis untuk memastikan keamanan data melalui teknik enkripsi dan dekripsi. Dan Diagram alir ini menunjukkan pendekatan metodologis yang terstruktur, mulai dari identifikasi masalah hingga validasi solusi. Dengan tahapan yang jelas, penelitian ini bertujuan untuk menciptakan sistem *e-voting* yang lebih aman dan terpercaya bagi mahasiswa.

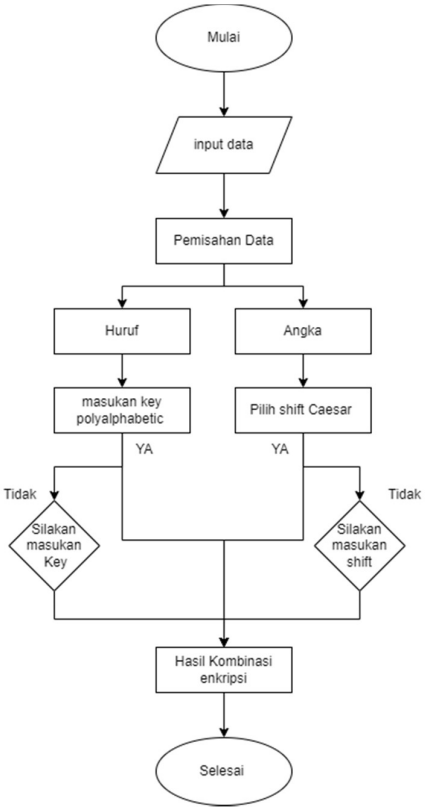
Serta Penelitian ini diawali dengan Observasi dan Studi Lapangan untuk mengidentifikasi kerentanan keamanan data pribadi mahasiswa (seperti NIM dan nama) pada sistem e-voting pemilihan Ketua Humanika. Selanjutnya, dilakukan Pengumpulan Data sebagai dasar perancangan sistem kriptografi, di mana NIM mahasiswa dienkripsi menggunakan Caesar Cipher mod 10 untuk menggeser digit-digit NIM secara siklis sesuai kunci numerik, sementara nama mahasiswa dienkripsi dengan Polyalphabetic Cipher mod 26 yang memanfaatkan deretan kunci huruf untuk menghasilkan substitusi alfabet yang dinamis. Proses enkripsi dan dekripsi dirancang dalam Flowchart yang sistematis, mencakup pembangkitan kunci, transformasi data, serta validasi integritas. Pada tahap Pengujian Keamanan, sistem dievaluasi terhadap serangan brute-force dan analisis frekuensi untuk memastikan kekuatan algoritma dalam melindungi kerahasiaan data. Hasil penelitian menunjukkan bahwa kombinasi kedua algoritma ini efektif meningkatkan keamanan data pribadi, dengan Caesar Cipher mod 10 menjaga kerahasiaan NIM dan Polyalphabetic Cipher mod 26 menyulitkan dekripsi nama tanpa kunci yang tepat, sehingga sistem e-voting menjadi lebih tahan terhadap kebocoran informasi sensitif.



Gambar 1.Diagram Alir Penelitian

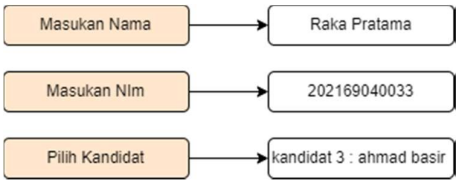
3. HASIL DAN DISKUSI

Pada hasil dan pembahasan ini menjelaskan bagaimana proses enkripsi dalam sistem *e-voting* yang sudah dijelaskan pada diagram alir dibawah ini. Pada diagram alir ini menjelaskan mekanisme enkripsi data yang menerapkan gabungan metode *Polyalphabetic Cipher* dan *Caesar Cipher* secara terstruktur. Tahapan awal dimulai dengan penerimaan data input yang akan dienkripsi, kemudian dilakukan klasifikasi data berdasarkan karakteristiknya menjadi komponen huruf dan numerik. Sistem kemudian memverifikasi validitas kunci enkripsi *Polyalphabetic Cipher* yang dimasukkan pengguna, dengan mekanisme permintaan input ulang jika kunci tidak memenuhi persyaratan.



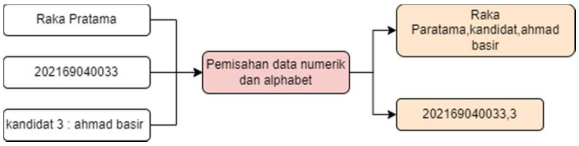
Gambar 2.Flowchart Proses Enkripsi

Pada penelitian selanjutnya adalah proses dari bagian enkripsi yang bertahap dari input data,proses pemisahan data dari huruf dan angka /alphabet dan numerik yang menggunakan huruf menggunakan *polyalphabetic cipher* dan numerik menggunakan *caesar cipher,* hasil kombinasi enkripsi.



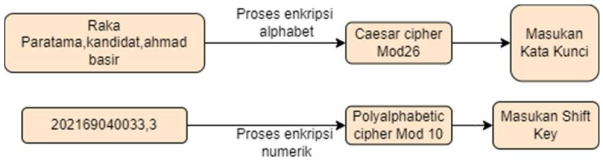
Gambar 3. Proses input data

Pada tahap ini, pengguna akan memasukkan data pribadi seperti nama, NIM, serta pilihan nama dan nomor urut calon Ketua Humanika. Data nama berupa teks, sedangkan NIM atau ID berupa angka.



Gambar 4. Proses Pemisahan data plainteks

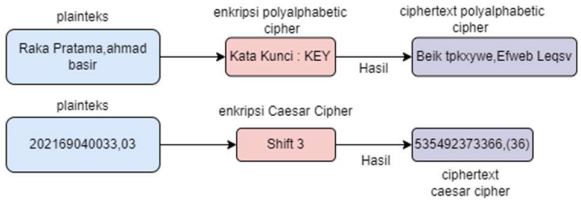
Setelah data diinput, tahap selanjutnya adalah memisahkan data menjadi dua kategori, yaitu huruf (alphabet) dan angka (non-alphabet). Pemisahan inidilakukan agar setiap jenis data dapat diproses menggunakan metode kombinasi enkripsi, yaitu *Caesar Cipher* untuk angka dan *Polyalphabetic Cipher* untuk huruf.



Gambar 5 Proses enkripsi data

Pada tahap ini, data huruf dan angka dienkripsi menggunakan metode yang berbeda. Data huruf dienkripsi menggunakan *Polyalphabetic Cipher*, di mana setiap huruf dienkripsi berdasarkan kunci yang telah ditentukan. Contohnya, teks "HELLO" dengan kunci "KEY" akan dienkripsi menjadi "RIJVS". Sementara itu, data angka dienkripsi menggunakan Caesar Cipher, di mana setiap digit angka digeser sesuai nilai shift yang telah ditentukan. Contohnya, angka "1234" dengan shift = 6 akan dienkripsi menjadi "7890".

Setelah proses enkripsi selesai, hasil dari kedua metode enkripsi digabungkan menjadi satu data terenkripsi yang sulit dibaca oleh pihak lain. Contohnya, jika data huruf terenkripsi adalah "RIJVS" dan data angka terenkripsi adalah "7890", maka data gabungannya adalah "RIJVS7890

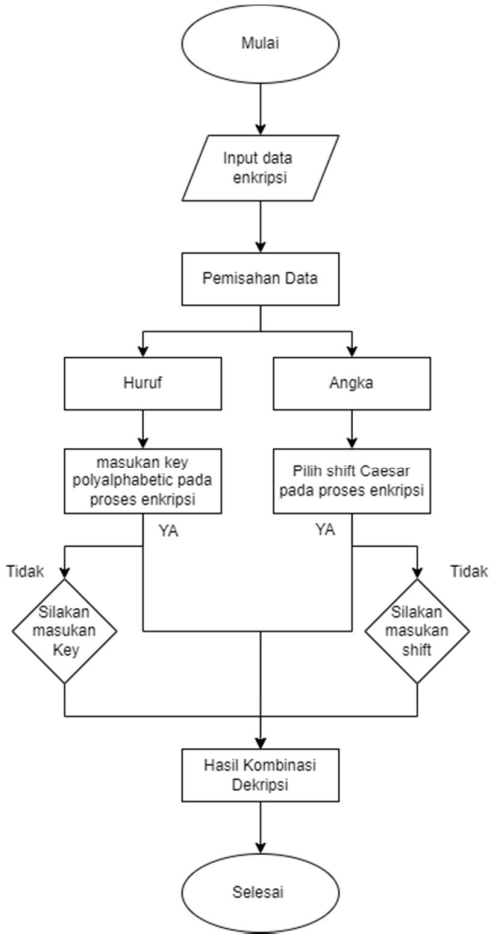


Gambar 6. Hasil proses enkripsi data

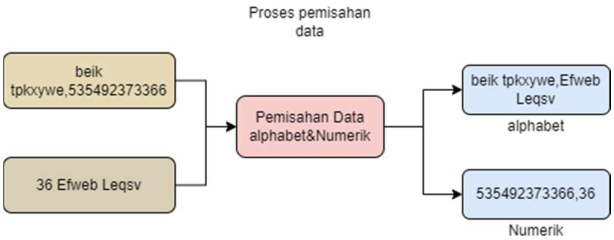
`

Pada Proses Hasil ini Metode *Polyalphabetic Cipher* menerapkan proses enkripsi pada plainteks "Raka Pratama, ahmad basir" dengan memanfaatkan kata kunci "KEY", menghasilkan ciphertext "Belk tpkovwe, Efweb Legsv". Pada metode ini, setiap karakter pada plainteks mengalami pergeseran sesuai dengan huruf kunci yang bersesuaian. Di sisi lain, Caesar Cipher mengimplementasikan pergeseran tetap sebesar 3 posisi (Shift 3) pada plainteks numerik "202169040033.03", sehingga menghasilkan ciphertex"535492373366.(36)", di mana setiap digit dan simbol mengalami transformasi berdasarkan urutan ASCII/alfabet.

Serta Pada *Flowchart* ini menjelaskan prosedur dekripsi data yangsebelumnya dienkripsi menggunakan gabungan *Polyalphabetic Cipher* dan *Caesar Cipher.* Proses diawali dengan memasukkan data terenkripsi, kemudian sistem akan memisahkan data menjadi komponen huruf dan angka. Tahap krusial berikutnya adalah penginputan kunci *Polyalphabetic* yang harus sama persis dengan yang digunakan saat enkripsi - sistem akan memverifikasi validitas kunci dan meminta input ulang jika tidak sesuai. Demikian pula dengan nilai shift Caesar yang harus dimasukkan secara akurat sesuai parameter enkripsi awal. Setelah semua parameter terverifikasi, sistem akan menjalankan dekripsi dua tahap: pertama dengan *Caesar Cipher* menggunakan shift yang ditentukan, dilanjutkan *Polyalphabetic Cipher* dengan kunci yang dimasukkan. Proses ini menghasilkan data asli yang telah berhasil dikembalikan, menekankan pentingnya konsistensi parameter antara proses enkripsi dan dekripsi untuk memastikan keakuratan hasil akhir. *Flowchart* ini secara jelas menunjukkan bahwa dekripsi merupakan proses kebalikan dari enkripsi dengan urutan algoritma yang terbalik namun tetap mempertahankan mekanisme validasi yang ketat.

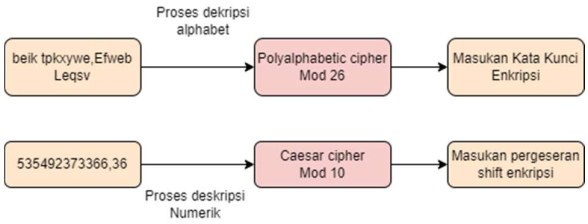


Gambar 7.Flowchart Proses Dekripsi



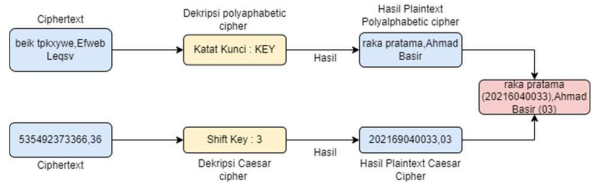
Gambar 8.Proses .Pemisahan Data Dekripsi (cipherteks)

Setelah data dipisahkan menjadi bagian alfabet dan numerik, langkah berikutnya adalah mengembalikan data yang telah terenkripsi (*ciphertext*) menjadi data terdekripsi (*plaintext*) atau data yang dapat dibaca oleh pengguna dengan memasukan key dan shift yang telah dimasukkan.



Gambar 9. Proses dekripsi data

Proses dekripsi data dilakukan melalui dua tahap utama, yaitu dekripsi alfabet dan dekripsi numerik. Untuk data alfabet seperti "belk tpkoywe, Erweb Legsv", digunakan metode Polyalphabetic Cipher dengan perhitungan Mod 26. Sedangkan data numerik seperti "535492373366,36" didekripsi menggunakan Caesar Cipher dengan operasi Mod 10



Gambar 10. Hasil pengabungan dekripsi data

Data asli kemudian ditampilkan kepada pengguna atau sistem dalam tahap "Tampilkan Data Asli", yang bertujuan memastikan data dapat diakses dan digunakan kembali dalam bentuk semula. Setelah kedua proses selesai, data alfabet dan numerik digabungkan, menghasilkan output akhir berupa "raka pratama (202169040033), Ahmaq Basir (03)". Gambar tersebut memperlihatkan konversi ciphertext ke plaintext melalui metode dekripsi yang sesuai untuk masing-masing jenis data.

Pada proses Pengujian diawali dengan menyiapkan skenario simulasi serangan siber, seperti *brute force attack* serta data *Dummy* yang digunakan berupa daftar pemilih mahasiswa beserta informasi sensitif seperti NIM dan nama mahasiswa. Data ini kemudian dienkripsi menggunakan kombinasi Caesar Cipher (pergeseran karakter) dan Polyalphabetic Cipher (menggunakan kunci berbasis kata/frase) agar tidak terjadi manipulasi data dan kebocoran data pada sistem pemilihan ketua HUMANIKA menggunakan E-voting. Dengan pengambilan sample 20 nama mahasiswa dan nim mahasiswa :

Nama	NIM	Nama	NIM
Nur Romadhoni Hidayat	2021690 40001	Al Quddus Himalaya Anwar	2021690400 15
Zuhriya Ning Toyibah	20216904 0017	Nur Kholis Majid	2021690400 18
Abdul Mujib	20216904 0029	Mukhamm ad Fuad	2021690400 35
raka pratama	20216904 0033	Salman Alfarizy	2021690400 36
Ulul Albab	20216904 0037	Rizki Azizah	2021690400 34
lailul Karim	20216904 0045	Uliana	2021690400 38
Jajang Seto	20226904 0010	Ahmad Farid Anwari	2022690400 30
Fadia Ita Wulandari	20226904 0014	Akhmad Zainal Abidin	2022690400 32
Muhammad Ikhwan	20226904 0018	Mochamad Zidan Bisry	2022690400 38
Danava Alvinur Rahma	20226904 0021	Abdurahm an	2022690400 48

Gambar 1. Sample Nama dan Nim Asli

Pada sample nama diatas bedasarkan sampling 3 nama tersebut akan di enkripsi pada sistem e-voting pemilihan ketua humanika yang menggunakan algoritma kriptografi kombinasi untuk huruf menggunakan algoritma polyalphabetic cipher mod 26 dan untuk nim/numerik menggunakan algoritma caesar cipher mod 10.

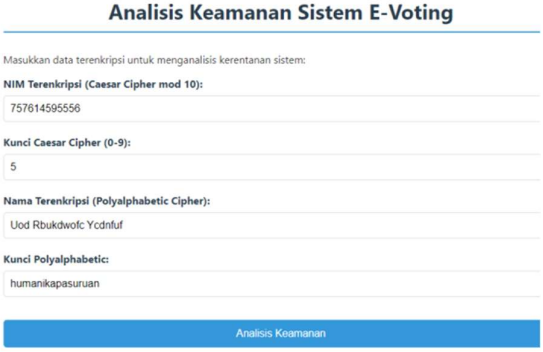
Dan berikut adalah sampling data nama mahasiswa yang terenkripsi nama menggunakan kunci polyalphabetic cipher mod 26 dan untuk numerik menggunakan caesar cipher mod 10 :

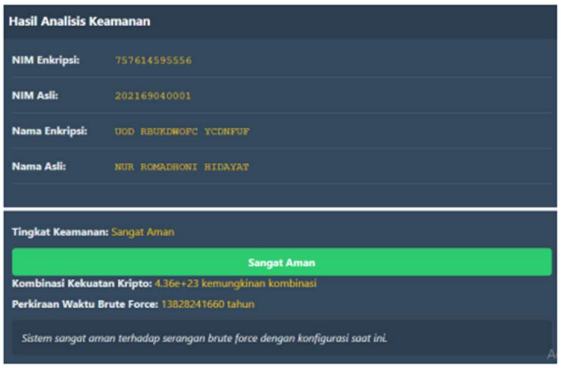
Nama	NIM	Nama	NIM
Uod Rbukdwofc Ycdnfuf	7576145955 56	Gotrvgk Nxny Nfsiohb	7576145955 62
Hf Cuqles Wieucuyn Hhiae	7576145955 60	Uod Kuwvih Msdzx	7576145955 63

Hvpuy Uejxb	757614595574	Yuwa Czktpms	757614595588
Towhnuwas Fmuu	757614595580	Zuxmnv Kluajcqs	757614595581
Towhnukd Jlmf Rfbni	757614595582	Yclkv Ijityw Hgmlvi	424381262256
fyxsox Knzsm	424381262267	Bfuaai	424381262250
Quvaao Cenm Cbadouw	424481262232	Mupin qda qsahhpaeq	424481262236
Totazukd Ciwduz Ay Uebupdr	424481262230	Kuzaii Klpgcbl Dauuk	424481262243
Hbyaq Nkrcb Puqmrv	424481262252	Hvpueirmul	424481262260
Ammbvbkh Jsiyc Eayakbcjp	424481262261	Hxxiz Usfnywbxpia	424381262293

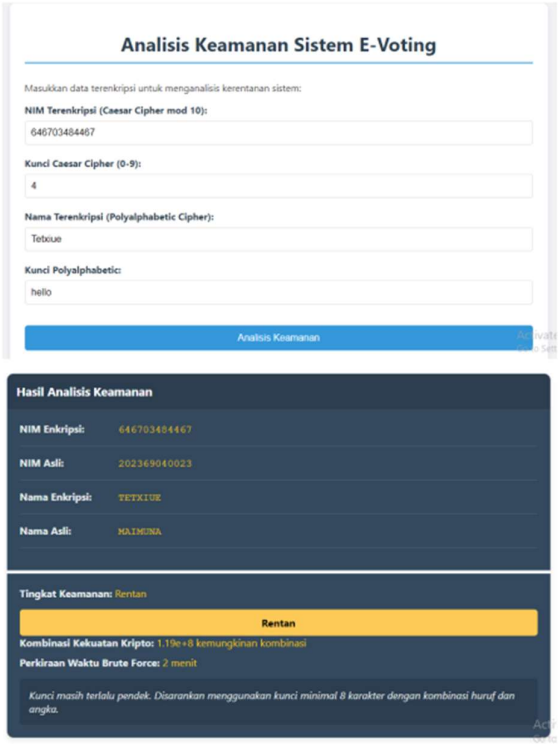
Tabel 2. Sample nama dan nim terenkripsi

Setelah dilakukan pengujian terhadap 20 data sampel mahasiswa yang telah dienkripsi untuk mengukur kerentanan terhadap serangan brute force. Proses pengujian dilakukan dengan menggunakan berbagai variasi kunci enkripsi seperti KEY, HELLO, dan HUMANIKAYUDHARTA Hasil pengujian tersebut kemudian dianalisis untuk mengevaluasi tingkat keamanan sistem proteksi data pemilih mahasiswa di organisasi Humanika. Serta pada hasil pengujian algoritma kombinasi kriptografi caesar cipher dan polyaphabetic cipher yang menggunakan bahasa pemograman php pada gambar pengujian di bawah ini :





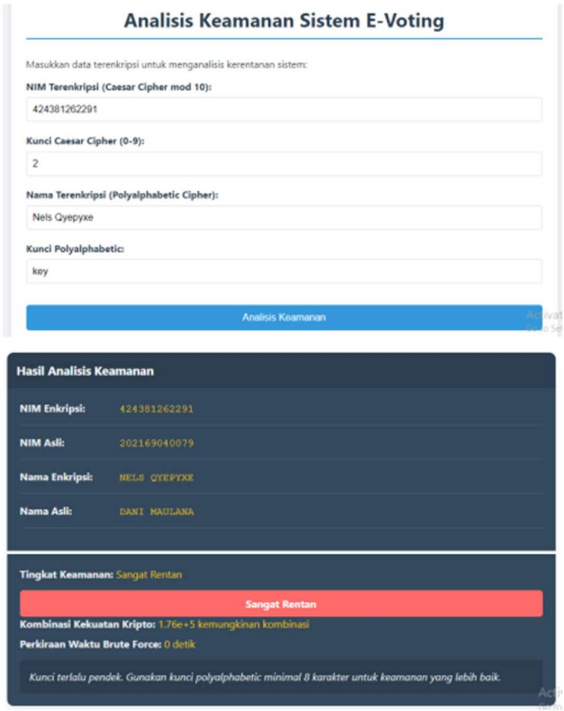
Gambar 13. Pengujian hasil keamanan kunci Humanika pasuruan



Gambar 14. Pengujian kerentanan dengan kunci hello

Pada hasil pengujian ini menghasilkan nama asli "maimuna" dan untuk nim asli "202369040023" dengan tingkat Keamanan sistem ini dinilai Rentan. Analisis menunjukkan bahwa kombinasi kekuatan kriptografi hanya menghasilkan 1.19×10^8 kemungkinan kombinasi, yang tergolong sangat rendah. Dengan kekuatan komputasi modern, kunci ini dapat dibobol melalui serangan brute force dalam waktu sekitar 2 menit. serta Kunci yang digunakan saat ini terlalu pendek dan mudah

ditebak. Untuk meningkatkan keamanan, disarankan menggunakan kunci minimal 8 karakter dengan kombinasi huruf(baik huruf besar maupun kecil) Hal ini akan secara signifikan memperbesar kompleksitas kunci dan memperpanjang waktu yang dibutuhkan untuk membobol sistem.

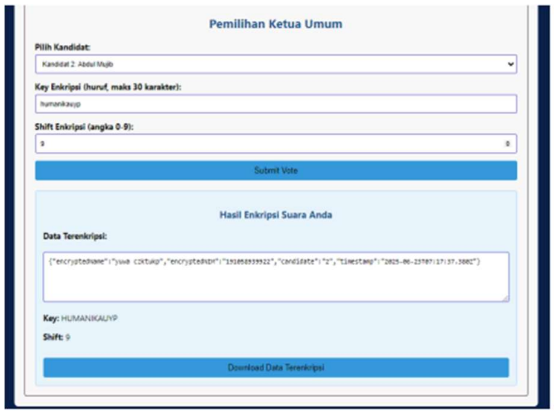


Gambar 15. Pengujian kerentanan kunci KEY

Hasil evaluasi menunjukkan bahwa mekanisme enkripsi yang saat ini diterapkan memiliki tingkat proteksi yang sangat rendah. Kriptografi yang digunakan dinilai "Sangat Rentan" dengan kompleksitas kunci yang hanya menyediakan sekitar 166.666 variasi kombinasi ($1/6\times10^5$). Kondisi ini memungkinkan proses pembongkaran kunci dapat dilakukan secara instan (0 detik) melalui teknik brute force. Masalah utama terletak pada implementasi kunci yang terlalu sederhana, baik dari segi panjang maupun kompleksitas karakter. Kunci enkripsi yang pendek dan mudah diprediksi ini tidak mampu memberikan perlindungan data yang memadai. implementasi algoritma Caesar Cipher mod 10 dan Polyalphabetic Cipher mod 26 pada sistem e-voting pemilihan ketua umum menawarkan peningkatan keamanan berlapis melalui proteksi ganda terhadap data pemilih.

Jadi untuk kesimpulan hasil seperti testing ujicoba beberapa sample nama dan nim mahasiswa diatas dengan kata kunci yang berbeda akan menghasilkan hasil kekuatan kombinasi yang berbeda serta semakin panjang kunci kosakata yang digunakan maka lebih baik untuk digunakan sebagai kata kunci agar tidak terjadi perentasan data manipulasi data dan menangkal serangan brute force dan frekuensi analisis data.

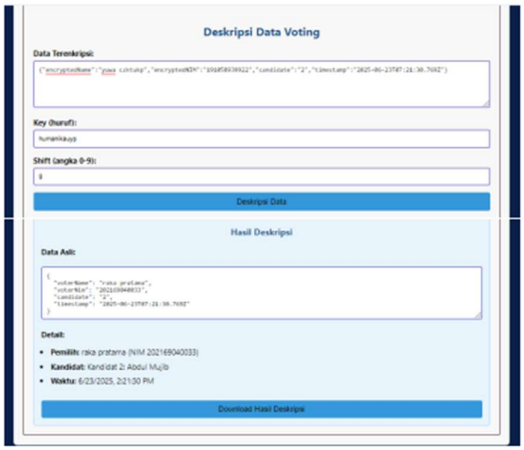
Gambar 16.Tampilan e-voting pemilihan kandidat



Gambar 17.Tampilan enkripsi data

Setelah pemilih atau mahasiswa sudah vertifikasi pada form yang pertama jika vertifikasi berhasil akan langsung menuju pada form tabel pemilihan pada tahapan ini para pemilih atau para mahasiswa yang memiliki hak suara akan memilih siapa calon kandidatnya dan akan memasukkan key yang digunakan dan sudah

disiapkan oleh panitia terkait key dari polyalphabetic cipher dan key dari caesar cipher itu sendiri. Serta Pada gambar 17. Menjelaskan tentang hasil enkirpsi data. Setelah mengisikan pada form pemilihan dan sudah menginputkan key pada cesar cipher dan polyalphabetic cipher makan akan keluar dengan hasil enkripsinya yang berupa cipher teks.



Gambar 18. Hasil proses dekripsi data

pada gambar diatas menjelaskan terkait bagaimana cara untuk mendekripsikan terkait teks yang sudah dienkripsi menggunakan algoritma caesar cipher dan polyalphabetic cipher agar teks bisa dibaca atau di pahami.dan secara keseluruhan pada proses ini menjelaskan terkait proses enkripsi dan deskripsi data voting dengan memasukan teks yang sudah dienkripsi serta memasukan kunci caesar cipher yang sudah digunakan dan kunci polyalphabetic yang sudah digunakan untuk mengetahui hasil teks dekripsi dari teks enkripsi pada data e-voting tersebut.

Bedasarkan penelitian ini terdapat keunggulan utama dalam implementasi sistem enkripsi berlapis yang mengintegrasikan algoritma caesar cipher dan Polyalphabetic Cipher. Pendekatan ini mampu meningkatkan keamanan data secara signifikan melalui peningkatan kompleksitas enkripsi, sehingga meminimalisasi kemungkinan pembobolan atau manipulasi hasil pemilihan oleh pihak yang tidak berwenang. Algoritma Caesar Cipher, meskipun sederhana dalam struktur, memberikan efisiensi dalam proses enkripsi dasar. Sementara itu, Polyalphabetic Cipher berfungsi sebagai penguat keamanan dengan menerapkan multi-kunci yang menghasilkan pola enkripsi acak dan sulit diprediksi. Kombinasi kedua algoritma ini menjamin perlindungan ganda terhadap kerahasiaan data pemilih dan integritas hasil pemilihan, dimana semua data akan melalui proses enkripsi dua lapis sebelum penyimpanan atau transmisi. Keunggulan tambahan mencakup kemampuan sistem dalam menangkal serangan brute force dan analisis frekuensi yang umumnya menjadi kelemahan sistem enkripsi tunggal. Dengan demikian, integrasi kedua algoritma tersebut tidak hanya memperkuat keamanan sistem e-voting, tetapi juga menjamin keandalan dan akurasi proses penghitungan suara.

4. KESIMPULAN DAN SARAN

Kombinasi algoritma Caesar Cipher (mod 10) dan Polyalphabetic Cipher (mod 26) terbukti efektif dalam meningkatkan keamanan sistem e-voting melalui enkripsi berlapis. Caesar Cipher berfungsi mengamankan data numerik seperti NIM, sementara Polyalphabetic Cipher melindungi data tekstual seperti nama. Pendekatan ini menciptakan lapisan keamanan ganda yang spesifik untuk masing-masing jenis data, memperkuat pertahanan terhadap serangan brute force dan analisis frekuensi. Dengan mekanisme enkripsi yang berbeda pada tiap tipe data, sistem ini mampu mengurangi risiko peretasan secara signifikan.

pada penelitian ini kombinasi kriptografi klasik yang memiliki keterbatasan keamanan ketika penyerangan cyber lebih modern Berdasarkan penemuan tersebut, peneliti merekomendasikan untuk mempertimbangkan integrasi dengan metode kriptografi modern seperti AES (simetris) atau RSA (asimetris),blowfish,sha-256 dan kontemporer guna meningkatkan tingkat proteksi data dan menjaga kerahasiaan informasi pemilih dalam sistem evoting Humanika secara lebih optimal dan meningkatkan efektivitas perlindungan kerahasiaan data pemilih dalam sistem e-voting Humanika.

5. DAFTAR PUSTAKA

[1] M. B. Yel dan M. K. M. Nasution, "KEAMANAN INFORMASI DATA PRIBADI PADA MEDIA SOSIAL," *JIK*, vol. 6, no. 1, hlm. 92–101, Jan 2022, doi: 10.59697/jik.v6i1.144.

[2] V. M. Hidayah, D. I. Mulyana, dan Y. Bachtiar, "Algoritma Caesar Cipher atau Vigenere Cipher pada Pengenkripsian Pesan Teks," *joe*, vol. 5, no. 3, hlm. 8563–8573, Feb 2023, doi: 10.31004/joe.v5i3.1647.

[3] A. W. Aranski, R. Wahdini, F. Anggraini, dan F. Khairani, "IMPLEMENTASI ALGORITMA CAESAR CIPHER UNTUK KEAMANAN DATA ANGGOTA PERPUSTAKAAN DI UNIVERSITAS XYZ," vol. 2, no. 1, 2023.

[4] A. I. Simamora, O. K. Sulaiman, M. Kom, M. Z. Siambaton, dan M. Kom, "KEAMANAN DATA HASIL E-VOTING PEMILIHAN KEPALA DESA DENGAN ALGORITMA VIGENERE CIPHER PERTUKARAN KUNCI THREE PAS PROTOCOL PADA KECAMATAN BARUS KABUPATEN TAPANULI TENGAH," 2022.

[5] A. F. Al Firah, "EVALUASI KEBIJAKAN SISTEM E-VOTING PEMILIHAN KETUA OSIS SEBAGAI MEDIA PARTISIPASI DEMOKRASI PADA SISWA SMK SWASTA TIK DARUSSALAM MEDAN," *WDW*, vol. 15, no. 4, hlm. 443–452, Nov 2021, doi: 10.46576/wdw.v15i4.1520.

[6] H. D. Purnomo dan I. Sembiring, "Modifikasi Algoritma Caesar Cipher pada Kode ASCII dalam Meningkatkan Keamanan Pesan Teks," *JOURNAL OF INFORMATION TECHNOLOGY*, 2022.

[7] Z. Qowi dan N. Hudallah, "Combining caesar cipher and hill cipher in the generating encryption key on the vigenere cipher algorithm," *J. Phys.: Conf. Ser.*, vol. 1918, no. 4, hlm. 042009, Jun 2021, doi: 10.1088/1742-6596/1918/4/042009.

[8] M. Mahmudah, T. N. Irawati, dan F. B. N. Aini, "Polyalphabetic cipher cryptosystem application in making anti-hacker passwords learning management systems in junior high schools," *Alifmatika J. Pendidik. dan Pembelajaran Mat.*, vol. 6, no. 1, hlm. 90–103, Jun 2024, doi: 10.35316/alifmatika.2024.v6i1.90-103.

[9] Veronika Primadyanti Jaga Waleng, I Gede Putu Krisna Juliharta, dan Ketut Queena Fredlina, "IMPLEMENTASI E-VOTING PEMILU RAYA MAHASISWA UNIVERSITAS PRIMAKARA BERBASIS WEB (STUDI KASUS PADA UNIVERSITAS PRIMAKARA)," *JUTIK*, vol. 9, no. 5, Okt 2023, doi: 10.36002/jutik.v9i5.2640.

[10] M. Hidayat, M. Tahir, A. Sukriyadi, A. Sulton, C. A. S. A, dan S. A. F, "PENERAPAN KRIPTOGRAFI CAESAR CHIPER DALAM PENGAMANAN DATA," *JUKIM*, vol. 2, no. 03, hlm. 35–41, Mei 2023, doi: 10.56127/jukim.v2i03.619.

[11] D. Bhatia dan M. Dave, "Elliptic Curve Layered: A Secure Polyalphabetic Vignere Cryptographic Algorithm for Textual Data," *JSR*, vol. 65, no. 01, hlm. 222–229, 2021, doi: 10.37398/JSR.2021.650128.