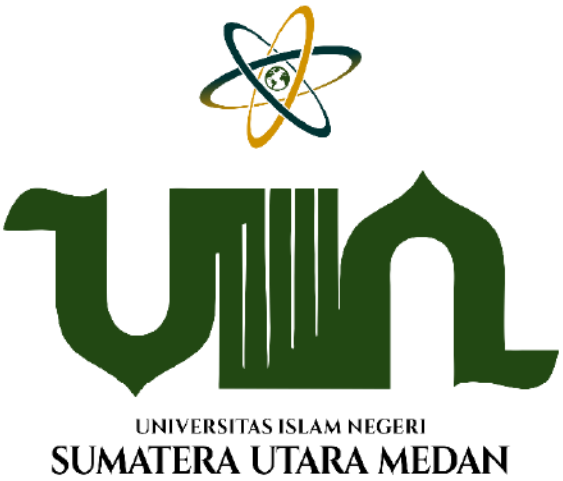


LAPORAN PENELITIAN
PENGAMANAN PESAN TEKS MENGGUNAKAN ALGORITMA MYSZKOWSKI BERBASIS WEB

OLEH:
ADNAN BUYUNG NASUTION
NIP: 199008092019031014

PROGRAM STUDI SISTEM INFORMASI
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI SUMATERA UTARA MEDAN
2023

KATA PENGANTAR

Segala puji dan syukur penulis lantunkan ke hadirat Allah Swt yang mana atas karunia-Nya penulis telah dapat menyusun laporan penelitian ini hingga proses pengerjaannya telah selesai. Kemudian kami hadiah salam serta ucapan Allahumma sholli ’ala Muhammad wa ’ala ali Muhammad untuk nabi kita Nabi besar Muhammad SAW yang telah membimbing kita kea lam yang terang benerang seperti saat ini.

Alhamdulillah, penulis telah menyelesaikan **Laporan Penelitian Pengamanan Pesan Teks Menggunakan Algoritma Myszkowski Berbasis Web** . Laporan penelitian ini disusun guna menunjang salah satu tri dharma perguruan tinggi yaitu dibidang penelitian. Semoga laporan penelitian ini dapat berguna dimasa akan datang dan dapat menjadi salah satu referensi khususnya dibidang keamanan pesan.

Penulis paham betul sebenarnya bahwa laporan penelitian ini belumlah sempurna dan masih banyak hal yang kurang dalam proses pengerjaannya. Oleh karena itu penulis sangat berlapang dada dan siap menerima arahan ataupun masukan serta kritikan yang konstruktif oleh berbagai pihak untuk menjadikan laporan penelitian ini lebih sempurna lagi kedepannya. Akhir kata penulis memohon maaf apabila terjadi kesalahan dalam pengerjaan diktat ini.

Medan, Maret 2023

Penulis
Adnan Buyung Nasution, M.Kom.
NIP: 199008092019031014

ABSTRAK

Perkembangan zaman di masa kini lumayan pesat diera milinenial saat ini. Adapun yang menjadi kendala saat ini ialah masalah keamanan dari informasi tersebut. Semakin majunya teknologi banyaknya penggunaan teknologi untuk bertukar pesan, membuat banyak orang melakukan pencurian serta sabotase informasi terhadap data yang dikirimkan. Adapaun salah satu yang dapat digunakan agar pesan yang dikirim tetap aman dengan menggunakan kriptografi. Kriptografi ialah sebuah seni ataupun bidang ilmu yang digunakan dalam proses pengamanan suatu pesan atau dokumen rahasia. Algoritma myszkowski merupakan salah satu algoritma kriptografi klasik yang proses penyandiannya dengan cara mengubah posisi karakter pada pesan asli (plainteks). Adapun keunikan dari algoritma ini adalah terdapat pada kunci. Jika terdapat karakter kuncinya sama maka proses enkripsi dan deskripsi dilakukan secara horizontal dan jika tidak terdapat karakter kuncinya sama maka proses enkripsi dan deskripsi dilakukan secara vertikal. Pada penelitian ini akan menjelaskan proses enkripsi dan deskripsi yang dilakukan menggunakan algoritma myszkowski. serta membangun sistem yang berbasis website. Hasil dari penelitian ini ialah Algoritma Myszkowski dapat mengaman pesan teks yaitu dengan cara mengacak pesan teks secara vertikal sesuai dengan urutan nomor karakter kunci yang ada di matriks. Pengacakan dapat terjadi secara horizontal apabila terdapat karakter kunci yang sama. Pada penelitian ini, sudah dirancang dan dibangun sistem pengamanan pesan teks berbasis web.

Kunci : algoritma myszkowski, keamanan, kunci, pesan teks

ABSTRACT

The development of the times at the present time is quite rapid in the current millennial era. The current obstacle is the security issue of the information. The more advanced technology is, the more use of technology to exchange messages, making many people commit theft and sabotage of information on the data sent. There is one that can be used to keep messages sent safe by using cryptography. Cryptography is an art or a field of science that is used in the process of securing a secret message or document. Myszkowski's algorithm is one of the classic cryptographic algorithms which processes the encoding by changing the position of the characters in the original message (plaintext). The uniqueness of this algorithm is found in the key. If there are the same key characters then the encryption and description process is carried out horizontally and if there are no the same key characters then the encryption and description process is carried out vertically. In this study will explain the process of encryption and description carried out using the myszkowski algorithm. and build a website-based system. The results of this study are that the Myszkowski Algorithm can secure text messages by scrambling text messages vertically according to the sequence of key character numbers in the matrix. Randomization can occur horizontally if there are the same key characters. In this research, a web-based text message security system has been designed and built.

Keyword : myszkowski algorithm, security, key, text message

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan zaman di masa kini lumayan pesat diera milinenial saat ini. Banyaknya fasilitas terbaru serta inovasi yang bermunculan menjadikan teknologi semakin diminati oleh penggunanya dari waktu ke waktu. Hal tersebut juga mempengaruhi akan kebutuhan dari masyarkat akan menikmati teknologi yang ada sehingga menjadikan masyarakat ketergantungan akan kebutuhan penggunaan teknologi tersebut. Teknologi sudah menjadi rumah kedua bagi masyarakat sebab semua akan keinginan yang ada masyarakat sebagian besar sudah terpenuhi. Kebutuhan akan hiburan, sebagai alat bantu pekerjaan sampai sebagai alat untuk berkomunikasi sudah bisa masyarakat dapatkan dengan penggunaan teknologi yang ada. Adapun alat teknologi yang ada saat ini, seperti smart tv, komputer, laptop, hp, dan lainnya. Komputer tercipta agar dapar memudahkan kegiatan masyakarak di dunia nyata mulai menghitung, menyimpan, memproses data hingga memperoleh output yang dapat menjadi andalan masyarakat dalam penyeselesaia atan pemberian solusi atas permasalahan yang ada [1]. Penggunaan akan komputer itu sendiri sudah memiliki perkembangan bukannya hanya dari perkembangan perangkat keras saja tetapi juga dalam perkembangan perangkat lunaknya.

Kemajuan akan perkembangan teknologi juga mempengaruhi hal lainnya salah satunya perkembangan akan informasi. Hal tersebut dikarenakan dengan adanya penggunaan internet yang semakin ramai dan mendunia di masyarakat dunia. Kemajuan akan komunikasi menjadi salah satu yang paling berdampak pada masa perkembangan teknologi yang mana aplikasi serta pendukungnya membuat komunikasi menjadi semakin kompleks di banyak hal. Hal tersebut menunjukkan bahwa semakin banyak orang yang menginginkan penggunaan akses serta koneksi dalam bentuk komunikasi yang ada. Dampak lainnya dari kemajuan tersebut ialah saat proses pengiriman pesan pastinya dapat dilakukan dengan mudah dan cepat. Proses penyimpanan informasi tersebut juga kalah baiknya dengan adanya kapasitas memori yang semakin besar juga. Adapun yang menjadi kendala saat ini ialah masalah keamanan dari informasi tersebut. Semakin majunya teknologi yang ada serta banyak masyarakat menggunakan teknologi untuk bertukar pesan, membuat banyak orang untuk melakukan pencurian serta sabotase informasi terhadap data yang dikirimkan. Adapaun salah satu yang dapat digunakan agar pesan yang dikirim tetap aman dengan menggunakan kriptografi.

Kriptografi ialah sebuah seni ataupun bidang ilmu dimana didalamnya mempunya banyak jenis algoritma yang sering sekali digunakan dalam proses pengamanan suatu pesan atau dokumen rahasia [2]. Kriptografi merupakan suatu ilmu tentang pembelajaran penulisan secara rahasia dimana pesan tersebut mengalami

[1]Chyquitha Danuputri, Nico Santosa, Fernando Dedi Samuel. 'Pengujian Pengembangan Terhadap Algoritma Vigener Key Kriptografi'.Jurnal Resistor. (2022). Vol. 5. No.1.26-37 .

[2]R. A. Indra and W. Pramusinto, 'Aplikasi Email (Electronic Mail) Menggunakan Algoritma Advanced Encryption Standard(AES-128) dan Algoritma Rivest Cipher 4 (RC4) Berbasis Web,' in *SKANIKA*, (2018), vol. 1, no. 2, pp. 704–710.

pengkodean yang disebut enkripsi (*endcode/*encrypt) dan juga deskripsi (*decodeldecrypt*) [3]. Penggunaan kriptografi menjadi salah satu alternatif dalam pencegahan pesan yang tersadap saat melakukan pengiriman. Adapun hal yang dilakukan dalam mengamankan pesan menggunakan kriptografi ialah dengan melakukan penyandian akan pesan. Proses penyadian dilakukan dengan cara mengubah pesan yang masih dapat dipahami (plainteks) menjadi sebuah pesan yang sulit dipahami (cipherteks) dengan menggunakan kunci.

Penggunaan jenis kunci dalam penyandian pesan memiliki ciri khas tersendiri tergantung dengan algoritma kriptografi apa yang digunakan dalam proses penyandian tersebut. Kunci tersebut diatur sesuai dengan algoritma kriptografi yang digunakan pada saat proses penyandian. Algoritma kriptografi yang beraneka ragam pastinya memiliki tujuan tersendiri yaitu agar pesan yang akan dikirim menjadi sangat rumit sehingga pesan tersebut dapat melakukan pengiriman dengan aman. Kemudian, orang yang tidak memiliki kepentingan tidak dapat menggunakan pesan tersebut sesuai dengan yang diinginakannya. Adapun salah satu algoritma kriptografi ialah algoritma myszkowski.

Algoritma myszkowski merupakan salah satu algoritma kriptografi klasik yang proses penyandiannya dengan cara mengubah posisi karakter pada pesan asli (plainteks). Algoritma myszkowski merupakan variasi lain dari algoritma transposisi kolom. Algoritma ini diusulkan oleh Emile Victor Theodore Myszkowski pada tahun 1902 [4]. Pada algoritma transposisi kolom, apabila terjadi munculnya karakter kunci yang sama maka karakter kunci yang selanjutnya dianggap sebagai karakter yang berikutnya dalam urutan abjad. Sebagai contoh kata “saya”, jika menggunakan algoritma transposisi kolom maka urutan kuncinya adalah [3 1 4 2]. Sedangkan pada algoritma myszkowski, apabila terdapat karakter kunci yang sama maka penomoran dalam urutan kunci menjadi sama. Sebagai contoh kata “saya”, jika menggunakan algoritma myszkowski kolom maka urutan kuncinya adalah [2 1 3 1].

Pada penelitian yang dilakukan oleh Juwita (2018) [5] yang berjudul “Analisa Algoritma *Ciphers Transpotion : Study Literature* “ dimana penulis melakukan analisa empat algoritma transposisi cipher yaitu rail fence cipher, route cipher, columnar cipher dan terakhir myszkowski cipher. Dari keempat algoritma tersebut penulis menjelaskan bagaimana proses enkripsi pada setiap algoritma kemudian penulis juga juga memberikan penjelasan mengenai kekurang serta kelebihan dari setiap algoritma tersebut. Pada penelitian ini pula, penulis juga melakukan analisa trend dari beberapa penelitian sebelumnya untuk mengetahui bagaiamana trend penelitian yang terjadi setiap periode tahun. Adapun kesimpulan dari penelitian ini ialah bahwa algoritma myskowski merupakan algoritma yang memiliki pengembangan yang baik diantara algoritma transposisi lainnya. Kedepannya, algoritma ini diharapkan menjadi algoritma pengembangan yang lebih banyak untuk diteliti dikemudian harinya.

---

[3]Leo Dearman Simatupang, Khairil.'Pengamanan Dokumen Teks Dengan Menerapkan Algortima Kriptografi Klasik. Jurnal Teknik Informastik Unik St. Thomas (JTIUST). (2022). Vo. 07. No.1 133-140.

[4]Hardi, S.M. Rachmawati. D, Chairinnisa F, Jaya. I. Tarigan. J.T. 'Combination of myszkowski transposition algorithm and modified least significant bit (mlsb) green channel on png image security. IOP Conf. Series : Journal of Physics: Conf. Series 1235. (2019). 1-7.

[5]Juwita Artanti Kusumaningtyas. 'Analisa Algoritma *Cipher Trnasposition : Study Literature*. Multimatrix. (2018). Vol 1. No. 1. 1-12.

Penelitian yang dilakukan oleh Nurul (2019) [6] yang berjudul "Modifikasin *Myszkowski Transposition Cipher* dengan *Chess Board Pattern* " membahas tentang pengkombinasian kedua algoritma tersebut. Pada proses enkripsi dan deskripsinya, matriks yang dihasil dibuat layaknya papan catur dimana matriks yang bertanda hitam tidak dimasukkan karakter plainteksnya. Selanjutnya, proses enkripsi dilakukan menggunakan algoritma myszkowski cipher. Hasil pembahasan pada penelitian ini ialah bahwa terdapat 2 variasi yang dapat dilakukan dalam melakukan proses enkripsi dan deskripsi dengan menggunakan kombinasi kedua algoritma tersebut. Pada penelitian ini juga hanya melakukan pembahasan proses enkripsi dan deskripsi secara proses manual.

Adapun penelitian yang akan penulis buat adalah "Pengamanan Pesan Teks Menggunakan Algoritma Myszkowski Berbasis Web". Dimana pada penelitian ini, penulis akan menjelaskan proses enkripsi dan deskripsi yang dilakukan menggunakan algoritma myszkowski. Adapun pesan yang akan diproses adalah teks. Penelitian ini juga akan membangun sistem yang berbasis website.

1.2 Rumusan Masalah

Berdasarkan dari latar belakang yang telah dibuat diatas, adapun rumusan masalah pada penelitian ini adalah :

1. Bagaimana mengamankan pesan teks menggunakan algoritma myszkowski?
2. Bagaimana merancang dan membangun sistem pengamanan pesan teks menggunakan algoritma myszkowski?

1.3 Tujuan Penelitian

Adapun tujuan masalah pada penelitian ini adalah :

1. Untuk mengamankan pesan teks menggunakan algoritma myszkowski.
2. Untuk merancang dan membangun sistem pengamanan pesan teks menggunakan algoritma myszkowski.

1.4 Batasan Penelitian

Adapun batasan masalah penelitian ini adalah sebagai berikut :

1. Pesan yang akan dibuat dalam bentuk teks yang hanya menggunakan abjad, spasi dan angka.
2. Pada penelitian ini, karakter spasi tidak dihapuskan dan digunakan juga dalam proses enkripsi dan deskripsi.
3. Apabila dalam penentuan jumlah baris matriks terdapat nilai angka dibelakang koma maka hasil baris tersebut akan dilakukan penggenapan nilai bilangan bulat keatas.

---

[6]Nurul Khairina. Muhammad Khoiruddin Harahap. ' Modifikasin *Myszkowski Transposition Cipher* dengan *Chess Board Pattern'*. Seminar Nasional Teknologi Informatikan (Semantika). (2019). Vo. 2. No.1. 28-34 .

4. Penelitian ini juga akan menambahkan karakter tambahan apabila terdapat matriks yang belum terisi karakter plainteks yaitu karakter simbol at (@).
5. Kunci yang digunakan pada penelitian ini adalah dalam bentuk abjad.
6. Pembuatan sistem yang dilakukan pada penelitian ini ialah menggunakan bahasa pemogrman PHP.

1.5 Manfaat Penelitian

Adapun manfaat dari penelitian ini dapat dilihat sebagai berikut :

a. Bagi Peneliti
    1. Dapat menjadi pelatihan diri bagi penulis dalam melakukan penganalisaan permasalahan, perancangan serta pembangunan program.
    2. Dapat mengembangkan wawasan keilmuan penulis saat pengerjaan penelitian khususnya pembahasan kemanan pesan ini.

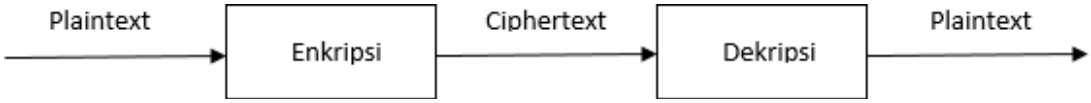
b. Bagi Instansi
    1. Dapat dijadikan referensi bagi penulis lainnya pada saat pelaksanaan peneletian mengenai keamanan pesan.
    2. Menjadikan salah satu kontribusi terkait pengamanan pesan dibidang pengembangan IPTEK.

BAB II
TINJAUAN PUSTAKA

2.1 Kriptografi

Pada era seperti saat ini, kehidupan manusia dikelilingi oleh kode.Dimulai pada transaksi ATM, transaksi perbankan, transaksi kartu kredit, obrolan melalui telepon seluler, akses internet, hingga aktivasi roket, mereka juga menggunakan kriptografi. Standar penulisan kriptografi dapat ditulis dalam bahasa matematika[7]. Pada mulanya kriptografi diartikan oleh manusia sebagai ilmu dalam proses menyembunyikan pesan[8].

Pada kriptografi terdapat skema berarti adalah enkripsi serta dekripsi. Enkripsi ialah teknik dimana data yang hendak dikirim diganti sebagai struktur yang nyaris tidak diketahuii. Dekripsi ialah teknik merombak pulang struktur tidak dikenali sebagai data pangkal. serupa pesan alias data yang sedang asli serta belum menghadapi penyandian dikenal dengan sebutan plaintext. seterusnya sehabis disamarkan dengan sebuah teknik penyandian, alkisah plaintext ini diujarkan selaku ciphertext selaku lumrah, teknik enkripsi serta dekripsi sanggup dicerminkan selaku selanjutnya:



Gambar 2. 1 Proses Enkripsi dan Deskripsi [9]

2.1.1 Definisi dan Terminologi

Dikala anda melakukan tukar menukar pesan (layaknya surat) dengan seseorang, Anda pastinya menginginkan pesan yang anda kirimkan dapat diterima oleh orang yang anda tuju dengan rasa aman. Definisi dalam arti aman dapat diartikan sangatlah luas. Aman dapat diartikan ketika dalam pengiriman pesan anda untuk orang lain, tidak ada satu orang pun selain orang yang anda tuju yang membaca pesan tersebut. Hal ini pastinya diharapkan secara alami oleh anda. Pesan yang anda kirim biasanya memiliki informasi penting atau bersifat rahasia yang dimana hanya orang yang bersangkutan yang hanya ingin anda beritahu. Apabila pesan tersebut diketahui oleh orang yang bukan anda inginkan terima maka keharasiaan dari pesan tersebut pastinya akan hilang. Hal tersebut yang sering dikenal sebagai kerahasiaan atau sering disebut juga sebagai privasi.

---

[7]Ajar Rohmanu, 'METODE ALGORITMA DES DAN METODE END OF FILE Ajar Rohmanu', *Jurnal Informatika*, 2.1 (2017), 1–11.

[8]M Haris Syarifuddin and Meini Sondang Sumbawati, 'Pengembangan E-Komik Sebagai Media Pembelajaran Keamanan Jaringan Materi Kkriptografi', *Jurnal IT-Edu Volume 01 Nomor 01 Tahun 2016 , 30-36*, 01.1971 (2016), 30–36.

[9]Scheneier, Bruce. 2016.Applied Cryptography 2nd ed. Buku. Illinois, USA..

Suatu pesan dapat diartikan menjadi aman apabila pesan yang terkirim dari si pengirim dapat diterima seutuhnya ke tangan penerima tanpa adanya kebocoran informasi saat pesan tersebut dikirim. Dalam hal lainnya dapat diartikan juga bahwa pesan tersebut tidak ada rekayasa atau mengalami perubahaan informasi oleh orang yang tidak diinginkan. Setelah sampai kepada orang yang bersangkutan pastinya dicek pula keaslian dari pesan yang diterima apakah sudah terdapat manipulasi pesan atau tidak. Hal ini yang sering disebut sebagai integrasi data. Selain daripada itu, dari sisi penerima juga pastinya akan ada pengecekan juga apakah pesan yang diterima oleh si penerima / orang yang bersangkutan merupakan benar pesan dari yang dikirim oleh si pengirim yang sesungguhnya. Proses yang dilakukan hal tersebut dikenal dengan auntentifikasi dimana si penerima melakukan pengecekan bahwa pesan tersebut benar dari si pengirimnya.

Andaikan Anda merupakan si penerima pesan, maka anda juga tidak ingin bahwa si pengirim pesan tersebut menyangkal bahwa si pengirim tidak mengirimkan person tersebut kepada. Hal Ini merupakan bagian keamanan yang sering dikenal sebagai penyangkalan (repudiation). Saat ini, banyak sekali orang menolak atau membantah bahwa dirikanya yang mengirim atau menerima pesan. Meskipun Anda yakin bahwa anda sudah menerima SMS dari orang ini. Jika pengirim menyangkal telah mengirim pesan, maka Anda harus membuktikan bahwa penolakan itu salah (no repudiation). Keempat permasalahan keamanan yang telah disampaikan pada alinea diatas yaitu kerahasiaan, integritas data, otentifikasi dan penyangkalan dapat terselesaikan dengan salah satu cara menggunakan kriptografi. Kriptografi bukan hanya memiliki alat agar dapat mengamankan pesan, akan tetapi kriptografi juga merupakan sekumpulan cara dengan teknik yang berguna.

Kriptografi (cryptography) berawal dari Bahasa Yunani: “cryptós” maksudnya “secret” (rahasia), sementara itu “gráphein” maksudnya “writing” (karya). Jadi, kriptografi berarti “secret writing” (tulisan rahasia). terdapat sebagian makna kriptografi yang dikemukakan di dalam bermacam kepustakaan. penjelasan yang digunakan di dalam buku-buku yang lama (saat sebelum tahun 1980-an) menerangkan jika kriptografi ialah ilmu serta seni guna melindungi kerahasian pesan dengan metode menyandikannya ke dalam wujud yang tidak bisa diketahui lagi maknanya. penjelasan ini barangkali sesuai pada waktu berlanjut di mana kriptografi dikenakan guna keamanan komunikasi berguna serupa komunikasi di golongan angkatan bersenjata, kuasa usaha, serta mata-mata. tapi masa ini kriptografi lebih dari semata-mata privacy, namun serta guna tujuan data integrity, authentication, serta non-repudiation[10].

Ada beberapa definisi menurut beberapa peneliti yaitu sebagai berikut ;

- Kriptografi dapat diartikan sebagai salah satu seni ataupun ilmu yang menyajikan hasil pesan yang rahasia[11].
- Kriptografi juga dapat didefiniskan suatu kombinasi ilmu serta seni dalam menjaga pesan agar tetap aman ketika pesan tersebut dikirimkan dari suatu tempat ke tempat yang lainnya[12].

[10]AriMuzakir,„Prototype Model Keamanan Data Menggunakan Kriptografi Data Encryption Standar(Des) Dengan Mode Operasi Chiper Transposisi , *Seminar Nasional Inovasi Dan Tren (SNIT) 2014*, 20 (2014), 1–4.

[11]Yusfrizal, ‘Rancang Bangun Aplikasi Kriptografi Pada Teks Menggunakan Metode Reverse Chiper Dan Rsa Berbasis Android’, *Jurnal Teknik Informatika Kaputama (JTIK)*, 3.2 (2019), 29–37.

- Kriptografi juga merupakan ilmu yang mengenai teknik-teknik matematika yang berhubungan dengan aspek pengamanan informasi, integritas dari data dan juga otentifikasi suatu data[13].

Kata " seni " di dalam batasan di berdasarkan berawal dari kenyataan asal usul kalau pada periode- periode awalsejarah kriptografi, tiap orang barangkali ada metode yang spesial guna menutupi pesan. teknik- metode spesial itu barangkali berselisih- beda pada tiap pemain kriptografi akibatnya tiap metode menulis pesan rahasia pesan ada ponten estetika tersendirisesampai kriptografi bertumbuh selaku semacam seni menutupi pesan(kata " graphy " di dalam " cryptography " itu sendiri telah menyiratkan semacam seni). kamu hendak menatap di dalam bagian 3 sampel-sampel metode keriptografi dari masa awal hingga masa kini akibatnya kamu mampu mamahami kalau kriptografi mampu ditilik selaku semacam seni menutupi pesan. Pada pertumbuhan kemudian, kriptografi bertumbuh selaku semacam patuh ilmu sendiri lantaran metode- metode kriptografi mampu dirumuskan dengan cara matematik akibatnya selaku semacam teknik yang resmi. Kriptografi mempunyai bervariasi teknik guna menyandikan pesan ataupun data yang berharap kita sembunyikan, serupa Caesar Cipher, Affine, Monoalphabetic, Polyalphabetic, Vigenere, Transposisi, serta banyak lagi teknik- teknik dalam kriptografi ini [14].

2.1.2 Istirlah-Istilah Pada Kriptografi

Adapun istilah-istilah yang ada di kriptografi [15] :

A. Plainteks

Plaintext adalah pesan ataupun data yang hendak dikirimkan dalam bentuk yang gampang dibaca ataupun dalam aslinya[16]. Plain text umumnya dipakai antar-komputer yang tidak ada kesepakatan guna silih berganti informasi bentuk serta layout teks. Plaintext berupa data ataupun data yang mampu dibaca serta dimengertimaknanya. sapaan lain guna pesan yakni plainteks (plaintext) ataupun teks-jelas (cleartext). Pesan mampu berbentuk data ataupun data yang dikirim (via kurir, salurantelekomunikasi, dsb) ataupun yang dikemas di dalam alat perekaman (kertas, storage,dsb). Pesan yang terpendam tidak cuma berbentuk teks, tapi pula mampu berupa citra(image), suara/bunyi (audio), serta film, ataupun bendel biner yang lain. Contoh : Sistem Informasi Solid Selalu.

---

[12]Albert Ginting, R. Rizal Isnanto, and Ike Pertiwi Windasari, 'Implementasi Algoritma Kriptografi RSA Untuk Enkripsi Dan Dekripsi Email', *Jurnal Teknologi Dan Sistem Komputer*, 3.2 (2015), 253 <https://doi.org/10.14710/jtsiskom.3.2.2015.253-258>.

[13]Deny Adhar, 'Pengamanan Sqlite Database Menggunakan Kriptografi Elgamal', *Snif*, Vol.1.No.1 (2014), 432–37.

[14]Angga Aditya Permana, 'Penerapan Kriptografi Pada Teks Pesan Dengan Menggunakan Metode Vigenere Cipher Berbasis Android', *JURNAL Al-AZHAR INDONESIA SERI SAINS DAN TEKNOLOGI*, 4.3 (2018), 110 <https://doi.org/10.36722/sst.v4i3.280>.

[15]Nurul Hayaty, 'Buku Ajar: Sistem Keamanan', Teknik Informatika UMRAH *2020*.

[16]Jati Sasongko, 'Pengamanan Data Informasi Menggunakan Kriptografi Klasik', Jurnal Teknologi Informasi Dinamik X.3 (2005), 160–67.

B. Cipherteks

Ciphertext ini ialah wujud sesudah pesan dalam plaintext sudah diganti wujudnya sebagai lebih nyaman serta tidak sanggup dibaca. cara mengganti plaintext sebagai ciphertext diucap encryption (enciphering), serta cara membalikkannya pulang diucap decryption (deciphering). Supaya pesan tidak sanggup dipahami maknanya oleh pihak lain, hingga pesan perludisandikan ke wujud lain yang tidak sanggup dimengerti. wujud pesan yang tersandi diucap cipherteks (ciphertext) alias kriptogram (cryptogram). Cipherteks perlu sanggup ditransformasikan balik selaku plainteks awal biar pesan yang diperoleh bias dibaca.

Contoh : a eh3ounanaj3 aaihelnaoiejahe

C. Enkripsi

Enkripsi merupakan serupa cara penyandian yang menjalankan pergantian serupa (pesan) dari yang mampu dipahami (plaintext) sebagai serupa yang tidak mampu dipahami (chipertext) [17]. Dengan enkripsi, sesuatu data hendak sebagai lebih kompleks guna diketahui oleh orang yang tidak berkuasa[18].

Pikirkan berapa banyak data berguna yang ditaruh pada file, berkas, serta alat kepunyaan perseroan kamu. kini bayangkan apa yang hendak terjalin apabila data itu jatuh ke tangan orang yang salah. Mulai data individu mengenai pegawai (misalnya tujuan, nomor agunan sosial, pajak, dan lainnya.) sampai perinci mengenai moneter serta nomor rekening bank perseroan, kayanya besar kamu mempunyai banyak data yang patut dibatasi penggunaannya oleh orang-orang yang berwajib. Enkripsi merupakan salah satu teknik terbaik guna memelihara data rahasia usaha dagang kamu dari gertakan keamanan siber.

D. Deskripsi

Teknik menyandikan plainteks jadi cipherteks diucap enkripsi (encryption) ataupun enciphering (standard sapaan). sementara itu prosedur mengembalikan cipherteks jadi plainteks tadinya disebut dekripsi (decryption) ataupun deciphering (standard sapaan). Dekripsi merupakan tahapan pengubahan kembali suatu bentuk yang kurang dipahami menjadi informasi aslinya[19]. Dekripsi juga bisa dijalani sebagai otomatis ataupun pedoman dengan memanfaatkan kata kode ataupun password. sepanjang teknik itu sistem bakal mengekstraknya serta mengubahnya jadi

[17]M Miftakul Amin, 'Implementasi Kriptografi Klasik Pada Komunikasi Berbasis Teks', *Pseudocode*, 3.2 (2017), 129–36 <https://doi.org/10.33369/pseudocode.3.2.129-136>.

[18]Faturungi Muharram, Huzain Azis, and Abdul Rachman Manga, 'Analisis Algoritma Pada Proses Enkripsi Dan Dekripsi File Menggunakan Advanced Encryption Standard (AES)', *Proc. of the Seminar Nasional Ilmu Komputer Dan Teknologi Informasi*, 3.2 (2018), 112–15.

[19]A Afandi, 'Sistem Keamanan Data Menggunakan Algoritma Myszkowski Transposition Pada Penyimpanan Cloud', *Kumpulan Karya Ilmiah Mahasiswa Fakultas Sains ...*, 2021 <http://jurnal.pancabudi.ac.id/index.php/fastek/article/view/1907%0Ahttp://jurnal.pancabudi.ac.id/index.php/fastek/article/download/1907/1745>.

teks serta lukisan biar tidak cukup dimengerti oleh pembaca saja tapi sistem pula bisa membacanya sebagai totalitas.

Enkripsi serta dekripsi mampu digunakan baika pada pesan yang dikirim ataupun pada pesan terkubur. sebutan encryption of data in motion mengarahkan pada enkripsi pesan yang disebarkan lewat saluran komunikasi, sementara itu sebutan enrypton of data at-rest mengarahkan pada enkripsi akta yang ditaruh di dalam storage. ilustrasi encryption of data in motion yakni pengiriman nomor medali dari mesin ATM ke pc server di kantorbank pusat. ilustrasi encryption of data at-rest yakni enkripsi file pangkalan data di dalam hard disk.

E. Kunci (Key)

Kunci kriptografi merupakan serangkaian bit yang oleh algoritma kriptografi buat mengalihkan teks umum sebagai teks rahasia ataupun kebalikannya. Kunci ini senantiasa individu serta meyakinkan komunikasi yang nyaman. Kunci kriptografi ialah bagian inti dari pembedahan kriptografi. Banyak sistem kriptografi terhitung pendamping pembedahan, semacam enkripsi serta dekripsi. Kunci ialah bagian dari data peubah yang disajikan selaku input ke algoritma kriptografi buat melaksanakan pembedahan sejenis ini. Dalam rancangan kriptografi yang didesain dengan betul, keamanan rancangan pada keamanan kunci yang . separuh cipher membutuhkan algoritma yang berlainan buat enciphering serta deciphering.Proses enkripsi serta dekripsi mengenakan satu ataupun sebagian kunci kriptografi[20].

2.1.3 Macam-Macam Algoritma Kriptografi

Algortima kriptografi dipecah jadi 3 bagian berdasarkan kunci yang dipakainya [21] :

A. Algoritma Simetri (memanfaatkan satu kunci guna enkripsi serta deskripsnya).

Algoritma ini diujarkan selaku algoritma klasik karna mengenakan kunci yang sepadan guna aktivitas enkripsi serta sketsa. kalau mengirim pesan dengan algoritma ini, si penyambut pesan wajib diberiketahui kunci dari pesan itu supaya mampu menggambarkan pesan yang dikirim. Keterjaminan dari pesan yang memanfaatkan algoritma ini terpaut pada kunci. apabila kunci itu diketahui oleh orang lain sehingga orang itu hendak mampu mengerjakan enkripsi serta sketsa pesan. Algoritma yang mengenakan kunci simetri antara lain merupakan:
keterangan Encryption Sisyaratrd (DES)

[20]Aditia Rahmat Tulloh, Yurika Permanasari, and Erwin Harahap, 'Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen', *Jurnal Matematika UNISBA*, 2.1 (2016), 118–25 <https://ejournal.unisba.ac.id/index.php/matematika/article/view/4067>.

[21]Jamaluddin, dkk., *KRIPTOGRAFI Teknik Keamanan Data*, ed. by Adbul Karim and Janner Simarmata, Cetakan Pertama (Yayassan Kita Menulis, 2022).

- RC2, RC4, RC5, RC6
- International Data Encryption Algorithm (IDEA)
- Advance Encryption Standard (AES)
- One Time Pad (OTP)
- A5 serta yang ada

B. Algoritma Asimetri (memanfaatkan kunci yang berselisih guna enkriipsi serta sketsa).

Algoritma asimetri kerap pula diujarkan dengan algorita kunci khalayak, dengan makna kata kunci yang dikenakan guna mengerjakan enkripsi serta deskripsi berselisih. Pada algoritma asimetri kunci terpecah jadi 2 bagian, ialah :

- Kunci normal (public key) ialah kunci yang dapat seluruh orang tahu (dikhalayakasikan).
- Kunci rahasia (private key) ialah kunci yang disembunyikan (cukup dapat diketahui oleh satu orang saja).

Kunci-kunci itu berkaitan satu sepadan lain. Dengan kunci khalayak orang mampu mengenkripsi pesan tapi tidak mampu mendeskripsinya. cukup orang yang mempunyai kunci rahasia yang mampu menggambarkan pesan itu. Algoritma asimetri mampu mengirimkan pesan dengan lebih aman dari algoritma simetri. Algoritma yang mengenakan kunci publik antara lain adalah :

- Digital Signature Algorithm (DSA)
- RSA
- Diffie-Hellman (DH)
- Elliptic Curve Cryptography (ECC)
- Kriptografi Quantum serta lainnya

2.2 Algoritma Myzkowski

Algoritma Myszkowski Transposisi adalah semacam bagian kelanjutan dari columnar transposition cipher yang diusulkan oleh Emile Victor Thedore Myszkowski. sira yaitu satu orang purnawirawan colonel dari serdadu Perancis yang diterbitkan via komik yang sempat ditulisnya adalah "Cryptographie Indéchiffrable" di tahun 1902 yang memublikasikan semacam varietas teknik penyadian dengan membutuhkan semacam kata kunci yang ada kepribadian berulang [22]. Kunci rahasia yang dibubuhkan dalam algoritma Myszkowski Transposition yaitu huruf yang serupa dengan deretan abjad yang seterusnya disusun selaku deretan nomor. Dalam teknik penyandian kunci rahasia transposition dilakoni dengan teknik mewalakkan plaintext yang hendak dienkripsi serta guna membaca pesan aslinya pulang, dilakoni dengan mengembalikan posisi dari pesan itu berlandaskan kunci rahasia serta algoritma perpindahan yang disetujui. Adapun tahapan dari algoritma Myszkowski Transposition Cipher dapat dilihat pada tahapan berikut ini :

[22]Hardi, S.M., dkk., Combination of myszkowski transposition algorithm and modified least significant bit (mlsb) green channel on png image security, IOP Conf. Series: Journal of Physics: Conf. Series 1235 (2019) , 1-6.

A. Proses Enkripsi

Saat sebelum melaksanakan sistem enkripsi, terlebih dulu dijalani penyusunan kunci. Beberapa huruf yang dibentuk sebagai manual maupun random bisa menambahkan selingan penyusunan kunci [23]. contoh dari plaintext serta kunci dapat dilihat dibawah ini:

Plainteks : FAKULTAS SAINS DAN TEKNOLOGI
Kunci : UIN

Tahapan enkripsi diawali dengan membuat beberapa baris serta kolom agar dapat dimasukkan semua karakter plaintext. ada 25 huruf pada plainteks yang bakal jadi bagian dalam pembentukan baris, serta 3 huruf pada kunci bakal jadi teladan guna pembentukan kolom. akibatnya jumlah kolom serta baris yang diinginkan yakni:

Kunci = 3 huruf menjadi matriks 3 kolom
Plainteks = 25 huruf menjadi matiks 25/3 = 8.333 atau di genapkan ke atas menjadi 9 baris.

Kunci yang terdapat pada contoh diatas adalah 3 huruf yang mana dapat kita buat penomorannya sesuai dengan urutan abjad yaitu U = 3, I = 1, N =2.

Setelah mengetahui pembentukan dari baris dan juga kolom yang memungkinkan, selanjutnya adalah peletakan plainteks pada setiap matriks hingga seluruh karakter plainteks masuk kedalam matriks. Berikut adalah proses dari pemasukan plainteks kedalam matriks :

Tabel 2. 1 Proses Enkripsi (a), (b), (c), (d), (e), (f) dan (g)

U	I	N
3	1	2
F		

(a)

U	I	N
3	1	2
F	A	K

(b)

[23]J. A. Kusumaningtyas, "Analisa Algoritma Ciphers Transposition : Study Literature," Multimatrix, vol. I, no. 1, pp. 1–12, 2018..

U	I	N
3	1	2
F	A	K
U		

(c)

U	I	N
3	1	2
F	A	K
U	L	T

(d)

U	I	N
3	1	2
F	A	K
U	L	T
A		

(e)

U	I	N
3	1	2
F	A	K
U	L	T
A	S	S

(f)

U	I	N
3	1	2
F	A	K
U	L	T
A	S	S
A		

(g)

U	I	N
3	1	2
F	A	K
U	L	T
A	S	S
A	I	N
S	D	A
N	T	E
K	N	O
L	O	G
I	@	@

(h)

Pada tabel 2.1 dapat dilihat bahwa terdapat 2 huruf tambahan yaitu @ pada matriks terakhir. Hal ini merupakan sebuah dummy yang dilakukan agar dapat memenuhi setiap matriks yang tidak terdapat karakter plainteks pada contoh diatas. Oleh karena itu, pemberian dummy dilakukan agar dapat mengisi semua matriks yang telah ditentuntakan sebelumnya.

Dari proses yang diatas maka hasil cipherteks dapat dimiliki dengan cara melakukan pembacaan secara vertikal mulai dari atas hingga ke bawah sesuai dengan setiap penomoran kunci sesuai dengan tabel dibawah ini :

Tabel 2. 2 Pembacaan Karakter Proses Enkripsi

Kunci	1	2	3
Cipherteks	ALSIDTNO@	KTSNAEOG@	FUAASNKLI

Sehingga cipherteks yang dihasilkan adalah :

Cipherteks : ALSIDTNO@ KTSNAEOG@ FUAASNKLI

Algoritma myszkowski memiliki sebuah keunikan dimana keunikan tersebut terdapat pada karakter kunci yang sama. Jika terdapat karakter yang sama pada kunci maka pada tahap pembacaan karakter pada proses enkripsi dilakukan secara horizontal yang hanya memiliki nomor kunci yang sama kemudian dilanjutkan ke vertikal kebawah. Adapun contoh dapat dilihat pada kasus dibawah ini:

Plainteks : FAKULTAS SAINS DAN TEKNOLOGI
Kunci : JUARA
Proses Enkripsi:
Kunci : 5 huruf menjadi matriks 5 kolom
Plainteks : 25 huruf menjadi matiks 25/5 = 5 baris.
Urutan Abjad : J = 2, U = 4, A = 1, R = 3 dan A = 1

Tabel 2. 3 Proses Enkripsi

J	U	A	R	A
2	4	1	3	1
F	A	K	U	L
T	A	S	S	A
I	N	S	D	A
N	T	E	K	N
O	L	O	G	I

Cipherteks : KL SA SA EN OI FTINO USDKG AANTL

Pada tabel 2.3, dapat dilihat bahwa ada dua karakter kunci yang memiliki huruf yang sama ialah huruf A yang mempunyai penomoran kunci = 1. Proses pembacaan karakternya tidak dilakukan dengan vertikal melainkan dengan horizontal yang menghasilkan cipherteks **KL SA SA EN OI**.

Tabel 2. 4 Proses Enkripsi Dengan Nomor Kunci Sama

A	A
1	1
K	L
S	A
S	A
E	N
O	I

B. Proses Deskripsi

Pada proses ini dapat dilaksanakan jikalau si pihak yang menerima pesan rahasia (cipherteks) memperoleh kunci dan banyaknya baris serta kolom yang dibuat oleh pihak yang mengirim pesan tersebut. Proses deskripsi dilaksanakan dengan cara mengurutkan cipherteks tersebut secara vertikal ke bawah secara berurut yang mana sesuai dengan penomoran kunci. Akan tetapi, jika terdapat penomoran yang sama maka proses pengurutannya dilakukan mulai dari horizontal terlebih dahulu yang memiliki nomor urut yang sama. Adapun contoh kasusnya adalah sebagi berikut :

Cipherteks	: KL SA SA EN OI FTINO USDKG AANTL
Kunci	: JUARA
Proses Deskripsi	:
Kunci	: 5 huruf menjadi matriks 5 kolom
Plainteks	: 25 huruf menjadi matiks 25/5 = 5 baris.
Urutan Abjad	: J = 2, U = 4, A = 1, R = 3 dan A = 1

Tabel 2. 5 Proses Deskripsi

J	U	A	R	A
2	4	1	3	1
		K		L

(a)

J	U	A	R	A
2	4	1	3	1
		K		L
		S		A

(b)

J	U	A	R	A
2	4	1	3	1
		K		L
		S		A
		S		A

(c)

J	U	A	R	A
2	4	1	3	1
		K		L
		S		A
		S		A
		E		N

(d)

J	U	A	R	A
2	4	1	3	1
		K		L
		S		A
		S		A
		E		N
		O		I

(e)

J	U	A	R	A
2	4	1	3	1
F		K		L
T		S		A
I		S		A
N		E		N
O		O		I

(f)

J	U	A	R	A
2	4	1	3	1
F		K	U	L
T		S	S	A
I		S	D	A
N		E	K	N
O		O	G	I

(g)

J	U	A	R	A
2	4	1	3	1
F	A	K	U	L
T	A	S	S	A
I	N	S	D	A
N	T	E	K	N
O	L	O	G	I

(h)

Dari tabel 2.4 dapat dilihat proses deskripsi dalam pemasukan karakter cipherteks mulai dari proses deskripsi di poin (a) sampai poin (h). Pada poin (a) sampai poin (e) merupakan proses pemasukan karakter secara horizontal dikarenakan terdapat 2 karakter kunci yang memiliki huruf abjad yang sama. Kemudian, pada poin (f) sampai pon (h) dilakukan proses pemasukan karakterk cipherteks secara vertikal. Hal ini dikarenakan tidak adanya karakter sama pada kunci yang saat diproses pemasukkan karakter cipherteksnya. Proses selanjutnya adalah pembacaan plainteks pada matriks tabel. Dari tabel tersebut akan menghasilkan plainteks dimana proses pembacaan plainteks dilakukan secara horizontal. Adapun proses pembacaannya dimulai dari ujung kiri atas tabel sampai ke ujung dan seterusnya

tanpa peduli nomor pada kunci [24]. Maka dari hasil pembacaan plainteks pada tabel diatas dapa diperoleh :

Plainteks : FAKULTAS SAINS DAN TEKNOLOGI

2.3 Website

Website ialah salah satu media yang terdapat beberapa halaman yang berhubungan satu dengan yang lainnya (*hyperlink*). Website mempunyai fungsi dalam menyajikan sebuah informasi bisa dalam bentuk animasi, video, suara, gambar serta teks ataupun kombinasi dari beberapa atau semua bentuk tersebut [25]. Pada umumnya, website dapat diakses melalui jalur koneksi internet sehingga informasi yang terdapat pada website dapat dilihat dan dibagi ke seluruah dunia. Website juga dapat dilihat kapan saja diwaktu yang diinginkan oleh penggunanya selama masih terhubung dengan jaringan internet.

Setiap halaman website dibangun menggunakan bahasa pemograman standar yang disebut HTML. Skrip HTML tersebut yang akan diartikan oleh web browser dan hasilnya ditampilkan kedalam bentuk informasi yang dapat dipahami oleh para pengguna yang menggunakan web browser tersebut [26]. Web adalah fasilitas hypertext yang berguna dalam penampilan teks, gambar, suara, animasi dan data multimedia yang lainnya. Web juga menjadi salah satu alat yang dapat mengiklankan produk ataupun digunakan untuk diri sendiri [27]. Website juga bisa menjadi sarana dan peransana pendidikan serta edukasi untuk masyarakat. Pastinya, setiap website dibangun sesuai dengan informasi yang diberikan atau dibuat oleh pembuat website tesebut.

Website yang telah terkoneksi internet memiliki penyimpanan khusus yang sering disebut dengan wes server. Web server merupakan suatu kebutuhan yang harus dibuat oleh pemilik website guna menyimpan website yang memiliki daya simpan yang cukup besar sehingga dalam pengaksesan dapat lebih cepat. Fungsi web server tersebut untuk menghindari traffic yang besar sehingga dapat tercegahnya dalam down suatu website atau aplikasi [28]. Maka dari itu, penyempinan dalam web server harus dilakukan guna menghingdari hal-hal tersebut saat pengguna membuka website tersebut. Website dapat dibagi menjadi 3 jenis kategori yaitu [29] :

---

[24]Nurul Khairina dan Muhammad Khoiruddin Harahap, Modifikasi Myszkowski Transposition Cipher dengan Chess Board, Semantika, Vol. 2, No. 1 (2019), 1-4.

[25]Elgamar. (2020). Buku Ajar Konsep Dasar Pemrograman Website Dengan PHP. CV. Multimedia Edukasi.

[26]Abdulloh, R. (2018). 7 IN 1 Pemrograman Web Untuk Pemula. Jakarta: Elex Media Komputindo..

[27]Limbong, T., & Sriadhi. (2021). Pemrograman Web Dasar. Yayasan Kita Menulis.

[28]Sabarudin, Raja & Eka Jayanti, Wanti. 2019. Jago Ngoding Pemrograman web dengan PHP untuk Pemula. CV. Kanaka Media: Surabaya.

[29]Salamah, I., Fadhli, M., Sriwijaya, P. N., & Quality, I. EVALUASI PENGUKURAN WEBSITE LEARNING MANAGEMENT SYSTEM POLSRI DENGAN METODE WEBQUAL 4 . 0. (2020). Vol. 10 No.1, 1–10.

1. Website statis : Pada website statis guna melaksanakan pergantian pada sebuah laman dijalani dengan cara manual dengan menyunting kode yang jadi rupa web itu, sebab web itu mempunyai laman yang tidak bertukar.
2. Website dinamis : Pada website dinamis dimana menyajikan laman backend guna membetulkan konten situs maka mampu di pembaharuan, serta mampu diakses oleh user. sampel website dinamis merupakan situs portal maupun situs buletin yang mempunyai sarana polling serta pembaharuan buletin.
3. Website interaktif : Pada website interaktif user mampu berhubungan dengan user lain, selaku sampel yaitu situs serta forum. Website terdiri dari page alias pagina, serta berkas pagina yang disebut homepage. Homepage berkecukupan pada posisi paling atas, dengan pagina-halaman terpaut berkecukupan di bawahnya yang diujarkan child page, yang berbobot hyperlink ke halaman lain dalam web. Website interaktif saat ini sangat digemari oleh kalangan masyarakat guna menukar informasi antara pengguna satu dengan yang lainnya. Informasi tersebut diberikan antar pengguna untuk menambahkan pengetahuan bagi pengguna tersebut.

Gambar 2. 2 Website Prodi Sistem Informasi (sumber : si.uinsu.ac.id)

2.4 HTML

Hypertext Markup Language (HTML) dapat diartikan sebagai sebuah tulisan dalam bentuk link yang mana ketika penggunanya mengklik maka link tersebu dipindahkan ke dalam salah satu dokumen ke dokumen lainnya [30]. HTML ialah bahasa pemograman utama website terdiri dari format data yang memiliki fungsi sebagai pembuatan dokumen hypertext. Dokumen hypertext yang dihasilkan dapat terbaca dan terinterprestasikan pada sebuah platform komputer serta ke antar

[30]Enterprise, J. (2017). HTML5 Komplet. Jakarta: Elex Media Komputindo.

platform komputer lainnya tanpa terjadi perubahan apapun. Adapun yang pelu dilakukan daripada HTML adalah sebagai berikut [31]:

- Melakukan pengontrolan tampilan pada web page serta kontennya.
- Pembulikasian dokumen dilakukan secara online dan juga dapat diakses oleh pengguna seluruh dunia.
- Pembuatan form online yang dapat difungsikan untuk penanganan data masuk dan juga transaksi online.
- Penambahan objek yang menarik seperti image, suara, video serta java applet ke dalam dokumen HTML.

Pada dasarnya, setiap halaman pada website dibangun dengan menggunakan HTML atau *Hypertext Markup Language*. Dengan penggunaan HTML, dalam proses pengembangan pada halaman web dapat memungkinkan bahwa teks, gambar serta multimedia menjadi satu kesatuan antara elemen satu dengan elemen lainnya saat browser pengguna dijalankan.HTML memiliki standarisasi yaitu lembaga konsorium di tahun 1997. Adapun nama standarisasi untuk HTML ialah W3C atau *World Wide Web Consortium*. HTML juga mempunyai tag yang dapat digunakan untuk melakukan pendefinisian struktur serta elemen dengan penggunaan karakter < atau >. Tampilan halaman website yang ada di *browser* merupakan penggunaan dari tag-tag tersebut. HTML merupakan salah satu *standard development* yang sering digunakan oleh pembuat website[32].

2.5 PHP

PHP merupakan sebuah bahasa pemogrman yang dapat digunakan dalam mengartikan setiap kode program hingga dapat menjadi kode mesin yang mana kode tersebut dapat dipahami komputer. Kode program tesebut bersifat *server-side* dimana kode yang dimaksud dapat ditambah ke dalam HTML. Bahasa pemograman PHP dapat juga dijeniskan kedalam *Server Side Programming* dimana pada bahasa pemograman ini diperlukan penerjemahan dalam konteks ini adalah web server untuk melakukan jalannya program [33].

PHP dapat juga diartikan sebagai bahasa pelengkap untuk HTML yang berkemungkinan dapat membuat aplikasi dinamis. Aplikasi yang dibuat menggunakan PHP memungkinkan tedapat pengolahan serta pemrosesan data. Semua syntax yang terdapat di PHP yang dimasukkan akan sepenuhnya dikelola oleh server selanjutnya hasil dari pembacaan syntax tersebut ditampilkan ke dalam browser. Hasil pengiriman tersebut diperoleh ke client, tempat pemakai bagi yang menggunakan browser tersebut [34].

---

[31]Pamungkas, C. A. (2017). Dasar Pemrograman Web dengan PHP. Yogyakarta: Deepublish..

[32]Muthohir, Moh. 2021. Mudah Mmbuat Web Bagi Pemula (Pemrograman Web I). Yayasan Prima Agus Teknik: Semarang.

[33]Supono, & Putratama, V. (2018). Pemogramam Web dengan Menggunakan PHP dan Framework Codeigniter. Deepublish.

[34]Fadel, A. Aplikasi Sistem Pakar Pusat Informasi Konseling Remaja (Pik-R) Di Sman 2 Dumai Dengan Metode Backward Chaining Menggunakan Bahasa Pemograman Php. (2018). Https://Doi.Org/Https://Doi.Org/10.33322/Petir.V11i1.1.

Bahasa pemograman dari PHP pertama sekali diciptakan oleh Rasmus Lerdoff. Adapun dasar dari kinerja PHP ialah data yang didapatkan melalu *form* dan menampilkan isi dari setiap halaman website secara dimanik. PHP juga dapat menerima *cookies* serta *feature* PHP memimiliki kemampuan yang dapat diandalkan karena dukungan atas *database* dari PHP yang sangatlah signifikan[35]. Atas dari dukungan fitur yang ada menjadikan PHP sering digunakan oleh pengguna untuk membuat website dinamis yang sangat bagus.

Gambar 2. 3 Logo PHP (www.php.net)

Bahasa pemograman PHP tersendiri memiliki keunggulan yang membuat para penggunanya tetap setia menggunakan bahasa pemograman tersebut. Adapun keunggulan dari bahasa pemograman PHP adalah sebagai berikut [36] :

1. PHP merupakan bahasa yang multifplatform Maksdunya ialah bahasa pemograman dari PHP itu sendiri dapat berjalan di segala mesin dan juga sistem operasi seperti Linux, Unix, Mac serta Windows. PHP juga dapat berjalan secara *runtime* lewat *console* serta dapat juga memperoses perintah-perintah sistem yang lainnya sesuai dengan kebutuhan penggunanya.
2. PHP bersifat *Open Source* yang memiliki arti bahwa PHP dapat dipakai oleh siapapun tanpa menggunakan biaya.
3. PHP memiliki dukungan penyimpanan data atau *Web Server* yang dapat diperoleh dari mana-mana seperti apache, IIS, Lighttpd, nginx, dan juga Xitami. Proses dari konfigurasi PHP serta *web server* tersebut sangat relatif gampang serta tidak terbelit-belit bahkan ada beberapa yang menggabungkan konfigurasi tersebut dalam bentuk sebuah paket contohnya seperti menggabungkan antara PHP, MYSQL dan juga *Web Server*.
4. Dalam proses penggembangannya, PHP dapat mudah dikembangkan sebab banyaknya milis-milis, komunitas sert *developer* yang siap dalam mengembangkan bahasa pemograman PHP.

[35]Irawan, M. D., & Nasution, M. K. I. Rancang Bangun Sistem Pakar Mendiagnosa Penyakit Tanaman Kelapa Sawit Menggunakan Metode Bayes Berbasis Android (Studi Kasus : Perkebunan PTPN 4 Air Batu). Jurnal Teknologi Informasi. (2018). Vol. 2. No. 1, 15.
[36]Supono, & Putratama, V. (2018). Pemogramam Web dengan Menggunakan PHP dan Framework Codeigniter. Deepublish.

5. Pada area pemahaman, PHP merupakan sebuah bahasa *scripting* yang sangatlah gambang sebab terdapat banyak sekali referensi-referensi yang telah ada saat ini.
6. Aplikasi dan pemograman PHP sudah banyak yang telah bermunculan di internet secara gratis serta dapat digunakan langsung seperti Wodpress, Prestashop dan banyak lagi lainnya.
7. PHP juga dapat didukung banyak sekali *database* yang dapat dikonfigurasi bersama seperti MySQL, Oracle, MS-SQL dan banyak lagi lainnya.

PHP dapat juga ditanam pada bagian server dengan penggunaan *script*nya. Proses yang dilakukan pada server seperti windows dan lainnya ialah saat halaman yang sedang dibuka memiliki kandungan kode PHP. Prosessor yang malakukan penerjermahan dan pengeksekusian semua perintar yang ada pada halaman tersebut. Setelah tidak ada masalah maka di *browser* akan tetampil hasil dari proses tersebut dan sebagai halaman HTML biasa. Sebab proses menerjemahkannya dilakukan di *server*, sebuah halaman yang sudah tertulis menggunakan bahasa pemograman PHP dapat terlihat dengan menggunakan segala jenis browser yang ada saat ini dan juga dapat terlihat di sistem operasi apapun juga. Sama seperti dengan bahasa *script* pada umumnya, PHP dapat juga menanamkan *script*nya langsung kedalam halaman HTML. Proses pemisahan halaman PHP dan HTML terletak dari kode pemisahnya yaitu dengan menggunakan *Start* dan juga *End*. Saat pembacaaan suatu dokumen, prosesor PHP hanya melakukan penerjemahan di area yang ditandai saja kemudian hasilnya ditampilkan pada tempat yang sama juga.

PHP disebut juga sebagai bahasa *script server-side* yang dapat didisain untuk pengembangan suatu *website*. Disebut dengan hal tersebut sebab PHP dikelola pada komputer server. PHP merupakan suatu bahasa *script* yang digunakan agar menghasilkan sebuah program situs web yang dinamis. Inilah yang menjadi pembeda antara PHP dengan pemograman yang bersifat *client-side* seperti Javascript yang prosenya dilakukan pada web browser (*client*) [37]. PHP juga memiliki kelemahan antara lain sebagai berikut [38]:

1. PHP tidak mengerti *package*.
2. Jika tidak dilakuka proses *encoding* maka proses *endcoding*nya memerlukan *tool* dari Zend dan itu sangat mahal sekali biayanya.
3. PHP sangat lemah dengan masalah keamanan. Maka dari itu, *programmer* haruslah detail serta berhati-hati dalam melaksanakan proses pemograman serta melakukan konfigurasi dari PHP tersebut.

[37]Ikhwan, A., Nofriansyah, D., & Sriani. Penerapan Data Mining dengan Algoritma Fp-Growth untuk Mendukung Strategi Promosi Pendidikan (Studi Kasus Kampus STMIK Triguna Dharma). Saintikom. (2015). Vol. 14 No. 3, 211–226..

[38]Supono, & Putratama, V. (2018). Pemogramam Web dengan Menggunakan PHP dan Framework Codeigniter. Deepublish.

2.6 XAMPP

XAMPP adalah salah satu paket yang terdapat beberapa bahasa pemograman yang bersifat *open source*. XAMPP dikembangkan oleh sebuah komunitas *Open Source*. Dengan adanya penggunaan XAMPP maka kita tidak butuh lagi mengintasll beberapa program lainnya sebab seluruh keingian yang kita butuhkan salah satunya untuk membuat web sudah tersedia didalam XAMPP. Adapun paket yang terdapat didalam XAMPP yaitu apache, MySQL, PHP, Phpmyadmin [39].

Gambar 2. 4 Logo XAMPP (www.xampp.com)

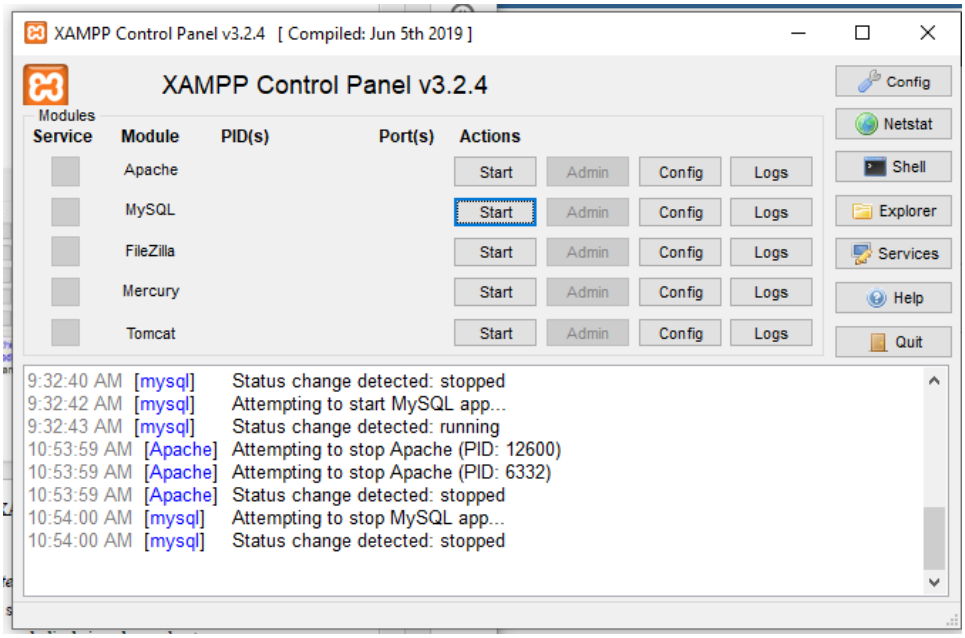
XAMPP merupakan sebuah perangkat bebas yang mana didalamnya terdapat dukungan dari banyaknya sistem operasi serta merupakan kolaborasi dari beberapa program. Adapun fungsi dari PHP ialah sebagai server yang dapat berdiri sendiri (*localhost*). Didalam XAMPP terdapat pogram seperti Apache sebagai HTTP Server, MySQL sebagai database serta penerjemah bahasa yang dapat diketikkan dalam bahasa pemograman PHP dan Perl. Nama dari XAMPP itu sendiri merupakan dari singkatan yang mana huruf X dapat diartikan sebagai dapat dilakukan dengan sistem operasi apapun dan dapat berjalan dikomputer atau sering disebut dengan *Cross-Paltform*, huruf A yang merupakan Apache, huruf M merupakan MySQL serta kedua huruf P untuk PHP dan juga Perl [40]. Ketersediaan prangkat XAMPP ini dalam GNU General Public License serta bebas. XAMPP ialah web server yang cara penggunaannya sangat mudah dan dapat melayani tampilan halaman web yang dinamis. Pada dasarnya, XAMPP dijadikan sebagai tuan rumah local atau sering dikatakan sebagai server lokal. Server lokal tesebur memiliki fungsi lokal pada prangkat komputer atau laptop. Tahapan dari penggunaan itu sendiri ialah untuk melakukan pengujian client atau website sebelum melakukan pengunggahan ke server web jarak jauh[41].

---

[39]Nugroho, A. (2011). Perancangan dan Implementasi Sistem Basis Data. Andi..

[40]Kinaswara, T. A. (2019). *Rancang Bangun Aplikasi Inventaris Berbasis Website Pada Kelurahan Bantengan*. https://doi.org/10.36352/jt-ibsi.v3i2.140.

[41]Saputra, M. H. K., & Aprilian, L. V. (2020). *Belajar Cepat Metode SAW*. Kreatif Industri Nusantara.



Gambar 2. 5 Tampilan XAMPP [42]

[42]Fitri, R. (2020). *Pemrograman Basis Data Menggunakan MySQL*. Deepublish..

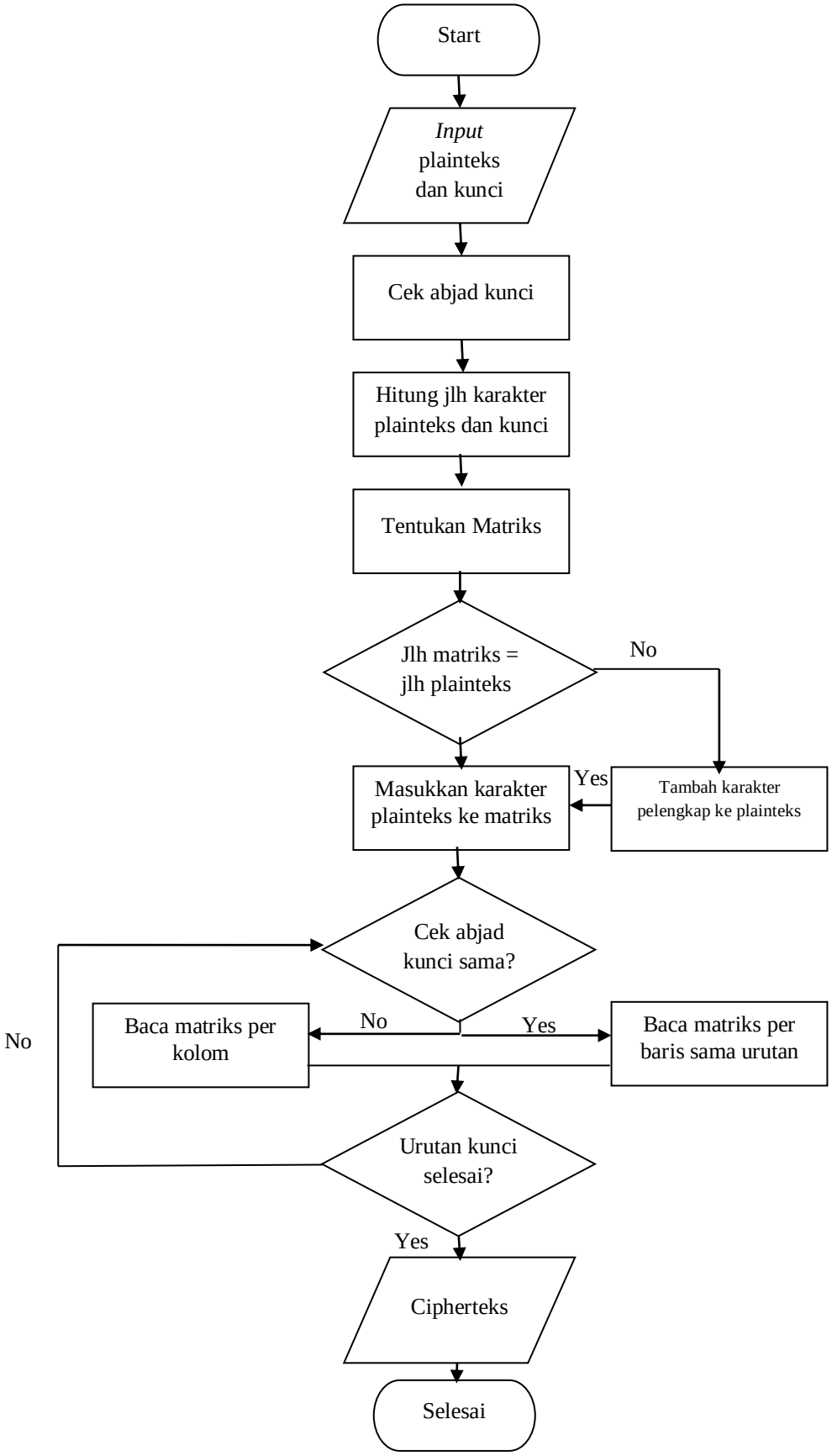
BAB III
HASIL DAN PEMBAHASAN

3.1 Alur Proses Algoritma Myszkowski

3.1.1 Alur Proses Enkripsi

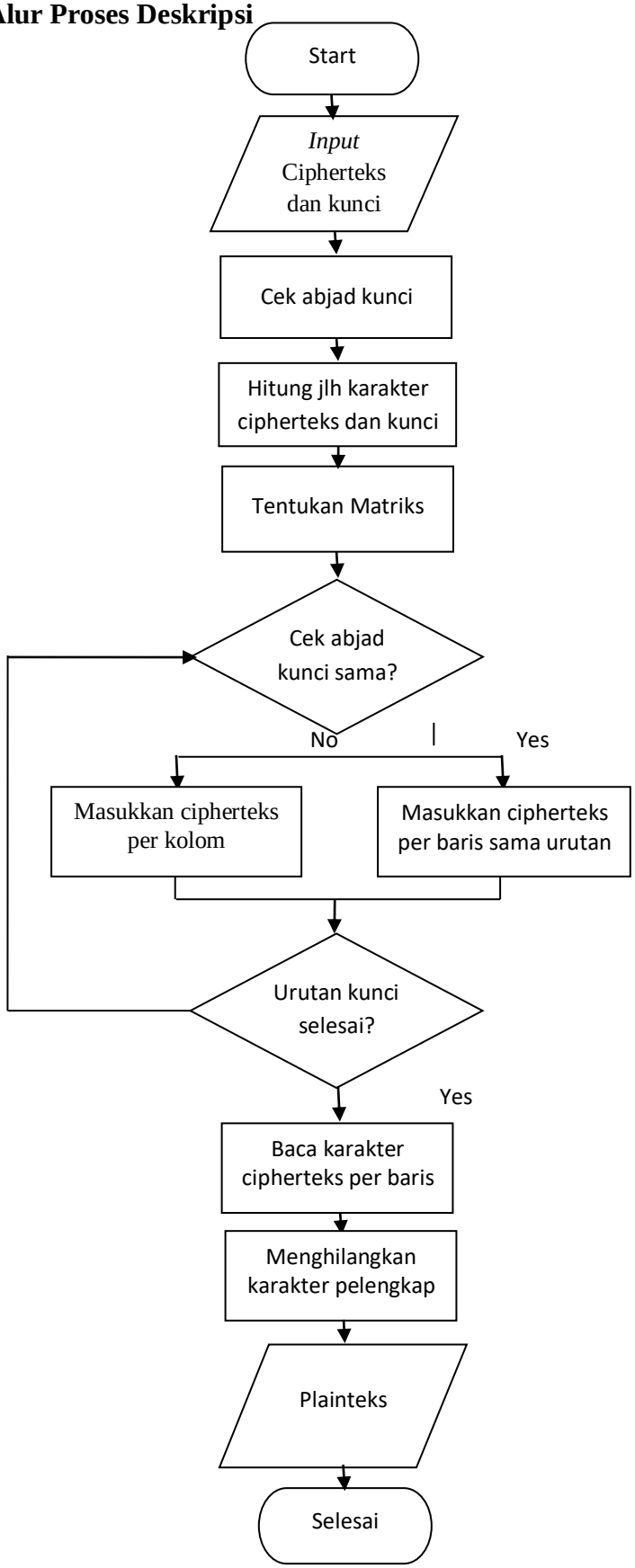
Pada alur proses enkripsi merupakan gambaran dari proses enkripsi algoritma myszkowski. Langkah pertama adalah menginput plainteks dan kunci. Pada plainteks data yang dapat diinputkan abjad dan angka sedangkan pada kunci adalah abjad saja. Proses berikutnya adalah mengcek abjad kunci. Karakter kunci yang diinputkan akan dinilai dalam bentuk angka. Penentuan angka dimulai dari angka 1 dimana penentuan dilihat dari urutan karakter yang muncul dalam alphabet. Selanjutnya, plainteks dan kunci akan dihitung berapa panjang karakter yang ada dimana untuk plainteks karakter spasi dihitung menjadi 1 karakter. Setelah itu, dihitung brapa matriks yang akan dibuat dimana banyaknya kolom dihitung brapa banyak jumlah karakter kunci sedangkan untuk baris dihitung dari penggenapan keatas dari pembagian jumlah karakter plainteks dengan jumlah karakter kunci. Kemudian, dilakukan perbandingan dimana jika jumlah kotak matriks sama dengan jumlah plainteks maka akan dilakukan tahap berikutnya. Akan tetapi, jika jumlah kotak matriks tidak sama dengan jumlah plainteks maka akan dilakukan penambahan karakter pelengkap bintang (*) sampai jumlah karakter pada plaintek sama dengan jumlah kotak pada matriks.

Proses berikutnya adalah memasukan karakter plainteks kedalam kotak matriks sampai kotak matriks tersebut terisi semua. Tahap berikutnya adalah pengecekan kesamaan abjad kunci. Proses pengecekan tersebut dimulai dari angka yang lebih kecil. Pada tahapan ini, karakter kunci yang telah dibuat dalam bentuk angka akan dicek berapa banyak angka yang sama dimana apabila angka tersebut terdapat angka yang sama maka proses membaca matriks dalam mendapatkan cipherteks dimulai dari baris yang pertama sampai baris terakhir yang memiliki angka kunci yang sama aja. Akan tetapi, apabila angka tersebut tidak terdapat angka yang sama maka proses membaca matriks dalam mendapatkan cipherteks dilakukan per kolom sesuai dengan urutan angka yang dicek. Selanjutnya, jika karakter kunci yang telah dilabelkan angka sudah selesai dicek maka akan dilakukan tahap berikutnya. Akan tetapi, jika karakter kunci yang telah dilabelkan angka belum selesai dicek maka proses pengecekan kesamaan abjad kunci dilakukan kembali. Tahap terakhir adalah keluaran dari proses pembacaan matriks dimana hasil dari proses pembacaan matrik merupakan cipherteks dari plainteks yang telah diinputkan. Adapun tampilan pada alur proses enkripsi dapat diperhatikan pada tampilan gambar 3.1 dibawah:



Gambr 3. 1 Alur Proses Enkripsi Algoritma Myszkowski

3.1.2 Alur Proses Deskripsi



Gambr 3. 2 Alur Proses Deskripsi Algoritma Myszkowski

Pada Gambar 3.2 adalah gambaran dari alur proses deskripsi algoritma myszkowski. Langkah pertama adalah menginput cipherteks dan kunci. Pada cipherteks data yang dapat diinputkan abjad, angka dan symbol bintang (*) sedangkan pada kunci adalah abjad saja. Proses berikutnya adalah mengcek abjad kunci. Karakter kunci yang diinputkan akan dinilai dalam bentuk angka. Penentuan angka dimulai dari angka 1 dimana penentuan dilihat dari urutan karakter yang muncul dalam alphabet. Selanjutnya, cipherteks dan kunci akan dihitung berapa panjang karakter yang ada dimana untuk cipherteks karakter spasi dihitung menjadi 1 karakter. Setelah itu, dihitung brapa matriks yang akan dibuat dimana banyaknya kolom dihitung brapa banyak jumlah karakter kunci sedangkan untuk baris dihitung dari penggenapan keatas dari pembagian jumlah karakter cipherteks dengan jumlah karakter kunci.

Tahap berikutnya adalah pengecekan kesamaan abjad kunci. Proses pengecekan tersebut dimulai dari angka yang lebih kecil. Pada tahapan ini, karakter kunci yang telah dibuat dalam bentuk angka akan dicek berapa banyak angka yang sama dimana apabila angka tersebut terdapat angka yang sama maka masukkan cipherteks dari baris yang pertama sampai baris terakhir yang memiliki angka kunci sama saja. Akan tetapi, apabila angka tersebut tidak terdapat angka yang sama maka proses masukkan cipherteks ke dalam kolom angka tersebut sampai kolom penuh. Selanjutnya, jika karakter kunci yang telah dilabelkan angka sudah selesai dicek maka akan dilakukan tahap berikutnya. Akan tetapi, jika karakter kunci yang telah dilabelkan angka belum selesai dicek maka proses pengecekan kesamaan abjad kunci dilakukan kembali. Proses selanjutnya adalah proses pembacaan cipherteks dimatrik. Pada proses ini, setiap karakter cipherteks akan dibaca dimulai dari baris awal sampai baris akhir matriks. Selanjutnya, proses penghapusan simbol at (@) dimana pada karakter ciphertek yang telah dibaca ulang apabila terdapat simbol at (@) maka simbol tersebut dihapuskan sampai tidak terapat lagi symbol tersebut. Tahap terakhir adalah keluaran dari penghapusas dari symbol at (@) dimana hasil dari proses penghapusas dari symbol at (@) merupakan plainteks dari cipherteks yang telah diinputkan.

3.2 Analisis Algoritma Myszkowski

Dari pemaparan alur gambar 3.1 dan gambar 3.2 mengenai tahapan-tahapan dalam proses enkripsi dan deskripsi algoritma myszkowski. Adapun yang dibuat sebagai contoh kasus adalah sebagai berikut :

3.2.1 Proses enkripsi

Berikut adalah penjelasan melalui contoh kasus proses enkripsi pada algoritma myszkowski:
Contoh kasus :

Plainteks = Amankan datamu selalu ya
Kunci = akuraja

- Setelah mengetahui masukan plainteks dan juga kunci maka langkah berikutnya adalah pengecekan abjad kunci. Proses pengecekan diawali dengan melihat karakter mana yang posisinya paling kiri menurut abjad maka karakter tersebut akan dinilai duluan. Proses penilaian akan dilakukan dalam bentuk angka yang dimulai dari angka 1 sampai seterusnya. Contohnya, kunci pada contoh kasus diatas adalah akuraja dimana dari kunci tersebut karakter "a" merupakan karakter paling kiri dari urutan abjad maka karakter "a" akan akan dinilai 1. Karakter berikutnya yang karakternya paling kiri dari urutan abjad setelah karakter "a" pada kunci adalah karakter "j". Begitu seterusnya sampai mendapatkan urutan abjad kunci sebagai berikut :
  Kunci : **a k u r a j a**
  Urutan abjad kunci : **1 3 5 4 1 2 1**
- Setelah cek abjad kunci selesai, maka proses berikutnya adalah menghitung jumlah karakter plainteks dan kunci. Pada kasus ini, karakter spasi (" ") dinilai menjadi 1 karakter. Dari contoh kasus diatas, palinteks "Amankan datamu selalu ya" memiliki jumlah karakter sebanyak **24 karakter**. Sedangkan, kunci "akuraja" memiliki jumlah karakter sebanyak **7 karakter**.
- Kemudian, dilakukan penentuan matriks pada proses berikutnya. Banyak kolom yang akan dibuat pada matriks sama dengan jumlah karakter kunci yaitu sebanyak 7 kolom. Sedangkan untuk penentuan baris dapat dilakukan dengan cara penggenapan keatas dari pembagian jumlah karakter plainteks dengan jumlah karakter kunci yaitu 24 : 7 = 3.428 atau digenapkan keatas menjadi 4 baris. Maka, matriks yang akan digunakan adalah **7x4 matriks**.
- Pada proses selanjutnya dilakukan kesamaan jumlah karakter plainteks dengan jumlah kotak matriks. Jika jumlah karakter plainteks sama dengan jumlah kotak matriks maka lanjut ke proses berikutnya. Akan tetapi, jika jumlah karakter plainteks tidak sama dengan jumlah kotak matriks maka sisa dari kotak matriks akan ditambahkan karakter pelengkap. Adapun karakter pelengkapnya adalah simbol @. Dari contoh kasus diatas, hasil dari cek kesamaan abjad dan kunci adaah sebagai berikut :
  Jumlah kotak matriks = 7x4 = 28
  Jumlah karakter plainteks = 24
  Sisa kotak kosong pada matriks = 28 modulo 24 = 4
  Adapun penambahan karakter pelengkap pada contoh kasus diatas adalah sebanyak 4 simbol @. Maka plainteks pada kasus diatas menjadi **Amankan datamu selalu ya@@@@**.
- Proses berikutnya adalah memasukkan setiap karakter plainteks ke kotak matriks. Pengaturan posisi plainteks dimulai dari kotak paling kiri pada baris pertama matriks dilanjutkan dengan baris berikutnya. Maka hasilnya terdapat di tabel 3.1 dibawah :

Tabel 3. 1 Penysunan Plainteks Dalam Matriks

1	**3**	**5**	**4**	**1**	**2**	**1**
A	m	a	n	k	a	n
(spasi)	d	a	t	a	m	u
(spasi)	s	e	l	a	l	u
(spasi)	y	a	@	@	@	@

- Setelah proses diatas, maka proses selanjutnya adalah pembacaan karakter cipherteks pada matriks. Adapun hal dilakukan pertama adalah cek kesamaan nilai abjad kunci. Jika terdapat nilai abjad kunci yang sama maka pembacaan cipherteks dilakukan mulai dari kiri baris pertama yang memiliki hanya nilai abjad kunci yang sama. Jika tidak terdapat nilai abjad kunci yang sama maka pembacaan cipherteks dilakukan mulai dari atas sampai kebawah pada kolom nilai abjad kunci tersebut. Pada contoh kasus, abjad kunci dengan nilai angka 1 pada abjad kunci adalah karakter “a". Pada nilai abjad kunci tersebut terdapat 3 kolom yang memiliki nilai yang sama. Adapun pembacaan cipherteks pada nilai angka 1 pada abjad kunci (karakter “a”) dilakukan mulai dari kiri baris pertama yang memiliki hanya nilai abjad kunci yang sama. Maka proses pembacaannya adalah sebagai berikut :
-

Tabel 3. 2 Pembacaan nilai Angka 1 Pada Abjad Kunci

	1	**3**	**5**	**4**	**1**	**2**	**1**
Baris 1	**A**	m	a	n	**k**	a	**n**
Baris 2	**(spasi)**	d	a	t	**a**	m	**u**
Baris 3	**(spasi)**	s	e	l	**a**	l	**u**
Baris 4	**(spasi)**	y	a	@	**@**	@	**@**

Hasil dari pembacaan nilai angka 1 pada abjad kunci adalah **Akn au au @@**.

- Selanjutnya, proses yang akan dilakukan adalah pengecekan nilai abjad kunci sudah selesai atau belum. Jika nilai abjad kunci sudah selesai maka ke tahap berikutnya. Akan tetapi, jika nilai abjad belum selesai maka dilakukan kembali proses pembacaan cipherteks. Pada contoh kasus diatas, terdapat nilai abjad kunci berikutnya dengan nilai angka 2 yaitu karakter “j” maka dilakukan tahap selanjutnya yaitu pembacaan cipherteks pada matriks. Pada nilai abjad kunci bernilai angka 2 tidak terdapat nilai abjad kunci yang sama. Oleh karena itu, pembacaan cipherteks pada nilai angka 2 pada abjad kunci (karakter “j”) dilakukan mulai dari atas sampai kebawah pada kolom nilai abjad kunci tersebut. Maka proses pembacaannya adalah sebagai berikut :
-

Tabel 3. 3 Pembacaan nilai Angka 2 Pada Abjad Kunci

1	**3**	**5**	**4**	**1**	**2**	**1**
A	m	a	n	k	**a**	n
(spasi)	d	a	t	a	**m**	u
(spasi)	s	e	l	a	**l**	u
(spasi)	y	a	@	@	**@**	@

Hasil dari pembacaan nilai angka 2 pada abjad kunci adalah **aml@**.

- Kemudian, pada contoh kasus diatas terdapat nilai abjad kunci berikutnya dengan nilai angka 3 yaitu karakter “k” maka dilakukan tahap selanjutnya yaitu pembacaan cipherteks pada matriks. Pada nilai abjad kunci tersebut tidak terdapat nilai abjad kunci yang sama. Oleh karena itu, pembacaan cipherteks pada nilai angka 3 pada abjad kunci (karakter “k”) dilakukan mulai dari atas sampai kebawah pada kolom nilai abjad kunci tersebut. . Maka proses pembacaannya adalah sebagai berikut :
-

Tabel 3. 4 Pembacaan nilai Angka 3 Pada Abjad Kunci

1	**3**	**5**	**4**	**1**	**2**	**1**
A	**m**	a	n	k	a	n
(spasi)	**d**	a	t	a	m	u
(spasi)	**s**	e	l	a	l	u
(spasi)	**y**	a	@	@	@	@

Hasil dari pembacaan nilai angka 2 pada abjad kunci adalah **mdsy**.

- Lalu, pada contoh kasus diatas terdapat nilai abjad kunci berikutnya dengan nilai angka 4 yaitu karakter “r” maka dilakukan tahap selanjutnya yaitu pembacaan cipherteks pada matriks. Pada nilai abjad kunci tersebut tidak terdapat nilai abjad kunci yang sama. Oleh karena itu, pembacaan cipherteks pada nilai angka 4 pada abjad kunci (karakter “r”) dilakukan mulai dari atas sampai kebawah pada kolom nilai abjad kunci tersebut. . Maka proses pembacaannya adalah sebagai berikut :

Tabel 3. 5 Pembacaan nilai Angka 4 Pada Abjad Kunci

1	**3**	**5**	**4**	**1**	**2**	**1**
A	m	a	**n**	k	a	n
(spasi)	d	a	**t**	a	m	u
(spasi)	s	e	**l**	a	l	u
(spasi)	y	a	**@**	@	@	@

Hasil dari pembacaan nilai angka 2 pada abjad kunci adalah **ntl@**.

- Berikutnya, pada contoh kasus diatas terdapat nilai abjad kunci berikutnya dengan nilai angka 5 yaitu karakter “u” maka dilakukan tahap selanjutnya yaitu pembacaan cipherteks pada matriks. Pada nilai abjad kunci tersebut tidak terdapat nilai abjad kunci yang sama. Oleh karena itu, pembacaan cipherteks pada nilai angka 5 pada abjad kunci (karakter “u”) dilakukan mulai dari atas sampai kebawah pada kolom nilai abjad kunci tersebut. . Maka proses pembacaannya adalah sebagai berikut :

Tabel 3. 6 Pembacaan nilai Angka 5 Pada Abjad Kunci

1	**3**	**5**	**4**	**1**	**2**	**1**
A	m	**a**	n	k	a	n
(spasi)	d	**a**	t	a	m	u
(spasi)	s	**e**	l	a	l	u
(spasi)	y	**a**	@	@	@	@

Hasil dari pembacaan nilai angka 2 pada abjad kunci adalah **aaea**.

- Selanjutnya, pada contoh kasus diatas sudah tidak terdapat nilai kunci berikutnya maka proses selanjutnya adalah menampilkan hasil cipherteks. Hasil cipherteks merupakan penggabungan dari pembacaan cipherteks mulai dari nilai abjad kunci terendah hingga nilai abjad tertinggi. Adapun hasil cipherteks dari pembacaan matriks contoh kasus diatas adalah **Akn au au @@aml@mdsyntl@aaea** .

3.2.2 Proses Deskripsi

Contoh Kasus Deskripsi:

Cipherteks = Akn au au @@aml@mdsyntl@aaea
Kunci = akuraja

- Setelah mengetahui masukan cipherteks dan juga kunci maka langkah berikutnya adalah pengecekan abjad kunci. Proses pengecekan diawali dengan melihat karakter mana yang posisinya paling kiri menurut abjad maka karakter tersebut akan dinilai duluan. Proses penilaian akan dilakukan dalam bentuk angka yang dimulai dari angka 1 sampai seterusnya. Contohnya, kunci pada contoh kasus deskripsi adalah akuraja dimana dari kunci tersebut karakter “a” merupakan karakter paling kiri dari urutan abjad maka karakter “a” akan akan dinilai 1. Karakter berikutnya yang karakternya paling kiri dari urutan abjad setelah karakter “a” pada kunci adalah karakter “j”. Begitu seterusnya sampai mendapatkan urutan abjad kunci sebagai berikut :
  Kunci : **a k u r a j a**
  Urutan abjad kunci : **1 3 5 4 1 2 1**
- Setelah cek abjad kunci selesai, maka proses berikutnya adalah menghitung jumlah karakter plainteks dan kunci. Pada kasus ini, karakter spasi (“ “) dinilai menjadi 1 karakter. Dari contoh kasus deskripsi, cipherteks “Amankan datamu selalu ya” memiliki jumlah karakter sebanyak **28 karakter**. Sedangkan, kunci “akuraja” memiliki jumlah karakter sebanyak **7 karakter**.
- Kemudian, dilakukan penentuan matriks pada proses berikutnya. Banyak kolom yang akan dibuat pada matriks sama dengan jumlah karakter kunci yaitu sebanyak 7 kolom. Sedangkan untuk penentuan baris dapat dilakukan dengan cara penggenapan keatas dari pembagian jumlah karakter plainteks dengan jumlah karakter kunci yaitu 28 : 7 = 4. Maka, matriks yang akan digunakan adalah **7x4 matriks**.

- Proses berikutnya adalah memasukkan cipherteks ke dalam kotak matriks. Apabila terdapat nilai abjad kunci yang sama maka pemasukan cipherteks ke dalam kotak matriks dilakukan mulai dari kiri baris pertama yang memiliki hanya nilai abjad kunci yang sama. Jika tidak terdapat nilai abjad kunci yang sama maka pemasukan cipherteks ke dalam kotak matriks dilakukan mulai dari atas sampai kebawah pada kolom nilai abjad kunci tersebut. Pada contoh kasus, abjad kunci dengan nilai angka 1 pada abjad kunci adalah karakter “a". Pada nilai abjad kunci tersebut terdapat 3 kolom yang memiliki nilai yang sama. Adapun pembacaan cipherteks pada nilai angka 1 pada abjad kunci (karakter “a”) dilakukan mulai dari kiri baris pertama yang memiliki hanya nilai abjad kunci yang sama. Maka proses pemasukan cipherteks ke dalam kotak matriks adalah sebagai berikut :

-

Tabel 3. 7 Pemasukan Cipherteks Dengan Nilai Angka 1 Pada Abjad Kunci

	1	3	5	4	1	2	1
Baris 1	A				k		n
Baris 2							
Baris 3							
Baris 4							

(a)

	1	3	5	4	1	2	1
Baris 1	A				k		n
Baris 2	(spasi)				a		u
Baris 3							
Baris 4							

(b)

	1	3	5	4	1	2	1
Baris 1	A				k		n
Baris 2	(spasi)				a		u
Baris 3	(spasi)				a		u
Baris 4							

(c)

	1	3	5	4	1	2	1
Baris 1	A				k		n
Baris 2	(spasi)				a		u
Baris 3	(spasi)				a		u
Baris 4	(spasi)				@		@

(d)

- Selanjutnya, proses yang akan dilakukan adalah pengecekan nilai abjad kunci sudah selesai atau belum. Jika nilai abjad kunci sudah selesai maka ke tahap berikutnya. Akan tetapi, jika nilai abjad belum selesai maka dilakukan kembali pemasukan cipherteks ke dalam kotak matriks. Pada contoh kasus deskrispsi, terdapat nilai abjad kunci berikutnya dengan nilai angka 2 yaitu karakter "j" maka dilakukan tahap selanjutnya yaitu pembacaan cipherteks pada matriks. Pada nilai abjad kunci bernilai angka 2 tidak terdapat nilai abjad kunci yang sama. Oleh karena itu, pembacaan cipherteks pada nilai angka 2 pada abjad kunci (karakter "j") dilakukan mulai dari atas sampai kebawah pada kolom nilai abjad kunci tersebut. Maka proses pemasukan cipherteks ke dalam kotak matriks adalah sebagai berikut :

Tabel 3. 8 Pemasukan Cipherteks Dengan Nilai Angka 2 Pada Abjad Kunci

1	**3**	**5**	**4**	**1**	**2**	**1**
A				k	**a**	n
(spasi)				a	**m**	u
(spasi)				a	**l**	u
(spasi)				@	**@**	@

- Kemudian, pada contoh kasus deskripsi terdapat nilai abjad kunci berikutnya dengan nilai angka 3 yaitu karakter "k" maka dilakukan tahap selanjutnya yaitu pemasukan cipherteks ke dalam kotak matriks. Pada nilai abjad kunci tersebut tidak terdapat nilai abjad kunci yang sama. Oleh karena itu, pembacaan cipherteks pada nilai angka 3 pada abjad kunci (karakter "k") dilakukan mulai dari atas sampai kebawah pada kolom nilai abjad kunci tersebut. Maka proses pemasukan cipherteks ke dalam kotak matriks adalah sebagai berikut :
-

Tabel 3. 9 Pemasukan Cipherteks Dengan Nilai Angka 3 Pada Abjad Kunci

1	**3**	**5**	**4**	**1**	**2**	**1**
A	**m**			k	a	n
(spasi)	**d**			a	m	u
(spasi)	**s**			a	l	u
(spasi)	**y**			@	@	@

- Lalu, pada contoh kasus deskripsi terdapat nilai abjad kunci berikutnya dengan nilai angka 4 yaitu karakter "r" maka dilakukan tahap selanjutnya yaitu pemasukan cipherteks ke dalam kotak matriks. Pada nilai abjad kunci tersebut tidak terdapat nilai abjad kunci yang sama. Oleh karena itu, pembacaan cipherteks pada nilai angka 4 pada abjad kunci (karakter "r") dilakukan mulai dari atas sampai kebawah pada kolom nilai abjad kunci tersebut. Maka proses pemasukan cipherteks ke dalam kotak matriks adalah sebagai berikut :

Tabel 3. 10 Pemasukan Cipherteks Dengan Nilai Angka 4 Pada Abjad Kunci

1	**3**	**5**	**4**	**1**	**2**	**1**
A	m		**n**	k	a	n
(spasi)	d		**t**	a	m	u
(spasi)	s		**l**	a	l	u
(spasi)	y		**@**	@	@	@

- Berikutnya, pada contoh kasus deskripsi terdapat nilai abjad kunci berikutnya dengan nilai angka 5 yaitu karakter "u" maka dilakukan tahap selanjutnya yaitu pemasukan cipherteks ke dalam kotak matriks. Pada nilai abjad kunci tersebut tidak terdapat nilai abjad kunci yang sama. Oleh karena itu, pembacaan cipherteks pada nilai angka 5 pada abjad kunci (karakter "u") dilakukan mulai dari atas sampai kebawah pada kolom nilai abjad kunci tersebut. Maka proses pemasukan cipherteks ke dalam kotak matriks adalah sebagai berikut :

Tabel 3. 11 Pemasukan Cipherteks Dengan Nilai Angka 5 Pada Abjad Kunci

1	**3**	**5**	**4**	**1**	**2**	**1**
A	m	**a**	n	k	a	n
(spasi)	d	**a**	t	a	m	u
(spasi)	s	**e**	l	a	l	u
(spasi)	y	**a**	@	@	@	@

- Selanjutnya pada contoh kasus deskripsi sudah tidak terdapat nilai abjad kunci. Adapun proses berikutnya adalah pembacaan kembali cipherteks. Proses pembacaan kembali cipherteks dimulai dari paling kiri baris pertama hingga paling kanan baris terakhir. Berikut adalah proses pembacaan kembali cipherteks :
-

Tabel 3. 12 Pembacaan Kembali Cipherteks

	1	**3**	**5**	**4**	**1**	**2**	**1**
Baris 1	A	m	a	n	k	a	n
Baris 2	(spasi)	d	a	t	a	m	u
Baris 3	(spasi)	s	e	l	a	l	u
Baris 4	(spasi)	y	a	@	@	@	@

Hasil pembacaan kembali cipherteks adalah **Amankan datamu selalu ya@@@@**.

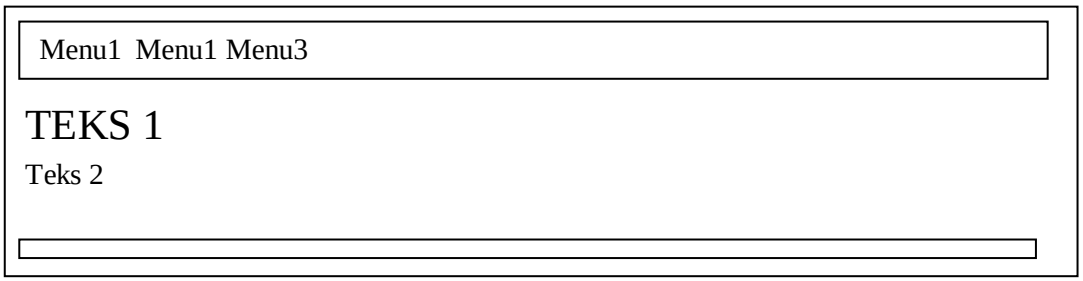
- Setelah memperoleh hasil pembacaan kembali cipherteks maka proses berikutnya adalah pengahapusan simbol at (@). Pada proses ini, semua simbol yang bertanda at (@) akan dihapuskan semua. Maka hasil dari penghapusan simbol at (@) adalah **Amankan datamu selalu ya**.

- Selanjutnya, proses terakhir adalah menampilkan plainteks. Pada proses ini, hasil hasil dari penghapusan simbol at (@) merupakan plainteks yang dihasilkan. Oleh karena itu, plainteks untuk contoh kasus deskrispi adalah adalah **Amankan datamu selalu ya**.

3.3 Tampilan Antarmuka Program

3.3.1 Tampilan Antarmuka Menu Home

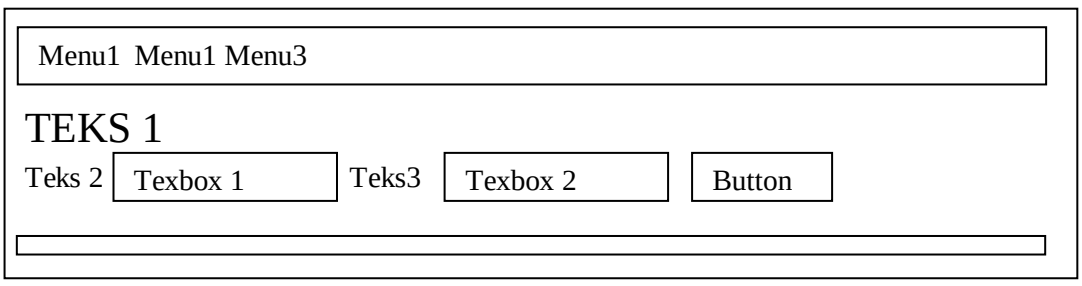
Pada tampilan antarmuka menu home terdapat menubar yang terdiri dari 3 menu yaitu menu1, menu2 dan menu 2. Terdapat pula 2 jenis teks dimana font size teks1 lebih besar dari font size teks 2. Adapun tampilan antarmuka menu home dapat dilihat pada gambar berikut ini :



Gambr 3. 3 Tampilan Antarmuka Menu Home

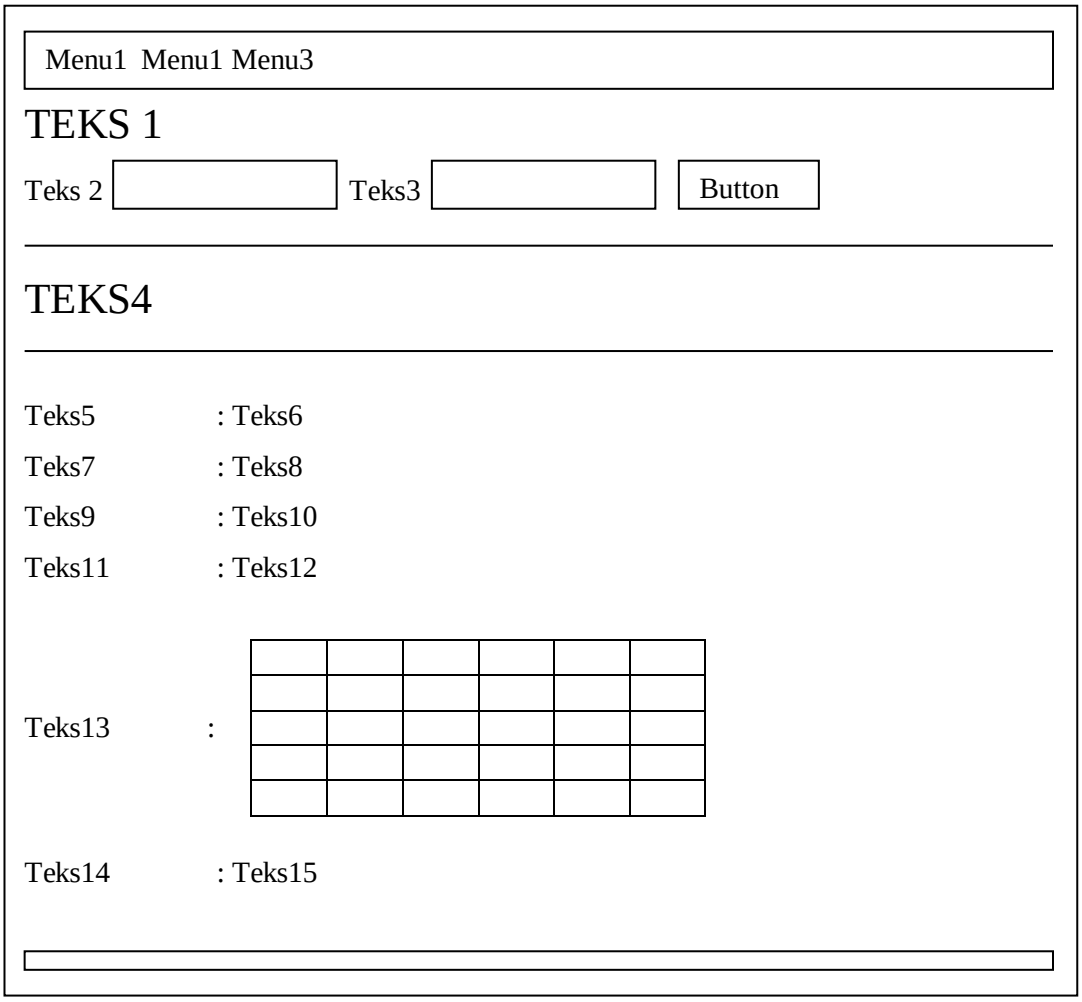
3.3.2 Tampilan Antarmuka Menu Enkripsi dan Deskripsi

Tampilan antarmuka menu enkripsi dibuat sama dengan tampilan antarmuka deskripsi. Pada tampilan antarmuka enkripsi dan deskripsi ini terdapat 2 tampilan. Pada tampilan pertama terdapat menubar yang terdiri dari 3 menu yaitu menu1, menu2 dan menu 2. Terdapat pula 3 teks dimana font size teks 1 lebih besar dari font size teks 2 dan teks 3. Pada tampilan antarmuka enkripsi dan deskripsi terdapat 2 textbox yaitu disebelah textbox 1 disebelah kanan teks2 dan textbox 2 disebalah kanan teks 3. Selanjutnya terdapat tombol button disebelah kanan textbox 2. Adapun tampilan 1 menu antarmuka enkripsi dan deskripsi dapat dilihat pada gambar berikut ini :



Gambr 3. 4 Tampilan 1 Antarmuka Menu Enkripsi dan Deskripsi

Pada tampilan kedua antarmuka menu enkripsi dan deskripsi terdapat 3 menu yaitu menu1, menu2 dan menu 2. Terdapat pula 15 teks dimana font size teks 1 dan teks 4 lebih besar dari font size teks lainnya. Pada tampilan antarmuka enkripsi dan deskripsi terdapat 2 textbox yaitu disebelah textbox 1 disebelah kanan teks2 dan textbox 2 disebalah kanan teks 3. Selanjutnya terdapat tombol button disebelah kanan textbox 2. Setelah itu terdapat tabel dimana jumlah tabel akan menyesuaikan dengan matriks yang didapatkan saat proses enkripsi dan deskripsi. Adapun tampilan 2 antarmuka menu enkripsi dan deskripsi dapat dilihat pada gambar berikut ini :

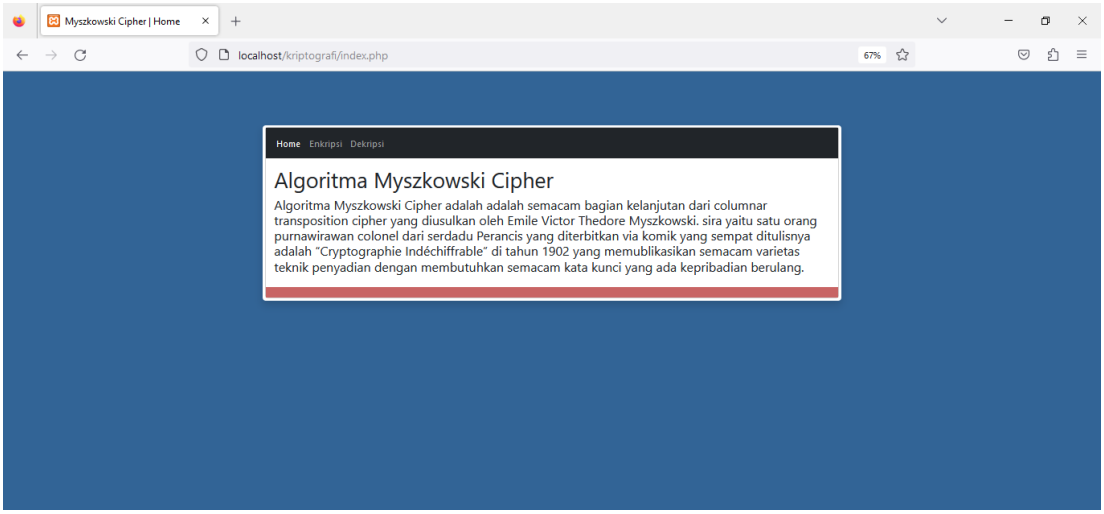


Gambr 3. 5 Tampilan 2 Antarmuka Menu Enkripsi dan Deskripsi

3.4 Tampilan Program

3.4.1 Tampilan Program Menu Home

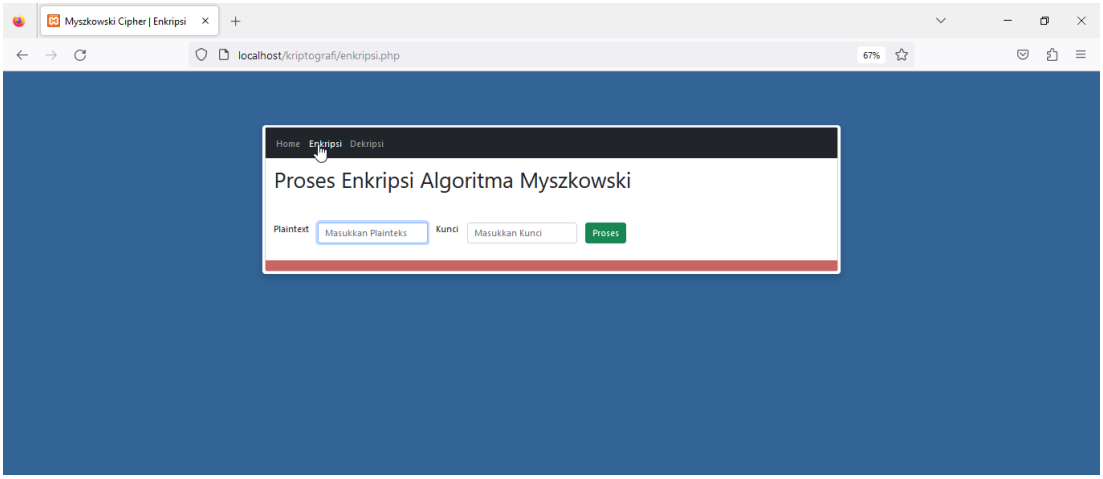
Pada tampilan program home terdapat 3 menu pada menubar yaitu menu home, menu enkripsi dan menu deskripsi. Pada tampilan home juga terdapat penjelasan singkat mengenai algoritm myzkoski cipher. Adapun tampilan program menu home dapat diperoleh di gambar 3.6 dibawah ini:



Gambr 3. 6 Tampilan Program Menu Home

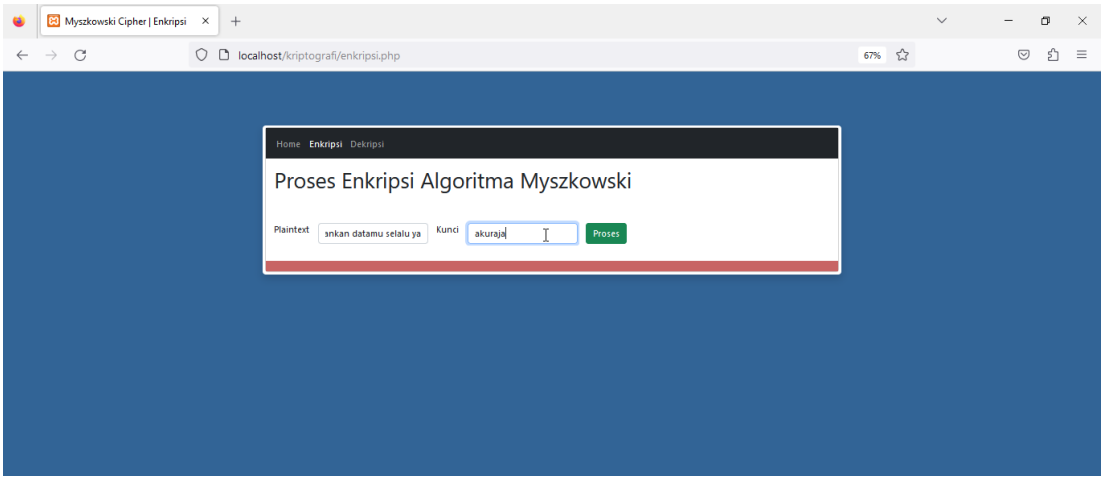
3.4.2 Tampilan Program Menu Enkripsi

Pada tampilan program menu enkripsi ini terdapat 3 tampilan. Pada tampilan 1 program menu enkripsi terdapat 3 menu pada menubar yaitu menu home, menu enkripsi dan menu deskripsi. Terdapat pula teks yang menampilkan tulisan "Enkripsi Myszkowski Cipher". Pada tampilan program ini pula terdapat 2 textbox yaitu textbox plainteks dan texbox kunci. Disetiap textbox terdapat tulisan yang berisi informasi masukan seperti apa yang dianjurkan pada texbox masing-masing. Terdapat pula 1 button yang bertuliskan "Proses" yang kegunaannya untuk memproses masukkan yang telah diisi dari plainteks dan juga kunci. Adapun tampilan 1 program menu enkrispsi adalah sebagai berikut :



Gambr 3. 7 Tampilan 1 Program Menu Enkripsi

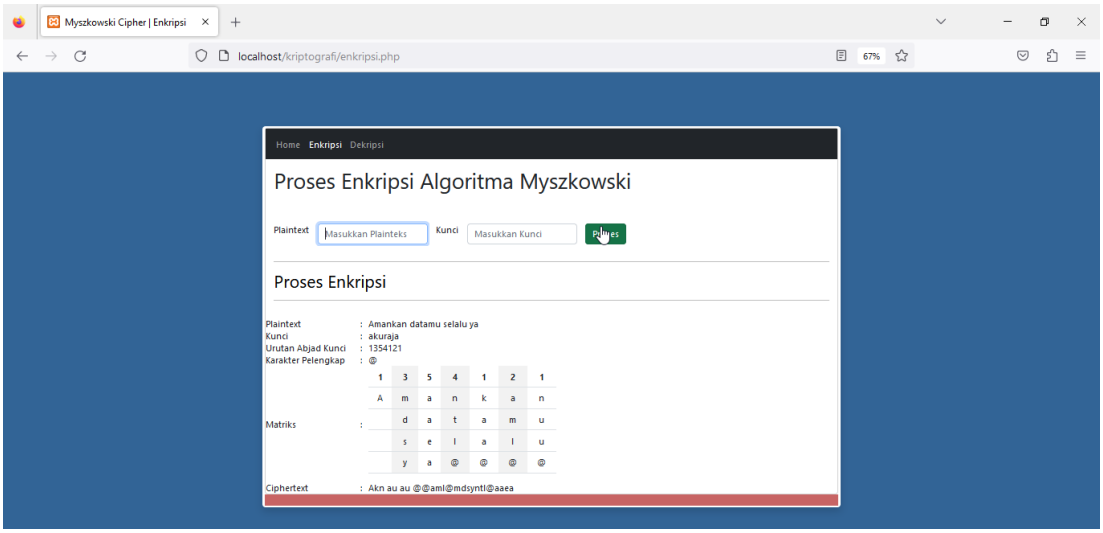
Pada tampilan 2 program menu enkripsi hampir sama dengan tampilan 1 program menu enkripsi. Perbedaan antara keduanya adalah terdapat informasi pada kedua textbox. Pada tampilan 2 program menu enkripsi informasi yang ditampilakan ditextbox adalah contoh kasus masukkan plainteks dan kunci. Adapun tampilan 2 program menu enkrispsi adalah sebagai berikut :



Gambr 3. 8 Tampilan 2 Program Menu Enkripsi

Pada tampilan 1 program menu home terdapat 3 menu pada menubar yaitu menu home, menu enkripsi dan menu deskripsi. Terdapat pula teks yang menampilkan tulisan “Enkripsi Myszkowski Cipher”. Pada tampilan program ini pula terdapat 2 textbox yaitu textbox plainteks dan texbox kunci. Disetiap textbox terdapat tulisan yang berisi informasi masukan seperti apa yang dianjurkan pada texbox masing-masing. Terdapat pula 1 button yang bertuliskan “Proses” yang kegunaannya untuk memproses masukkan yang telah diisi dari plainteks dan juga kunci. Kemudian, pada tampilan 3 menu enkripsi ini terdapat tulisan teks yang bertuliskan “Proses Enskripsi”. Dibawah tulisan tersebut terdapat tampilan penjelasan singkat mengenai tahapan proses enkripsi mulai dari plainteks, kunnci

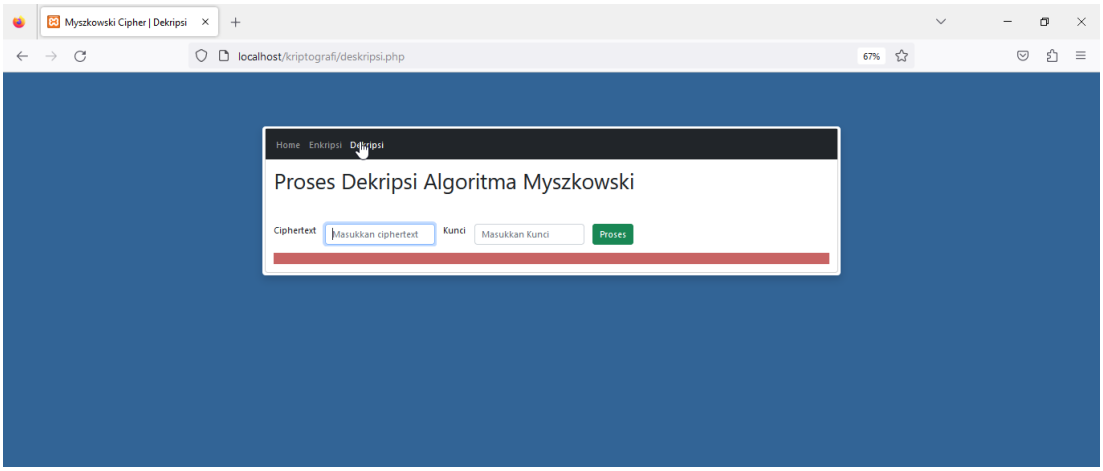
urutan abjad kunci, karakter pelengkap, matriks serta cipherteks yang dihasilkan pada proses enkripsi. Adapun tampilan 3 program menu enkrispsi adalah sebagai berikut :



Gambr 3. 9 Tampilan 3 Program Menu Enkripsi

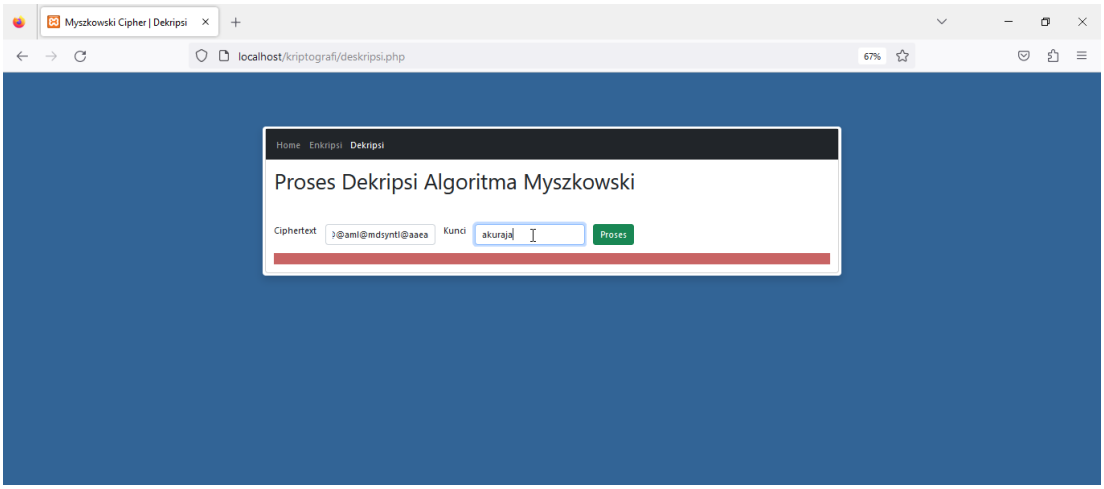
3.4.3 Tampilan Program Menu Deskripsi

Pada tampilan program menu deskripsi ini terdapat 3 tampilan. Pada tampilan 1 program menu deskripsi terdapat 3 menu pada menubar yaitu menu home, menu enkripsi dan menu deskripsi. Terdapat pula teks yang menampilkan tulisan "Deskripsi Myszkowski Cipher". Pada tampilan program ini pula terdapat 2 textbox yaitu textbox cipherteks dan texbox kunci. Disetiap textbox terdapat tulisan yang berisi informasi masukan seperti apa yang dianjurkan pada texbox masing-masing. Terdapat pula 1 button yang bertuliskan "Proses" yang kegunaannya untuk memproses masukkan yang telah diisi dari plainteks dan juga kunci. Adapun tampilan 1 program menu enkrispsi adalah sebagai berikut :



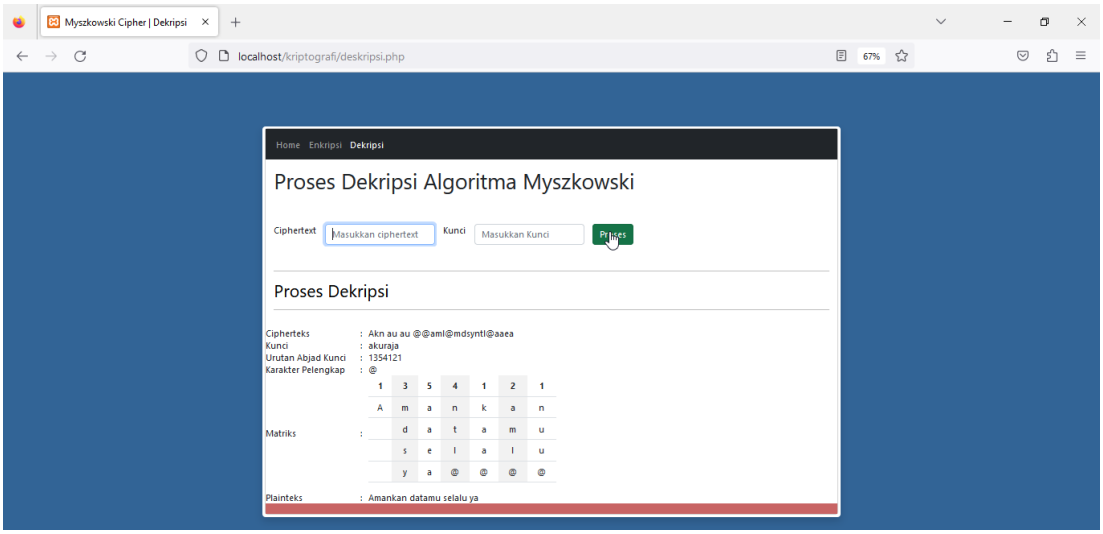
Gambr 3. 10 Tampilan 1 Program Menu Deskripsi

Pada tampilan 2 program menu deskripsi hampir sama dengan tampilan 1 program menu deskrispi. Perbedaan antara keduanya adalah terdapat informasi pada kedua textbox. Pada tampilan 2 program menu deskripsi informasi yang ditampilakan ditextbox adalah contoh kasus masukkan cipherteks dan kunci. Adapun tampilan 2 program menu deskripsi adalah sebagai berikut :



Gambr 3. 11 Tampilan 2 Program Menu Deskripsi

Pada tampilan 3 program menu home terdapat 3 menu pada menubar yaitu menu home, menu enkripsi dan menu deskripsi. Terdapat pula teks yang menampilkan tulisan “Deskripsi Myszkowski Cipher”. Pada tampilan program ini pula terdapat 2 textbox yaitu textbox plainteks dan texbox kunci. Disetiap textbox terdapat tulisan yang berisi informasi masukan seperti apa yang dianjurkan pada texbox masing-masing. Terdapat pula 1 button yang bertuliskan “Proses” yang kegunaannya untuk memproses masukkan yang telah diisi dari cipherteks dan juga kunci. Kemudian, pada tampilan 3 menu deskripsi ini terdapat tulisan teks yang bertuliskan “Proses Deskripsi”. Dibawah tulisan tersebut terdapat tampilan penjelasan singkat mengenai tahapan proses deskripsi mulai dari informasi cipherteks, kunci, urutan abjad kunci, karakter pelengkap, matriks serta informasi plaints yang dihasilkan pada proses deskripsi. Adapun tampilan 1 program menu deskripsi adalah sebagai berikut :



Gambr 3. 12 Tampilan 3 Program Menu Deskrispsi

BAB IV
PENUTUP

4.1 Kesimpulan

Berdasarkan dari hasil dan pembahasan pada penelitian ini, maka dapat disimpulkan bahwa :

1. Algoritma Myszkowski dapat mengaman pesan teks. Pengamanan dilakukan dengan cara mengacak pesan teks secara vertikal sesuai dengan urutan nomor karakter kunci yang ada di matriks. Pengacakan dapat terjadi secara horizontal apabila terdapat karakter kunci yang sama.
2. Pada penelitian ini, sudah dirancang dan dibangun sistem pengamanan pesan teks berbasis web.

4.2 Saran

Adapun saran yang penulis buat untuk penyempurnaan pada penelitian berikutnya adalah sebagai berikut :

1. Sistem ini masih menggunakan plainteks yang berkarater abjad, spasi dan angka. Diharapkan kedepan penelitian kedepannya dapat menggunakan karakter ASCII.
2. Sistem ini masih menggunakan 1 karakter tambahan, sehingga kedepannya agar menambahkan lebih dari 1 karakter tambahan.

DAFTAR PUSTAKA

Abdulloh, R. 2018. "7 IN 1 Pemrograman Web Untuk Pemula". Jakarta: Elex Media Komputindo.

Adhar, D. 2014. "Pengamanan Sqlite Database Menggunakan Kriptografi Elgamal". *Snif* 1, no.1: 432–37.

Danuputri, C, Santosa, N, dan Samuel, F D. 2022 "Pengujian Pengembangan Terhadap Algoritma Vigener Key Kriptografi" .*Jurnal Resistor* 5. no.1: 26-37.

Elgamar .2020. "Buku Ajar Konsep Dasar Pemrograman Website Dengan PHP". Penerbit: CV. Multimedia Edukasi

Fadel, A, Mardayulis, M, Yunita, P. 2018. "Aplikasi Sistem Pakar Pusat Informasi Konseling Remaja (Pik-R) Di Sman 2 Dumai Dengan Metode Backward Chaining Menggunakan Bahasa Pemograman Php". Jurnal Informatika, Manajemen dan Komputer 10, no. 2: 47-55.

Fitri, R. 2020. "Pemrograman Basis Data Menggunakan MySQL". Deepublish.

Ginting, A, Isnanto, R R dan Windasari, I P. 2015. "Implementasi Algoritma Kriptografi RSA Untuk Enkripsi Dan Dekripsi Email". *Jurnal Teknologi Dan Sistem Komputer* 3, no. 2 : 253.

Hardi, S M, Rachmawati, D, Chairinnisa, F, Jaya, I, Tarigan, J T. 2019. "Combination of myszkowski transposition algorithm and modified least significant bit (mlsb) green channel on png image security". *IOP Conf. Series : Journal of Physics: Conf. Series 1235* : 1-7.

Hayaty. N. 2020 "Buku Ajar: Sistem Keamanan". *Teknik Informatika UMRAH*

Ikhwan, A, Nofriansyah, D, dan Sriani. 2015. "Penerapan Data Mining dengan Algoritma Fp-Growth untuk Mendukung Strategi Promosi Pendidikan (Studi Kasus Kampus STMIK Triguna Dharma)". *Saintikom* 14, no. 3: 211–226

Indra, R A, dan Pramusinto, W. 2018. "Aplikasi Email (Electronic Mail) Menggunakan Algoritma Advanced Encryption Standard(AES-128) dan Algoritma Rivest Cipher 4 (RC4) Berbasis Web". *SKANIKA* 1, no. 2: 704–710.

Irawan, M D, dan Nasution, M K I. 2018. "Rancang Bangun Sistem Pakar Mendiagnosa Penyakit Tanaman Kelapa Sawit Menggunakan Metode Bayes Berbasis Android (Studi Kasus : Perkebunan PTPN 4 Air Batu)". *Jurnal Teknologi Informasi*. 2. no. 1: 15.

Jamaluddin, dkk. 2022. "KRIPTOGRAFI Teknik Keamanan Data, ed. by Adbul Karim and Janner Simarmata" Cetakan Pertama : Penerbit Yayassan Kita Menulis.

Khairina, N, Harahap, M K. 2019. "Modifikasin Myszkowski Transposition Cipher dengan Chess Board Pattern". *Seminar Nasional Teknologi Informatikan (Semantika)* 2, no. 1: 28-34.

Kinaswara, T A. 2019. "Rancang Bangun Aplikasi Inventaris Berbasis Website Pada Kelurahan Bantengan".*Seminar Nasional Teknologi Informasi dan Komunikasi* 2, no. 1: 71-75.

Kusumaningtyas, J A. 2018. "Analisa Algoritma Cipher Trnasposition : Study Literature". *Multimatrix* 1, no. 1: 1-12.

Limbong, T, dan Sriadhi. 2021. "Pemrograman Web Dasar". Yayasan Kita Menulis.

Muthohir, M. 2021. "Mudah Mmbuat Web Bagi Pemula (Pemrograman Web I)".

Semarang : Yayasan Prima Agus Teknik.
Muzakir, A. 2014. "Prototype Model Keamanan Data Menggunakan Kriptografi Data Encryption Standar (Des) Dengan Mode Operasi Chiper Transposisi". *Seminar Nasional Inovasi Dan Tren (SNIT) 2014*: 1–4.
Nugroho, A. 2011. "Perancangan dan Implementasi Sistem Basis Data". Andi.
Pamungkas, C A. 2017. Dasar Pemrograman Web dengan PHP. Yogyakarta: Deepublish.
Permana, A A. 2018. "Penerapan Kriptografi Pada Teks Pesan Dengan Menggunakan Metode Vigenere Cipher Berbasis Android". *JURNAL Al-AZHAR INDONESIA SERI SAINS DAN TEKNOLOGI* 4, no. 3: 110.
Rohmanu, A. 2017. "Metode Algoritma Des Dan Metode End Of File", *Jurnal Informatika*, 2, no. 1: 1–11.
Sabarudin, R, dan Jayanti, W E. 2019. "Jago Ngoding Pemrograman web dengan PHP untuk Pemula". CV. Surabaya : Kanaka Media.
Salamah, I, Fadhli, M, Sriwijaya, P N, dan Quality, I. 2020. "Evaluasi Pengukuran Website Learning Management System Polsri Dengan Metode Webqual 4.0". *Jurnal Digit* 10, no.1: 1–10.
Saputra, M H K, dan Aprilian, L V. 2020. "Belajar Cepat Metode SAW". Bandung: Kreatif Industri Nusantara.
Sasongko, J. 2005 'Pengamanan Data Informasi Menggunakan Kriptografi Klasik', *Jurnal Teknologi Informasi Dinamik* X, no.3: 160–67.
Scheneier, Bruce. 2016.Applied Cryptography 2nd ed. Buku. Illinois, USA.
Simatupang, L D, Khairil. 2022. "Pengamanan Dokumen Teks Dengan Menerapkan Algortima Kriptografi Klasik". *Jurnal Teknik Informastik Unik St. Thomas (JTIUST)* 07, no. 1: 133-140.
Supono, dan Putratama, V. 2018. "Pemogramam Web dengan Menggunakan PHP dan Framework Codeigniter". Deepublish.
Syarifuddin, M H, dan Sumbawati, M S. 2016. "Pengembangan E-Komik Sebagai Media Pembelajaran Keamanan Jaringan Materi Kkriptografi". *Jurnal IT-Edu* 1, no. 1: 30-36.
Tulloh, A R, Permanasari, Y, dan Harahap, E. 2016. "Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen". *Jurnal Matematika UNISBA* 2, no.1: 118–25.
Yusfrizal. 2019. "Rancang Bangun Aplikasi Kriptografi Pada Teks Menggunakan Metode Reverse Chiper Dan Rsa Berbasis Android". *Jurnal Teknik Informatika Kaputama (JTIK)* 3, no. 2: 29–37.