WEB EDUKASI KRIPTOGRAFI KLASIK

TUGAS AKHIR

Diajukan Sebagai Salah Satu Syarat

Untuk Memperoleh Gelar Sarjana

Jurusan Teknik Informatika

Disusun oleh :

Nama : Gusri Hermawan

No. Mahasiswa : 09523323

JURUSAN TEKNIK INFORMATIKA

FAKULTAS TEKNOLOGI INDUSTRI

UNIVERSITAS ISLAM INDONESIA

2016

LEMBAR PENGESAHAN

WEB EDUKASI KRIPTOGRAFI KLASIK

TUGAS AKHIR

DISUSUN OLEH :

Nama : Gusri Hermawan

No. Mahasiswa : 09523323

Yogyakarta, 27 Agustus 2016

Pembimbing Tunggal

(Ahmad Luthfi, S. Kom, M.Kom.)

LEMBAR PENGESAHAN PENGUJI

WEB EDUKASI KRIPTOGRAFI KLASIK

Disusun oleh :

Nama : **Gusri Hermawan**

No. Mahasiswa : **09523323**

Telah Dipertahankan di Depan Sidang Penguji Sebagai Salah Satu Syarat Untuk Memperoleh Gelar Sarjana Jurusan Teknik Informatika

Yogyakarta, 27 Agustus 2016

Tim Penguji

Ahmad Luthfi, S.Kom.,M.Kom.

Ketua

Beni Suranto, S.T.,M.SoftEng.

Anggota 1

Taufiq Hidayat, ST.,MCS.

Anggota 2

Mengetahui

Ketua Jurusan Teknik Informatika

Fakultas Teknologi Industri

Universitas Islam Indonesia

Hendrik, ST.,M.Eng.

LEMBAR PERNYATAAN KEASLIAN

HASIL TUGAS AKHIR

Saya yang bertanda tangan dibawah ini:

Nama : Gusri Hermawan

No. Mahasiswa : 09523323

Menyatakan seluruh komponen dan isi dalam laporan Tugas Akhir ini adalah hasil karya sendiri. Apabila dikemudian hari terbukti ada beberapa dari bagian Tugas Akhir ini adalah bukan dari hasil karya sendiri, maka saya siap menanggung resiko dan konsekuensi apapun.

Demikian pernyataan ini saya buat, semoga dapat dipergunakan sebagaimana mestinya.

Yogyakarta, 27 Agustus 2016

Gusri Hermawan

HALAMAN PERSEMBAHAN

Tugas Akhir Ini Kupersembahkan Untuk

Allah SWT

Karena telah memberikan saya kesempatan untuk menyelesaikan Tugas Akhir ini. Terima kasih atas scenario hidup yang Engkau rancang untukku begitu indah Terima kasih Engkau telah memberikan kekuatan hati, pikiran, raga . serta selalu menuntut langkahku pada saat mengerjakan Tugas Akhir ini.

Pembaca Tugas Akhir Saya

Setiap Ilmu akan sangat berguna jika diajarkan walaupun hanya sedikit.

HALAMAN MOTO

Belajar kemudian lakukan.

Belajar kemudian lakukan.

Belajar kemudian lakukan.

Jangan takut untuk gagal, orang yang bodoh adalah

orang yang takut gagal kemudian tidak pernah belajar.

HAPPY CODING☺

KATA PENGANTAR

Assalamu'alaikum Warohmatullahi Wabarokatuh.

Alhamdulillah segala puji dan syukur penulis panjatkan kehadirat Allah SWT yang telah melimpahkan rahmat, serta hidayah-Nya, sehingga Tugas Akhir dengan judul "Web Edukasi Kriptografi" ini dapat terselesaikan dengan baik dan lancar.

Tugas akhir ini merupakan penerapan ilmu yang diperoleh dari proses belajar dan disusun untuk melengkapi salah satu syarat memperoleh gelar Sarjana Jurusan Teknik Informatika di Universitas Islam Indonesia.

Dalam penyelesaian tugas akhir ini tidak terlepas dari bimbingan, dukungan dan bantuan dari berbagai pihak. Oleh karena itu, penulis menyampaikan ucapan terima kasih dan penghargaan yang setinggi – tingginya kepada :

1. Allah SWT yang senantiasa memberikan Rahmat dan Hidayah-Nya serta selalu memberikan kesehatan dan perlindungan.
2. Nabi Muhammad SAW yang telah memberikan petunjuk dan menjadi panutan bagi setiap umatnya.
3. Orang tua penulis (Ayah dan Ibu tercinta) terima kasih atas segala doa dan dukungan selama penulis menyelesaikan tugas akhir ini.
4. Bapak Dr. Ir. Harsoyo, M.Sc. selaku Rektor Universitas Islam Indonesia.
5. Bapak Dr. Drs. Imam Djati Widodo, M.Eng.Sc. selaku Dekan Fakultas Teknologi Industri Universitas Islam Indonesia.
6. Bapak Hendrik, ST.,M.Eng. selaku ketua jurusan Fakultas Teknologi Industri Universitas Islam Indonesia.
7. Bapak Ahmad Luthfi, S.Kom., M.kom. selaku pembimbing dalam penyelesaian tugas akhir ini.
8. Adik dan Abang saya yang selalu memberikan keceriaan dan memberikan semangat kepada penulis.

9. Serta semua pihak yang tidak bisa disebutkan satu persatu dalam tugas akhir ini.

Menyadari bahwa dalam pembuatan laporan Tugas Akhir ini banyak sekali kekurangan dan kesalahan, untuk itu permohonan maaf yang sebesar-besarya. Diharapkan kritik dan saran yang membangun untuk penyempurnaan di masa mendatang.

Akhir semoga laporan ini berguna bagi kita semua, Amin.

Wassalaamu'alaikum Wr. Wb.

Yogyakarta, 27 Agustus 2016

Gusri Hermawan

SARI

Kriptografi merupakan ilmu yang mempelajari teknik - teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data. Dengan perkembangan teknologi yang sangat maju seperti sekarang ini keamanan bertransaksi informasi sangatlah dibutuhkan. Peran Kriptografi sangat penting bagi keamanan sebuah informasi karena dapat menyembunyikan atau menyamarkan sebuah pesan agar informasi tersebut tidak dapat dibaca oleh orang yang tidak memiliki hak untuk membaca, karena kriptografi memiliki metode atau algoritma atau cipher yang sangat beragam yang dapat menjamin sebuah keamanan informasi. Penelitian ini dilakukan dengan tahapan-tahapan studi literatur, perancangan, implementasi algoritma dan pembangunan web edukasi ini. Adapun beberapa pengujian yang dilakukan adalah melakukan pengujian terhadap algoritma-algoritma yang di implemetasikan di web ini, pengujian terhadap proses enkripsi dan deskripsi, apakah berjalan dengan baik atau tidak. Adapun hasil dari penelitian ini adalah terbangunnya sebuah web edukasi yang dapat memberikan informasi tentang kriptografi dan metode-metodenya.

Kata Kunci: plaintext, ciphertext, enkripsi, dekripsi, cipher, kriptografi

TAKARIR

Plaintext	Teks yang belum dienkripsi
Chipertext	Teks yang telah dienkripsi
Userfriendly	Mudah dipahami
Use case	Diagram perilaku
Key	Kunci yang digunakan algoritma-algoritma kriptografi
Activity	Diagram aktifitas
Paper	Makalah atau jurnal
Syntax	Aturan penulisan kode
Sublime	Software yang digunakan dalam membangun WEB
Database	Kumpulan data secara sistematis pada komputer
Server	Sistem computer yang menyediakan layanan
User	Pengguna

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Kriptografi merupakan ilmu yang mempelajari teknik - teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data. Kriptografi pada dasarnya memiliki empat komponen utama, yaitu *plaintext* (pesan yang dapat dibaca), *ciphertext* (pesan acak yang tidak dapat dibaca), Algorithm (metode untuk melakukan enkripsi dan dekripsi). Kemudian dalam kriptografi ada 2 proses utama, yaitu Enkripsi dan Dekripsi. Enkripsi adalah sebuah proses menjadikan pesan yang dapat dibaca (*plaintext*) menjadi pesan acak yang tidak dapat dibaca (*ciphertext*). Dan Deskripsi adalah kebalikan dari proses enkripsi dimana proses ini akan mengubah *ciphertext* menjadi *plaintext* dengan menggunakan algoritma pembalik dan key yang sama.

Salah satu bidang matematika pada ilmu teknologi informasi adalah ilmu kriptologi. Untuk dapat mempelajari dan memahami bidang itu, dibutuhkan ketelitian dan konsentrasi yang lebih. Salah satu masalah yang di hadapi adalah ketika mempelajari dan memahami bidang ini kemungkinan untuk melakukan kesalahan sangatlah tinggi dan membuthkan waktu yang cukup lama. Ketika mengubah *plaintext* ke *ciphertext* ataupun sebealiknya masalah yang dihadapi adalah jika *plaintext* yang di cipher hanya sedikit atau beberapa kata mungkin cukup mudah dan dapat dikerjakan dengan cepat dan dengan tingkat kesalahan yang kecil, tetapi ketika kami harus mengubah sebuah paragraf *plaintext* ke *ciphertext*, pengerjaan akan menjadi sangat sulit dan membutuhkan waktu yang sangat lama dan dengan tingkat kesalahan yang lebih besar lagi, karena kami harus mengubah *plaintext* tersebut huruf demi huruf atau karakter demi karakter.

Seiring dengan perkembangan teknologi, mencari atau bertukar informasi menjadi sangat mudah untuk dilakukan semua orang, cukup dengan menggunakan *phone* atau *smartphone* (telepon genggam), komputer, laptop atau gadget kita dapat bertukar informasi dengan sangat mudah dimanapun dan kapanpun kita inginkan. Dengan mudahnya berkomunikasi atau saling bertukar informasi, kerahaasian sebuah informasi menjadi sebuah kebutuhan/keharusan dan sangatlah penting. Untuk mengatasi kerahasiaan sebuah informasi, kriptografi adalah solusi yang tepat, karena kriptografi dapat menyamarkan sebuah informasi yang dapat dibaca (*plaintext*) menjadi tidak dapat dibaca (*ciphertext*).

Untuk mengatasi masalah yang ada, perlu dicarikan sebuah solusi, yaitu dengan membuat sebuah Web Edukasi Kriptografi Klasik yang di dalamnya tidak hanya menjelaskan kriptografi dan metode - metodenya saja tetapi juga memberikan alur atau proses bagaimana terjadinya perubahan dari *plaintext* ke *ciphertext* maupun sebaliknya.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang ada, maka didapatkan rumusan masalah sebagai berikut :

1. Bagaimana Web Edukasi Kriptografi Klasik ini harus dapat mengubah sebuah *plaintext* ke *ciphertext* maupun sebaliknya dan juga dapat menampilkan alur atau prosesnya.
2. Bagaimana Web Edukasi Kriptografi Klasik ini akan memberikan beberapa metode cipher, yaitu : Monophabetic Caesar Cipher, Keyword Cipher, Transposisi Cipher, dan Vigenere Cipher.

1.3 Batasan Masalah

1. Web Edukasi Kriptografi ini tidak dapat login untuk pengguna lain selain admin

2. Perancang Web Edukasi Kriptografi ini hanya memberikan informasi seperti penjelasan tentang kriptografi dan metode - metodenya dan implementasi untuk mengubah *plaintext* ke *ciphertext* atau sebaliknya.
3. Untuk Transposisi Cipher harus memasukan matrixnya secara manual, contoh 5x5.

1.4 Tujuan Penelitian

Adapun tujuan yang akan dicapai dalam pelaksanaan tugas akhir ini :

1. Membuat sebuah Web Edukasi Kriptografi Klasik.
2. Memberikan informasi kriptografi dan metode - metodenya.
3. Memberikan alur atau proses perubahan dari *plaintext* ke *ciphertext* maupun sbaliknya.

1.5 Manfaat Penelitian

Adapun manfaat penelitian ini adalah :

1. Web yang dibangun dapat mempermudah dalam proses belajar kriptografi.
2. Menerapkan dan memperluas wawasan teori dan pengetahuan kriptografi klasik kepada penulis.

1.6 Metode Penelitian

Dalam tugas akhir ini, tahapan - tahapan uang akan dilalui diantaranya :

1. Studi literatur.

   Membaca sumber pustaka untuk mendalami atau memahami konsep - konsep yang mendukung pembangunan web edukasi ini.

2. Perancangan.

Melalukan perancangan pembuatan web yang akan memberikan informasi metode - metode kriptografi.

3. Implementasi metode kriptografi.

   Melakukan implementasi metode - metode kriptografi di web ini untuk mengubah *plaintext* ke *ciphertext* atau sebaliknya

4. Kesimpulan dan Saran.

   Membuat kesimpulan dari seluruh tahapan yang telah dilalui.

1.7 Sistematika Penulisan

Laporan Tugas akhir ini disusun secara sistematis dalam bentuk bab, sebagai berikut :

BAB I : PENDAHULUAN

Bab ini terdiri dari Latar Belakang, Rumusan Masalah, Batasan Masalah, Tujuan Penelitian, Manfaat Penelitian, Metode Penelitian, dan Sistematika Penulisan tugas akhir.

BAB II : LANDASAN TEORI

Bab ini berisi landasan teori yang akan digunakan dalam melakukan analisis, perancangan, dan implementasi tugas akhir yang dilakukan pada bab - bab selanjutnya. Meliputi teori dan basik kriptografi.

BAB III : METODOLOGI DAN PERANCANGAN

Bab ini berisi analisis terhadap penggunaan metode - metode kriptografi sehingga dapat membantu dalam melakukan perancangan dan implementasi.

BAB IV : IMPLEMENTASI HASIL DAN ANALISIS

Bab ini membahas tentang implementasi sebuah metode - metode kriptografi yang mengubah sebuah *plaintext* ke *ciphertext* sesuai dengan metode yang ada di rumusan masalah.

BAB V : KESIMPULAN DAN SARAN

Membuat kesimpulan - kesimpulan dari hasil penelitian dan saran – saran yang harus diperhatikan dari keterbatasan yang ditemukan dalam penelitian. Hali ini diharapkan akan berguna ketika ada penelitian lain yang akan mengankat topic yang sama.

BAB II
LANDASAN TEORI

2.1 Kriptografi

Menurut Pabokory, Astuti, and Kridalaksana kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya.(Pabokory, Astuti, and Kridalaksana 2015).

Menurut Riyanarto and Iffano kriptografi adalah ilmu matematika yang berhubungan dengan transformasi data agar arti dari data tersebut menjadi sulit untuk dipahami (untuk menyembunyikan maknanya), mencegahnya dari perubahan tanpa izin, atau mencegahnya dari penggunaan yang tidak sah**.**(Riyanarto and Iffano 2012)**.**

Pada umumnya kriptografi itu adalah sebuah teknik dimana sebuah *plaintext* (teks yang dapat dibaca) diubah menjadi *ciphertext* (teks yang tidak dapat dibaca), dengan tujuan agar sebuah informasi tidak dapat dibaca atau dilihat oleh orang-orang yang tidak memiliki hak untuk membacanya atau melihat isi dari informasi tersebut.

Pada umumnya algoritma kriptografi terbagi 2, yaitu :

1. Algoritma Simetri (konvensional)
2. Algoritma Asimetri (kunci public)

Menurut Fairuzabadi Kriptografi sesungguhnya telah dikenal dan dipakai cukup lama sejak kurang lebih tahun 1900 sebelum masehi pada prasasti-prasasti kuburan. Kriptografi sendiri berasal dari kata “Crypto” yanng berarti rahasia dan “graphy” yang berarti tulisan. Jadi, dapat dikatakan kriptografi adalah

tulisan yang tersembunyi. Dengan adanya tulisan yang tersembunyi ini, orang-orang yang tidak mengetahui bagaimana tulisan tersebut disembunyikan tidak akan mengetahui bagaimana cara membaca maupun menerjemahkan tulisan tersebut.(Fairuzabadi 2010).

Perang Dunia Pertama (WWI) dimulai dengan keberhasilan Sekutu mengungkap pesan menteri luar negeri Jerman Arthur Zimmermann kepada kedutaan Jerman di Meksiko yang berisi perintah untuk menggerakkan kekuatan kapal selam Jerman. Pesan tersebut disandikan dengan menggunakan teknik subti-tusi kata dengan huruf. Code Book adalah buku berisi daftar kata dan angka yang menjadi ciphertext kata tersebut. Perkembangan kriptografi dan kripanalisis memuncak Perang Dunia Kedua (WWII), dimana semua pihak yang ber- perang mengembangkan teknik kriptografinya masing-masing. Diantaranya adalah Jerman dengan mesin sandi Enigma dan Jepang dengan Purple Cipher. Mesin sandi Enigma merupakan kunci kemenangan Jerman dalam perang, sehingga Sekutu berusaha memecahkan dan mengungkap sandi mesin tersebut untuk mengetahui langkah dan strategi militer Jerman dalam perang.(Tarigan 2014).

Pada dasarnya kriptografi memiliki elemen-elemen dasar, yaitu :

a. Enkripsi

   Enkripsi adalah hal yang sangat penting dalam kriptografi, merupakan pengamanan data agar terjaga kerahasiaannya. *Plaintext* diubah menjadi kode-kode *ciphertext*. Enkripsi juga dapat diartikan sebagai cipher atau kode. Untuk mengubah sebuah *plaintext* ke *ciphertext* kita memerlukan sebuah algoritma yang dapat mencipher sebuah data atau informasi yang kita inginkan.

b. Deskripsi

   Deskripsi adalah kebalikan dari enkripsi. Pesan atau *plaintext* yang telah dienkripsi dikembalikan kebentuk aslinya, disebut dengan deskripsi pesan.

Algoritma yang digunakan untuk deskripsi berbeda dengan algoritma yang digunakan untuk enkripsi.

c. Kunci atau Key

Kunci atau adalah kunci yang dipakai untuk melakukan enkripsi dan deskripsi.

d. Plaintext

Plaintext adalah pesan atau informasi yang dapat dibaca atau bentuk asli dari sebuah pesan

e. Ciphertext

Ciphertext adalah pesan atau informasi yang tidak dapat dibaca dengan mudah atau plaintext yang telah diubah dengan cipher tertentu.

Kriptografi sendiri terbagi menjadi dua jenis, kriptografi klasik dan kriptografi modern.

2.2 Kriptografi Klasik

Keamanan sebuah algoritma yang digunakan dalam enkripsi atau dekripsi bergantung kepada beberapa aspek. Salah satu aspek yang cukup penting adalah sifat algoritma yang digunakan. Apabila kekuatan dari sebuah algoritma sangat tergantung kepada pengetahuan (tahu atau tidaknya) orang terhadap algoritma yang digunakan, maka algoritma tersebut disebut “restricted algorithm”. Apabila algoritma tersebut bocor atau ketahuan oleh orang banyak, maka pesan-pesan dapat terbaca. Tentunya hal ini masih bergantung kepada adanya kriptografer yang baik. Jika tidak ada yang tahu, maka sistem tersebut dapat dianggap aman (meskipun semu).(Sasongko 2005)

Kriptografi memiliki sejarah yang sangat panjang, dan pada dasarnya teknik enkripsi kriptografi klasik terrbagi menjadi 2 algoritma, yaitu:

1. Metode Substitusi, yaitu metode enkripsi dengan mengganti tiap - tiap karakter pesan dengan kunci tertentu, dan metode substitusi dibagi menjadi 2, yaitu :

   - *Monoalphabetic*, yaitu setiap karakter pesan disubstitusi oleh satu karakter kunci. Contoh *Caesar Cipher.*

   - *Polyalphabetic*, yaitu setiap karakter pesan disubstitusi oleh beberapa karakter kunci dengan pola tertentu. Contoh *Viginere Cipher.*

2. Metode transposisi, yaitu metode enkripsi dengan memindahkan posisi tiap - tiap karakter pesan dengan pola tertentu.Contohnya adalah *Blocking Cipher* dan *Permutation*.

2.2.1 Metode Substitusi

A. Monoalphabetic Caesar Cipher

Metode *Caesar Cipher* adalah salah satu cipher yang sangat sederhana, dan cara pemakaian metode ini adalah dengan menggeserkan atau mengganti *plaintext* yang ada sesuai dengan key dan alphabet yang ada, contoh :

Plaintext : NAMA SAYA GUSRI HERMAWAN

Key : 3

Ciphertext : QDPD VDBD JXVUL KHUPDZDQ

Proses pengenkripsian pada contoh diatas adalah menggeser tiap huruf yang ada di *plaintext* sebanyak 3 karakter yang ada di alphabet. Seperti karakter pertama, yaitu **N**, lalu huruf N digeser 3 huruf setelahnya menjadi huruf **Q** (N,O,P,Q, dan Q adalah huruf ketiga setelah N), dan huruf lain menjadi :

N + 3 = Q A + 3 = D M + 3 = P S + 3 = V

Y + 3 = B G + 3 = J U + 3 = X R + 3 = U

I + 3 = L H + 3 = K E + 3 = H W + 3 = Z

Dan untuk proses secara matematisnya dapat menggukan operasi modulus. Untuk

Enkripsi : E (P) = (P + K) mod 26

Deskripsi : D (C) = (C - K) mod 26

Dengan keterangan sebagai berikut, D (deskripsi) E (enkripsi), P (plaintext yang ingin di ubah), C (ciphertext hasil dari (P + K) mod 26), dan K (key). Mod 26 (jumlah karakter dalam alphabet ada 26 huruf). Untuk contoh diatas maka dapat dijelaskan sebagai berikut.

N = 14, Enkripsi = (14 + 3) mod 26 = 17, 17 = Q

A = 1, Enkripsi = (1 + 3) mod 26 = 4, 4 = D

M = 13, Enkripsi = (13 + 3) mod 26 = 16, 16 = P

S = 19, Enkripsi = (19 + 3) mod 26 = 22, 22 = V

Y = 25, Enkripsi = (25 + 3) mod 26 = 2, 2 = B

G = 7, Enkripsi = (7 + 3) mod 26 = 10, 10 = J

U = 21, Enkripsi = (21 + 3) mod 26 = 24, 24 = X

R = 18, Enkripsi = (18 + 3) mod 26 = 21, 21 = U

I = 9, Enkripsi = (9 + 3) mod 26 = 12, 12 = L

H = 8, Enkripsi = (8 + 3) mod 26 = 11, 11 = K

E = 5, Enkripsi = (5 + 3) mod 26 = 8, 8 = H

W = 23, Enkripsi = (23 + 3) mod 26 = 0, 0 = Z (karena Z = 26 atau 0)

Tentara romawi kuno menggunakan perangkat roda atau *wheel device* sebagai alat bantu untuk menengkripsi atau mendeskripsi sebuah text.

Gambar 2.1 Gambar *whell device*

Salah satu pengembangan dari *Caesar cipher* adalah ROT13. Pada sistem ini sebuah huruf digantikan dengan huruf yang letaknya 13 posisi darinya. Sebagai contoh,huruf "A" digantikan dengan huruf "N", huruf "B" digantikan dengan huruf "O",dan seterusnya. Secara matematis, hal ini dapat dituliskan sebagai: *C = ROT13 (M).* Dasar keilmuan dari *Caesar cipher* sebagian besar adalah matematika yang antara lain mencakup teori bilangan, aljabar dan fungsi. Subbab matematika tersebut sudah diajarkan sejak pendidikan sekolah bahkan diperluas lagi di perguruan tinggi. (Seftyanto and Haryanto 2012)

B. Keyword Cipher

Metode *monoalphabetic* ini berbeda dengan *Caesar Cipher* karena proses enkripsinya bukan menggeserkan huruf yang ada sesuai dengan key yang ditentukan, tetapi mengganti karakter yang ada sesuai dengan key, contoh :

Plaintext : NAMA SAYA GUSRI HERMAWAN

Key : SANGAT SEMANGAT

Ciphertext : JSIS QSYS MUQPC BTPISWSJ

Proses pengenkripsian diatas dapat dijelaskan sebagai berikut :

1. Ubahlah key terlebih dahulu dengan cara membuang semua duplikasi huruf dan sambung dengan huruf yang belum ada, sehingga menjadi susunan algabet yang baru, SANGTEMBCDFHIJKLOPQRUVWXYZ
2. Buat table alphabet dan letak key yang telah di ubah dibawahnya, seperti berikut :

Tabel 2.1 Tabel alphabet acak yang baru

Alfabet																									
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Key																									
S	A	N	G	T	E	M	B	C	D	F	H	I	J	K	L	O	P	Q	R	U	V	W	X	Y	Z

3. Lalu cocokan tiap huruf *plaintext* dengan table alfabet dan masukan huruf yang ada di table key, seperti berikut :

   Ubahlah huruf demi huruf yang ada di plaintext, dengan memasukan huruf di plaintext ke dalam tabel alphabet, setelah plaintext dimasukan ke dalam table alfabet lalu dicocokan dengan huruf yang ada di table key, harus berada di kolom yang sama, sehingga menjadi :

   N menjadi J A menjadi S M menjadi I A menjadi S

S menjadi Q A menjadi S Y menjadi Y A menjadi S

G menjadi M U menjadi U S menjadi Q R menjadi P

I menjadi C H menjadi B E menjadi T R menjadi P

M menjadi I A menjadi S W menjadi W A menjadi S

N menjadi J

C. Vigenere cipher

Menurut Sasongko *vigenere* Termasuk ke dalam *cipher* abjadmajemuk (*polyalpabetic substitution cipher*). Ditemukan oleh diplomat (sekaligus seorang kriptologis) Perancis, Blaise de Vigènere pada abad 16. Sudah berhasil dipecahkan pada Abad 19. *Vigènere Cipher* menggunakan Bujursangkar *Vigènere* untuk melakukan enkripsi. Setiap baris di dalam bujursangkar menyatakan huruf-huruf cipherteks yang diperoleh dengan *Caesar Cipher*. Jika panjang kunci lebih pendek daripada panjang plainteks, maka kunci diulang secara periodik. Bila panjang kunci adalah *m*, maka periodenya dikatakan *m*.(Sasongko, 2005)

Vigenere Cipher pada dasarnya cukup rumit untuk dipecahkan, tetapi *Vigenere Cipher* tetap memiliki kelemahan, salah satunya adalah dapat diketahui panjang kuncinya dengan menggunakan metode Kasiski. Untuk rumus matematis *Vigenere Cipher* adalah

Enkripsi : C = (P + K) mod 26 atau mod n (untuk *Vigenere Cipher* dengan jumlah karakter n)

Deskripsi : P = (C - K) mod 26 atau mod n

Dengan penjelasan C adalah *ciphertext*, P adalah *plaintext*, K adalah key, dan mod 26 adalah jumlah huruf dalam alabet. Atau kita dapat menggunakan table bujursangkar *Vigenere* untuk mengenkripsi maupun mendeskripsi.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
W	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Gambar 2.2 Gambar table bujursangkar viginere

Contoh untuk *Viginere Cipher*, sebagai berikut :

Plaintext : NAMA SAYA GUSRI HERMAWAN

Key : SANGAT SEMANGAT

Ciphertext : FAZG STQE SUFXI AWRZGWTF

Proses pengenkripsiannya hampir mirip dengan *monoalphabetic*, dan prosesnya adalah sebagai berikut :

1. Samakan jumlah key dengan *plaintext.* Jika tidak sama, maka tambahlah hurufnya dengan cara menambah hingga jumlah karakter key dan jumlah karakter plaintext menjadi sama, contoh key ‘nama’ dan plaintext ‘namasay’, maka key akan ditambahkan dengan dirinya sendiri dimulai dari huruf pertama, menjadi ‘namanam’.

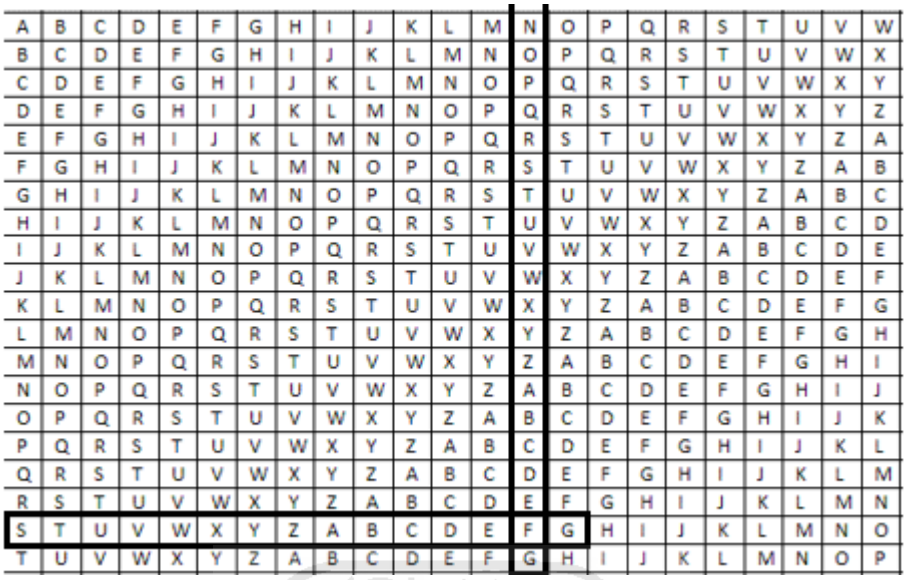
Tabel 2.2 Tabel *Viginere*

Plaintext																			
N	A	M	A	S	A	Y	A	G	U	S	R	I	H	E	R	M	A	W	A	N
Key																			
S	A	N	G	A	T	S	E	M	A	N	G	A	T	S	A	N	G	A	T	S

Perbedaan antara *monoalphabetic* dengan *viginere* adalah pada keynya. Di *monoalphabetic* duplikasi huruf pada key di buang lalu masukan huruf yang belum ada. Sedangkan di *Viginere Cipher* tidak huruf yang dibuang, tetapi mengulang – ulang key sebanyak jumlah karakter atau huru yang ada pada *plaintext*. Seperti yang dapat kita lihat pada table *viginere* diatas, jumlah plaintext ada 21 karakter sedangkan key ada 14 karakter, jadi kita harus menyamakan jumlah karakter key dan plaintext, sehingga menjadi SANGATSEMANGATSANGATS yang berjumlah 21 karakter.

2. Cocokan karakter/huruf yang ada di tabel plaintext dengan karakter/huruf yang ada di tabel key dan cari koordinat karakter/hurufnya di table bujursangkar *viginere*, maka akan didapatkan ciphertext sebagai berikut :

N bertemu S = F	A bertemu A = A	M bertemu N = Z
A bertemu G = G	S bertemu A = S	A bertemu T = T
Y bertemu S = Q	A bertemu E = E	G bertemu M = S
U bertemu A = U	S bertemu N = F	R bertemu G = X
I bertemu A = I	H bertemu T = A	E bertemu S = W
R bertemu A = R	M bertemu N = Z	A bertemu G = H
W bertemu A =W	A bertemu T = T	N bertemu S = F



Gambar 2.3 Gambar pertemuan N dan S

Seperti gambar 2.3 diatas, maka karakter/huruf yang lain akan diubah menjadi seperti ini :

Table 2.3 Tabel *ciphertext*

Plaintext																				
N	A	M	A	S	A	Y	A	G	U	S	R	I	H	E	R	M	A	W	A	N
Key																				
S	A	N	G	A	T	S	E	M	A	N	G	A	T	S	A	N	G	A	T	S
Ciphertext																				
F	A	Z	G	S	T	Q	E	S	U	F	X	I	A	W	R	Z	G	W	T	F

Atau juga dapat dimasukan dalam rumus matematis seperti yang telah dijelaskan dan urutan huruf dimulai dari **A = 0** sampai dengan **Z = 25**, sehingga menjadi :

N = 13 dan S = 18, Enkripsi = (13 + 18) mod 26 = 5, 5 = F

A = 0 dan A = 0, Enkripsi = (0 + 0) mod 26 = 0, 0 = A

M = 12 dan N = 13, Enkripsi = (12 + 13) mod 26 = 25, 25 = Z

A = 0 dan G = 6,	Enkripsi = (0 + 6) mod 26 = 6,	6 = G
S = 18 dan A = 0,	Enkripsi = (18 + 0) mod 26 = 18,	18 = S
A = 0 dan T = 19,	Enkripsi = (0 + 19) mod 26 = 19,	19 = T
Y = 24 dan S = 18,	Enkripsi = (24 + 18) mod 26 = 16,	16 = Q
A = 0 dan E = 4,	Enkripsi = (0 + 4) mod 26 = 4,	4 = E
G = 6 dan M = 12,	Enkripsi = (6 + 12) mod 26 = 18,	18 = S
U = 20 dan A = 0,	Enkripsi = (20 + 0) mod 26 = 20,	20 = U
S = 18 dan N = 13,	Enkripsi = (18 + 13) mod 26 = 5,	5 = F
R = 17 dan G = 6,	Enkripsi = (17 + 6) mod 26 = 23,	23 = X
I = 8 dan A = 0,	Enkripsi = (8 + 0) mod 26 = 8,	8 = I
H = 7 dan T = 19,	Enkripsi = (7 + 19) mod 26 = 0,	0 = A
E = 4 dan S = 18,	Enkripsi = (4 + 18) mod 26 = 22,	23 = W
R = 17 dan A = 0,	Enkripsi = (17 + 0) mod 26 = 17,	17 = R
M = 12 dan N = 13,	Enkripsi = (12 + 13) mod 26 = 25,	25 = Z
A = 0 dan G = 6,	Enkripsi = (0 + 6) mod 26 = 6,	6 = G
W = 22 dan A = 0,	Enkripsi = (22 + 0) mod 26 = 22,	22 = W
A = 0 dan T = 19,	Enkripsi = (0 + 19) mod 26 = 19,	19 = T
N = 13 dan S = 18,	Enkripsi = (13 + 18) mod 26 = 5,	5 = F

2.2.2 Metode Transposisi

Pada teknik transposisi huruf-huruf pada plaintext dan chipertext tetap sama, tetapi urutannya diubah. Dengan kata lain, teknik ini melakukan transpose terhadap rangkaian karakter di dalam teks. Nama lain untuk metode ini adalah permutasi, karena transpose setiap karakter di dalam teks sama dengan mempermutasikan karakter-karakter tersebut. (Fairuzabadi, 2010)

Contoh metode transposisi adalah sebagai berikut :

Ciphertext : NASRNAYRMAMAIAMAGHWASUEAN

Dengan matrix 5x5 akan menjadi seperti ini

N	A	S	R	N
A	Y	R	M	&
M	A	I	A	&
A	G	H	W	&
S	U	E	A	&

Dengan matrix ini kita akan menemukan pola baca dari atas ke bawah, dan menghasilkan plaintext seperti berikut :

Plaintext : NAMASAYAGUSRIHERMAWANAMAN

Atau sebaliknya kita dapat menenkripsi sebuah plaintext, contoh :

Plaintext : NAMASAYAGUSRIHERMAWANAMAN

Dengan matrix 5x5 akan didapatkan ciphertext seperti ini

N	A	M	A	S

A	Y	A	G	U
S	R	I	H	E
R	M	A	W	A
N	&	&	&	&

Dengan matrix diatas kita dapat membacanya dari kiri ke kanan dan menghasilkan sebuah ciphertext seperti berikut :

Ciphertext : NASRNAYM&MAIA&AGHW&SUEA&

BAB III
METODOLOGI

3.1 Analisis Kebutuhan

Analisis kebutuhan adalah menganalisis kebutuhan apa saja yang diperlukan dalam pengoperasian web ini. Kebutuhan disini berupa data imputan, data proses dan data keluaran.

Web Edukasi Kriptografi ini digunakan untuk mengolah inputan data atau plaintext menjadi sebuah ciphertext maupun sebaliknya. Web ini akan memberikan 4 jenis cipher, yaitu : *Caesar Cipher*, *Monoalphabetic* dengan kalimat sebagai key, *Vigenere Cipher*, dan Transposisi.

3.1.1 Analisis Kebutuhan Input

Berikut data inputan yang akan diproses di dalam system :

a. Memasukan username
b. Memasukan password
c. Memasukan *plaintext* atau *ciphertext*
d. Memasukan key dan submit agar text berubah

3.1.2 Analisis Kebutuhan Proses

Kebutuhan proses dalam Web Edukasi Kriptografi ini adalah :

a. Proses login
b. Proses logout
c. Proses tambah
d. Proses edit

e. Proses hapus artikel
f. Proses enkripsi Caesar cipher
g. Proses enkripsi Keyword cipher
h. Proses enkripsi Vigenere cipher
i. Proses enkripsi Transposisi cipher
j. Proses deskripsi Caesar cipher
k. Proses deskripsi Vigenere cipher
l. Proses deskripsi Transposisi cipher

3.1.3 Analisis Kebutuhan Output

Output yang akan ditampilkan di web ini adalah berupa materi atau artikel untuk kriptografi dan setiap metode-metode yang dipakai di web ini. Setelah itu terdapat juga output untuk enkripsi sebuah *plaintext* menjadi *ciphertext* dan deskripsi sebuah *ciphertext* menjadi *plaintext*.

3.2 Rancangan Web

Web ini akan dibagi menjadi beberapa tahapan perancangan yang dibahas satu-persatu pada sub-bab dibawah.

3.2.1 Perancangan Web Edukasi Kriptografi

Dalam Web Edukasi Kriptografi ini terdapat beberapa menu yang ditampilkan, seperti Home yang berisi artikel atau materi tentang kriptografi klasik, Caesar Cipher yang berisi artikel atau materi tentang *Caesar Cipher* dan juga implementasinya, Keyword Cipher yang berisi artikel atau materi tentang *Keyword Cipher* dan juga implementasinya, Vigenere Cipher yang berisi artikel atau materi tentang *Vigenere Cipher* dan juga implementasinya, dan menu Transpose Cipher yang berisi artikel atau materi tentang metode transposisi *cipher* dan juga implementasinya. Berikut adalah rancangan tahapan Web ini :

1. Menu Caesar Cipher

Adapun tahapan yang dilakukan adalah sebagai berikut:

a. Buka Web Edukasi Kriptografi.
b. Pilih menu caesar cipher.
c. Dalam menu ini akan terdapat tombol artikel yang akan menampilkan artikel atau materi *Caesar Cipher*.
d. Dalam menu Caesar cipher ini juga akan terdapat Implementasi yang akan mengimplementasikan metode *Caesar Cipher* dan dapat menampilkan alur atau prosesnya.

Adapun tahapan untuk melakukan proses enkripsi dan deskripsi adalah sebagai berikut :

a. Buka menu Caesar Cipher.
b. Masukan key.
c. Masukan *plaintext*.
d. Pilih tombol encrypt untuk enkripsi dan descrypt untuk deskripsi
e. Pilih tombol Alurnya untuk melihat proses enkripsi maupun deskripsi

Contoh proses enkripsi , masukan key “2”, lalu *plaintext* “gusri” dan tekan tombol encrypt, akan menghasilkan *ciphertext* “esqpg”. Untuk proses deskripsi juga sama dengan proses enkripsi, hanya saja yang tombol yang ditekan bukan tombol encrypt melainkan tombol descrypt, contoh, masukan key “2”, lalu masukan *cihpertext* “esqpg”, lalu tekan tombol descrypt, maka akan menghasilkan *plaintext* “gusri” yang dapat dilihat di table result.

2. Menu Keyword Cipher

Adapun tahapan yang dilakukan adalah sebagai berikut:

a. Buka Web Edukasi Kriptografi.
b. Pilih menu Keyword Cipher.
c. Dalam menu ini akan terdapat tombol artikel yang akan menampilkan artikel atau materi *Keyword Cipher*.

d. Dalam menu Keyword Cipher ini juga akan terdapat Implementasi yang akan mengimplementasikan metode *Keyword Cipher* dan dapat menampilkan alur atau prosesnya.

Adapun tahapan untuk melakukan proses enkripsi dan deskripsi adalah sebagai berikut :

a. Buka menu Keyword Cipher.
b. Masukan key.
c. Masukan *plaintext*.
d. Tekan tombol encrypt untuk enkripsi dan descrypt untuk deskripsi
e. Pilih tombol Alurnya untuk melihat proses enkripsi maupun deskripsi

Contoh proses enkripsi , masukan key "nama", lalu *plaintext* "gusrihermawan" dan tekan tombol encrypt, akan menghasilkan *ciphertext* "eusrgfcrknwnl". Untuk proses deskripsi juga sama dengan proses enkripsi, hanya saja yang tombol yang ditekan bukan tombol encrypt melainkan tombol descrypt, contoh, masukan key "nama", lalu masukan *cihpertext* "eusrgfcrknwnl", lalu tekan tombol descrypt, maka akan menghasilkan *plaintext* "gusrihermawan" yang dapat dilihat di table result.

3. Menu Vigenere Cipher

Adapun tahapan yang dilakukan adalah sebagai berikut:

a. Buka Web Edukasi Kriptografi.
b. Pilih menu Vigenere Cipher.
c. Dalam menu ini akan terdapat tombol artikel yang akan menampilkan artikel atau materi *Vigenere Cipher*.
d. Dalam menu Vigenere Cipher ini juga akan terdapat Implementasi yang akan mengimplementasikan metode *Vigenere Cipher* dan dapat menampilkan alur atau prosesnya.

Adapun tahapan untuk melakukan proses enkripsi dan deskripsi adalah sebagai berikut :

a. Buka menu Vigenere Cipher.
b. Masukan key.
c. Masukan *plaintext*.
d. Pilih tombol encrypt untuk enkripsi dan descrypt untuk deskripsi
e. Pilih tombol Alurnya untuk melihat proses enkripsi maupun deskripsi

Contoh proses enkripsi , masukan key “nama”, lalu *plaintext* “gusrihermawan” dan tekan tombol encrypt, akan menghasilkan *ciphertext* “tuervhqrzaiaa”. Untuk proses deskripsi juga sama dengan proses enkripsi, hanya saja yang tombol yang ditekan bukan tombol encrypt melainkan tombol descrypt, contoh, masukan key “nama”, lalu masukan *cihpertext* “tuervhqrzaiaa”, lalu tekan tombol descrypt, maka akan menghasilkan *plaintext* “gusrihermawan” yang dapat dilihat di table result.

4. Menu Transpose Cipher

Adapun tahapan yang dilakukan adalah sebagai berikut:

a. Buka Web Edukasi Kriptografi.
b. Pilih menu Transpose Cipher.
c. Dalam menu ini akan terdapat tombol artikel yang akan menampilkan artikel atau materi *Transpose Cipher*.
d. Dalam menu Transpose Cipher ini juga akan terdapat Implementasi yang akan mengimplementasikan metode *Transpose Cipher* dan dapat menampilkan alur atau prosesnya.

Adapun tahapan untuk melakukan proses enkripsi dan deskripsi adalah sebagai berikut :

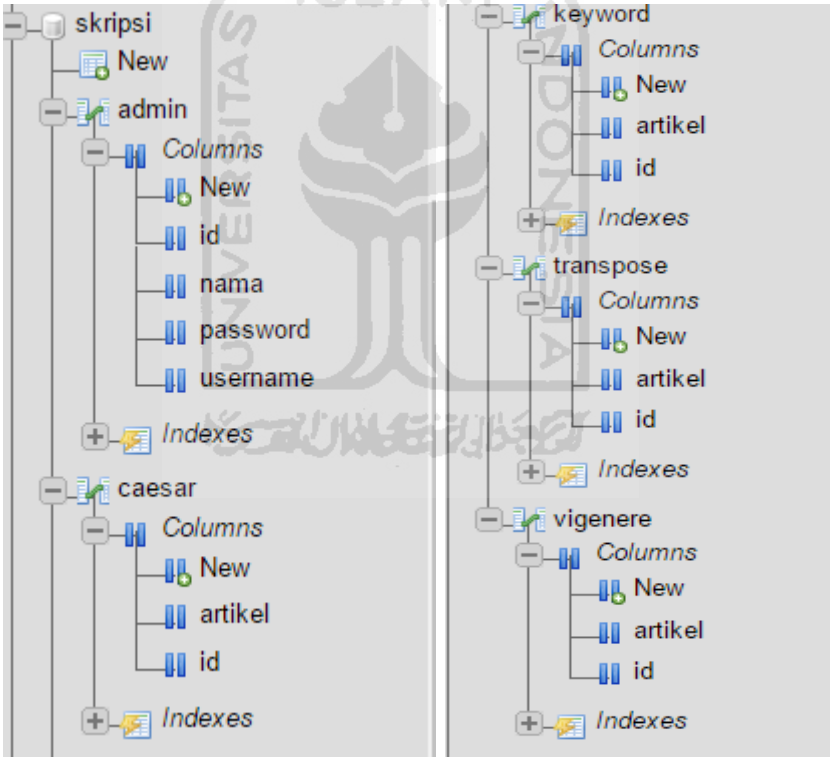
a. Buka menu Transpose Cipher.
b. Masukan key.
c. Masukan *plaintext*.
d. Tekan tombol encrypt untuk enkripsi

e. Pilih tombol Alurnya untuk melihat proses enkripsi maupun deskripsi

Contoh proses enkripsi , masukan key “3”, lalu *plaintext* “gusriherm” dan tekan tombol encrypt, akan menghasilkan *ciphertext* “greuirshm”. Untuk proses deskripsi juga sama dengan proses enkripsi contoh, masukan key “3”, lalu masukan *cihpertext* “greuirshm”, lalu tekan tombol encrypt, maka akan menghasilkan *plaintext* “gusriherm” yang dapat dilihat di table result.

3.2.2 Database

Data admin dan key maupun teks yang di input akan disimpan kedalam database skripsi dan berada di server lokal XAMPP yang dapat diakses di localhost/phpmyadmin.



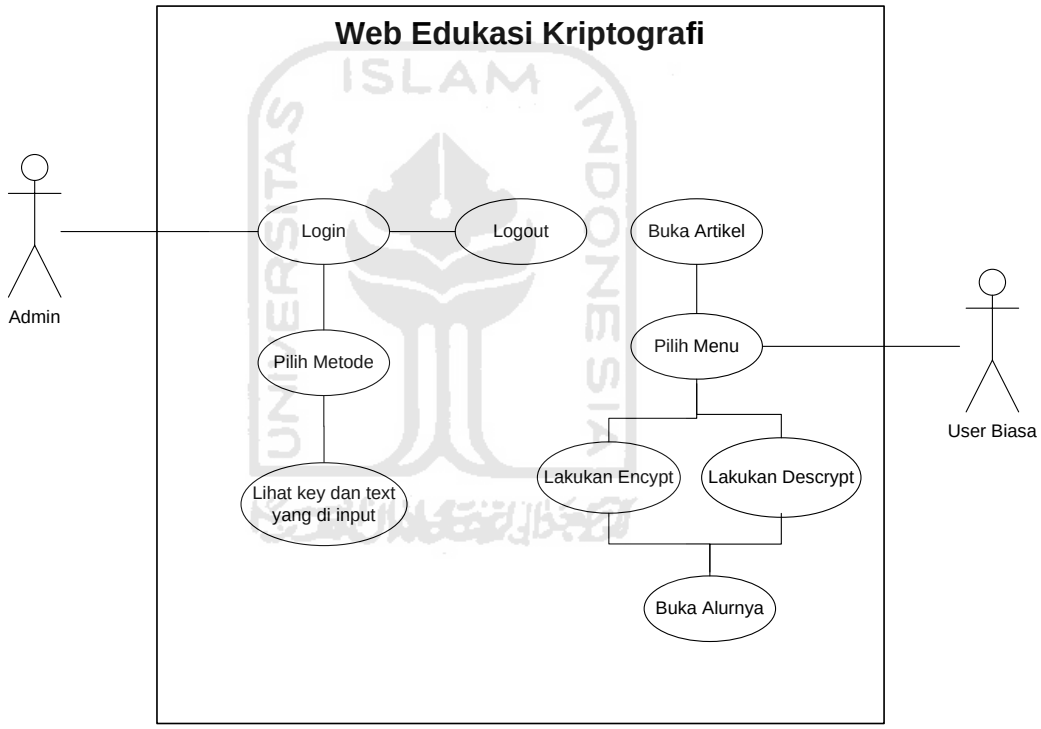
Gambar 3.1 Gambar database skripsi

3.2.3 Use Case Diagram

Use case diagram menggambarkan fungsionalitas yang diharapkan dari sebuah sistem. Sebuah use case merepresentasikan sebuah interaksi antara aktor dengan sistem. Use case diagram merupakan alat komunikasi tingkat tinggi

untuk mewakili persyaratan system. Pada use case ini terdiri dari dua actor yaitu user biasa dan admin, admin adalah seseorang yang akaan bertanggung jawab dengan Web Edukasi Kriptografi ini dan dapat menghapus, mengedit, dan menambahkan sebuah artikel atau materi yang ada didalam Web Edukasi Kriptografi ini dan user biasa adalah seseorang yang mengunjungi Web Edukasi Kriptografi dan dapat menjalankan fungsi implementasi.

Berikut ini adalah gambar dari rancangan use case Web Edukasi Kriptografi :



Gambar 3.2 Gambar use case diagram

3.2.4 Rancangan Antarmuka

Tahap perancangan desain bertujuan untuk mencari mentuk yang optimal dari Web Edukasi Kriptografi yang akan dibangun dengan mempertimbangkan faktor-faktor permasalahan dan kebutuhan yang ada pada system seperti yang telah di tetapkan pada tahap analisis. Dalam tahap ini upaya yang dilakukan yaitu medengan mengkombinasikan penggunaan teknologi

perangkat keras dan perangkat lunak yang tepat sehingga diperoleh hasil yang optimal. Antar muka yang dikembangkan pada Web Edukais Kriptografi ini diharapkan bersifat *userfriendly* dikarenakan berjalan dilayar computer maupun laptop. Berikut rancangan antarmuka Web Edukasi Kriptografi :

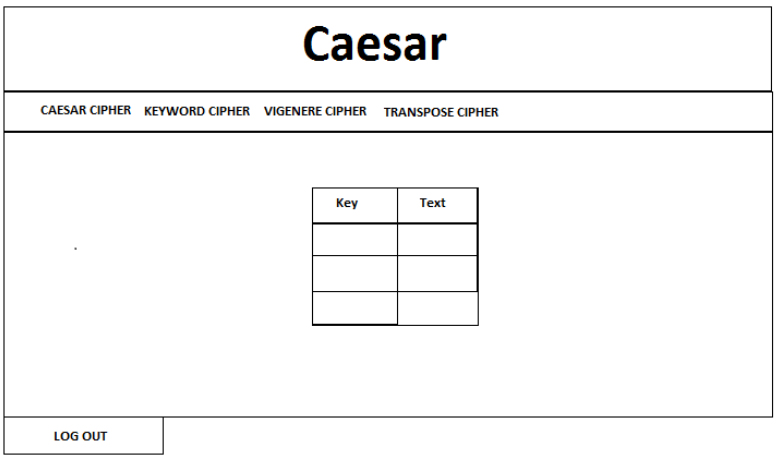
- Antar muka untuk admin

1. Antarmuka index.php

Gambar 3.3 Gambar Antarmuka index.php

Gambar 3.3 di atas digunakan seorang admin untuk masuk kedalam system atau halaman dimana seorang admin dapat melihat key dan text apa saja yang di masukan user biasa.

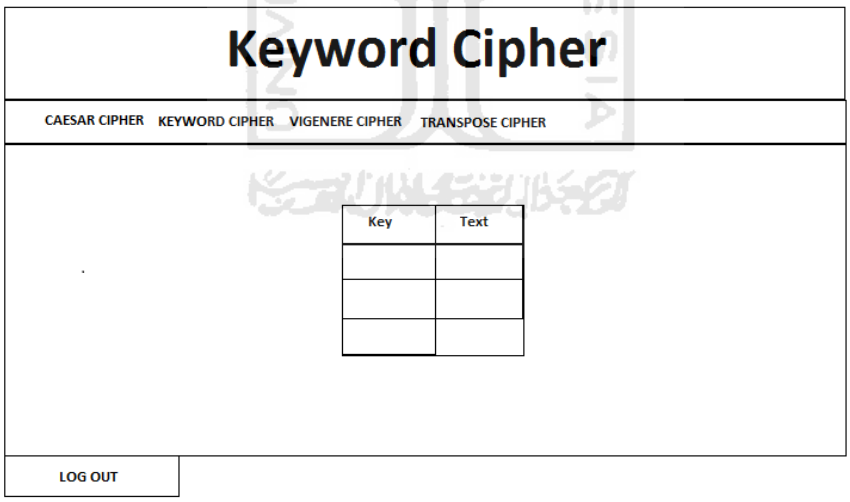
2. Antarmuka admin/halamanCaesar.php



Gambar 3.4 Gambar Antarmuka admin/halamanCaesar.php

Gambar 3.4 di atas adalah gambar antarmuka dimana seorang admin akan melaukan edit, hapus, dan tambah artikel untuk Caesar Cipher.

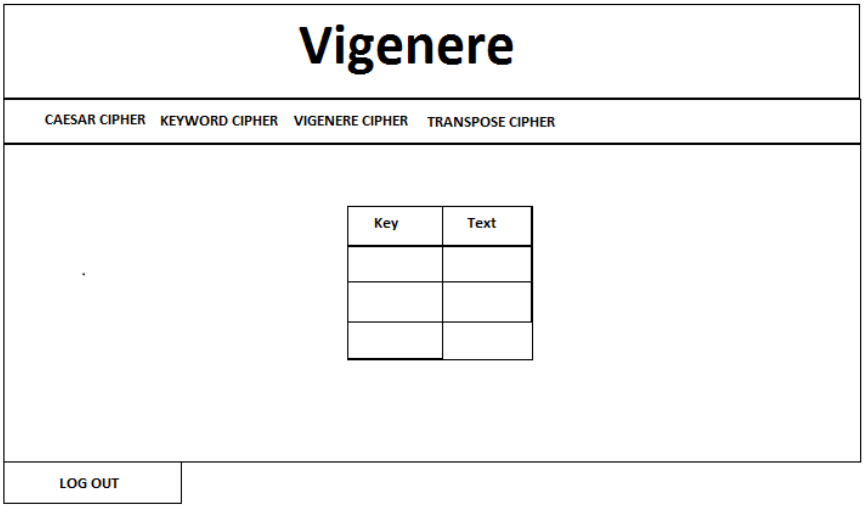
3. Antarmuka admin/halamanKeywordCipher.php



Gambar 3.5 antarmuka admin/halamanKeyword.php

Gambar 3.5 di atas adalah gambar antarmuka dimana seorang admin akan melaukan edit, hapus, dan tambah artikel untuk Keyword Cipher.

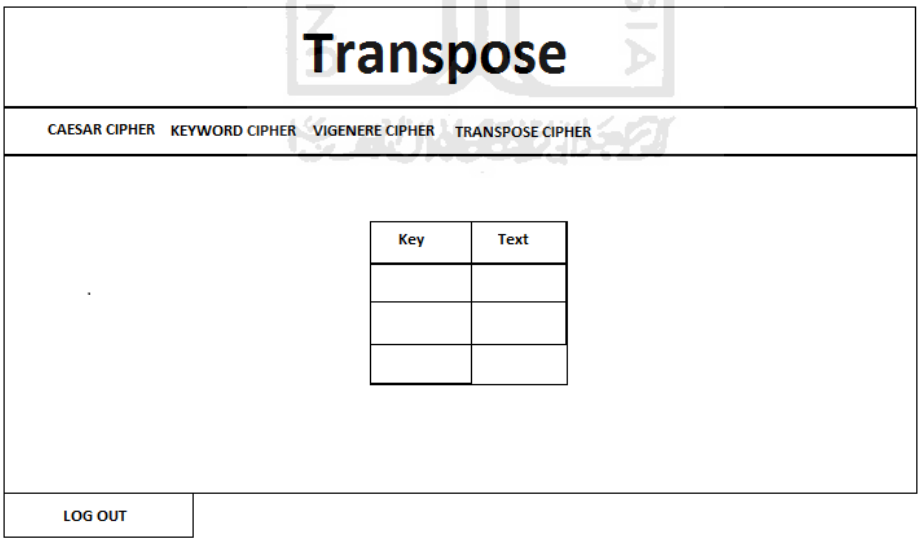
4. Antarmuka admin/halamanVigenere.php



Gambar 3.6 Gambar antarmuka admin/halamanVigenere.php

Gambar 3.6 di atas adalah gambar antarmuka dimana seorang admin akan melaukan edit, hapus, dan tambah artikel untuk Vigenere Cipher.

5. Antarmuka admin/halamanTranspose.php



Gambar 3.7 Gambar antarmuka admin/halamanTranspose.php

Gambar 3.7 di atas adalah gambar antarmuka dimana seorang admin akan melaukan edit, hapus, dan tambah artikel untuk Transpose Cipher.

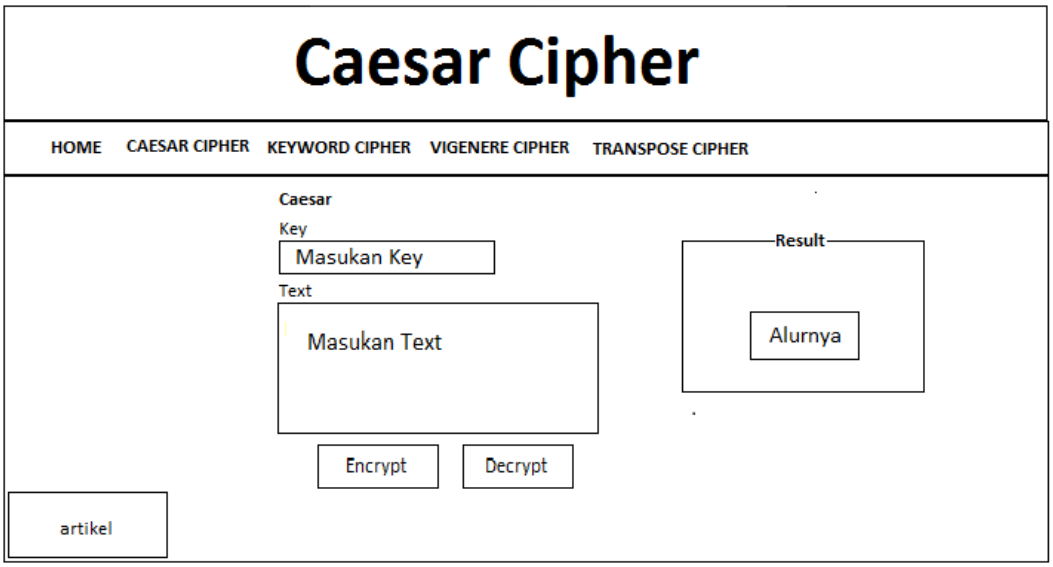
- Antar muka untuk user biasa

1. Antarmuka home.php

Gambar 3.8 Gambar antarmuka home.php

Gambar 3.8 di atas adalah gambar antarmuka pertama ketika seorang user biasa mengunjungi Web Edukasi Kriptografi.

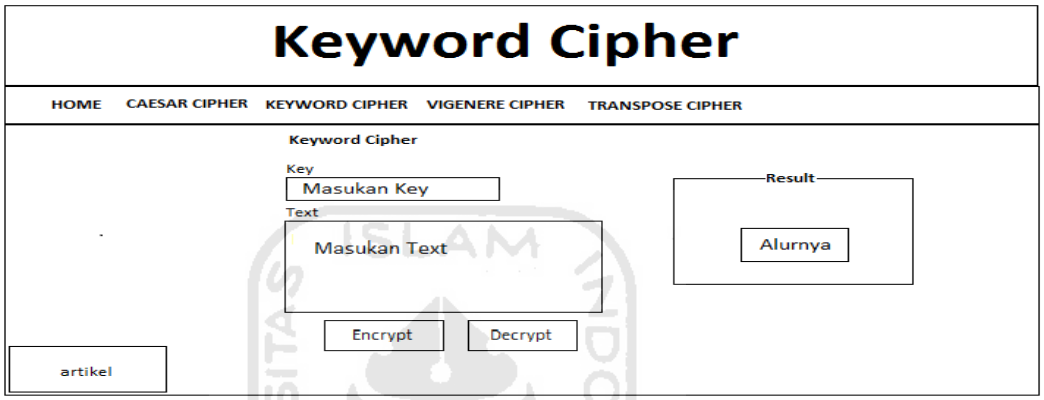
2. Antarmuka user/halamanCaesar.php



Gambar 3.9 Gambar antarmuka user/halamanCaesar.php

Gambar 3.9 di atas adalah gambar antarmuka untuk menu Caesar Cipher, dimana seorang user biasa dapat melihat artikel atau materi yang admin sediakan dan juga dapat menjalankan implementasi yang berfungsi sebagai implementasi dari *Caesar Cipher*.

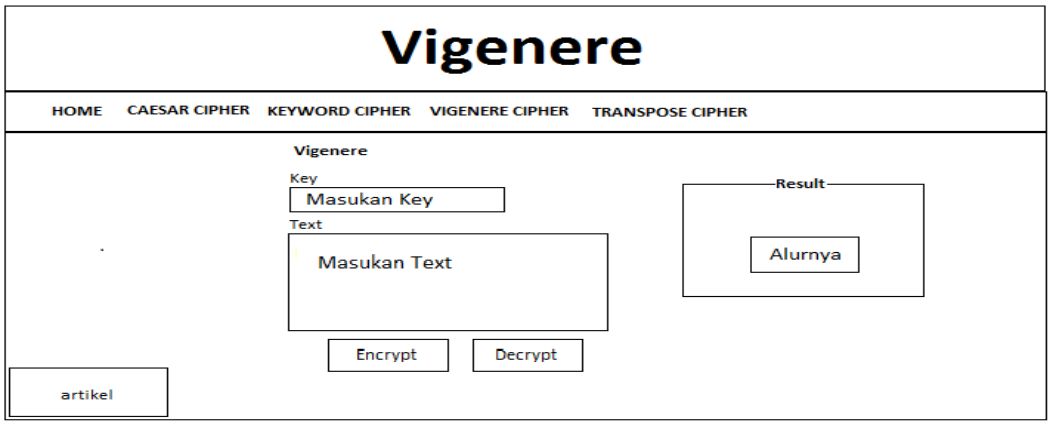
3. Antarmuka user/halamanKeywordCipher.php



Gambar 3.10 Gambar antarmuka user/halamanKeywordCipher.php

Gambar 3.10 di atas adalah gambar antarmuka untuk menu Keyword Cipher, dimana seorang user biasa dapat melihat artikel atau materi yang admin sediakan dan juga dapat menjalankan implementasi yang berfungsi sebagai implementasi dari *Keyword Cipher*.

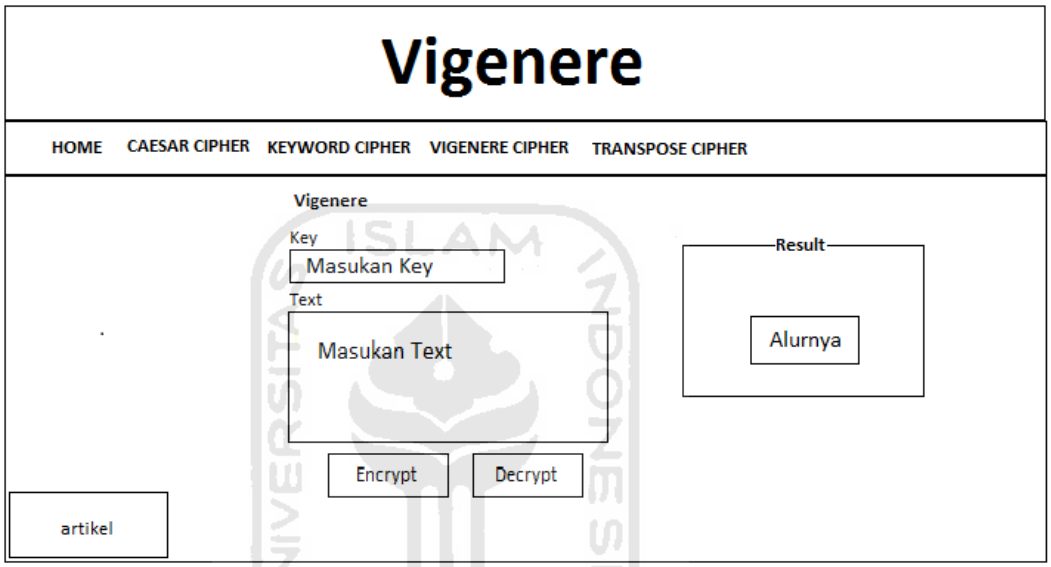
4. Antarmuka user/halamanVigenere.php



Gambar 3.11 Gambar antarmuka user/halamanVigenere.php

Gambar 3.11 di atas adalah gambar antarmuka untuk menu Vigenere Cipher, dimana seorang user biasa dapat melihat artikel atau materi yang admin sediakan dan juga dapat menjalankan implementasi yang berfungsi sebagai implementasi dari *Vigenere Cipher*.

5. Antarmuka user/halamanTranspose.php



Gambar 3.12 Gambar antarmuka user/halamanTranspoe.php

Gambar 3.12 di atas adalah gambar antarmuka untuk menu Transpose Cipher, dimana seorang user biasa dapat melihat artikel atau materi yang admin sediakan dan juga dapat menjalankan implementasi yang berfungsi sebagai implementasi dari *Transpose Cipher*.

Kriptografi ini adalah dasar atau awal dari kriptografi-kriptografi modern yang dipakai sekarang, walau pun sudah sangat jarang diimplementasikan untuk aplikasi-aplikasi maupun system-sistem yang ada saat ini, kriptografi klasik masih dipakai sebagi dasar untuk mempelajari ilmu atau teknik kriptografi.

BAB IV
HASIL DAN PEMBAHASAN

4.1 Impelementasi secara umum

Implementasi yang dilakukan menggunakan sebuah laptop untuk membangun web ini. Laptop yang digunakan untuk melakukan implementasi memiliki implementasi sebagai berikut :

1. Prosesor AMD A4 5000 APU
2. RAM 4 GB
3. Hardixk 500 GB

Sedangkan perangkat lunak yang digunakan dalam implementasi adalah Sublime Text.

4.2 Implementasi Pembuatan Web

Bahasa permrograman yang digunakan untuk membangun ini adalah PHP, Html, dan CSS yang ditulis dalam sublime text. Html dibuat untuk membangun sebuah halaman web dan CSS sendiri untuk mendesain halaman web tersebut. Sedangkan bahasa pemrograman PHP digunakan untuk membuat implementasi kriptografi seperti Caesar cipher, Keyword cipher, Vigenere cipher dan membangun koneksi ke database lokal XAMPP.

4.3 Implementasi Pembuatan Database

Database sangat dibutuhkan untuk penyimpanan data, pada web ini database dipakai untuk menyimpan key dan text (plaintext maupun ciphertext) yang diinputkan. Database ini bertujuan untuk melihat key dan text yang paling banyak digunakan. Implementasi dapat dilihat pada gambar di bawah ini.

```php
<?php

$connection = mysql_connect("localhost", "root", "");

$db = mysql_select_db("skripsi", $connection);

?>
```

Gambar 4.1 Gambar session.php

Penjelasan untuk gambar 4.1 adalah untuk mengubah database default agar terkoneksi sehingga dapat di *include* di halaman web lain, contoh :

```php
<?php
    include('session.php');
    if (isset($_POST['key_caesar'])){
        $key_caesar = $_POST['key_caesar'];
        $plantext_caesar = $_POST['plantext_caesar'];
        $querys = mysql_query("INSERT INTO caesar VALUES(null, '$key_caesar' , '$plantext_caesar')", $
            connection);
    }
?>
```

Gambar 4.2 Gambar kode MySql

Penjelasan untuk gambar 4.2 adalah dengan menggunakan include('session.php'); kita tidak perlu menulis ulang apa yang ada di dalam session.php agar web kita terkoneksi dengan database. Dengan $connection perintah mysql yang kita buat dapat diexekusi oleh dataase yang kita aktifkan di session.php.

```php
<?php
session_start();

if (isset($_POST['submit'])) {
if (empty($_POST['username']) || empty($_POST['password'])) {
$error = "Username or Password is invalid";
}
else
{

$username=$_POST['username'];
$password=$_POST['password'];

$connection = mysql_connect("localhost", "root", "");

$username = stripslashes($username);
$password = stripslashes($password);
$username = mysql_real_escape_string($username);
$password = mysql_real_escape_string($password);

$db = mysql_select_db("skripsi", $connection);

$query = mysql_query("select * from admin where password='$password' AND username='$username'", $connection);
$rows = mysql_num_rows($query);
if ($rows == 1) {
$_SESSION['login_user']=$username;
header("location: admin/halamanCaesar.php");
} else {
$error = "Username atau Password belum terdaftar";
}
mysql_close($connection);
}
}
?>
```

Gambar 4.3 Gambar login admin

Penjelasan untuk gambar 4.3 adalah membangun sebuah database untuk admin sehingga admin dapat melakukan login. Admin dapat melakukan login dengan username dan password yang telah didaftarkan ke dalam database skripsi secara manual.

4.4 Implementasi Caesar Cipher

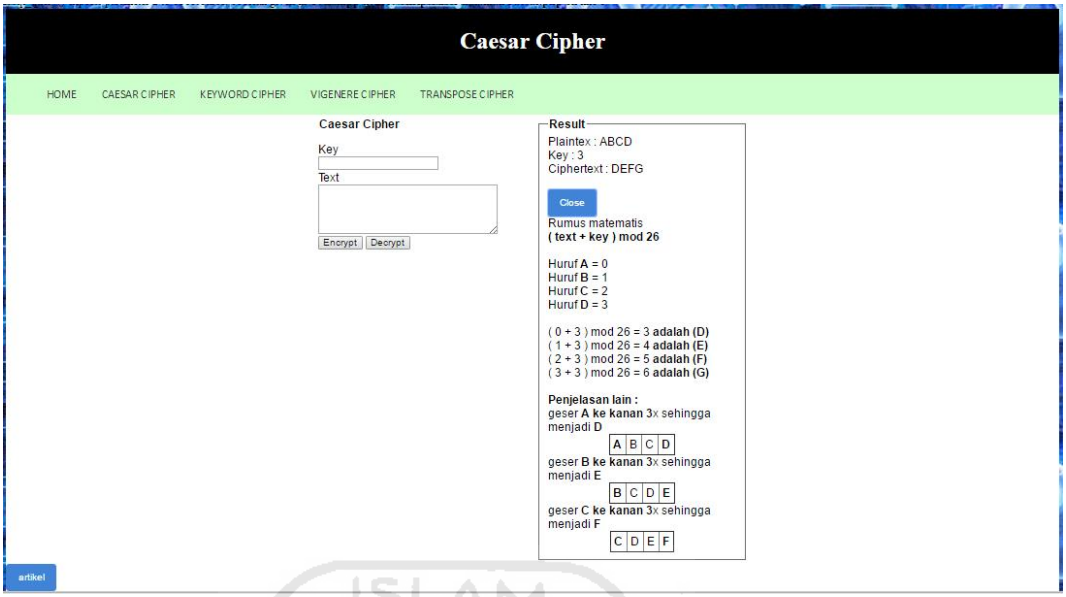
Seperti yang dijelaskan di bab sebelumnya cara kerja Caesar cipher adalah memindahkan huruf demi huruf yang ada di plaintext maupun di ciphertext sesuai dengan key (keynya dalam bentuk angka seperti 1,2,3, dan seterusnya). Implementasi dapat dilihat pada gambar di bawah ini.

```
$chipertxt="";
foreach($split_plaintext as $chr){
    $i=ord(strtoupper($chr)) - 65;
    $chiper = ($key+$i) % 26;
    $chipertxt .= chr($chiper+65);

}
$enc = $chipertxt;
echo "Plaintex : ".$p."<br>";
echo "Key : ".$ke."<br>";
echo "Ciphertext : ".$enc."<br>"."<br>";
$chip = str_split($chipertxt);
```

Gambar 4.4 Gambar Kode enkripsi Caesar cipher

Penjelasan untuk gambar 4.4 adalah proses dari enkripsi Caesar cipher. Key diinput dalam bentuk angka. Plaintext diinputkan lalu akan displit sehingga dapat diubah huruf demi huruf seseuai dengan key yang telah diinputkan dengan rumus ($key + $i) % 26, dengan penjelasan $key sebagai key, $i sebagai plaintext yang telah displit dan diubah menjadi kode ASCII, dan % 26 adalah mod 26. Sebagai contoh jika diberi key ‘3’ dan plaintext ‘abcd’ maka huruf abcd d geser kekanan sebanyak 3 kali sesuai dengan key dan akan menghasilkan ciphertext ‘defg’,



Gambar 4.5 Gambar proses enkripsi Caesar Cipher

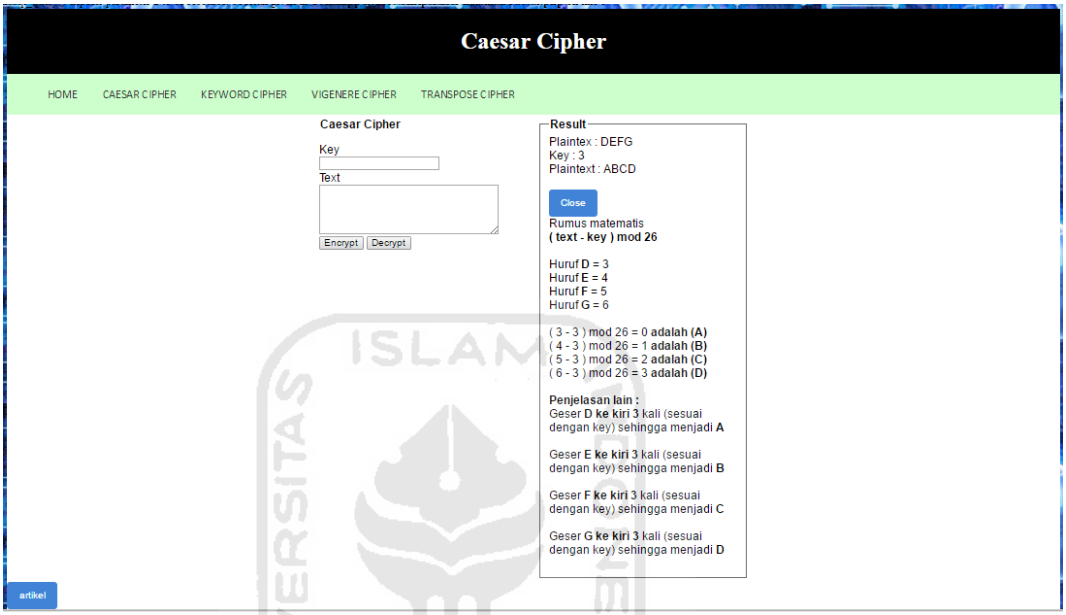
Penjelasan gambar 4.5 diatas adalah screenshot enkripsi yang pada halaman Caesar Cipher beserta dengan alurnya. Dengan memasukan key dan text ditempat yang telah disediakan lalu menekan tombol encrypt, hasil dapat dilihat di kolom result. Tombol alur digunakan untuk melihat proses perubahan dari *plaintext* ke *ciphertext.*

```
$plaintex="";
foreach($split_chipertxt as $chr){
    $i=ord(strtoupper($chr)) - 65;
    $chiper = ($i-$key) % 26;
    // echo $chiper." ";
    if($chiper<0){
        $plaintex .= chr($chiper+65+26);
    }else{
        $plaintex .= chr($chiper+65);
    }
}
echo "Plaintex : ".$p."<br>";
echo "Key : ".$ke."<br>";
echo "Plaintext : ".$des = $plaintex."<br><br>";
$chip = str_split($plaintex);
```

Gambar 4.6 Gambar kode deskripsi caesar cipher

Penjelasan gambar 4.6 diatas adalah mirip seperti proses enkripsi tetapi karena fungsi ini untuk deskripsi rumusnya dibalik sehungga menjadi ($i -

$key) % 26. $i disini sebagai ciphertext yang telah displit dan diubah menjadi kode ASCII bukan sebagai plaintext. Sebagai contoh jika diberi key 3 dan ciphertext defg maka huruf defg d geser kekiri sebanyak 3 kali sesuai dengan key dan akan menghasilkan plaintext abcd.



Gambar 4.7 Gambar proses deskripsi Caesar cipher

Penjelasan gambar 4.7 diatas adalah screenshot deskripsi yang pada halaman Caesar Cipher beserta dengan alurnya. Dengan memasukan key dan text ditempat yang telah disediakan lalu menekan tombol decrypt, hasil dapat dilihat di kolom result. Tombol alur digunakan untuk melihat proses perubahan dari *ciphertext* ke *plaintext.*

4.5 Implementasi Keyword Cipher

Seperti yang sudah dijelaskan di bab sebelumnya keyword cipher ini adalah cipher yang menggunakan huruf sebagai key. Untuk implementasi pada koding dapat dilihat pada gambar dibawah ini.

```php
class en{
    public function check($key, $char){
        for ($p=0; $p <strlen($key) ; $p++) {
            if($key[$p] == $char){
                return false;
            }
        }
        return true;
    }
```

Gambar 4.8 Gambar fungsi chek key keyword cipher

Penjelasan pada gambar 4.8 adalah membuat sebuah fungsi chek didalam kelas en yang berfungsi untuk mengecek key.

```php
public function keyRemoveSameChar($key){
    $key2 = "";
    for ($i=0; $i <strlen($key) ; $i++) {
        $char = $key[$i];
        $bool = false;
        for ($p=0; $p <$i ; $p++) {
            if($char == $key[$p]){
                $bool = true;
                break;
            }
        }
        if($i == 1){
            if($char == $key[0]){
                $bool = true;
            }
        }
        if(!$bool){
            $key2 .= $char;
        }
    }
    return $key2;
}
```

Gambar 4.9 Gambar fungsi keyRemoveSameChar keyword cipher

Penjelasan untuk gambar 4.9 adalah menghilangkan karakter yang duplikat atau karakter yang sama seperti jika key nya saya, maka akan menjadi say, karena karakter terakhir dari kata saya sama dengan karakter ke-dua maka karakter terakhir di buang.

```
public function key($key){
    $arraykey = array();
    $key = $this->keyRemoveSameChar($key);
    $key = strtoupper($key);
    $abc="A";
    for ($i=0; $i <26 ; $i++) {
        if(strlen($key) > $i){
            $arraykey[$i] = $key[$i];
        }else{
            for ($o=0; $o < strlen($key); $o++) {
                if($this->check($key,$abc)){
                    $arraykey[$i] = $abc;
                    break;
                }
                $abc++;
            }
            $abc++;
        }
    }
    return $arraykey;
}
```

Gambar 4.10 Gambar fungsi key keyword cipher

Penjelasan pada gambar 4.10 adalah mengubah key menjadi susunan alphabet yang baru. Setelah huruf yang sama pada key dibuang makan akan terbentuk susunan alphabet baru, contoh :

Key = SAYAN

Maka akan menjadi susunan alphabet yang baru SAYNBCDEFGHIJKLMOPQRTUVWXZ. Pada koding di atas kita membuat variable key ($key) dan kemudian yang akan dicek oleh fungsi keyRemoveSameChar untuk menghapus huruf yang duplikat. Setelah duplikat huruf dibuang maka akan dilanjutkan dengan membuat alphabet yang baru.

```
public function plaintext($plain){
    $plain = str_replace(' ', '', $plain);
    $plain = strtoupper($plain);
    return $plain;
}
```

Gambar 4.11 Gambar fungsi plaintext keyword cipher

Penjelasan pada gambar 4.11 adalah untuk membuat plaintext yang akan diubah menjadi cipher text maupun sebaliknya.

```
public function encrypt($plain, $arraykey){
    $chiper = "";
    for ($i=0; $i <strlen($plain) ; $i++) {
        $index = ord($plain[$i]) - 65;
        $chiper .= $arraykey[$index];
    }
    return $chiper;
}
```

Gambar 4.12 Gambar fungsi enkripsi keyword cipher

Penjelasan pada gambar 4.12 adalah untuk membuat rumus enkripsi keyword cipher Proses pencocokan key yang baru dengan alphabet yang baru sesuai dengan *plaintext* yang ada sehingga menjadi *ciphertext*.

```
public function decrypt($chiper, $arraykey){
    $plain = "";
    for ($i=0; $i <strlen($chiper) ; $i++) {
        $char = $chiper[$i];
        for ($p=0; $p<26 ; $p++) {
            if($char == $arraykey[$p]){
                $plain .= chr($p+65);
            }
        }
    }
    return $plain;
}
```

Gambar 4.13 Gambar fungsi deskripsi keyword cipher

Penjelasan pada gambar 4.13 adalah untuk membuat rumus deskripsi keyword cipher. Proses pencocokan key yang baru dengan alphabet yang baru sesuai dengan *ciphertext* yang ada sehingga menjadi *plaintext.*

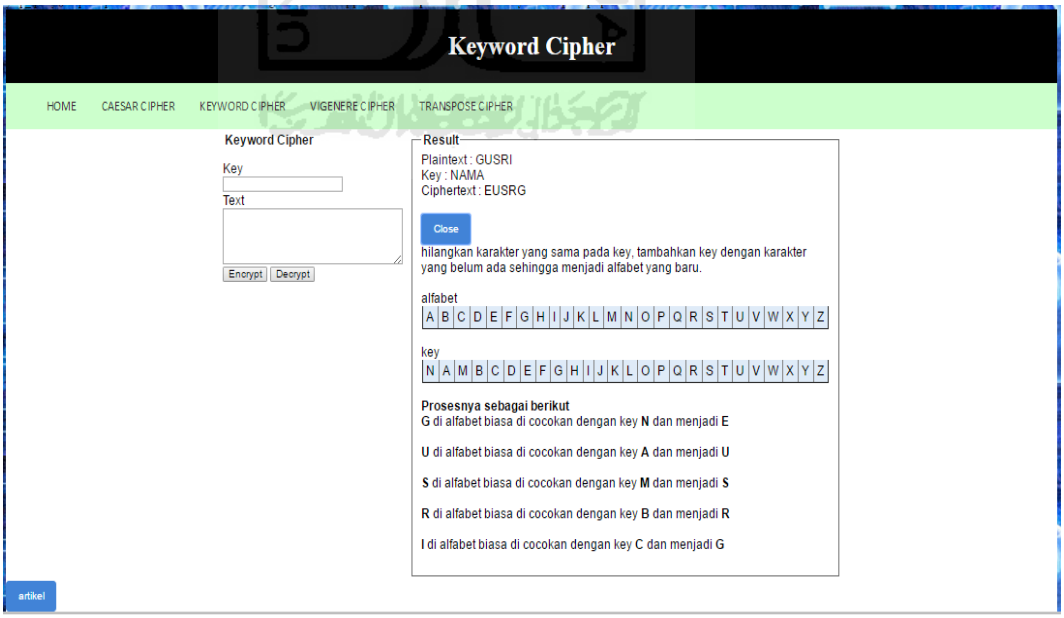
```
$arraykey = $panggil->key($key1);
$plain1 = $panggil->plaintext($plain1);
echo "Plaintext : ".$plx."<br>";
echo "Key : ".$k1."<br>";
echo "Ciphertext : ".$enc = $panggil->encrypt($plain1, $arraykey)."<br><br>";

$ke = str_split($enc);
echo "<button id='spinner'>Alurnya</button><br/><div id='hidden' style='display:none'>";
echo "hilangkan karakter yang sama pada key, tambahkan key dengan karakter yang belum ada sehingga
    menjadi alfabet yang baru.<br><br>";
echo "<table border = '1px'>";
echo "<tr>";
echo "alfabet";
echo "</tr>";
$x = "A";
$l = $x;
echo "<td>".$l."</td>";
for ($i=0; $i < 25; $i++) {
    $x++;
    echo "<td>".$x."</td>";
}

echo "</table>"."<br>";
echo "<table border = '1px'>";
echo "<tr>";
echo "key";
echo "</tr>";
for ($i=0; $i < 26; $i++) {
    echo "<td>".$arraykey[$i]."</td>";
}
echo "</table>"."<br>";
echo "<b>Prosesnya sebagai berikut</b><br>";
for ($g=0; $g < strlen($plain1); $g++) {
    $plan2 = $plain1[$g];
    $c_plan2 = $ke[$g];
    $ka2 = $arraykey[$g];
    echo "<b>$plan2</b>"." di alfabet biasa di cocokan dengan key "."<b>$ka2</b>"." dan menjadi "."<b>$
        c_plan2</b>"."<br><br>";
}
echo "</div>";
```

Gambar 4.14 Gambar kode enkripsi keyword cipher

Penjelasan pada gambar 4.14 adalah proses dari enkripsi pada keyword cipher. Proses ini akan mengubah ciphertext menjadi plaintext dengan memanggil fungsi en yang telah dijelaskan diatas.



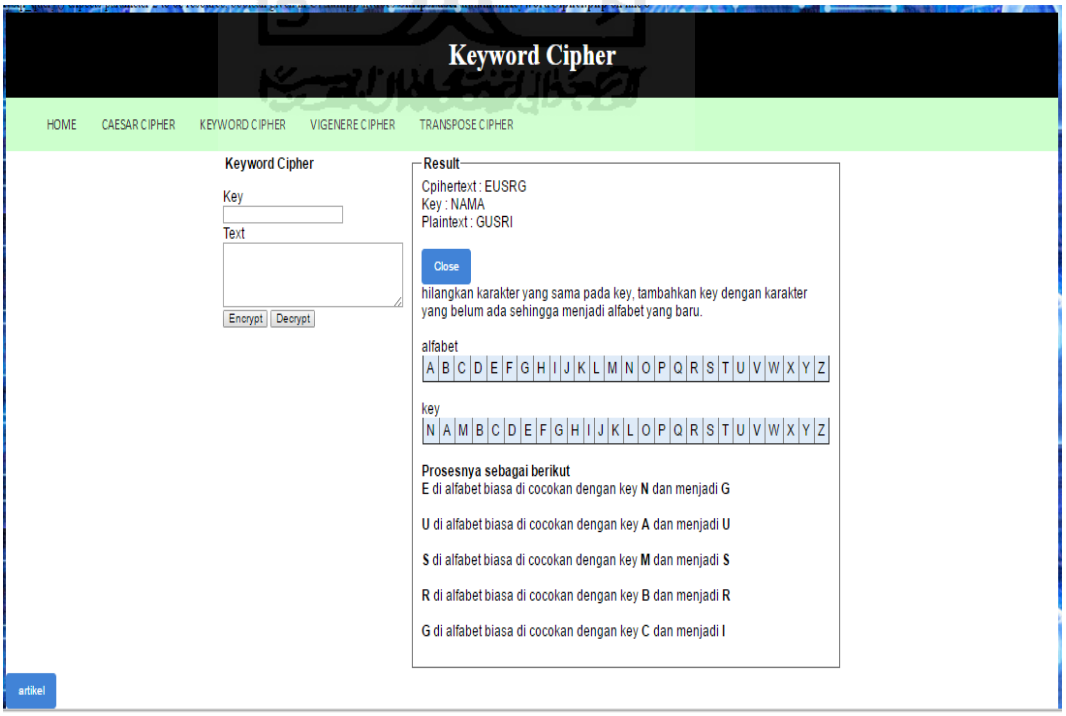
Gambar 4.15 Gambar proses emkripsi keyword cipher

Penjelasan gambar 4.15 diatas adalah screenshot enkripsi yang pada halaman Keyword Cipher beserta dengan alurnya. Dengan memasukan key dan text ditempat yang telah disediakan lalu menekan tombol encrypt, hasil dapat dilihat di kolom result. Tombol alur digunakan untuk melihat proses perubahan dari *ciphertext* ke *plaintext*.

```
}else if ((isset($_POST['key_simple'])) && (isset($_POST['plantext_simple'])) && (isset($
    _POST['decrypt_simple']))) {
    $key1 = $_POST['key_simple'];
    $plain1 = $_POST['plantext_simple'];
    $des = $_POST['decrypt_simple'];
    $arraykey = $panggil->key($key1);
    $plain1 = $panggil->plaintext($plain1);
    echo $des = $panggil->decrypt($plain1, $arraykey);
}
```

Gambar 4.16 Gambar kode deskripsi keyword cipher

Penjelasan pada gambar 4.16 adalah proses dari deskripsi pada keyword cipher. Proses ini akan mengubah ciphertext menjadi plaintext dengan memanggil fungsi en yang telah dijelaskan diatas.



Gambar 4.17 Gambar proses deskripsi keyword cipher

Penjelasan gambar 4.17 diatas adalah screenshot deskripsi yang pada halaman Keyword Cipher beserta dengan alurnya. Dengan memasukan key dan text ditempat yang telah disediakan lalu menekan tombol decrypt, hasil dapat dilihat di kolom result. Tombol alur digunakan untuk melihat proses perubahan dari *ciphertext* ke *plaintext.*

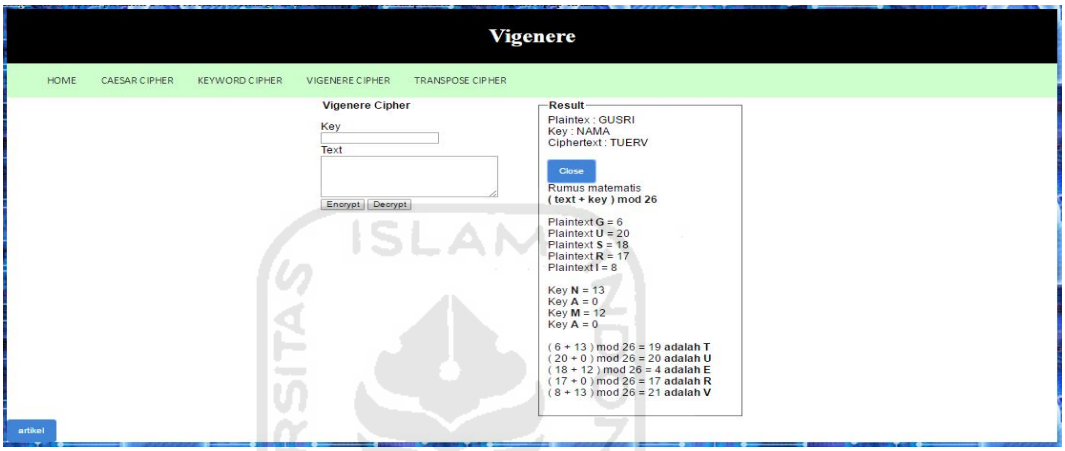
4.6 Implementasi Vigenere Cipher

Seperti yang dijelaskan di bab sebelumnya cara kerja vigenere cipher adalah memindahkan huruf demi huruf yang ada di plaintext maupun di ciphertext sesuai dengan key (key dalam bentuk huruf). Tetapi panjang key harus sama dengan plaintext maupun ciphertext, contoh key ‘nama’ dengan plaintext ‘namas’, karena panjang key 4 karakter dan plaintext 5 karakter, maka panjang key harus disamakaan dengan cara menambah huruf dengan huruf awal yang menjadi ‘naman’ Implementasi dapat dilihat pada gambar di bawah ini.

```php
while(strlen($key)<strlen($plantext)){
    $key .= $key;
}
$key2 = str_split($key);
$split_key= str_split($key);
$split_text= str_split($plantext);
$split_text_angka = array();
$split_key_angka = array();
$i= 0;
foreach($split_text as $chr){
$split_text_angka[$i] = ord(strtoupper($chr)) - 65;
$i++;
}
$i =0 ;
foreach($split_key as $chr){
    $split_key_angka[$i] = ord(strtoupper($chr)) - 65;
    $i++;
}
$cipher =""; $i =0 ; $b="";
$split_cbiper_angka = array();
$enkr = "";
foreach($split_text as $chr){
    $split_cbiper_angka[$i] = ($split_text_angka[$i] + $split_key_angka[$i])%26;
    $enkr .= chr($split_cbiper_angka[$i]+65);
    $i++;
}
$p = strtoupper($p);
echo "Plaintex : ".$p."<br>";
$ke = strtoupper($ke);
echo "Key : ".$ke."<br>";
echo "Ciphertext : ".$enkr."<br>"."<br>";
```

Gambar 4.18 Gambar kode enkripsi vigenere cipher

Penjelasan pada gambar 4.18 adalah proses dari enkripsi vigenere cipher, dengan membuat perulangan (while) agar panjang key sama dengan panjang plaintext. Setelah panjang key dan panjang plaintext sama, maka key dan plaintext akan displit dan diubah menjadi kode ASCII. Setelah key dan plaintext diubah menjadi kode ASCII, key dan plaintext dijumlahkan dan di mod 26 sesuai dengan rumusnya.



Gambar 4.19 Gambar proses enkripsi vigenere cipher

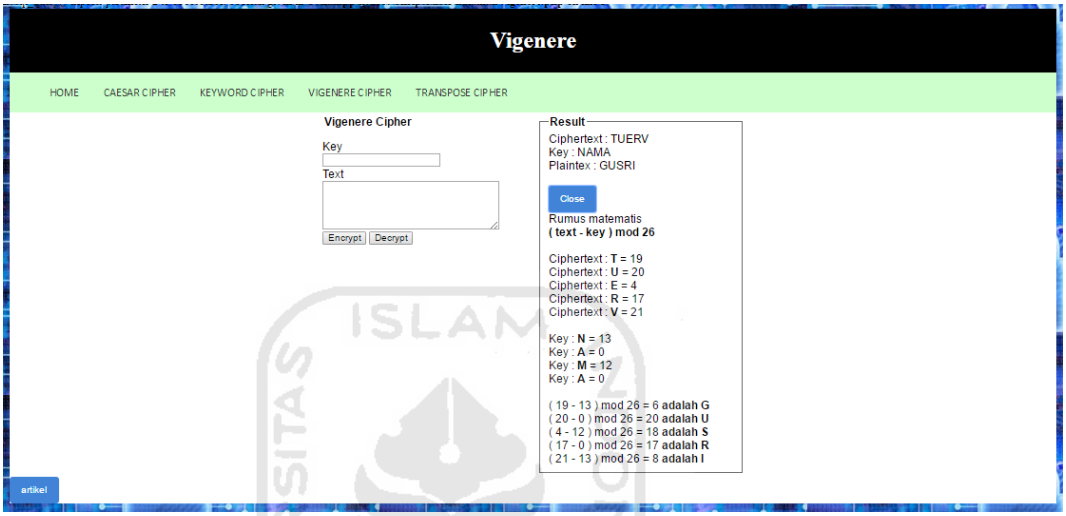
Penjelasan gambar 4.19 diatas adalah screenshot enkripsi yang pada halaman Vigenere Cipher beserta dengan alurnya. Dengan memasukan key dan text ditempat yang telah disediakan lalu menekan tombol encrypt, hasil dapat dilihat di kolom result. Tombol alur digunakan untuk melihat proses perubahan dari *plaintext* ke *ciphertext.*

```
while(strlen($key)<strlen($plantext)){
    $key .= $key;
}
$key2 = str_split($key);
$split_text= str_split($plantext);
$split_key= str_split($key);
$split_text_angka = array();
$split_key_angka = array();
$i= 0;
foreach($split_text as $chr){
$split_text_angka[$i] = ord(strtoupper($chr)) - 65;

$i++;
}
$i =0 ;
foreach($split_key as $chr){
    $split_key_angka[$i] = ord(strtoupper($chr)) - 65;
    $i++;
}
$i =0 ;
$dec = "";
foreach($split_text as $chr){
    $temp = ($split_text_angka[$i] - $split_key_angka[$i]) + 26;
    if($temp >= 26){
        $dec .= chr($temp - 26 + 65);
    }else{
        $dec .= chr($temp + 65);
    }
    $i++;
}
$plantext = strtoupper($plantext);
echo "Ciphertext : ".$plantext."<br>";
$k1 = strtoupper($k1);
echo "Key : ".$k1."<br>";
echo "Plaintex : ".$dec."<br><br>";
```

Gambar 4.20 Gambar kode deskripsi vigenere cipher

Penjelasan pada gambar 4.20 adalah proses dari deskripsi vigenere cipher, untuk proses sama dengan enkripsi, yang membedakan adalah rumusnya. Rumusnya adalah plaintext dikurangi key dan ditambahkan 26 atau dimod 26.



Gambar 4.21 Gambar proses deskripsi vigenere cipher

Penjelasan gambar 4.21 diatas adalah screenshot enkripsi yang pada halaman Vigenere Cipher beserta dengan alurnya. Dengan memasukan key dan text ditempat yang telah disediakan lalu menekan tombol decrypt, hasil dapat dilihat di kolom result. Tombol alur digunakan untuk melihat proses perubahan dari *ciphertext* ke *plaintext*.

4.6.1 Implementasi Transpose Cipher

Seperti yang dijelaskan di bab sebelumnya cara kerja transpose cipher adalah dengan mengubah sebuah plaintext menjadi sebuah matrix sesuai dengan keynya, key dsini berfungsi sebagai kolom dan baris untuk matrixnya (seperti 5x5). Implementasi dapat dilihat pada gambar dibawah.

```
for ($i=0; $i <$key ; $i++) {
    $newarray = array();
    for ($p=0; $p < $key; $p++) {
        if($index < strlen($plain)){
            $newarray[$p] = $plain[$index];
            $index++;
        }else{
            $newarray[$p] = "&";
        }
    }
    array_push($matrix, $newarray);
}
$chiper = "";
echo "<br>";
for ($i=0; $i <$key  ;$i++) {
    for ($p=0; $p < $key; $p++) {
        $chiper .= $matrix[$p][$i];   } } 
$chiper = strtoupper($chiper);
echo "Text : ".$pl."<br>";
echo "Key : ".$key."x".$key."<br>";
echo "Encrypt :".$chiper."<br><br>";
echo "<button id='spinner'>Alurnya</button><br/><div id='hidden' style='display:none'>";
echo "Bentuk matrix dari text diatas adalah <br>";
echo "<table border = '1px'>";
for ($i=0; $i <$key ; $i++) {
echo "<tr>";
    for ($p=0; $p < $key; $p++) {
        echo "<td>"; echo $matrix[$i][$p]; echo "</td>";
    }
echo "</tr>";
}
echo "</table>";
echo "<br>";
$oo = 0; $z = 0;
for ($i=0; $i < $k; $i++) {
    $z++;
    echo " bentuk pecahan matrix kolom ".$z;
    for ($p=0; $p < $k; $p++) {
        $array = $chiper[$oo];
        $oo++;
        echo "<table border = '1px'>";
        echo "<tr>"."<td>".$array."</td>"."</tr>";
        echo "</table>";
    }
}echo "<br>";
echo "Sesuai dengan namanya transpose berarti perpindahan posisi, plaintext disusun menjadi matriks sesuai dengan jumlah key yaitu "
    ."<b>$key</b>"."(menjadi "."<b>$key</b>"."<b>x</b>"."<b>$key</b>)"."<br>";
echo "Dan pola yan dipakai dalam cipher ini adalah dengan membacanya dari atas kebawah atau kolom sehingga menjadi "."<b>$chiper</b>
    ";
echo "</div>";
```

Gambar 4.22 Gambar kode transposisi cipher

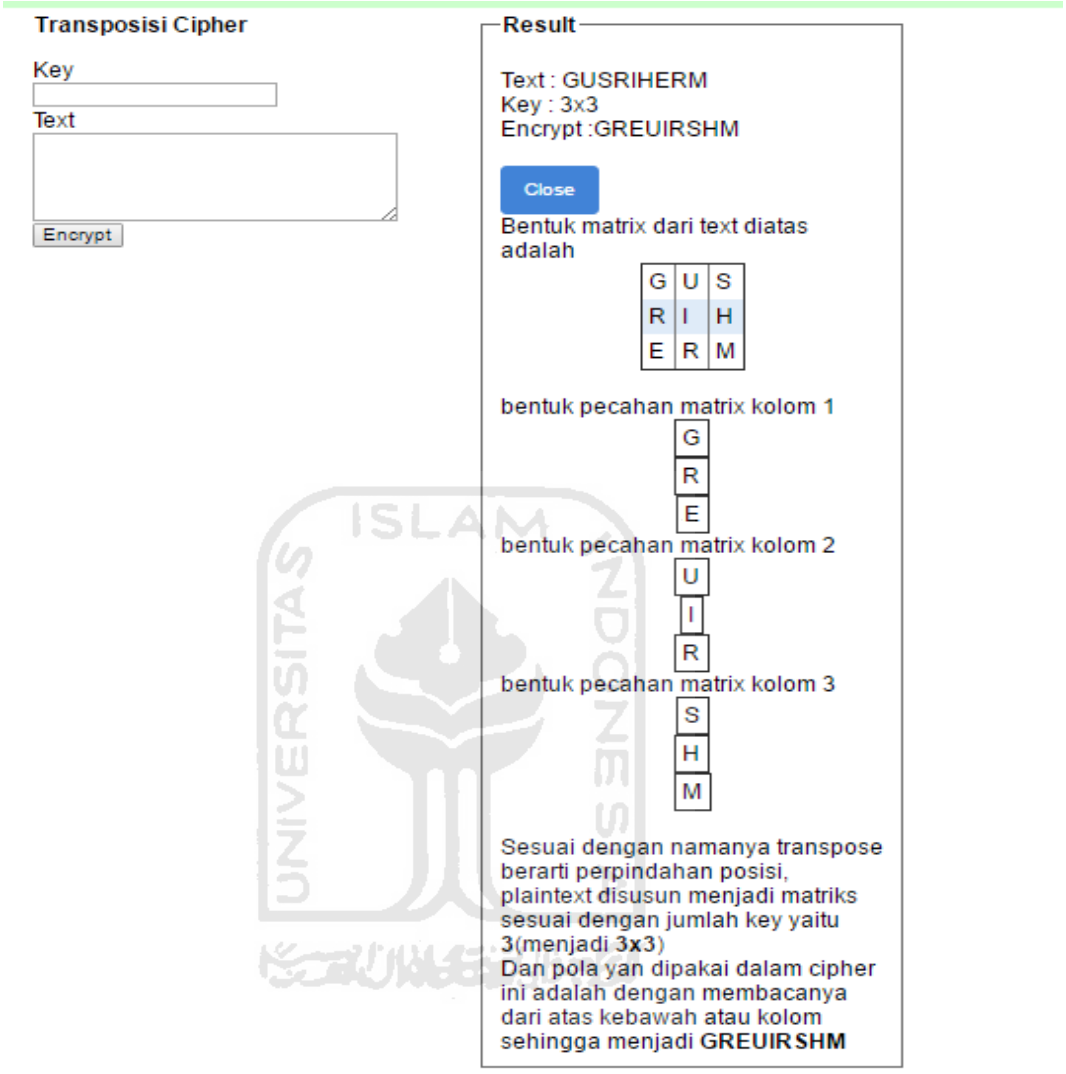
Penjelasan pada gambar 4.22 adalah proses dari transposisi cipher. Proses yang dilakukan adalah proses dimana key yang dijadikan sebagai kunci dari matrix, ketika kita memasukan bilangan 4, maka matrix akan menjadi 5x5 dan posisi plaintext pun akan berubah menjadi 4x4, contoh :

Key = 4 dan Plaintext = gusrihermawan maka akan terbentuk sebuah matrix seperti berikut :

Tabel 4.1 bentuk matrix

g	u	s	r
i	h	e	r
m	a	w	a
n	&	&	&

Dan menghasilkan ciphertext **gimnuha&sew&rra&**



Gambar 4.23 Gambar proses transposisi cipher

Penjelasan gambar 4.23 diatas adalah screenshot enkripsi yang pada halaman Vigenere Cipher beserta dengan alurnya. Dengan memasukan key dan text ditempat yang telah disediakan lalu menekan tombol encrypt, hasil dapat dilihat di kolom result. Tombol alur digunakan untuk melihat proses perubahan dari *plaintext* ke *ciphertext.*

BAB V
KESIMPULAN DAN SARAN

Pada bab ini akan diambil kesimpulan dari kegiatan-kegiatan yang telah dilakukan selama pengerjaan tugas akhir ini dan terdapat saran-saran untuk pengembangan lebih lanjut yang dapat diberikan dari tugas akhir ini.

5.1 Kesimpulan

Kesimpulan yang didapat selama pengerjaan tugas akhir ini adalah sebagai berikut :

1. Terbentuknya Web Edukasi Kriptografi Klasik.
2. Dengan Web Edukasi ini dapat memberikan informasi untuk memahami kriptografi klasik.
3. Web Edukasi Kriptografi Klasik ini juga memberikan alur atau proses perubahan dari plaintext ke ciphertext maupun sebaliknya.

5.2 Saran

Penelitian yang telah dilakukan tidak lepas dari kekurang-kekurangan dan kelemahan-kelemahan yang ada. Berikut saran-saran yang diberiakan oleh penulis untuk pengembangan lebih lanjut :

1. Untuk cipher dapat ditambah lagi, tidak hanya kriptografi klasik tetapi juga dapat ditambah dengan kriptografi modern.
2. Desain yang dapat diperbagus lagi karena desain Web Edukasi Kriptografi ini masih sangat sederhana.
3. Artikel atau informasi metode-metode cipher dapat ditambah lagi sehingga dapat memberikan pemahaman yang lebih lagi.

DAFTAR PUSTAKA

Fairuzabadi, M. (2010). Implementasi Kriptografi Klasik Menggunakan Borland Delphi. *Jurnal Dinamika Informatika*, *4*(2), 65–78. http://doi.org/10.1017/CBO9781107415324.004

Pabokory, F. N., Astuti, I. F., & Kridalaksana, A. H. (2015). Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard. *Jurnal Informatika Mulawarnan*, *10*(1), 20–31.

Riyanarto, S., & Iffano, I. (2012). Perancangan Aplikasi Pembelajaran Kriptografi Kunci Publik ElGamal Untuk Mahasiswa. *Jurnal Dunia Teknologi Informasi*, *1*(1), 56–62.

Sasongko, J. (2005). Pengamanan Data Informasi menggunakan Kriptografi Klasik. *Jurnal Teknologi Informasi DINAMIK*, *X*(3), 160–167.

Seftyanto, D., & Haryanto, T. (2012). PERAN ALGORITMA CAESAR CIPHER DALAM MEMBANGUN KARAKTER AKAN KESADARAN KEAMANAN INFORMASI, (November), 978–979.

Tarigan, A. (2014). Peran dan Perkembangan Kriptografi Dulu, Sekarang, dan di Masa yang Akan Datang, 1–4.

LAMPIRAN