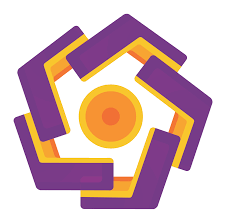
**LAPORAN FINAL PROJECT KRIPTOGRAFI**

**APLIKASI KRIPTOGRAFI BERBASIS PHP MENGGUNAKAN ALGORITMA SHIFT CAESAR DAN VIGENERE**



Disusun oleh :

Faisal Achmad Dwi Cahyono 14.11.7868

Didik Mardianto 14.11.7854

Arif Apriyatno 14.11.7867

Rizki Ramadhan 14.11.7813

Franssadea 14.11.7848

Yonanda Dwi Pratama 14.11.7849

Angga Destri Ulyadi 14.11.7847

**SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER**

**AMIKOM YOGYAKARTA**

**2012**

**DAFTAR ISI**

BAB I……………………………………………………………………………………………………3

* 1. Sejarah Kriptografi……………………………………………………………..3
  2. Tujuan Kriptografi………………………………………………………………4
  3. Terminologi Kriptografi………………………………………………………5
  4. Klasifikasi Algoritma Kriptografi………………………………………….6

BAB II…………………………………………………………………………………………………..8

* 1. Algoritma Shift Caesar………………………………………………………..8
  2. Algoritma Vigeneree…………………………………………………………..8

BAB III………………………………………………………………………………………………….9

ANALISA DAN PERANCANGAN APLIAKSI………………………………………………9

* 1. Analisis Aplikasi………………………………………………………………….9
     + 1. Analisis Kebutuhan Fungsional.…………………………………9
       2. Analisis Perangkat Lunak……….……..…………………………..9
  2. Flowchart Aplikasi…………………………………………………………….10
     1. Enkripsi & Dekripsi Shift Caesar……………………….10
     2. Enkripsi & Dekripsi Vigenere…..……………………….11

BAB IV………………………………………………………………………………………………..12

IMPLEMENTASI DAN PEMBAHASAN APLIKASI……………………………………12

* 1. Deskripsi Item…………………………………………………………………..12
  2. Uji Coba Aplikasi……………………………………………………………….12  
     BAB V…………………………………………………………………………………………………15

DAFTAR PUSTAKA………………………………………………………………………………16

**BAB I**

**PENDAHULUAN**

* 1. **Sejarah Kriptografi**

Kriptografi berasal berasal dari bahasa Yunani yaitu crypto berarti rahasia (secret) dan graphia berarti tulisan (writing). Menurut terminologinya kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika dikirim.

Sejak 4000 tahun lalu kriptografi telah dikenal oleh orang-orang Mesir lewat hieroglyph walaupun bukan dalam bentuk tulisan standard. Pada zaman Rumawi Kuno, Julius Caesar mengirimkan pesan rahasia kepada panglima perang di medan perang dengan mengganti semua susunan alfabet .

Dari : 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,

Menjadi : 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.

Pada zaman Rumawi Kuno, telah ada alat untuk mengirim pesan rahasia dengan nama Scytale yang digunakan oleh tentara Sparta. Scytale merupakan alat yang memiliki pita panjang dari daun papirus dan sebatang silinder. Pesan ditulis diatas pita yang dililitkan pada sebatang silinder, setelah itu pita dilepas dari batang silinder lalu dikirim. Untuk membaca pesan, pita tersebut dililitkan kembali pada sebatang silinder yang diameternya sama sehingga yang menjadi kunci pada Scytale adalah diameter silinder.

Seiring dengan perkembangan zaman, kriptografi mengalami pengembangan untuk menjaga kerahasiaan pesan (informasi) agar orang tidak berhak tidak dapat melihat/membaca pesan tersebut sehingga metode penyadian pesan semakin berkembang. Perkembangan teknologi yang begitu pesat memungkinkan manusia dapat berkomunikasi dan saling bertukar informasi/data secara jarak jauh. Antar kota antar wilayah antar negara bahkan antar benua bukan merupakan suatu kendala lagi dalam melakukan komunikasi dan pertukaran data. Seiring dengan itu tuntutan akan sekuritas (keamanan) terhadap kerahasiaan informasi yang saling dipertukarkan tersebut semakin meningkat. Begitu banyak pengguna seperti departemen pertahanan, suatu perusahaan atau bahkan individu-individu tidak ingin informasi yang disampaikannya diketahui oleh orang lain atau kompetitornya atau negara lain. Oleh karena itu dikembangkanlah cabang ilmu yang mempelajari tentang cara-cara pengamanan data atau dikenal dengan istilah Kriptografi. Dalam kriptografi terdapat dua konsep utama yakni enkripsi dan dekripsi. Enkripsi adalah proses dimana informasi/data yang hendak dikirim diubah menjadi bentuk yang hampir tidak dikenali sebagai informasi awalnya dengan menggunakan algoritma tertentu. Dekripsi adallah kebalikan dari enkripsi yaitu mengubah kembali bentuk tersamar tersebut menjadi informasi awal

* 1. **Tujuan Kriptografi**

Dalam teknologi informasi, telah dan sedang sedang dikembangkan cara cara untuk menangkal berbagai bentuk serangan semacam penyadapan dan pengubahan data yang dikirimkan. Salah satu cara yang ditempuh mengatasi masalah ini ialah dengan menggunakan kriptografi yang menggunakan transformasi data sehungga data yang dihasilkan tidak dapat dimengerti oleh pihak yang tidak berhak mengakses. Transformasi ini meberikan solusi pada dua macam masalah keamanan data, yaitu masalah privasi (privacy) dan keotentikan (authenticatioan). Privaci mengandung arti bahwa data yang diimkan hanya dapat dimengerti informasinya oleh penerima yang sah atau berhak. Sedangkan keotentikan mencegah pihak ketiga untuk mengirimkan data yang salah atau mengubah data yang dikirimkan.

Ada empat tujuan mendasar dari kriptografi yang juga merupakan aspek keamanan informasi, yaitu:

1. Kerahasiaan, adalah aspek yang berhubungan dengan penjagaan isi informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka informasi yang telah dienkripsi.
2. Integritas data, adalah aspek yang berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubsitusian data lain kedalam data yang sebenarnya
3. Autentikasi, adalah aspek yang berhubungan dengan identifikasi atau pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan harus diautentikasi keaslian, isi datanya, waktu pengiriman, dan lain-lain.
4. Non-repudiation (menolak penyangkalan), adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman suatu informasi oleh yang mengirimkan, atau harus dapat membuktikan bahwa suatu pesan berasal dari seseorang, apabila ia menyangkal mengirim informasi tersebut.
   1. **Terminiologi Kriptografi**

Kriptografi merupakan kumpulan teknik untuk Mengkode data dan pesan sedemikian sehingga data dan pesan tersebut dapat disimpan dan ditransmisikan dengan aman. Berikut ini beberapa terminologi dasar dari kriptografi serta hal-hal yang berkaitan dengan terminologi tersebut.

* Kriptografi dapat digunakan untuk meningkatkan keamanan komunikasi meskipun komunikasi tersebut dilakukan dengan media komunikasi yang sangat tidak aman (misalnya Internet). Kita juga dapat menggunakan kriptografi untuk melakukan enkripsi file-file sensitif kita, sehingga orang lain tidak dapat mengartikan data-data yang ada.
* Kriptografi dapat digunakan untuk memberikan jaminan integritas data serta menjaga kerahasiaan.
* Dengan menggunakan kriptografi, maka sangat mungkin untuk meverifikasi asal data dan pesan yang ada menggunakan digital signature.
* Pada saat menggunakan metoda kriptografi, hanya kunci sesi yang harus tetap dijaga kerahasiannya. Algoritma, ukuran kunci dan format file dapat dibaca oleh siapapun tanpa mempengaruhi keamanan.

Berikut ini istilah – istilah yang ada pada kriptografi :

* Plaintext yaitu informasi atau data yang dapat dibaca dan memiliki makna.
* Ciphertext yaitu plaintext atau pesan yang telah disandikan sehingga tidak dapat dibaca.
* Sender yaitu pengirim pesan.
* Receiver yaitu penerima pesan.
* Enkripsi yaitu proses penyandian dari plaintext menjadi ciphertext.
* Dekripsi yaitu proses pengembalian dari ciphertext menjadi plaintext.
* Algoritma kriptografi yaitu fungsi matematika yang digunakan untuk enkripsi dan dekripsi pesan.
  1. **Klasifikasi Algoritma Kriptografi**

Tingkat keamanan suatu algoritma diperoleh dengan menyembunyikan secara rahasia bagaimana algoritma itu bekerja, algoritma ini disebut dengan algoritma rahasia (restricted algorithm). Pada awalnya algoritma jenis ini yang berkembang, namun algoritma jenis ini mempunyai banyak kelemahan seperti setiap pengguna harus menggunakan algoritmanya sendiri dan jika algoritma ini telah diketahui orang, algoritma ini harus diganti dengan yang baru.

Kelemahan lain dari algoritma jenis ini adalah tidak memungkinkan dilakukan standardisasi sebagia kendali mutu, dimana setiap kelompok pengguna harus mempunyai algotima sendiri-sendiri dan unik.

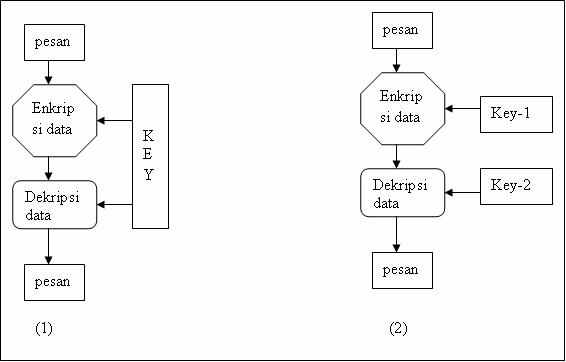
Kriptografi modern dapat memecahkan masalah algoritma tersebut diatas yaitu dengan algoritma kunci. Kunci ini dapat berupa sembarang dari suatu nilai dari sejumlah angka. Dengan demikian tingkat keamanan dari algoritma yang menggunakan kunci adalah berdasarkan kerahasiaan kuncinya, tidak berdasarkan detail dari algoritma itu sendiri. Oleh karena itu algoritma ini dapat dapat dipublikasikan dan dianalisa, dan algoritma ini dapat diproduksi secara masal.

Dewasa ini algoritma rahasia hanya digunakan terbatas pada aplikasi yang relatif kurang membutuhkan tingkat keamanan yang tinggi misalkan pada teknik pengacakan (scrembing) video, sedangkan algoritma algoritma kunci digunakan pada berbagai aplikasi yang membutuhkan tingkat keamanan yang sangat tinggi, misalkan pada kartu ATM dan secure mail.

Secara umum ada dua tipe algoritma yang berdasarkan kunci yaitu algoritma simetris (simetric algorithm) dan algoritma kunci publik (public-key algorithm). Perbedaan utama antara Symetric algorithm dengan public-key algoritm adalah pada kunci enkripsi

K1 dan kunci dekripsi K2 . Selain itu juga terdapat perbedaan dalam kecepatan proses dan keamananya.

Berikut ini bagan suatu sistem penyandian berdasarkan kunci beserta contoh-contoh algoritma yang digunakan.



**BAB II**

**DASAR TEORI**

* 1. **Algoritma Shift Cipher**

Teknik subsitusi shift cipher dengan modulus 26 dengan memberikan angka ke setiap alphabet.

seperti a=0, b=2, c=3,….,z=25.

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

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

Contoh :

Plaintext : “Lagi senang program”

Angka yang didapat P : “11 0 6 8 18 4 13 0 13 6 15 17 14 6 17 0 12”

Kalau key : 11

Angka C didapat :22 11 17 19 3 15 24 11 24 17 0 2 25 17 2 11 23

Kemudian angka hasil dikonver ke bentuk huruf, sehingga akan didapatkan ciphertext sebagai

berikut : WLRT DPYLYR ACZRCLX

* 1. **Algoritma Vigeneree**

Algoritma  Vigenere  termasuk  kode  abjad-majemuk (polyalphabetic  substitution cipher). Ide dasar menggunakan kode Kaisar, tetapi jumlah  pergeseran hurufnya berbeda-beda untuk setiap periode beberapa huruf  tertentu.

Algoritma abjad majemuk dibuat dibentuk dari kunci yang berbeda. Maksud dari kunci yang berbeda yaitu satu huruf dari plaintext menggunakan satu huruf kunci yang bersesuaian.

Contoh :

Plaintext : ABCDE

Key : KUNCI

Perhitungan :

(A+K) mod 26 = (0+10) mod 26 = 10 = K

(B+U) mod 26 = (1+20) mod 26 = 21 = V

(C+N) mod 26 = (2+13) mod 26 = 15 = P

(D+C) mod 26 = (3+2) mod 26 = 5 = F

(E+I) mod 26 = (4+8) mod 26 = 12 = M

Dari perhitungan diatas maka ciphertext : KVPFM

**BAB III**

**ANALISIS DAN PERANCANGAN APLIKASI**

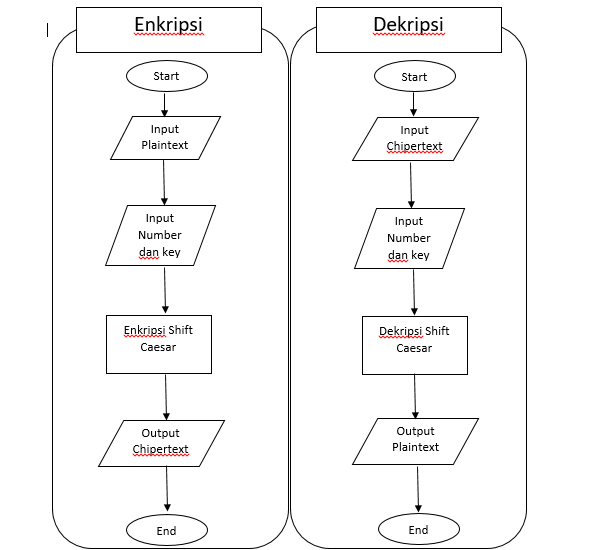
* 1. **Analisis Aplikasi**
     1. **Analisis Kebutuhan Fungsional**

Dengan aplikasi kriptografi ini, diharapkan dapat memenuhi kebutuhan fungsional yaitu enkripsi dan deskripsi pesan menggunakan algoritma Shift Caesar dan Vigenere.

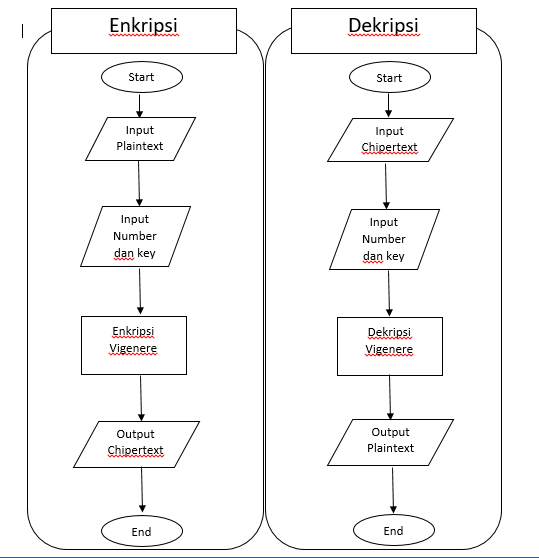
* + 1. **Kebutuhan Perangkat Lunak**

Kebutuhan perangkat lunak untuk pembuatan aplikasi kriptografi ini yaitu :

1. Notepad ++
2. Xampp
   1. **Flowchart Aplikasi**
      1. **Enkripsi & Dekripsi Shift Caesar**



* + 1. **Enkripsi & Dekripsi Vigenere**



**BAB IV**

**IMPLEMENTASI DAN PEMBAHASAN APLIKASI**

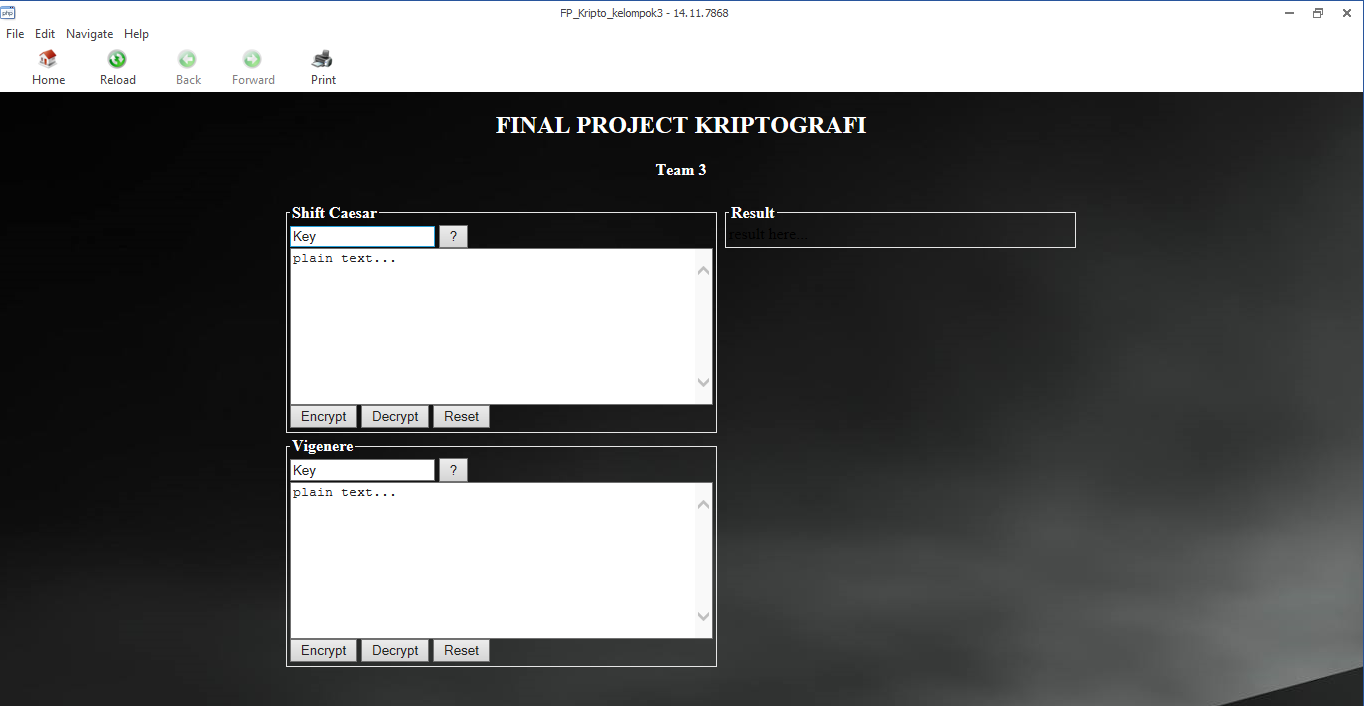
* 1. **Deskripsi Sistem**

Aplikasi kriptografi ini mendapat inputan berupa plaintext dan chipertext. Proses enkripsi aplikasi meminta inputan plaintext, number key dan text key. Proses dekripsi aplikasi meminta inputan chipertext, number key dan text key.

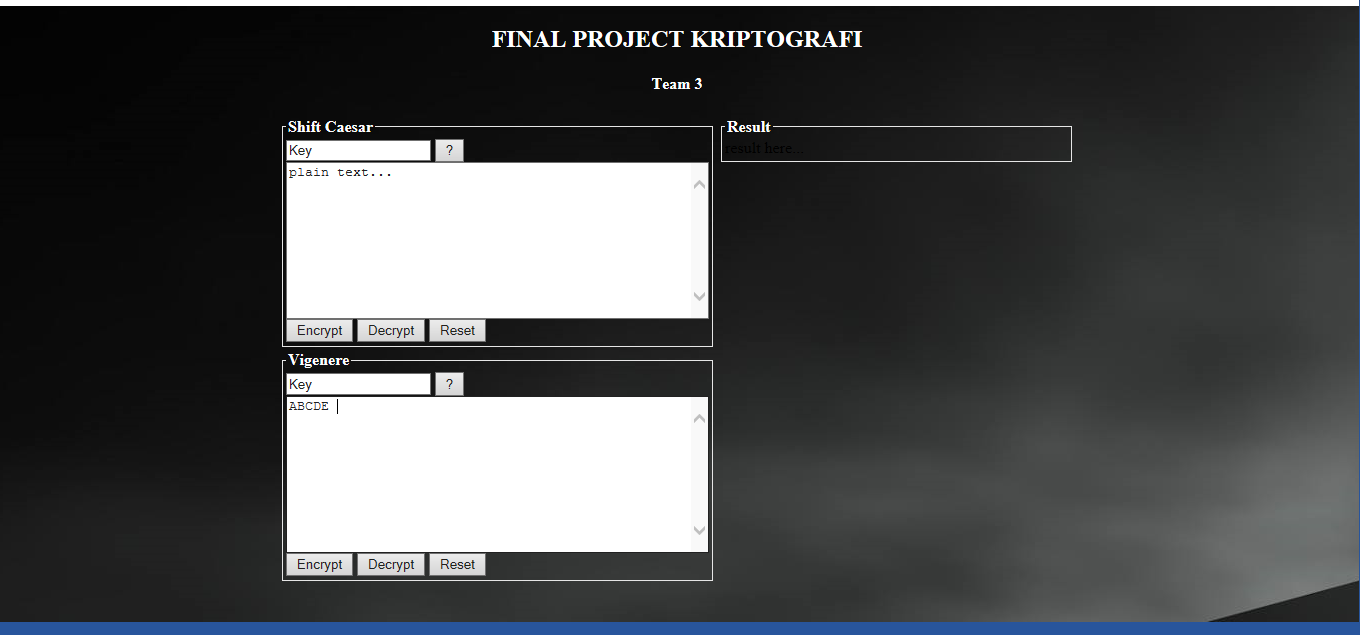
Number key digunakan untuk jumlah pergeseran karakter pada algoritma Shift Caesar, number key hanya bisa diisi dengan angka dari 1 sampai dengan 9. Sedangkan text key digunakan pada algoritma Vigenere, text key hanya bisa diisi dengan huruf tanpa ada spasi.

* 1. **Uji Coba Aplikasi**

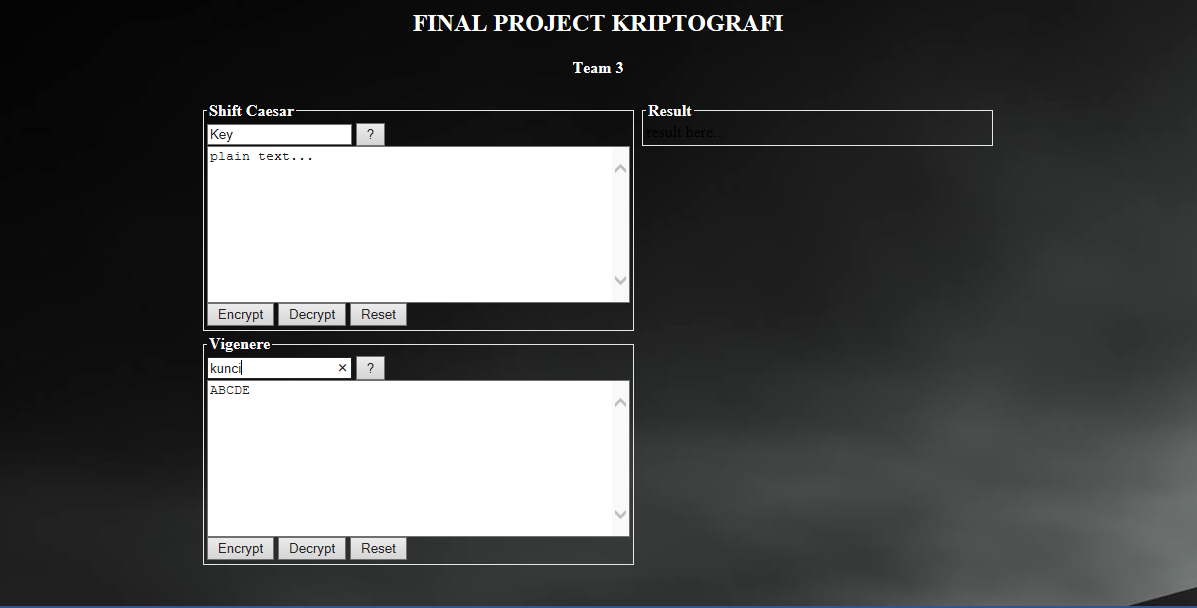
1. Tampilan Awal



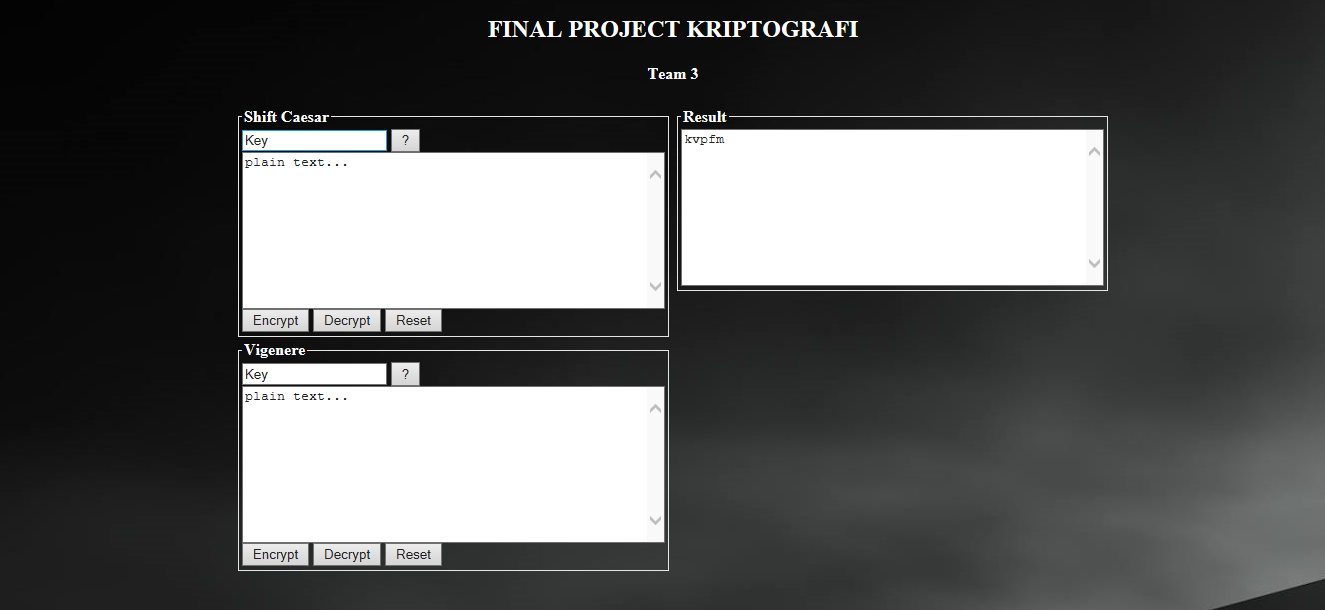
1. Input Plaintext



1. Input key



1. Klik Enkripsi / Dekripsi untuk mendapatkan chiper text



**BAB V**

**KESIMPULAN**

Aplikasi kriptografi ini menggunakan algoritma yaitu Shift Caesar, Vigenere. Aplikasikan dapat melakukan proses enkripsi dan dekripsi dengan menggunakan 2 algoritma diatas.

**DAFTAR PUSTAKA**

-Ariyus, Dony. 2008. Pengantar Ilmu KRIPTOGRAFI Teori, Analisi, dan Implementasi. Yogyakarta : Penerbit Andi.

- dosen.amikom.ac.id/index.php/profil/Salamah Permadyanti Putri, M.Kom