PENGAMANAN PESAN EMAIL DENGAN MENGGUNAKAN ALGORITMA CAESAR CHIPER , VIGENERE CIPHER DAN QR CODE BERBASIS WEB

Painem[1], Derian Rabbani[2]

[1, 2)]Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
Telp. (021) 5853753, Fax. (021) 5866369
[1] painem@budiluhur.ac.id, [2]derian.rabbani@gmail.com

ABSTRAK

Email merupakan sarana untuk mengirim pesan melalui jaringan internet. Pesan informasi yang dimaksud disini adalah berupa teks. Keamanan email sangat penting, apalagi jika emailnya sangat rahasia. Keamanan email belum tentu terjamin dan terjaga keaslian isi pesannya. Dan tidak jarang akun email seseorang menjadi kejahatan atas dunia maya, sehingga pesan informasi yang ada didalam email bisa diketahui oleh pihak-pihak yang tidak berkepentingan dan akan sangat merugikan. Untuk menjaga pesan email tersebut maka dibutuhkan pengaman pesan email sehingga pesan informasi yang dikirim melalui email akan aman sampai ke pihak penerima email atau pihak yang berkepentingan. Pengamanan pesan email dengan menggunakan algoritma Caesar Chiper, Vigenere Chiper dan QRCode. Dimana sebelum pesan email dalam bentuk teks (plainteks) tersebut sampai ke penerima email terlebih dahulu di rubah menjadi chiphertext atau isi email tersebut disandikan dalam bentuk lain yang tidak bisa dipahami oleh orang awam. Hanya penerima email yang bisa membuka isi email yang sudah disandikan tersebut. Ditambah lagi dengan QR Code untuk pengamanan kuncinya dari email yang akan di kirim. Sehingga email yang dikirim akan lebih dijamin keamanannya isi emailnya.

Kata Kunci : *Pengamanan email, Caesar Chiper, Vigenere Chiper, QR Code.*

I. PENDAHULUAN

Penggunaan internet baik di instansi pemerintah maupun swasta semakin meningkat. Salah satu dampak dari adanya internet adalah pengiriman pesan dengan menggunakan e-mail (Electronic mail) . Email adalah salah satu alat komunikasi dengan menggunakan jaringan internet. Dengan adanya email maka pesan akan sampai ke penerima dengan cepat, tidak membutuhkan biaya yang mahal. Namun pengiriman pesan dengan email saat ini belum tentu terjamin dan terjaga keaslian isi email sampai ke penerima email, karena adanya penyadapan terhadap isi email teks dari pihak-pihak yang tidak berkepentingan. Terkadang isi email sampai kepenerima sudah diubah oleh pihak-pihak yang tidak berkepentingan.

Berdasarkan latar belakang diatas maka dibutuhkan pengamanan isi email teks yang mampu mengamankan isi email dimana akan dapat melakukan enkripsi (merubah isi email menjadi sandi yang susah dibaca) terhadap pesan email sehingga memberikan keamanan yang lebih baik dalam berkomunikasi. Pengamanan isi email yang akan dibuta dengan menggunakan menggunakan algoritma Caesar Chiper, Vigenere Chiper dan Quick Read (QR) Code berbasis web.

II. LANDASAN TEORI

a. Algoritma Caesar Chiper

Dalam kriptografi, sandi caesar adalah salah satu tehnik enkripsi tertua. Sandi ini termasuk sandi subtitusi dimana setiap huruf pada plaintext digantikan oleh huruf lain yang memiliki selisih posisi tertentu dalam alphabet geseran. Nama Caesar diambil dari Julius Caesar, seorang pemimpin militer dan politikus Romawi. Julius Caesar menggunakan sandi ini untuk berkomunikasi dengan para panglimanya. Pada Perang Dunia I, Tentara Rusia menggunakan Caesar Cipher karena banyak ahli militer pada waktu itu tidak menguasai ilmu kriptografi yang lebih maju. Langkah enkripsi Caesar Cipher sering dijadikan bagian dari penyadian yang lebih rumit, seperti sandi vigenere. Inti dan cara kerja dari algoritma Caesar Cipher adalah melakukan pergeseran terhadap semua karakter pada plainteks dengan nilai pergeseran yang sama berdasarkan karakter pergeseran *(key)*. Adapun langkah-langkah yang dilakukan untuk membentuk *cipherteks* dengan Caesar Cipher adalah :

1) Menentukan besarnya pergeseran karakter *(key)* yang digunakan dalam membentuk cipherteks ke plaintext.
2) Menukarkan karakter pada plaintext menjadi *ciphertext* dengan berdasarkan pada pergeresaran yang ditentukan sebelumnya.

Secara matematis, enkripsi algoritma Caesar Cipher dapat dilakukan dengan cara menjumlahkan plaintext dengan kunci [1].

Ci = (Pi + Ki)

Dimana:
Ci : Nilai desimal karakter Ciphertext ke-i
Pi : Nilai desimal karakter Plaintext ke-i
Ki : Nilai desimal karakter Kunci ke-i
Nilai desimal karakter adalah A=0, B=1, C=2 ..., Z=25.

Lalu jika nilai **Ci** melebihi atau sama dengan jumlah karakter, maka nilai **Ci** akan dikurang dengan jumlah karakter [1].

Ci = (Ci – Jumlah Karakter)

Untuk proses dekripsi algoritma Caesar Cipher secara matematis, dapat dilakukan dengan cara mengkurangkan ciphertext dengan kunci [1].
Pi = (Ci - Ki)

Dimana:
Pi : Nilai desimal karakter Plaintext ke-i
Ci : Nilai desimal karakter Ciphertext ke-i
Ki : Nilai desimal karakter Kunci ke-i
Nilai desimal karakter adalah A=0, B=1, C=2 ..., Z=25.
Lalu jika nilai **Pi** kurang dari 0, maka nilai **Pi** akan ditambahkan dengan jumlah karakter [1].
Pi = (Pi + Jumlah Karakter)

b. Algoritma Vigenere Cipher

Algoritma Vigenere Cipher dikenal karena cara kerjanya mudah dimengerti dan dijalankan tetapi sulit untuk dipecahkan. Pada masa kejayaannya, sandi ini dijuluki "sandi yang tidak terpecahkan" (*Le Chiffre Indenchiffrable*). Hingga Matematikawan Charles Lutwidge Dodgson menyatakan bahwa algoritma ini tak terpecahkan. Metode Pemecah sandi ini baru ditemukan pada abad ke 19, tepatnya pada tahun 1854.

Charles Babbage menemukan cara untuk memecahkan sandi Vigenere. Metode ini dinamakan tes Kasiski karena Friedrich Kasiski adalah yang pertama mempublikasikannya. Vigenere Cipher sebenarnya merupakan pengembangan dari Caesar Cipher[2]. Pada Caesar Cipher, setiap huruf plaintext digantikan dengan huruf lain yang memiliki perbedaan tertentu pada urutan alfabet. Misalnya pada sandi Caesar dengan geseran 3, A menjadi D, B menjadi E and dan seterusnya. Sandi Vigenere terdiri dari beberapa sandi Caesar dengan nilai geseran yang berbeda. Untuk menyandikan suatu pesan, digunakan sebuah tabel alfabet yang disebut tabel Vigenere. Tabel Vigenère berisi alfabet yang dituliskan dalam 26 baris, masing-masing baris digeser satu urutan ke kiri dari baris sebelumnya, membentuk ke-26 kemungkinan sandi Caesar. Setiap huruf disandikan dengan menggunakan baris yang berbeda-beda disesuaikan dengan kata kunci. Kata kunci pada vigenere dibuat berulang sepanjang plaintext sehingga jumlah huruf pada kunci akan sama dengan jumlah huruf pada plaintext.

	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
S	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 1 : Tabel Bujursangkar Cipher (Tabule Rectura)

Tabel bujursangkar Vigenere digunakan untuk memperoleh ciphertext dengan menggunakan kunci yang sudah ditentukan sebelumnya. Jika panjang karakter kata kunci kurang dari panjang karater plaintext maka kata kunci akan diulang penggunaanya.

Selain menggunakan tabel bujursangkar vigenere, untuk melakukan enkripsi algoritma kriptografi vigenere cipher juga dapat dilakukan secara matematis, dengan menjumlahkan plaintext dengan kunci kemudian di modulo dengan jumlah karakter [3].

Ci = (Pi + Ki) mod (Jumlah Karakter)

Dimana:
Ci : Nilai desimal karakter Ciphertext ke-i
Pi : Nilai desimal karakter Plaintext ke-i
Ki : Nilai desimal karakter Kunci ke-i
Nilai desimal karakter adalah A=0, B=1, C=2 ..., Z=25.

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
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

Setiap hasil dari perhitungan proses enkripsi kemudian dirubah dan disesuaikan dengan nilai desimal karakter, setelah itu akan menghasilkan Ciphertext.

Lalu untuk melakukan dekripsi algoritma Vigenere Cipher secara matematis, dapat dilakukan dengan mengurangkan plaintext dengan kunci kemudian di modulo dengan jumlah karakter [3].

Pi = (Ci - Ki) mod (Jumlah Karakter)
Dimana:
Pi : Nilai desimal karakter Plaintext ke-i
Ci : Nilai desimal karakter Ciphertext ke-i
Ki : Nilai desimal karakter Kunci ke-i
Nilai desimal karakter adalah A=0, B=1, C=2 ..., Z=25.

Lalu jika nilai **Pi** kurang dari 0, maka nilai **Pi** akan ditambahkan dengan jumlah
karakter [3]

Pi = (Pi + Jumlah Karakter)

c. Quick Read (QR) Code

QR Code sebagai sebuah media yang dapat menyimpan informasi berupa url, teks hingga nomor telepon. Dapat dimaanfaatkan untuk menyimpan sebuah kunci yang dapat digunakan untuk melakukan enkripsi dan dekripsi dalam kriptografi. Dengan menggunakan QR Code sebagai kunci, akan memberikan keamanan yang lebih baik karena QR Code tidak akan dapat dibaca tanpa menggunakan aplikasi QR Code Scanner.

QR *Code* merupakan pengembangan dari *barcode* satu dimensi, QR *Code* salah satu tipe dari *barcode* yang dapat dibaca menggunakan kamera handphone[4]. Setiap versi simbol QR *Code* memiliki kapasitas data yang sesuai dengan jumlah data, jenis karakter dan tingkat kesalahan koreksi. Untuk pemeriksaan data dengan kapasitas maksimum ditentukan pada setiap versinya. Untuk versi dan kapasitas data maksimum, maka jumlah data dan modul akan meningkat sehingga simbol QR *Code* semakin besar[5]

Gambar 2 : Versi simbol QR Code

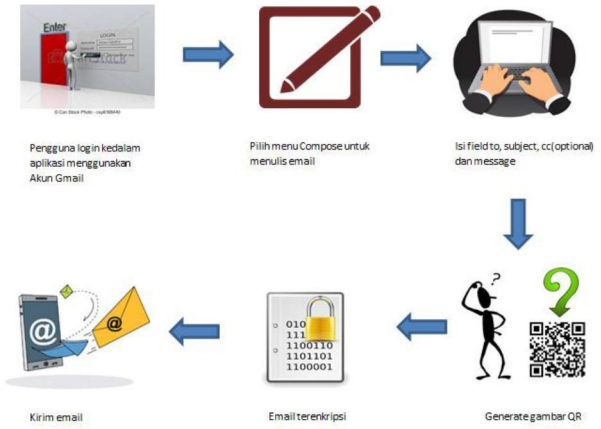
III. ARSITEKTUR APLIKASI

a. Arsitektur kirim email

Arsitektur alur proses kirim email berfungsi untuk menjelaskan proses bagaimana aplikasi mengirim sebuah email yang dimulai dari user melakukan login hingga email berhasil terkirim ke email yang dituju

Alur arsitektur proses kirim email :

1) User login kedalam aplikasi
2) Pilih menu Compose
3) Isikan to, subject, cc (optional) dan pesan email
4) Generate QR Code(Isi QR Code adalah 3 huruf pertama dan 3 huruf terakhir dari Subject)
5) Pesan email akan terenkripsi
6) Kirim email dengan pesan yang telah terenkripsi

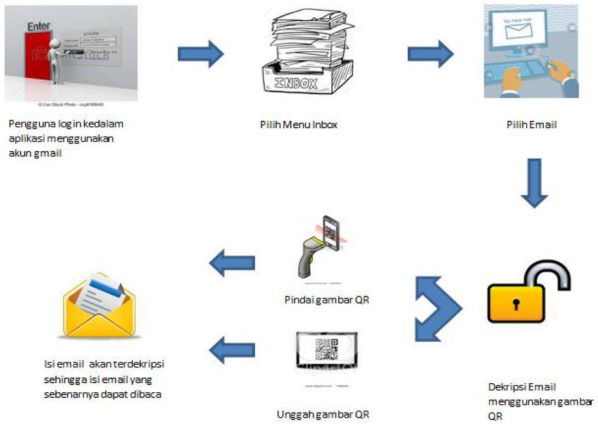


Gambar 3 : Arsitektur kirim email

b. Arsitektur baca email

Arsitektur alur proses baca email berfungsi untuk menjelaskan proses bagaimana aplikasi membaca sebuah email masuk yang terenkripsi hingga melakukan dekripsi pada isi email tersebut. Alur arsitektur proses baca email :

1) User login kedalam aplikasi
2) Pilih menu Inbox
3) Pilih email yang ingin dibaca.
4) Dekripsi email dengan menggunggah atau pindai QR Code
   a. Sistem akan melakukan pencocokan isi QR Code dengan kunci dari email. Jika benar, maka email akan terdekripsi
   b. Kunci dari email adalah 3 huruf pertama dan 3 huruf terakhir pada *subject* email.
5) Pesan email yang terdekripsi akan ditampilkan oleh aplikasi.

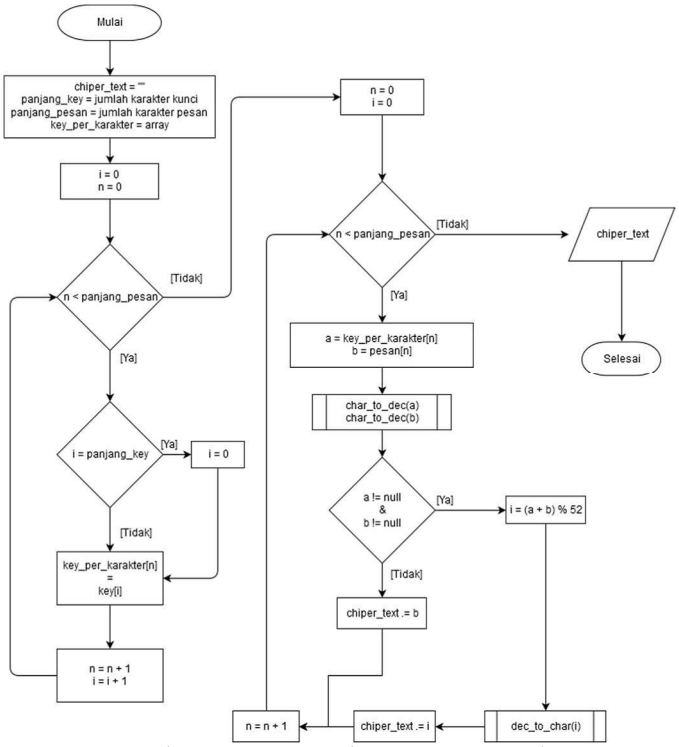


Gambar 4 : Arsitektur baca email

c. Flowchart Algoritma

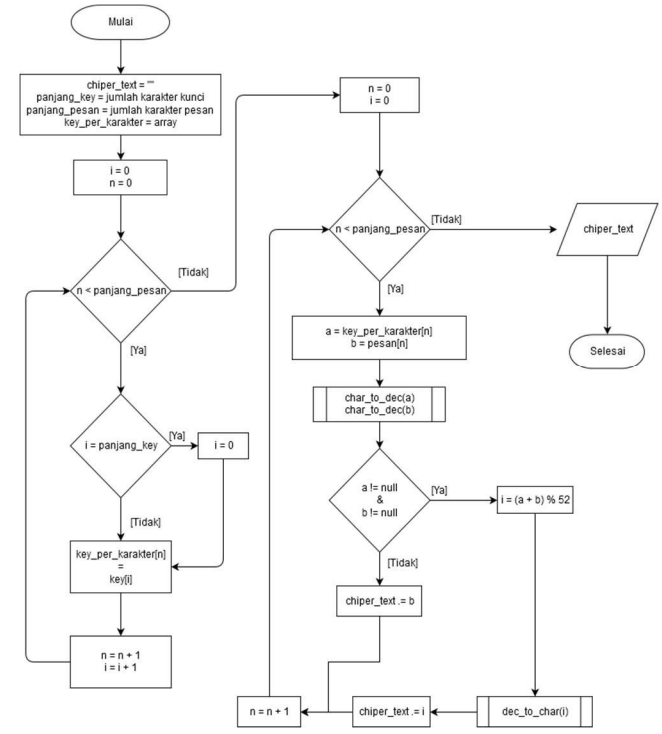
Berikut ini adalah *flowchart* yang digunakan untuk menelusuri proses algoritma *Caesar Cipher* dan *Vigenere Cipher* untuk proses enkripsi dan deskripsi

1) Enkripsi Caesar cipher



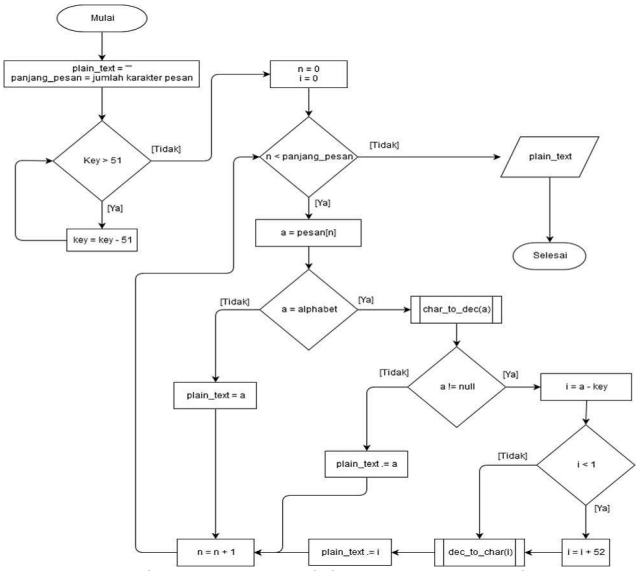
Gambar 5 : Proses enkripsi Caesar Cipher

2) Enkripsi Vigenere Chiper



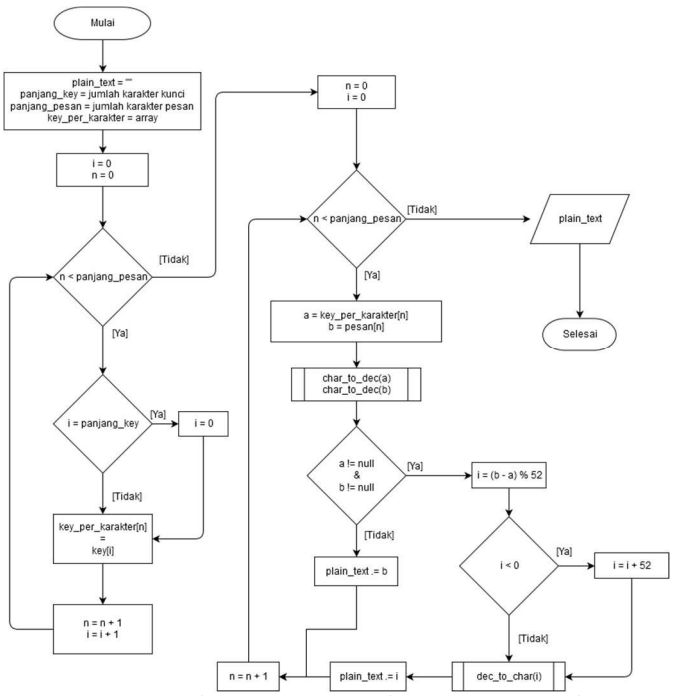
Gambar 5 : Proses Enkripsi Vigenere Chiper

3) Dekripsi Caesar Cipher



Gambar 6 : Proses dekripsi Caesar Cipher

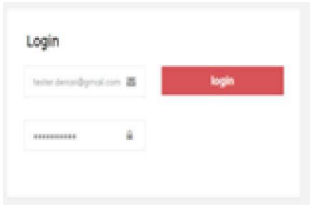
4) Dekripsi Vigenere Chiper



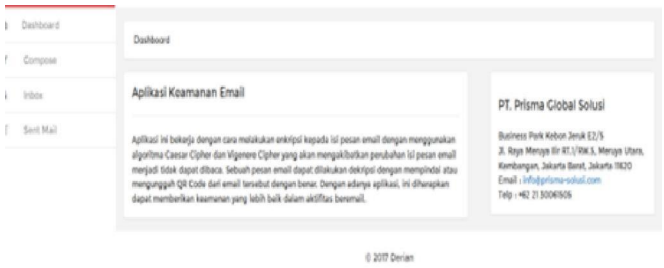
Gambar 7 : Proses Enkripsi Vigenere Chiper

d. Prototype Aplikasi

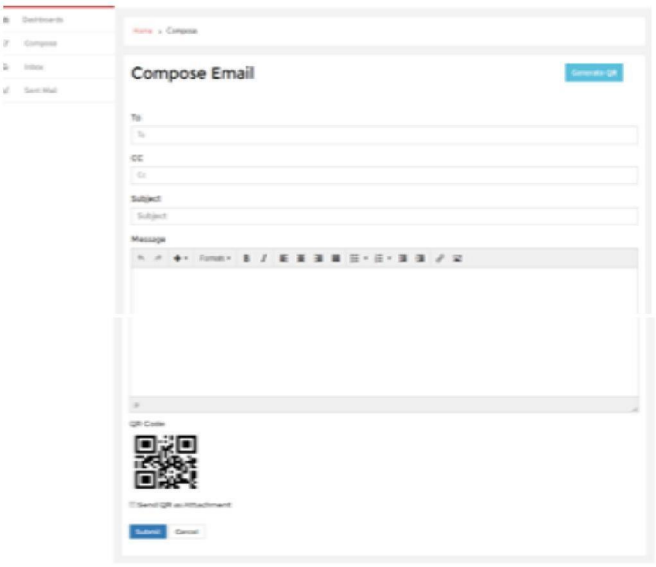
Berikut ini akan diberikan gambaran mengenai tampilan-tampilan yang ada pada aplikasi kemanan *email* ini.



Gambar 8 : Form Login



Gambar 9 : : Tampilan Menu Dashboard



Gambar 10 : : Tampilan Menu Compose

IV. KESIMPULAN

Berdasarkan hasil analisa yang telah dilakukan terhadap permasalahan maka kesimpulan yang di dapat adalah sebagai berikut :.

a. Algoritma Caesar Cipher dan Vigenere Cipher berhasil mengamankan isi pesan yang terdapat pada email sehingga tidak dapat dibaca oleh pihak – pihak yang tidak berkepentingan.
b. Isi email tidak dapat dibaca oleh pengguna tanpa masuk kedalam aplikasi lalu memindai atau mengunggah QR Code yang benar untuk email tersebut karena pada layanan email biasa tidak adanya proses dekripsi, sehingga keamanan informasi dapat terjaga

DAFTAR PUSTAKA

[1] Sweigart, Al. 2013. Hacking Secret Ciphers with Python. North Charleston USA: CreateSpace.

[2] Sadikin, Rofki. 2012. Kriptografi untuk keamanan jaringan. Yogyakarta: CV Andi Offset. [2] Ariyus, Dony 2008, Pengantar Ilmu Kriptografi Teori, Analisis, dan Implementasi, Yogyakarta: Andi Offset.

[3] Hidayatulloh, Mahmud dan Entik Insannudin. 2014. Enkripsi dan Dekripsi Menggunakan Vigenere Cipher ASCII Java. Bandung: UIN Bandung.

[4] Rouillard, J., 2008, *Contextual QR Codes, Proceedings* of *the Third International Multi - Conference on Computing in the Global Information Technology*, ICCGI, Athens, Greece

[5] Rahmawati, Anita., Rahman, Arif. 2011. *Sietem Pengamanan Keaslian Ijasah Menggunakan QR-Code dan Algoritma Base64.* Universitas Ahmad Dahlan