

**PENGIRIMAN PESAN EMAIL RAHASIA MENGGUNAKAN  
ALGORITMA RSA DAN ALGORITMA  
MODIFIKASI VIGENERE**

**NASKAH PUBLIKASI**



diajukan oleh

**Levi Yolanza**

**14.11.8432**

kepada  
**FAKULTAS ILMU KOMPUTER  
UNIVERSITAS AMIKOM YOGYAKARTA  
YOGYAKARTA  
2017**

**NASKAH PUBLIKASI**

**PENGIRIMAN PESAN EMAIL RAHASIA MENGGUNAKAN  
ALGORITMA RSA DAN ALGORITMA  
MODIFIKASI VIGENERE**

yang dipersiapkan dan disusun oleh

**Levi Yolanza**

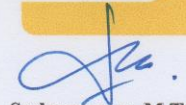
**14.11.8432**

**Dosen Pembimbing**

  
**Hartatik, S.T., M.Cs**  
**NIK. 190302232**

Tanggal, 26 Agustus 2017

**Ketua Program Studi  
S1 - Informatika**

  
**Sudarmawan, M.T**  
**NIK. 190302035**

# PENGIRIMAN PESAN EMAIL RAHASIA MENGGUNAKAN ALGORITMA RSA DAN ALGORITMA MODIFIKASI VIGENERE

Levi Yolanza<sup>1)</sup>, Hartatik<sup>2)</sup>,

<sup>1)</sup> Informatika Universitas AMIKOM Yogyakarta

<sup>2)</sup> Magister Ilmu Komputer Universitas Gadjah Mada Yogyakarta

Jl Ringroad Utara, Condongcatur, Depok, Sleman, Yogyakarta Indonesia 55283

Email : levi8432@students.amikom.ac.id<sup>1)</sup>, hartatik@amikom.ac.id<sup>2)</sup>

**Abstract** - *Advances in information technology now provides a lot of convenience to the community, especially in the message delivery method. E-mail (electronic mail) is one of method of delivery that has been commonly used in the community to send a message, but when sending email messages in plain (without encryption) still create an information security be easily identified. It would be a disadvantage if a confidential information to be known by others, therefore, to keep a message safe, it needs an encryption cryptographic techniques. Cryptography, a technique of changing a message so that the message can not be read when opening the message if the reader does not know the terms (key) that must be met first.*

*Vigenere and RSA are algorithms selected to design an application that allows to perform cryptographic encryption of the email. Vigenere is the main algorithm used to perform encryption techniques, but the results of the encryption vigenere will be modified with emoji characters, so that the encryption result looks even more vague. The RSA algorithm itself serves as encrypted key used to encrypt the vigenere algorithm. With the application of double encryption on email, the confidentiality of the information can be more safe and not easy to be known by others.*

**Keywords** – Email, Cryptography, Vigenere Algorithms, RSA Algorithms

## 1. Pendahuluan

### 1.1 Latar Belakang

Kebutuhan untuk berbagi informasi secara mudah terus dikembangkan teknologinya hingga saat ini. Banyaknya aplikasi pengiriman pesan secara instan dan gratis memberikan kemudahan yang sangat bermanfaat bagi masyarakat untuk saling berbagi informasi. Salah satu metode pengiriman pesan yang banyak digunakan oleh masyarakat hingga saat ini adalah pengiriman pesan melalui e-mail.

E-mail (Electronic Mail) merupakan surat elektronik yang digunakan sebagai sarana menerima dan mengirim surat melalui jalur internet atau bisa juga diartikan surat dengan format digital (ditulis dengan menggunakan komputer atau gadget yang telah mendukung aplikasi e-mail) dan dikirimkan melalui jaringan Internet. Namun keamanan

pesan yang dikirimkan secara terbuka (tanpa adanya pengubahan/enkripsi) menjadikan beberapa pesan yang seharusnya dirahasiakan menjadi mudah untuk diartikan sebagai suatu tujuan atau kalimat yang sesungguhnya.

Menjadi sebuah kerugian jika suatu informasi yang sangat penting bisa diketahui oleh pihak-pihak yang tidak berkepentingan, hal itu pernah terjadi pada sebuah perusahaan besar di Indonesia.

Pada tahun 2012 terjadi sebuah kasus pembobolan email pada grup Bakrie Tbk. Kasus yang pernah diselidiki oleh kepolisian Indonesia ini diduga dilakukan dengan sengaja oleh hacker untuk mencuri suatu informasi, menurut Karopenmas Polri Brigjen Boy Rafli Umar, kasus tersebut sudah ditangani oleh tim cyber Polda. "Dari laporan awal yang diterima sepertinya ada dugaan tindak pidana ITE (Informasi dan Transaksi Elektronik), sebagaimana diatur UU 11/2008, saat ini sedang ditelusuri," ujar Boy, kepada wartawan, Rabu (12/12/2012). [1]

Oleh karena itu pada penelitian kali ini peneliti akan mencoba untuk merancang suatu aplikasi yang mendukung enkripsi kriptografi pada pengiriman pesan melalui e-mail. Pada penelitian ini peneliti akan mencoba membuat sebuah aplikasi enkripsi pesan email dengan menerapkan dua algoritma yaitu Vigenere dan RSA (Rivest, Shamir, Adleman), diharapkan hasil dari penelitian ini dapat mendukung keamanan komunikasi yang menggunakan fasilitas email sebagai media pengirimnya..

### 1.2 Rumusan Masalah

Berdasar latar belakang yang telah peneliti tuliskan maka dari itu rumusan masalah pada penelitian ini adalah : Bagaimana merancang dan menggabungkan dua algoritma kriptografi yaitu Vigenere dan RSA pada sebuah aplikasi pengiriman pesan e-mail ?

### 1.3 Batasan Masalah

Batasan masalah yang diterapkan pada aplikasi enkripsi pesan e-mail dengan algoritma kriptografi Vigenere dan RSA adalah sebagai berikut :

1. Algoritma yang diterapkan pada aplikasi untuk enkripsi adalah Vigenere Chipper dan RSA.
2. Aplikasi hanya mendukung untuk pengiriman pesan melalui e-mail.

3. Karakter emotikon hanya akan menggantikan bentuk dari huruf dan angka.
4. Pengujian bilangan prima yang dipakai adalah Fermat's Little Theorem.
5. Aplikasi ini dibangun dengan bahasa pemrograman Java Script dan PHP.

#### 1.4 Tujuan

Adapun tujuan yang ingin dicapai dari penelitian ini adalah sebagai berikut :

1. Merancang sebuah aplikasi pengiriman pesan e-mail dengan enkripsi kriptografi
2. Mencoba untuk mengkombinasikan dua algoritma kriptografi yaitu algoritma RSA dan Vigenere.
3. Mencoba untuk memodifikasi hasil enkripsi pesan pada algoritma Vigenere chipper dengan emotikon

#### 1.5 Manfaat

Adapun manfaat yang ingin dicapai dari penelitian ini adalah sebagai berikut :

1. Menambah pengetahuan peneliti pada bidang kriptografi khususnya pada algoritma Vigenre dan RSA.
2. Membuat inovasi baru pada bidang kriptografi.
3. Menjadi referensi untuk penelitian selanjutnya pada bidang kriptografi.
4. Dengan adanya aplikasi untuk enskripsi pesan berbasis e-mail ini diharapkan pengguna dapat menerapkannya untuk meningkatkan penjagaan dan kerahasiaan pesan yang akan dikirimkan.

## 2. Landasan Teori

### 2.1 Email

Email merupakan sebuah layanan berupa pesan surat elektronik dengan format tertentu yang diterima dan dikirim melalui jaringan internet dengan aturan tertentu.

(David Alex Lamb, 1999) Dalam proses pengiriman dan penerimaan email terdapat beberapa elemen yang sangat berpengaruh terhadap proses tersebut. Elemen-elemen yang dimaksud adalah :

1. Sender, merupakan orang yang menyusun dan mengirimkan email.
2. Mail agent, merupakan perangkat lunak yang digunakan oleh pengirim untuk melakukan penyusunan email.
3. Message, merupakan representasi komputer dari apa yang ingin disampaikan oleh pengirim.
4. Email transport subsystem, merupakan sebuah sistem yang menangani transportasi email.
5. Receiver, merupakan tujuan atau orang yang menerima email.
6. Email agent software, merupakan sebuah perangkat lunak yang digunakan untuk membaca email.
7. Email address, merupakan sekumpulan karakter yang digunakan untuk mengenali pengirim dan penerima.

### 2.2 Kriptografi

Kriptografi berasal dari bahasa Yunani, crypto dan graphia. Crypto berarti secret (rahasia) dan graphia berarti writing

(tulisan). Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat yang lain. [2]

#### 2.2.1 Tujuan Kriptografi

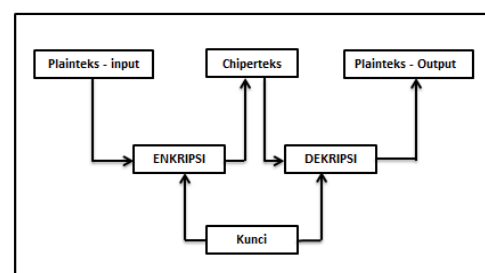
Kriptografi bertujuan untuk memberi layanan keamanan. Yang dimaksud dari aspek-aspek keamanan adalah sebagai berikut : [3]

1. Kerahasiaan (*Confidentiality*)  
Adalah layanan yang ditujukan untuk menjaga isi informasi dari siapapun kecuali yang memiliki otoritas.
2. Integritas Data (*Data Integrity*)  
Adalah layanan yang berhubungan dengan penjagaan dari perubahan data secara tidak sah.
3. Otentikasi (*Authentication*)  
Adalah layanan yang berhubungan dengan identifikasi, baik secara kesatuan sistem maupun informasi itu sendiri.
4. Penyangkalan (*Non-repudiation*)  
Adalah layanan untuk menjaga entitas yang berkomunikasi melakukan penyangkalan, yaitu pengirim pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan.

#### 2.2.2 Jenis-jenis Algoritma Kriptografi

##### 1. Algoritma Simetris

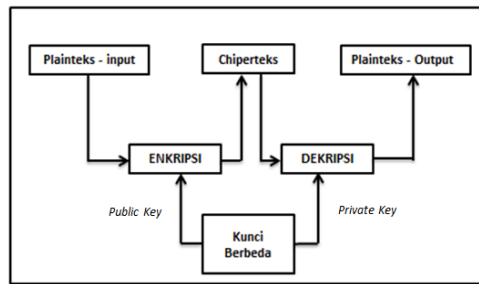
Algoritma simetris adalah algoritma yang menggunakan kunci yang sama untuk enkripsi dan dekripsinya, contoh : Alice ingin mengirimkan pesan x dengan aman menggunakan saluran umum kepada Bob. Alice menggunakan kunci x yang sebelumnya telah disepakati oleh Alice dan Bob. Untuk mengirim pesan e x (x) kepada Bob, dia akan mendeskripsikan teks-kode yang diterima dengan kunci yang sama dengan yang digunakan untuk memperoleh akses ke pesan yang diterima[2]



**Gambar 1** Skema Algoritma Simetris

##### 2. Algoritma Asimetris

Algoritma asimetris adalah pasangan kunci kriptografi yang salah satunya digunakan untuk proses enkripsi dan yang satunya lagi untuk dekripsi. Semua orang yang mendapatkan kunci publik dapat menggunakannya untuk mengenkripsi pesan, sedangkan hanya satu orang saja yang memiliki kunci rahasia untuk melakukan pembongkaran terhadap kode yang dikirimkan.[2]



Gambar 2 Skema Algoritma Asimetris

### 2.2.3 Algoritma Vigenere

(Dony Ariyus, 2006) vigenere chiper merupakan salah satu algoritma klasik dengan teknik substitusi. Nama vigenere diambil dari seorang yang bernama Blaise de Vigenere, Vigenere Chiper mungkin adalah contoh terbaik dari chipper alphabet-majemuk manual.[4]

Rumus Enkripsi Vigenere :

$$C_i = (P_i + K_i) \bmod 26$$

Rumus Dekripsi Vigenere :

$$P_i = (C_i - K_i) \bmod 26$$

Dimana :

$C_i$  = Nilai desimal karakter chiperteks ke-1

$P_i$  = Nilai desimal karakter plainteks ke-1

$K_i$  = Nilai Desimal karakter kunci ke-1

### 2.2.4 Algoritma RSA

Algoritma RSA melakukan pemfaktoran bilangan yang sangat besar, oleh karena alasan tersebut RSA dianggap aman. Untuk membangkitkan kedua kunci, yang dipilih dua bilangan prima acak yang besar. Skema yang dikembangkan oleh Rivest, Shamir dan Adleman yang mengekspresikan bahwa plainteks dienkripsi menjadi blok-blok yang setiap blok memiliki nilai bilangan biner yang diberi simbol "n", plainteks blok "M" dan chiperteks blok "C".[4]

Pembangkit Kunci RSA :

$$N = p \times q$$

$$(n) = (p - 1) \cdot (q - 1)$$

$$\Phi(n), \gcd(e, \Phi(n)) = 1$$

$$d = e^{-1} \text{ pada } Z(n)$$

$$K_{\text{publik}} = (e, n), K_{\text{privat}} = d$$

Rumus Enkripsi RSA :

$$\text{Input : } K_{\text{public}} = (e, n) \quad P \in Z_n$$

$$\text{Output : } C \in Z_n$$

$$C = P^e \bmod n$$

Rumus Dekripsi RSA :

$$\text{Input : } K_{\text{private}} = d, K_{\text{public}} = (e, n) \quad P \in Z_n$$

$$\text{Output : } P \in Z_n$$

$$P = C^d \bmod n$$

### 2.2.5 Emoji Emotikon

Emoji pertama diciptakan pada tahun 1998 atau 1999 oleh Shigetaka Kurita, yang merupakan bagian dari tim yang sedang mengerjakan platform Internet seluler i-mode milik NTT DoCoMo. Set pertama 172 emoji 12×12 piksel diciptakan sebagai bagian dari fitur perpesanan i-mode untuk membantu memfasilitasi komunikasi elektronik, dan berfungsi sebagai fitur yang membedakannya dari layanan lain. [5]

## 3. Analisis Dan Perancangan

### 3.1 Analisis SWOT

Tabel 1 Analisis SWOT

	INTERNAL	Strength (Kekuatan)	Weakness (Kelemahan)
	EKSTERNAL	<ol style="list-style-type: none"><li>1. Enkripsi/Denkripsi</li><li>2. Menggunakan 2 Algoritma Vigenere dan RSA</li><li>3. Modifikasi hasil enkripsi</li><li>4. Lebih aman dalam menyampaikan pesan</li></ol>	<ol style="list-style-type: none"><li>1. Penggunaan cukup rumit</li><li>2. Kesulitan bagi yang tidak mengenal kriptografi</li></ol>
Opportunity (Peluang)	<ol style="list-style-type: none"><li>1. Banyaknya pengguna <i>email</i></li><li>2. Ditujukan untuk yang membutuhkan privasi saat berbagi pesan</li></ol>	Strength – Opportunity	Weakness– Opportunity
		<ol style="list-style-type: none"><li>1. Dengan banyaknya pengguna <i>email</i> sebagai media untuk bertukar pesan maka dibuatlah sebuah aplikasi untuk mengamankan isi pesan dengan metode enkripsi kriptografi menggunakan dua algoritma</li></ol>	<ol style="list-style-type: none"><li>1. Dengan tingkat keamanan yang tinggi, sehingga untuk para pengguna awam yang tidak mengenal ilmu kriptografi dapat menggunakannya dengan maksimal untuk mendapatkan tingkat privasi yang tinggi</li></ol>
Threats (Ancaman)	<ol style="list-style-type: none"><li>1. Berkurangnya penggunaan <i>email</i> sebagai sarana pengiriman pesan</li></ol>	Strength– Threats	Weakness– Threats
		<ol style="list-style-type: none"><li>1. Dengan tidak banyaknya aplikasi yang digunakan, maka fungsionalitas pengamanan data adalah satu cara yang tepat</li></ol>	<ol style="list-style-type: none"><li>1. Maka dari itu dapat dilakukan pembahasan pada tampilan serta <i>function</i> agar mempermudah serta selalu dapat diperbarui.</li></ol>

### 3.2 Kebutuhan Fungsional

kebutuhan fungsional berisi tentang paparan proses-proses apa saja yang nantinya akan dilakukan oleh aplikasi atau paparan mengenai fitur-fitur yang akan digunakan di dalam aplikasi yang akan dibuat.

1. Pengguna dapat melakukan registrasi data agar dapat menggunakan aplikasi.
2. Pengguna dapat melakukan pencarian kunci publik dan kunci rahasia RSA pada aplikasi
3. Pengguna dapat melakukan enkripsi pesan email dan mengirimkannya langsung dari aplikasi
4. Pengguna dapat melakukan dekripsi pesan yang telah dienkripsi sebelumnya pada aplikasi.
5. Pengguna dapat melihat history pesan yang pernah dikirimkan melalui aplikasi.



### 3.3 Kebutuhan Non-Fungsional

#### 3.3.1 Kebutuhan Hardware

**Tabel 2** Kebutuhan Hardware

Hardware	Spesifikasi
Central Processing Unit (CPU)	Intel Core™2 Processor (3.00 GHz, 0.8500V-1.3625V, Socket LGA775)
Random Access Memory (RAM)	V-Gen DDR 2 (2 GB, PC-6400, 800Mhz)
Hard Disc (HDD)	Seagate (320 GB, +12V – 0.52A)

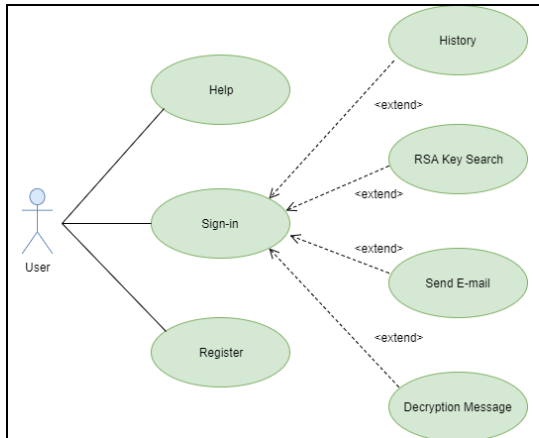
#### 3.3.2 Kebutuhan Software

**Tabel 3** Kebutuhan Software

Software	Spesifikasi
Operating system	Windows 10 Enterprise 32 bit
Text Editor	Sublime Text 3
Web Server	XAMPP V3.2.2
Brwoser	Google Chrome
Bahasa Program	HTML, CSS 3,PHP 5.5, SQL

#### 3.4 Use Case

Use Case akan menggambarkan hal apa yang dapat dilakukan aplikasi yang akan dibangun dan siapa saja yang akan berinteraksi dengan aplikasi.



**Gambar 3** Use Case Diagram

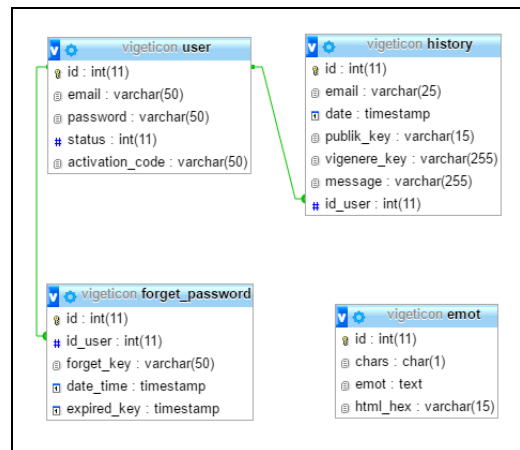
Dari gambar use case diatas dapat dilihat bahwa untuk mendapatkan fasilitas dari aplikasi, seorang user terlebih dahulu harus melakukan sign-in pada aplikasi dan untuk bisa sign-in seorang user terlebih dahulu harus melakukan register atau membuat akun dengan menggunakan email dari pemilik akun itu sendiri.

## 4. Implementasi Dan Pembahasan

### 4.1 Pembahasan Database

Database dibuat dengan menggunakan phpMyAdmin karena telah dilengkapi tampilan grafis yang dapat memudahkan pengguna dalam mengolah database. Berikut

merupakan tam pilan tabel yang telah dibuat berikut dengan relasinya



**Gambar 4** Tabel Relasi

### 4.2 Pembahasan Interface

#### 1. Halaman Home

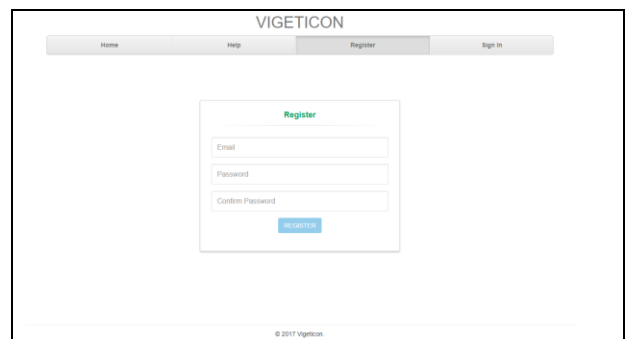
Halaman utama (home) merupakan halaman yang pertama kali akan dilihat oleh pengunjung saat pengunjung mengakses website ini.



**Gambar 5** Interface Home

#### 2. Halaman Register

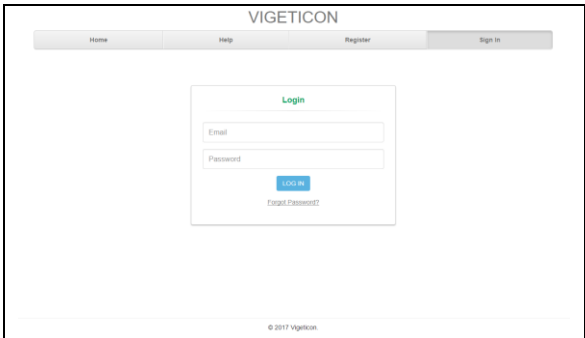
Halaman registrasi adalah halaman yang disediakan oleh peneliti agar pengguna aplikasi dapat mendaftarkan akun yang akan dibuat dan digunakan selama pengguna membutuhkan aplikasi



**Gambar 6** Interface Register

#### 3. Halaman Sign-in

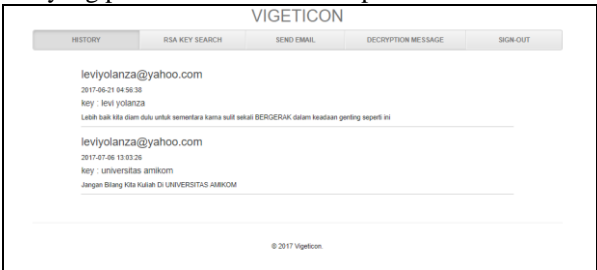
Halaman form sign-in merupakan halaman yang dirancang untuk pengguna agar pengguna dapat mengakses akun yang telah terlebih dahulu dibuat



Gambar 6 Interface Sign-in

#### 4. Halaman History

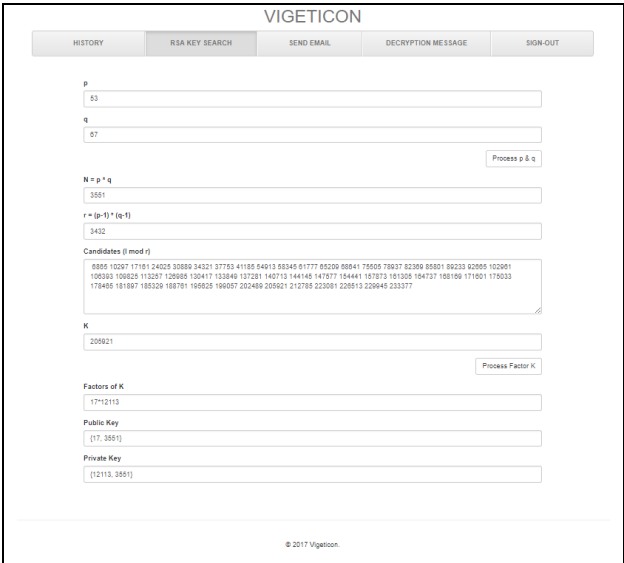
Tampilan history pesan merupakan bagian dari aplikasi dimana pada bagian ini aplikasi akan menyimpan semua pesan yang pernah dikirimkan oleh pemilik akun



Gambar 7 Interface History

#### 5. Halaman RSA Key Search

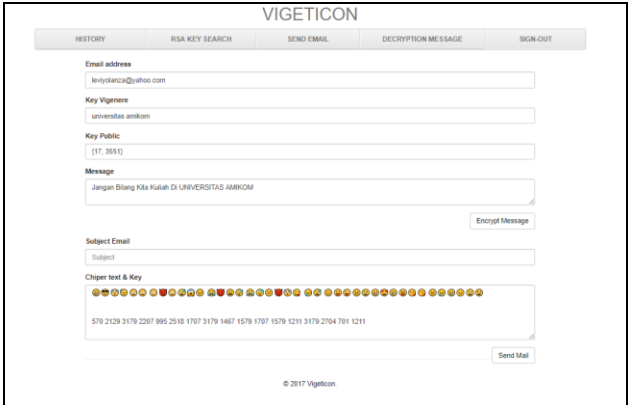
Halaman pencarian kunci RSA merupakan halaman yang disediakan untuk melakukan tahap awal peng-enkripsian pesan email. Pada halan ini pengguna akan melakukan pembangkitan kunci RSA untuk mendapatkan kunci publik dan kunci rahasia yang nantinya akan digunakan pada tahap peng-enkripsian pesan email



Gambar 8 Interface RSA Key Search

#### 6. Halaman Send Email

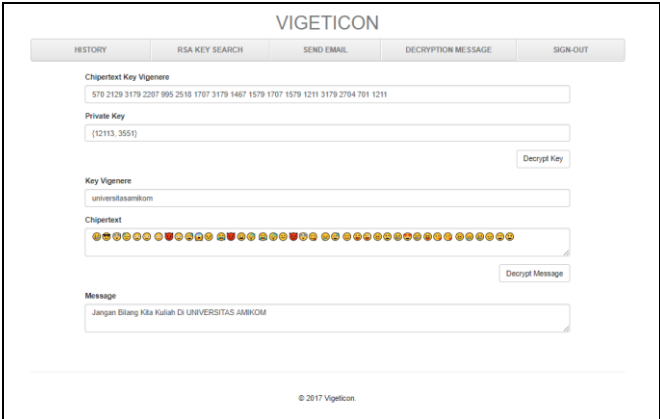
Pada halaman ini pengguna akan memasukkan setiap variabel yang dibutuhkan oleh aplikasi untuk melakukan proses peng-enkripsian.



Gambar 9 Interface Send Email

#### 7. Halaman Decryption Message

Halaman dekripsi pesan dibuat untuk menerjemahkan pesan yang telah dienkripsi sebelumnya agar dapat dimengerti isi dari pesan yang telah dikirimkan oleh pengirim sebelumnya, pada halaman ini penerima harus mempunyai pasangan kunci RSA untuk mengetahui terjemahan dari kunci vigenere yang digunakan untuk meng-enkripsi pesan asli atau plainteks.



Gambar 9 Interface Decryption Message

#### 4.3 Pengujian Waktu Eksekusi

Pengujian waktu eksekusi adalah pengujian untuk melihat lama dari waktu program mengeluarkan hasil dari proses sistem yang di bangun berdasarkan jumlah data yang dimasukkan. Pada pengujian ini percobaan pada pengujian dilakukan sebanyak 10 kali pada masing masing nilai/jumlah data, berikut merupakan hasil dari pengujian waktu eksekusi aplikasi vigeticon :

#### 1. Pengujian eksekusi p dan q pada halaman RSA Key Search

**Tabel 4** Pengujian Waktu Eksekusi p dan q

p	q	Time Execute
7	11	0.034
19	23	0.20
37	41	0.75
71	73	1.42
89	97	3.04
107	109	4.06
149	151	11.92

## 2. Pengujian Enkripsi pesan pada halaman Send Email

**Tabel 5** Pengujian Waktu Eksekusi Enkripsi

Jumlah Karakter	Time Execute
100	0.0004
200	0.0005
400	0.0007
800	0.0013
1000	0.0015
2000	0.0030
4000	0.0061
8000	0.016

## 3. Pengujian Dekripsi pesan pada halaman Decryption Message

**Tabel 4** Pengujian Waktu Eksekusi Dekripsi

Jumlah Karakter	Time Execute
100	0.0004
200	0.0006
400	0.0013
800	0.0026
1000	0.0032
2000	0.0066
4000	0.014
8000	0.026

## 5. Penutup

### 5.1 Kesimpulan

Berdasarkan pembahasan serta penjelasan yang dipaparkan pada bab-bab sebelumnya hingga sampai pada tahap implementasi dan perancangan program, maka dapat disimpulkan sebagai berikut :

1. Website vigeticon dapat dijadikan pilihan jika dalam komunikasi via email user menginginkan privasi yang lebih dari biasanya karna website vigeticon mampu mengenkripsi dan mendekripsi pesan yang dikirim via email.
2. Implementasi algoritma RSA dibuat dengan JavaScript, sehingga proses faktorisasi kunci public dan kunci private tidak membutuhkan waktu yang lama pada sisi user.
3. Implementasi algoritma Vigenere dan proses convert ke emoji dilakukan dengan PHP sehingga sulit untuk membuka susunan kode program untuk proses enkripsi pesan email.
4. Karakter-karakter emoji emoticon dapat ditampilkan dengan dengan HTML jika kita dapat mengetahui setiap HTML Entity dari setiap karakter.

5. Karakter-karakter emoji emoticon akan memiliki tampilan yang berbeda pada setiap browser, dan tampilan juga bergantung dari operating system yang digunakan.

### 5.2 Saran

Pada penulisan skripsi ini tentu masih banyak kekurangan yang mungkin dapat disempurnakan lagi oleh pengembang berikutnya, sehingga terdapat beberapa saran yang bisa menjadi pertimbangan agar website vigeticon nantinya menjadi lebih baik lagi, diantaranya :

1. Website vigeticon dapat ditambahkan algoritma-algoritma simetri lainnya sebagai proses enkripsi pesannya.
2. Tampilan Website yang mungkin dapat dibuat lebih menarik lagi agar tidak terlihat kaku dan membosankan.
3. Website Vigeticon saat ini hanya dapat mengirimkan pesan, dan untuk proses dekripsi user harus copy-paste dari halaman website yang dikirimkan, pengembang selanjutnya diharapkan mampu membuat penerimaan pesan langsung dari website vigeticon
4. Pencarian pada kunci RSA dapat dibuat lebih sederhana lagi agar pengguna aplikasi dapat langsung menggunakan fasilitas kunci publik dan kunci rahasia dengan mudah.

### Daftar Pustaka

- [1] Detik.com. "Tim Cyber Polda Selidiki Pembobolan Email Grup Bakrie". Detik inet. <https://inet.detik.com/security/d-2116960/tim-cyber-polda-selidiki-pembobolan-email-grup-bakrie>, (diakses 17 juni 2017)
- [2] Ariyus, Dony. (2008). "Pengantar Ilmu Kriptografi". Yogyakarta: Andi.
- [3] Rambe, Muhammad, Januar. (2011). "Analisis dan Keamanan E-mail Menggunakan Algoritma RSA Sebagai Enkripsi dan Dekripsi Pada Mozilla Thunderbird". Medan : Universitas Sumatera Utara (USU).
- [4] Ariyus, Dony. (2006). "Kriptografi Keamanan Data dan Komunikasi". Yogyakarta : Graha Ilmu.
- [5] Gordon, B. Davis. (1974). "Management Information Systems". Conceptual

### Biodata Penulis

**Levi Yolanza**, memperoleh gelar Sarjana Komputer (S.Kom), Jurusan Informatika Universitas AMIKOM Yogyakarta, lulus tahun 2017.

**Hartatik**, memperoleh gelar Sarjana Teknik (ST), Jurusan Teknik Informatika Universitas Muhammadiyah Cirebon, lulus tahun 2005. Memperoleh gelar Master of Computer Science (M.Cs), Jurusan Ilmu Komputer Universitas Gadjah Mada Yogyakarta, lulus tahun 2010. Saat ini menjadi Dosen di Universitas AMIKOM Yogyakarta, pada Program Studi Informatika dan Sistem Informasi.