Pengamanan Data pada Fitur BluPay Universitas Budi Luhur dengan Algoritma Hill Cipher dan Vigenere Cipher

Bayu Raditya Nasution[1] **Achmad Solichin**[2)]
[1]Program studi, Fakultas Teknologi Informasi, Universitas Budi Luhur
[1,2]Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
E-mail : bayuraditya87@gmail.com[1)] , achmad.solichin@budiluhur.ac.id[2)]

Abstrak

Perkembangan teknologi ini menimbulkan banyaknya kemudahan yang didapat, misalnya seperti pada transaksi pembayaran. Perkembangan yang terjadi memungkinkan transaksi pembayaran yang menjadi cashless. Di Universitas Budi Luhur transaksi pembayaran masih dilakukan dengan cara tradisional yaitu menggunakan uang fisik. Oleh karena itu maka dibuat fitur BluPay aplikasi BluCampus yang bertujuan mempermudah dalam proses pembayaran secara cashless dan online, di dalam fitur aplikasi BluAcademic ini juga di tambahkan kriptografi untuk keamanan data untuk mencegah terjadinya penyalahgunaan dari pihak-pihak yang tidak bertanggung jawab. Metode kriptografi yang digunakan adalah algoritma kriptografi Hill Cipher dan Vigenere Cipher akan diterapkan pada kasus ini. Hasil Pengujian rata-rata waktu proses enkripsi adalah 0.46 detik dan proses dekripsi memerlukan waktu 0.42 detik. Dari hasil tanggapan 21 pengguna yang mengisi kuesioner untuk 12 pertanyaan mendapatkan total nilai sebesar 948 (75%). Hal ini menunjukkan bahwa fitur BluPay aplikasi BluCampus dapat diterima dengan baik oleh 21 responden karena mendapatkan nilai keseluruhan sebesar 75% dari nilai yang ideal.

Kata kunci: Kriptografi*, Hill Cipher*, *Vigenere Cipher*, Enkripsi, Dekripsi

1. PENDAHULUAN

Perkembangan teknologi ini menimbulkan banyaknya kemudahan yang didapat, seperti pada transaksi pembayaran. Perkembangan yang terjadi memungkinkan transaksi pembayaran yang pada awalnya berbentuk fisik menjadi *cashless*. Di Universitas Budi Luhur transaksi pembayaran masih dilakukan dengan cara tradisional. Hal tersebut sangatlah tidak efisien, namun dengan adanya penerapan teknologi berbasis mobile bisa menjadi salah satu pilihan alternatif untuk mengatasi permasalahan transaksi pembayaran yang masih bersifat tradisional. Dengan adanya teknologi ini di harapkan proses transaksi dapat dilakukan secara *cashless* dan *online* sehingga memudahkan mahasiswa dalam transaksi pembayaran.

Namun penerapan teknologi ini memiliki dampak negatif yaitu pada permasalahan keamanan data, karena jaringan internet sebagai sarana yang sangat rentan terhadap penyalahgunaan oleh pihak-pihak yang tidak bertanggung jawab seperti terjadinya pencurian data. Untuk mengamankan data dari kejadian tersebut, salah satu cara yang dapat dilakukan adalah dengan menggunakan kriptografi.

Berkaitan dengan hal di atas, maka dibuat fitur BluPay pada aplikasi BluCampus yang bertujuan mempermudah proses pembayaran, di dalam fitur aplikasi BluPay ini juga menggunakan pengamanan data pada proses transaksi menggunakan algoritma *Hill Cipher* dan *Vigenere Cipher* sebagai enkripsi dan dekripsi. Teknik kriptografi ini dipilih karena diharapkan dengan adanya algoritma ini dapat menjaga informasi agar proses pertukaran data lebih aman.

Dalam penelitian ini metode peneliltian yang digunakan meliputi studi literatur, analisis data, perancangan sistem dan pengujian sistem.

2. TINJAUAN PUSTAKA

2.1. Definisi Kriptografi

kriptografi adalah suatu studi teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, otentikasi entitas dan otentikasi keaslian data. Kriptografi tidak hanya berarti penyediaan keamanan informasi, melainkan sebuah himpunan teknik – teknik [2].

Secara umum, kriptografi merupakan teknik pengamanan informasi yang di lakukan dengan cara mengolah informasi awal dengan suatu kunci tertentu menggunakan suatu metode enkripsi tertentu sehingga menghasilkan suatu informasi baru yang tidak dapat dibaca secara langsung. Informasi baru tersebut dapat dikembalikan menjadi informasi awal melalui proses dekripsi. Kriptografi merupakan bidang ilmu yang bisa menjadi solusi dari masalah keamanan data.

2.2. Tujuan Kriptografi

Aspek-aspek keamanan didalam kriptografi adalah:

1) *Confidentiality* (Kerahasiaan)
   Layanan yang ditujukan untuk menjaga agar pesan tidak dapat dibaca oleh pihak-pihak yang tidak berhak.

2) *Data Integrity* (Integritas)
   Layanan yang menjamin bahwa pesan masih asli/utuh atau belum pernah dimanipulasi selama pengiriman.

3) *Authentication* (Ontentikasi)
   Layanan yang berhubungan dengan idenfikasi, baik mengidentifikasi kebenaran pihak-pihak yang berkomunikasi (*user authentication* atau *entity authentication*).
4) *Non-repudiation* (Penyangkalan)
   Layanan untuk mencegah entitas yang berkomunikasi melakukan penyangkalan, yaitu pengirim pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan [1].

2.3. Konsep Dasar dan Bagian Kriptografi

1) *Plaintext*
   Teks asli yang ditulis atau diketik yang memiliki makna teks asli inilah yang akan diproses menggunakan algoritma kriptografi menjadi *ciphertext*.
2) *Ciphertext*
   Suatu pesan yang telah melalui proses enkripsi. Pesan yang ada pada teks kode ini tidak bisa dibaca karena berupa karakter-karakter yang tidak mempunyai makna.
3) *Encryption* (Enkripsi)
   Cara pengamanan data yang dikirimkan sehingga terjaga kerahasiaannya, enkripsi dapat diartikan juga sebagai penyandian data.
4) *Decryption* (Dekripsi)
   Kebalikan dari enkripsi. Pesan yang telah dienkripsi (*ciphertext*) akan dikembalikan ke bentuk teks asli (*plaintext)*.
5) *Key* (Kunci)
   Kunci yang digunakan untuk melakukan proses enkripsi dan dekripsi.
6) *Cryptanalysis* (Kriptanalis)
   Diartikan sebagai analisis kode atau ilmu untuk mendapatkan *plaintext* (teks asli) tanpa harus mengetahui kunci. Ilmu ini juga dapat menemukan kelemahan dari suatu algoritma kriptografi dan akhirnya dapat menemukan kunci atau *plaintext* dari *ciphertext* yang telah dienkripsi dengan algoritma tertentu. [3].

2.4. Algoritma Kriptografi

Proses algoritma kriptografi penyandian terdiri dari algoritma Enkripsi(E) dan algoritma Dekripsi(D), secara sistemati proses enkripsi dan dekripsi dapat diterangkan dalam persamaan sebagai berikut:

Proses enkripsi EK(P) = C

Proses dekripsi DK(C) = P

Keterangan:
E = Enkripsi
D = Dekripsi
P = *Plaintext*
C = *Ciphertext*
K = Kunci

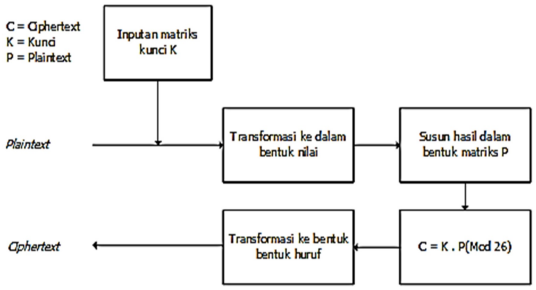
2.5. Algoritma Hill Cipher

Hill Cipher yang merupakan *polyalphabetic* karena teks yang akan diproses akan dibagi blok-blok dengan ukuran terentu. Setiap karakter dalam satu blok akan saling mempengaruhi karakter lainnya dalam proses enkripsi dan dekripsinya, sehingga karakter yang sama tidak dapat dipetakan menjadi karakter yang sama pula.

Dalam penerapannya, *Hill Cipher* menggunakan teknik perkalian matriks dan teknik invers terhadap matriks. Kunci pada *Hill Cipher* adalah matriks n x n dengan n merupakan ukuran blok. Matriks K yang menjadi kunci ini harus merupakan matriks yang *invertible*, yaitu memiliki *multiplicative inverse* K^{-1} sehingga K x K^{-1} = 1. Kunci harus memiliki *inverse* karena matriks K^{-1} tersebut adalah kunci yang digunakan untuk melakukan dekripsi[4].

2.5.1 Teknik Enkripsi Pada Hill Cipher

Proses enkripsi pada *Hill Cipher* dilakukan per blok *plaintext*. Ukuran blok tersebut sama dengan ukuran matriks kunci. Sebelum membagi teks menjadi dereta blok-blok, *plaintext*, terlebih dahulu dikonversi menjadi angka, masing-masing sehingga A=0, B=1, C=2, hingga Z=25.

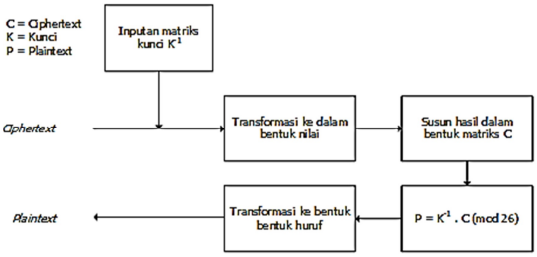


Gambar 1. Proses Enkripsi Hill Cipher

2.5.2 Teknik Dekripsi Pada Hill Cipher

Proses dekripsi pada *Hill Cipher* pada dasarnya sama dengan psroses enkripsinya. Namun matriks kunci yang dipakai adalah *inverse* dari matriks kunci (K^{-1}). Dimana untuk menentukan K^{-1} dengan menggunakan rumus:

$$\frac{1}{\det K} \ mod\ 26 = \text{x}$$

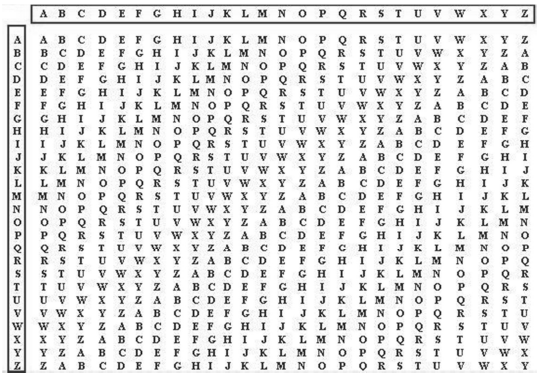


Gambar 2. Proses Dekripsi Hill Cipher

2.6. Algoritma Vigenere Cipher

Algoritma *Vigenere Cipher* adalah salah satu jenis kriptografi klasik yang pada dasarnya melakukan subtitusi *cipher* abjad majemuk (*polyalphabetic subtitution*). Metode ini pertama kali dipublikasikan oleh seorang diplomat (sekaligus seorang kriptologis) Prancis, Blaiise de Vigenere pada abad ke-16 tepatnya pada tahun 1586. Sebenarnya Giovan Batista Belaso telah menggambarkan algoritma ini pertama kali pada tahun 1553 seperti ditulis didalam bukunya *La Cifra del Sig*. *Vigenere Cipher* dipublikasikan pada tahun 1586, tetapi algoritma tersebut baru dikenal luas 200 tahun kemudian. Metode *Vigenere Cipher* ini berhasil dipecahkan oleh matematikawan Inggris Charles Babbage dan Kasiski pada pertengahan abad 19. Vigenere cipher ini digunakan oleh tentara konfiderasi pada perang sipil Amerika. Perang sipil akhirnya berhasil dihentikan setelah *Vigenere Cipher* berhasil dipecahkan. *Vigenere Cipher* ini menerapkan prinsip *Caesar Cipher* dalam metode enkripsinya.

Untuk memudahkan dalam proses enkripsi, maka dapat digunakan alat bantu berupa bujur sangkar *Vigenere.*



Gambar 3. Bujur Sangkar Vigenere

Pada dasarnya, setiap enkripsi huruf adalah *Caesar Cipher* dengan kunci yang berbeda-beda. Berikut merupakan perhitungan sandi *Vigenere Cipher*:

a. Rumus Enkripsi Vigenere Cipher
   Ci = (Pi + Ki) mod 26
b. Rumus Dekripsi Vigenere Cipher
   Pi = (Ci – Ki) mod 26 atau Pi = (Ci – Ki) + 26 jika hasil pengurangan Ci dengan Ki bernilai minus (mod 26).

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: A=0, B=1,…, Z=25

2.7. Studi Literatur

Table 1. Studi Literatur

No	Penulis	Judul	Metode	Hasil	Implikasi
1	Rafli [5]	Aplikasi Kriptografi Email menggunakan Algoritma Hill Cipher Dan Kompersi Huffman Berbasis Desktop Pada Kantor Perpustakaan Dan Arsip Kota Administrasi Jakarta Barat	Hill Cipher dan Kompresi Huffman	Menghasilkan proses pengamanan data dalam bentuk file dokumen yang tidak terbaca tapi juga dapat mengembalikannya ke bentuk file dokumen aslinya	penulis dapat memahami gambaran umum tentang algoritma Hill Cipher
2	Kurniawan [6]	Aplikasi Kriptografi Pesan Email Menggunakan Algoritma Hill Cipher Berbasis Java Desktop Pada Perusahaan Banten Smart Foundation	Hill Cipher	Implementasi enkripsi dan dekripsi Hill Cipher pada isi pesan email yang dikirim	penulis dapat memahami Proses enkripsi dan dekripsi pada algoritma Hill Cipher
3	Noval [7]	Aplikasi Enkripsi dan Dekripsi SMS (Short Message Service) Menggunakan Algoritma Vigenere Cipher, Caesar Cipher, dan DES (Data Encryption Standart) Berbasis Mobile Android Pada Cv. Karya Mandiri	Vigenere Cipher, Caesar Cipher, dan DES	Keamanan isi transaksi dan data yang dikirim melalui pesan	penulis dapat memahami gambaran umum tentang algoritma Vigenere Cipher
4	Efrandi, Asnawati, Yupiyanti [8]	Aplikasi Kriptografi Pesan Menggunakan Algoritma Vigenere Cipher	Vigenere Cipher	Implementasi enkripsi dan dekripsi algoritma Vigenere Cipher pada file .txt	penulis dapat memahami gambaran umum tentang algoritma Vigenere Cipher
5	Hidayat, dan Alawiyah [9]	Enkripsi dan Dekripsi Teks menggunakan Algoritma Hill Cipher dengan Kunci Matriks Persegi Panjang	Hill Cipher	Penggunaan matriks persegi panjang menghasilkan ukuran matriks yang lebih beragam dan menghasilkan ciphertext yang lebih panjang dari plaintext nya	penulis dapat memahami Proses enkripsi dan dekripsi pada Hill Cpher jika memakai lebih dari 26 karakter

3. METODE PENELITIAN

3.1. Metodologi Penelitian

Dalam penelitian ini, beberapa metode digunakan untuk memperoleh informasi yang diperlukan dan menyelesaikan masalah yang ditemui. Adapun metode – metode ini sebagai berikut:

a. Studi literatur

Metode ini digunakan untuk memperoleh pembelajaran data atau informasi dengan cara mengumpulkan berbagai referennsi baik itu dalam bentuk makalah, jurnal, serta referensi lainnya untuk mendapatkan informasi yang dibutuhkan.

b. Analisis Data

Metode ini digunakan untuk menganalisis Algoritma kriptografi yang digunakan yaitu metode algoritma kriptografi *Hill Cipher* dan *Vigenere Cipher*, serta teknik-teknik yang digunakan

c. Perancangan Sistem

Metode ini digunakan untuk merancang sistem aplikasi untuk mengimplementasikan metode algoritma kriptografi *Hill Cipher* dan *Vigenere Cipher* dengan menggunakan bahasa pemrograman JAVA berbasis Android.

d. Pengujian Sistem

Metode ini dilakukan dengan menguji dan mengecek jalannya program

3.2. Analisis dan Penyelesaian Masalah

Kemajuan yang pesat pada bidang teknologi saat ini telah memberikan berbagai kemudahan. Hal tersebut bisa dilihat dari bagaimana melakukan transaksi pembelian atau pembayaran suatu barang yang saat ini tidak lagi terpaku dengan menggunakan uang secara fisik sebagai alat pembayaran yang sah.

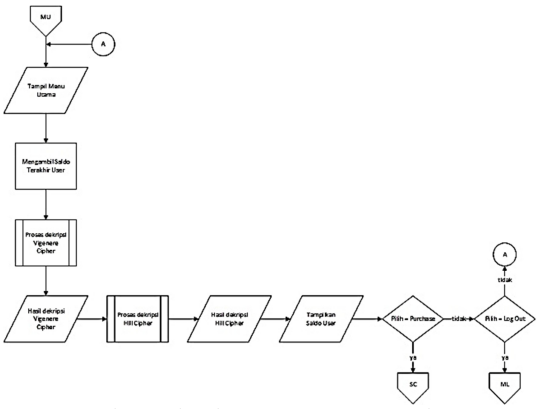
Namun dengan adanya kemudahan tersebut memungkinkan adanya kegiatan untuk mencari celah oleh orang yang tidak bertanggung jawab untuk melakukan pencurian data seperti halnya uang elektronik yang berada pada saku elektronik yang kita miliki. Dengan begitu kemudahan yang ada juga memiliki risiko yang harus dipikirkan kembali untuk bisa digunakan secara umum.

Dari permasalahan yang ada maka diperlukan sistem kemananan data pada fitur BluPay aplikasi BluCampus yang mampu menjaga kerahasiaan data sehingga data tersebut tidak dapat diakses oleh pihak yang tidak berhak atas data tersebut. Untuk dapat membuat data tersebut terjaga kerahasiannya, aplikasi ini akan memanfaatkan ilmu pengamanan data, yaitu kriptografi.

Aplikasi kriptografi ini menggunakan algoritma *Hill Cipher* dan juga menggunakan algoritma *Vigenere Cipher*. Algortima *Hill Cipher* dan *Vigenere Cipher* termasuk kedalam kriptografi klasik dan merupakan kriptografi simetris. Dengan menggunakan dua algoritma kriptografi yaitu *Hill Cipher* dan *Vigenere Cipher* dapat meningkatkan keamanan data dari pihak-pihak yang tidak bertanggung jawab untuk mengakses data tersebut karena untuk memecahkan *ciphertext*, diperlukan dua buah kunci, yaitu kunci matriks yang dipakai pada algoritma *Hill Cipher* dan kunci yang dipakai pada algoritma *Vigenere Cipher*.

3.3. Flowchart dan Algoritma Program

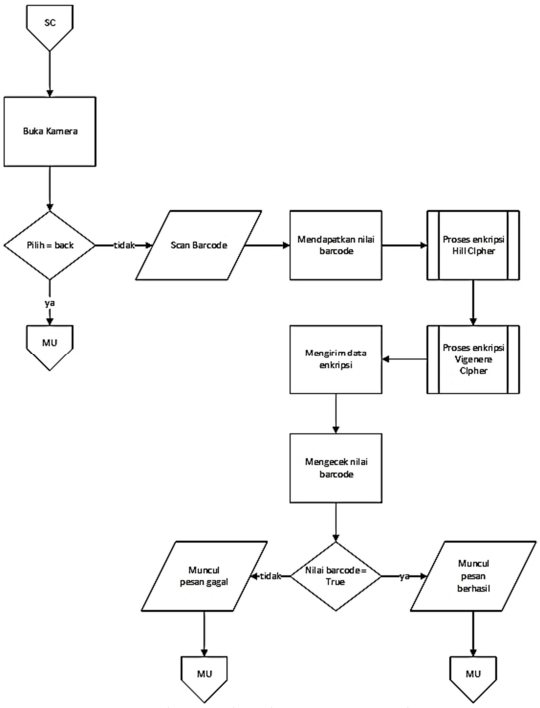
Berikut ini merupakan rancangan *flowchart* dan algoritma pemrograman pada form menu utama BluPay dan scan barcode serta *flowchart* dan algoritma untuk proses enkripsi dan dekripsi data menggunakan *Hill Cipher* dan *Vigenere Cipher*, berikut *flowchart* dan algoritmanya:



Gambar 4. Flowchart Form Menu Utama BluPay

Flowchart pada gambar 4 menjelaskan alur proses dimana pengguna dapat melihat saldo, melakukan proses transaksi, dan melakukan *log out*. Algoritma form menu utama BluPay dari *flowchart* di atas:

1. Tampilkan Menu Utama BluPay (MU)
2. Mengambil saldo terakhir user
3. Jalankan proses dekripsi Vigenere Cipher
4. Jalankan proses dekripsi Hill Cipher
5. Tampilkan Saldo User
6. Pilih action
7. If action = Purchase then
8. Jalankan Scan Barcode
9. Else if action = Log Out then
10. Kembali ke form log in
11. Else
12. Tetap di menu utama BluPay
13. End if

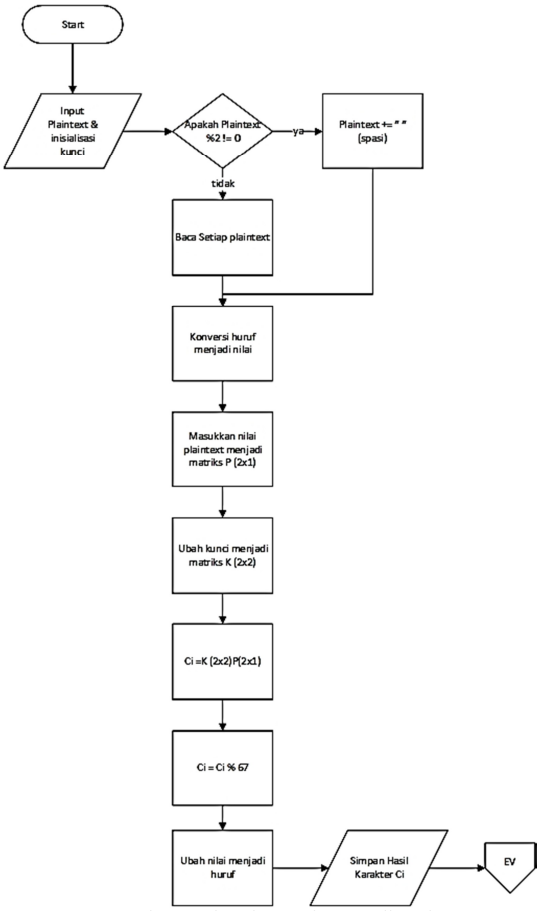


Gambar 5. Flowchart Scan Barcode

Flowchart pada gambar 5 menjelaskan alur proses dimana pengguna dapat melakukan proses *scanning barcode* dalam melakukan proses pembayaran. Algoritma scan barcode dari *flowchart* di atas:

1. Buka kamera
2. Pilih action
3. If action = back then
4. Kembali ke menu utama BluPay
5. Else
6. Lakukan scan pada barcode
7. Mendapatkan nilai barcode
8. Jalankan proses enkripsi Hill Cipher
9. Jalankan proses enkripsi Vigenere Cipher
10. Mengirim data enkripsi
11. Mengecek nilai barcode
12. If nilai barcode = True
13. Muncul pesan berhasil
14. Kembali ke menu utama Blupay
15. Else
16. Muncul pesan gagal
17. Kembali ke menu utama Blupay
18. End if
19. End if

Flowchart pada Gambar 6 menjelaskan alur proses dari enkripsi algoritma Hill Cipher.

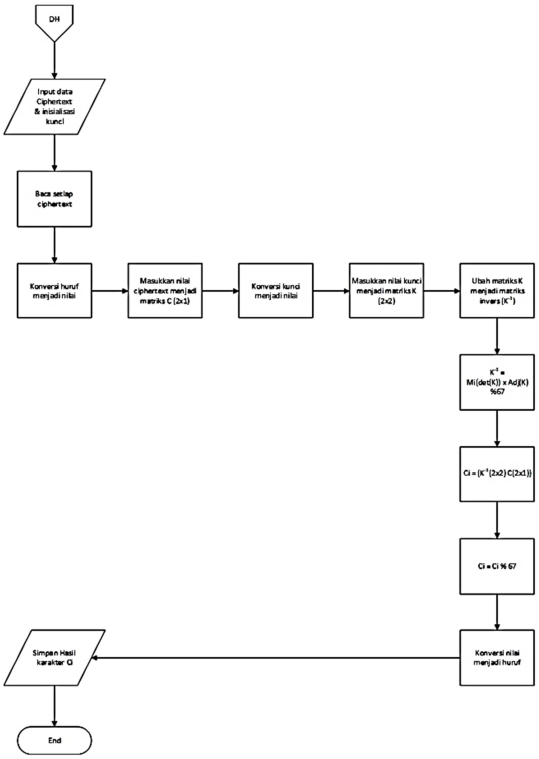


Gambar 6. Flowchart Enkripsi Hill Cipher

Algoritma di bawah ini menjelaskan bagaimana proses enkripsi Hill Cipher terjadi.

1. Start
2. Input plaintext & inisialisasi kunci
3. If plaintext %2 != 0 then
4. Plaintext ditambahkan karakter spasi(" ")
5. Else
6. Baca setiap plaintext
7. End if
8. konversi huruf menjadi nilai
9. masukkan nilai plaintext menjadi matriks $P_{(2x1)}$
10. konversi kunci menjadi nilai
11. masukkan nilai kunci menjadi matriks $K_{(2x2)}$
12. hitung Ci = K . P
13. Ci = Ci % 67
14. Konversi nilai menjadi huruf
15. Simpan hasil karakter Ci

Flowchart pada Gambar 7 menjelaskan alur proses dari dekripsi algoritma Hill Cipher.

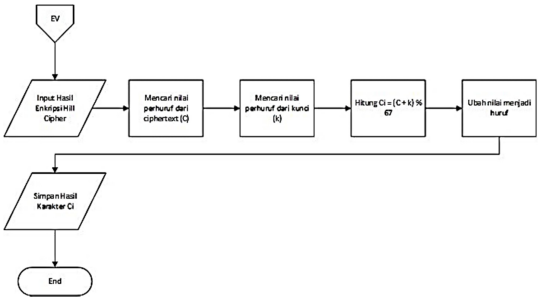


Gambar 7. Flowchart Dekripsi Hill Cipher

Algoritma di bawah ini menjelaskan bagaimana proses dekripsi Hill Cipher terjadi.

1. Ambil data hasil dekripsi Vigenere Cipher & inisialisasi kunci
2. Baca setiap ciphertext
3. Konversi huruf menjadi nilai
4. Masukkan nilai ciphertext menjadi matriks $C_{(2x1)}$
5. Konversi kunci menjadi nilai
6. Masukkan nilai kunci menjadi matriks $K_{(2x2)}$
7. Ubah matriks kunci K menjadi matriks Invers (K^{-1})
8. $K^{-1} = MI(\det(K))xAdj(K)$
9. $Ci = K^{-1}_{(2x2)} C_{(2x1)}$
10. Ci = Ci % 67
11. Konversi nilai menjadi huruf
12. Simpan hasil karakter Ci
13. End

Flowchart pada Gambar 8 menjelaskan alur proses dari enkripsi algoritma Vigenere Cipher.

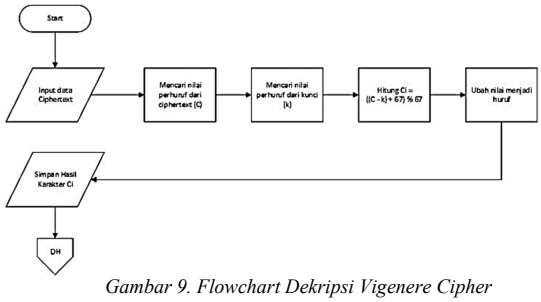


Gambar 8. Flowchart Enkripsi Vigenere Cipher

Algoritma di bawah ini menjelaskan bagaimana proses enkripsi Vigenere Cipher terjadi.

1. Ambil data hasil enkripsi Hill Cipher & inisialisasi kunci
2. Mencari nilai perhuruf dari ciphertext (c)
3. Mencari nilai perhuruf dari kunci (k)
4. Hitung Ci = (c + k) % 67
5. konversi nilai menjadi huruf
6. Simpan hasil karakter Ci
7. End

Flowchart pada Gambar 9 menjelaskan alur proses dari dekripsi algoritma Vigenere Cipher.



Gambar 9. Flowchart Dekripsi Vigenere Cipher

Algoritma di bawah ini menjelaskan bagaimana proses dekripsi Vigenere Cipher terjadi.

1. Start
2. Input data ciphertext & inisialisasi kunci
3. Mencari nilai perhuruf dari ciphertext (c)
4. Mencari nilai perhuruf dari kunci (k)
5. Hitung Ci = ((c - k) + 67) % 67
6. konversi nilai menjadi huruf
7. Simpan hasil karakter Ci

4. HASIL DAN PEMBAHASAN

4.1. Tampilan Layar

4.1.1. Tampilan Layar Menu Utama BluPay

Gambar 10. Tampilan Menu Utama BluPay

Gambar 10 merupakan tampilan menu utama BluPay yang akan memperlihatkan saldo terakhir pengguna jika terkoneksi dengan jaringan internet. Saldo tersebut telah melalui proses dekripsi dengan algoritma Vigenere cipher dan Hill Cipher.

4.1.2. Tampilan Layar Scan Barcode

Gambar 11. Tampilan Layar Scan Barcode

Gambar 11 merupakan tampilan layar scan barcode yang akan melakukan proses enkripsi dengan algoritma Hill cipher dan Vigenere cipher saat nilai barcode didapatkan setelah proses scanning.

4.2. Pengujian Program

Tabel 2. Hasil Pengujian Proses Enkripsi

Input	Output Hill Cipher	Output Vigenere Cipher	Waktu Enkripsi (detik)
Nomor Induk: 1411501114 Penyedia Jasa: blupay Nominal: 25863	Nomor Induk: JY IF IJY Penyedia Jasa: aGZeQb Nominal: hsmWp	Nomor Induk: jzV6fWV6jz Penyedia Jasa: 0hzNq2 Nominal: V8DVwB	0.18
Nomor Induk: 1436792543 Penyedia Jasa: blupay Nominal: 123467958	Nomor Induk: JYwqgc h80 penyedia Jasa: aGZeQb Nominal: W69JTkrOSl	Nomor Induk: jzHZ63VQTM Penyedia Jasa: 0hzNq2 Nominal: wSU7t?C!s!	0.43
Nomor Induk: 3645279850 Penyedia Jasa: blupay Nominal: 345786839	Nomor Induk: wqvSx,5eF penyedia Jasa: aGZeQb Nominal: 9J8KsmeWs?	Nomor Induk: HCGBIaQNfW Penyedia Jasa: 0hzNq2 Nominal: UkT8D.4FDX	0.23
Kode Barcode: 5035226500244	Kode Barcode: FV7wRgDJ,jywA	Kode Barcode: fWvqHs61ja9hHb	0.79
Kode Barcode: 4974365823382	Kode Barcode: VRfuwqU8IAjI?P	Kode Barcode: vs5dHCurib96Wq	0.53
Kode Barcode: 5030935500295	Kode Barcode: FUK4wGsJ,kgHa	Kode Barcode: fWu8PIgbjaPh1	0.58
Rata-rata waktu			0.46

Tabel 3. Hasil Pengujian Proses Dekripsi

Input (Ciphertext)	Output Vigenere Cipher	Output Hill Cipher	Waktu dekripsi (detik)
Saldo: 5GgCi0	Saldo: fuGTIZ	Saldo: 744137	0.43
Saldo: 6eDVwb	Saldo: gDsmWp	Saldo: 65863	0.38
Saldo: snTjV8Du	Saldo: SM80 hs?	Saldo: 7643259	0.47
Saldo: 90kfD.	Saldo: jZkwsm	Saldo: 100586	0.42
Saldo: ULvq	Saldo: 9zV7	Saldo: 2035	0.35
Saldo: CpDV8L?n	Saldo: rOsmizl4	Saldo: 9586471	0.48
Rata-rata waktu			0.42

Dari hasil pengujian pada tabel 1 dan 2 diketahui bahwa jumlah persentase keberhasilan pada proses enkripsi dan dekripsi mencapai 100% dengan waktu yang tidak dipengaruhi oleh jumlah karakter/data inputan yang akan dienkripsi atau didekripsi. Rata-rata waktu untuk proses enkripsi adalah 0.46 detik dan proses dekripsi 0.42 detik.

4.3. Tanggapan Pengguna

Dari 4 kategori aspek penilaian yaitu functionality, reliability, usability, dan efficiency skor dari 21 responden dapat dilihat pada Tabel 3 sebesar 64 jawaban sangat setuju, 122 jawaban setuju, 60 jawaban ragu-ragu, 3 jawaban tidak setuju dan 3 jawaban sangat tidak setuju.

Tabel 4. Tabel Skor Responden

Aspek Penilaian	Skor Responden				
	5	4	3	2	1
	SS	S	R	TS	STS
Functionality	19	36	8	0	0
Reliability	13	25	21	2	2
Usability	9	35	19	0	0
Efficiency	23	26	12	1	1
Jumlah	64	122	60	3	3

Pada Tabel 4 dapat dilihat hasil penilaian responden terhadap aplikasi dari 4 kategori aspek penilaian yaitu *functionality, reliability, usability, dan efficiency*. Total skor aktual untuk aspek *functionality* sebesar 263 (83%) dari skor ideal 315, aspek penilaian *reliability* sebesar 234 (74%) dari skor ideal 315, aspek penilaian *usability* sebesar 242 (76%) dari skor ideal 315, aspek penilaian *efficiency* sebesar 259 (82%) dari skor ideal 315, dan total skor aktual keseluruhan sebesar 948 (75%) dari skor ideal 1260.

Tabel 5. Tabel Skor Aktual

Aspek Penilaian	Skor Aktual					Total Skor Aktual	Skor Ideal	%
	5	4	3	2	1			
	SS	S	R	TS	STS			
Functionality	95	144	24	0	0	263	315	83%
Reliability	65	100	63	4	2	234	315	74%
Usability	45	140	57	0	0	242	315	76%
Efficiency	115	105	36	2	1	259	315	82%
Jumlah	320	489	130	6	3	948	1260	75%

4.4. Kelebihan Program

a. Aplikasi lebih aman karena menggunakan 2 algoritma kriptografi yaitu *Hill Cipher* dan *Vigenere Cipher*.
b. Tidak terjadinya perubahan pada isi data setelah dilakukannya proses dekripsi.
c. Proses enkripsi dan dekripsi berlangsung cepat.
d. Data yang dapat diinputkan berupa karakter huruf, angka, dan simbol.

4.5. Kekurangan Program

a. Proses penampilan hasil dekripsi dapat berlangsung lama jika jaringan internet tidak baik.
b. Kunci pada program tidak dapat diganti oleh pengguna.
c. Ada beberapa karakter simbol yang tidak bisa dienkripsi ataupun didekripsi.

5. KESIMPULAN

a. Dengan mengimplementasikan kriptografi dengan metode algoritma Hill Cipher dan Vigenere Cipher pada aplikasi ini, data input yang dikirim dan disimpan dalam database akan lebih aman.
b. Proses dekripsi dapat mengembalikan data seperti data asli tanpa mengalami perubahan sedikitpun pada data asli.
c. Panjang plaintext dan ciphertext tidak mempengaruhi kecepatan proses enkripsi dan dekripsi algoritma Hill Cipher dan Vigenere Cipher.
d. Hasil Pengujian rata-rata waktu proses enkripsi adalah 0.46 detik dan proses dekripsi memerlukan waktu 0.42 detik
e. Dari hasil tanggapan 21 pengguna yang mengisi kuesioner untuk 12 pertanyaan mendapatkan total nilai sebesar 948 (75%). Hal ini menunjukkan bahwa fitur BluPay aplikasi BluCampus dapat diterima dengan baik oleh 21 responden karena mendapatkan nilai keseluruhan sebesar 75% dari nilai yang ideal.

6. DAFTAR PUSTAKA

[1] Ariyus, Dony, 2008, *Pengantar Ilmu Kriptografi*, Yogyakarta, Penerbit Andi.

[2] Menezes, Alfred, Oorschot, Paul van, dan Vanstone, Scott, 1996, *Handbook of Applied Cryptography,* CRC Press.

[3] Sadikin, Rifki, 2012, *Kriptografi Untuk Keamanan Jaringan,* Yogyakarta, Andi.

[4] Widyanarko, Arya, 2009, *Studi Dan Analisis Mengenai Hill Cipher, Teknik Kriptanalis dan Upaya Penanggulangannya.*

[5] Rafli, H., 2017. *Aplikasi Kriptografi Email menggunakan Algoritma Hill Cipher Dan Kompersi Huffman Berbasis Desktop Pada Kantor Perpustakaan Dan Arsip Kota Administrasi Jakarta Barat*. Skripsi. Tidak diterbitkan. Fakultas Teknologi Informasi Universitas Budi Luhur: Jakarta Selatan.

[6] Kurniawan, A., 2016. *Aplikasi Kriptografi Pesan Email Menggunakan Algoritma Hill Cipher Berbasis Java Desktop Pada Perusahaan Banten Smart Foundation*. Skripsi. Tidak diterbitkan. Fakultas Teknologi Informasi Universitas Budi Luhur: Jakarta Selatan

[7] Noval, M. A., 2016. *Aplikasi Enkripsi dan Dekripsi SMS (Short Message Service) Menggunakan Algoritma Vigenere Cipher, Caesar Cipher, dan DES (Data Encryption Standart) Berbasis Mobile Android Pada Cv. Karya Mandiri*. Skripsi. Tidak diterbitkan. Fakultas Teknologi Informasi Universitas Budi Luhur: Jakarta Selatan.

[8] Efrandi, Asnawati, dan Yupiyanti. 2014. *Aplikasi Kriptografi Pesan Menggunakan Algoritma Vigenere Cipher*. Jurnal Media Infotama. Vol. 10, No. 2

[9] Hidayat, A., dan Alawiyah, T., 2013. *Enkripsi dan Dekripsi Teks menggunakan Algoritma Hill Cipher dengan Kunci Matriks Persegi Panjang.* Jurnal Matematika Integratif. Vol. 9, No 1. Hal. 39-51