PERANCANGAN APLIKASI KRIPTOGRAFI BERLAPIS MENGGUNAKAN ALGORITMA CAESAR, TRANSPOSISI, VIGENERE, DAN BLOK CHIPER BERBASIS MOBILE

Atmaja Basuki[1)], Upik Paranita[2)], Restu Hidayat[3)]

[1), 2), 3)] Teknik Informatika STMIK AMIKOM Yogyakarta
Jl Ring road Utara, Condongcatur, Sleman, Yogyakarta 55281
Email : atmaja.b@students.amikom.ac.id[1)], upik.p@students.amikom.ac.id[2)], restu.hi@students.amikom.ac.id[3)]

Abstrak

Data ataupun informasi menjadi aspek penting bagi kehidupan manusia. Selain itu data juga bisa digunakan sebagai alat untuk melakukan tindak kriminal. Untuk itulah diperlukan sebuah alat untuk mengamankannya. Teknik pengamanan data sangat beragam, diantaranya ada yang bersifat manual dan ada juga yang menggunakan sistem yang sudah terkomputerisasi. Teknik yang sudah terkomputerisasi biasanya menggunakan sebuah aplikasi untuk mengamankan data. Aplikasi-aplikasi ini lah yang sering menjadi incaran para pirates untuk diambil data dan informasi rahasianya. Dengan menggunakan 4 teknik sekaligus dalam mengamankan data dan informasi rahasia diyakini dapat membuat tingkat keamanannya lebih tinggi. Diantaranya menggunakan Algoritma Caesar, yaitu dengan mengganti posisi huruf awal dari alfabet atau disebut juga dengan algoritma ROT3. Algoritma Transposisi, yaitu dengan menggunakan permutasi karakter. Algoritma Vigenere, yaitu setiap teks-kode selalu menggantikan nilai teks-asli tertentu. Algoritma Blok Cipher, yaitu mengenkripsi satu blok plaintext dengan jumlah bit tertentu dan menghasilkan blok ciphertext dengan jumlah bit yang sama. Untuk memudahkan penggunanya, aplikasi ini dibuat berbasis mobile, jadi pengguna hanya membutuhkan smartphone untuk mengenkripsi data dan informasi rahasianya ke dalam media digital. Hasilnya, aplikasi ini bisa berjalan dan melakukan proses enkripsi dan dekripsi pada platform smartphone.

Kata kunci: *Caesar, Transposisi, Vigenere, Blok Cipher*

1. Pendahuluan

Kebutuhan masyarakat akan keamanan informasi, dengan adanya teknologi informasi, data-data informasi rahasia yang seharusnya tidak boleh diketahui orang lain kecuali pemilik informasinya sangat mungkin terjadi, karena hal tersebut termasuk dalam teknologi informasi dalam hal keamanan informasi. Kriptografi adalah ilmu sekaligus seni untuk menjaga kerahasiaan pesan, data, atau informasi dengan cara menyamarkannya menjadi bentuk tersandi yang tidak mempunyai makna[1]. Dengan membuat algoritma berlapis di yakini akan membuat data dan informasi tersebut memiliki level kemanan lebih tinggi. Lapisan itu diantaranya adalah algoritma caesar, transposisi, vigenere, dan blok cipher.

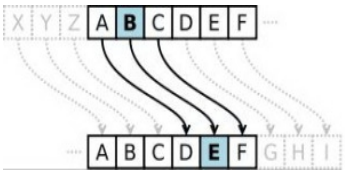
Algoritma caesar cipher yaitu algoritma dengan mengganti posisi huruf awal dengan alphabet atau disebut dengan algoritma ROT3. Algoritma transposisi yaitu dengan cara mengubah letak dari teks pesan yang akan disandikan dengan menggunakan bentuk tertentu. Algoritma vigenere yaitu setiap teks-kode selalu menggantikan nilai teks-asli tertetu. Algoritma blok cipher yaitu mengenkripsi satu blok plaintext dengan jumlah bit tertentu dan menghasilkan blok cipher dengan jumlah bit yang sama[2].

2. Pembahasan

Metode Caesar Cipher

Konsep Caesar Cipher adalah :

1. Menentukan besarnya pergeseran karakter yang digunakan dalam membentuk cipherteks ke plainteks.
2. Menukarkan karakter pada plainteks menjadi cipherteks dengan berdasarkan pada pergeseran yang telah ditentukan sebelumnya.
   Misalnya diketahui bahwa pergeseran = 3. maka huruf A akan digantikan oleh huruf D, huruf B menjadi huruf E, dan seterusnya.



Gambar 1.*Cara Kerja Caesar Chiper*

Teknik penyandian ini termasuk sandi tersubtitusi pada setiap huruf pada plaintext digantikan oleh huruf lain yang dimiliki selisih posisi tertentu dalam alphabet.

Metode Transposisi Cipher

Metode penyandian dengan cara mengubah letak dari teks pesan yang akan disandikan. Dan untuk membaca pesan aslinya kembali, cukup dengan mengembalikan letak dari

pesan tersebut berdasarkan kunci dan algoritma pergeseran huruf yang telah disepakati.
Plaintext : Reinforcementsarrivingnow

				R				
			E	I	N			
		F	O	R	C	E		
	M	E	N	T	S	A	R	
R	I	V	I	N	G	N	O	W

Gambar 2.*Tabel Transposisi Chiper*

Dibaca dari atas ke bawah mulai dari kolom pertama
Ciphertext : RMIFEVEONIRIRTNNCSGEANROW

Catatan : jika jumlah huruf tidak mencukupi untuk membentuk segitiga maka sisa kebutuhannya dapat ditambahkan huruf-huruf yang disepakati.

Metode Vigenere Chiper
Teknik untuk menghasilkan *ciphertext* bisa dilakukan menggunakan substitusi angka maupun bujursangkar *vigènere*. Teknik susbtitusi *vigènere* dengan menggunakan angka dilakukan dengan menukarkan huruf dengan angka, hampir sama dengan kode geser[3].
Contoh:

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Gambar 3.*Tabel Transposisi Chiper*

Plaintext: PLAINTEXT
Kunci: CIPHER

Plain	15	11	0	8	13	19	4	23	19
Kunci	2	8	15	7	4	17	2	8	15
Hasil	17	19	15	15	17	10	6	5	8
Ciphertext	R	T	P	P	R	K	G	F	I

Gambar 4.*Tabel Cara Kerja Transposisi Chiper*

Metode Block Cipher
Konsep Block Chiper

1. Bit – bit plainteks dibagi menjadi blok-blok bit dengan panjang sama, misalnya 64 bit.
2. Panjang kunci enkripsi = panjang blok
3. Enkripsi dilakukan terhadap blok bit plainteks menggunakan bit-bit kunci.
4. Algoritma enkripsi menghasilkan blok cipherteks yang panjangnya = blok plainteks.

Tahap pertama kali yang penulis lakukan dalam penelitian ini adalah pengumpulan data sehingga bisa digunakan untuk masuk dalam tahap selanjutnya yaitu tahap kedua atau bisa disebut menganalisis data. Hasil dari menganalisis data yang penulis telah lakukan diantaranya kelemahan pada sistem aplikasi yang lama, yaitu:

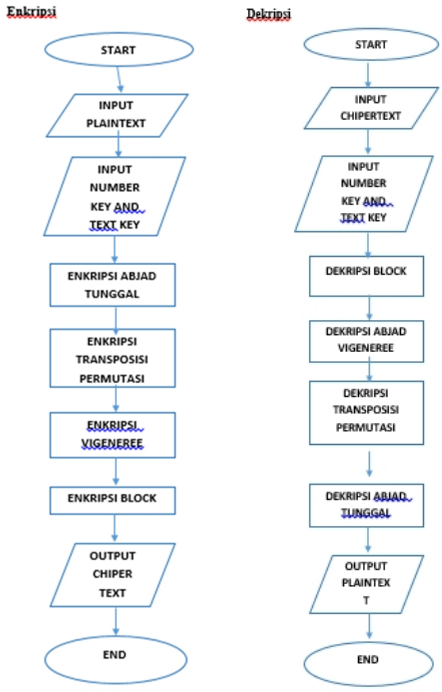
1. Hanya berjalan pada platform tertentu.
2. Masih menggunakan algoritma standar yang dengan adanya perkembangan teknologi berkemungkinan untuk lebih cepat di bobol.
3. Pengamanannya kurang kuat karena kunci yang digunakan untuk enkripsi tidak di enkripsi lagi.

Dari rujukan data diatas membuat penulis untuk membuat sistem aplikasi baru dengan kelebihan:

1. Bisa berjalan pada semua platform dengan syarat memiliki akses internet dan browser yang mendukung javascript.
2. Pengamanan kunci yang kuat, kunci yang digunakan untuk enkripsi.

Tahap ketiga adalah perancangan, untuk perancangannya menggunakan Eclipse. Perancangan sistem yang akan dilakukan meliputi tiga tahap, yaitu prosedural, perancangan proses, dan perancangan interface/antarmuka.

Perancangan prosedural ini berisi tentang flowchart dari aplikasi ini. Flowchart proses enkripsi dan dekripsi dapat dilihat pada gambar 5.



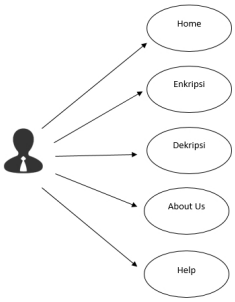
Gambar 5. *Flowchart enkripsi dan dekripsi*

Dari gambar 5 dapat dijelaskan, pertama kali sistem akan menampilkan menu enkripsi, menampilkan form yang harus diisi untuk proses enkripsi, diantaranya kunci, dan pesan yang akan di sembunyikan. Selanjutnya sistem akan mengecek ekstensi dari pesan tersebut.

Setelah pesan tersebut terenkripsi, untuk mengubahnya kembali menjadi plaintext dapat dilakukan dengan cara membalik aturan algoritma yang digunakan.

Perancangan proses aplikasi ini menggunakan *Use Case Diagram*, dan *Activity Diagram.*

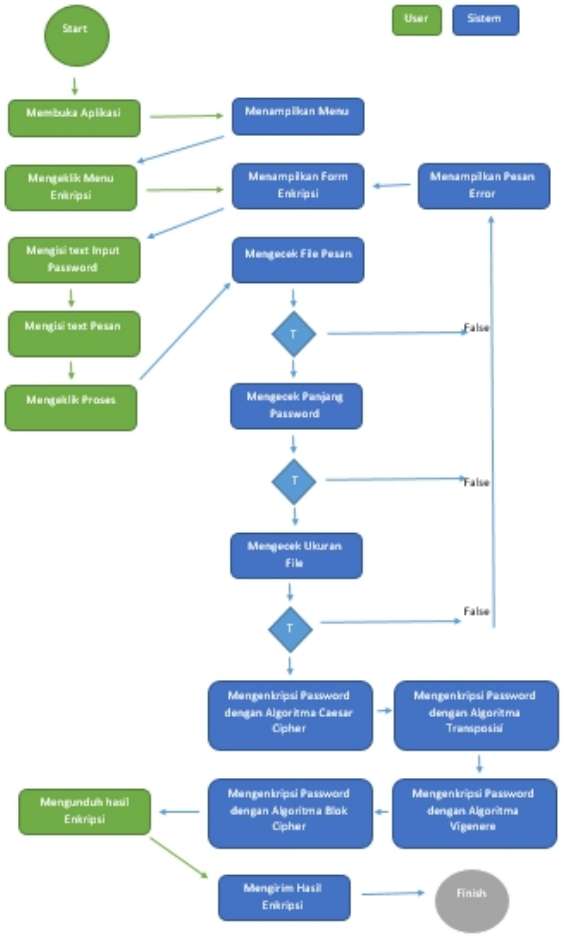
Use Case Diagram mempresentasikan dekripsi lengkap tentang interaksi yang terjadi antara para *actor* dengan sistem[4]. *Use Case* dari aplikasi yang akan dirancang bisa dilihat pada gambar 6.



Gambar 6. *Usecase Diagram*

Dari gambar 6 dapat dijelaskan, seorang *actor* yang dapat melakukan interaksi agar sistem melakukan berbagai proses seperti *home, enkripsi, dekripsi, about us,* dan *help.*

Activity diagram menggambarkan aktifitas-aktifitas, objek, *state*, *transisi state,* dan *event.* Dengan kata lain kegiatan diagram alur kerja menggambarkan perilaku sistem untuk aktifitas[5]. Gambar 8 menunjukan aktifitas diagram proses enkripsi.



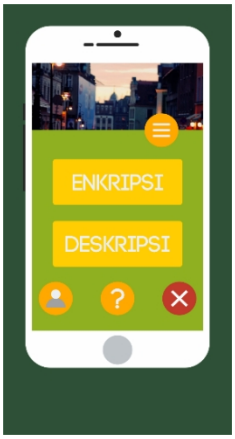
Gambar 7. *Activity Diagram*

Pada gambar 7 bisa menjelaskan urutan aktifitas user dan sistem mulai dari membuka aplikasi yang dilakukan user sampai berakhir pada sistem dengan mengirimkan hasil enkripsi.

Perancangan interface/antarmuka aplikasi ini adalah sebagai berikut :

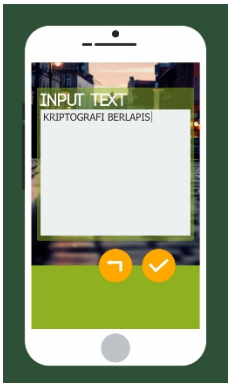
Gambar 8. *Tampilan Home*

Merupakan tampilan awal ketika membuka aplikasi kriptografi berlapis.



Gambar 9. *Tampilan Option*

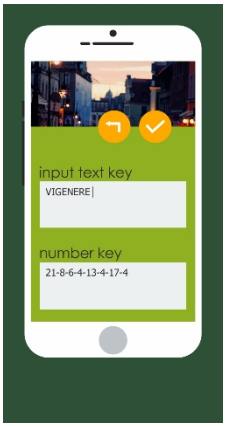
Pada menu *option* kita bisa memilih proses mana yang ingin kita lakukan, apakah enkripsi atau dekripsi. Disediakan juga icon **'?'**, sebagai *input key*, jadi kita bisa memasukkan atau menuliskan *key* seperti apa yang akan digunakan untuk proses *enkripsi* dan *dekripsi.*



Gambar 10. *Tampilan Input*

Pada menu *input* kita dapat memasukkan pesan atau teks yang ingin kita enkripsi atau dekripsi kan.

Jika kita sudah memasukkan pesan atau teks tersebut, klik icon '✓', untuk melihat hasilnya.



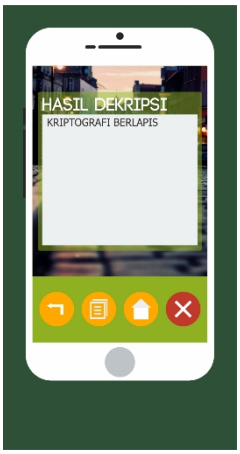
Gambar 11. *Tampilan Input Key*

Pada menu tampilan *input key* kita bisa memasukkan kunci apa yang akan digunakan sebagai *key* untuk membuka *ciphertext* atau *plaintext.*

Gambar 12. *Tampilan Hasil Enkripsi*

Pada menu tampilan hasil *enkripsi* kita bisa melihat hasil dari *plaintext* yang telah di *enkripsi*. Disediakan juga menu *back, input, home,* dan *close.*

Menu *back* digunakan jika kita ingin kembali ke menu *option.* Menu *input* digunakan jika kita ingin mengulangi kembali proses pengenkripsian pesan atau teks. Menu *home* digunakan untuk kembali ke tampilan awal aplikasi. Sedangkan menu *close* digunakan untuk keluar langsung dari aplikasi tersebut.



Gambar 13. *Tampilan Hasil Dekripsi*

Pada menu tampilan hasil *dekripsi* kita bisa melihat hasil dari *ciphertext* yang telah di *dekripsi* kan. Disediakan juga menu *back, input, home,* dan *close.*

Menu *back* digunakan jika kita ingin kembali ke menu *option.* Menu *input* digunakan jika kita ingin mengulangi kembali proses pendekripsian pesan atau teks. Menu *home* digunakan untuk kembali ke tampilan awal aplikasi. Sedangkan menu *close* digunakan untuk keluar langsung dari aplikasi tersebut.

Berikut contoh algoritma caesar pada penerapan aplikasi kami:

Plaintext : **KRIPTOGRAFI BERLAPIS**

Sandi algoritma caesar dengan kunci 3.

Alfabet Biasa	ABCDEFGHIJKLMNOPQRSTUVWXYZ
Alfabet Sandi	DEFGHIJKLMNOPQRSTUVWXYZABC

Menjadi,

Teks Terang	KRIPTOGRAFI BERLAPIS
Teks Tersandi	NULSWRJUDIL EHUODSLV

Ciphertext :

Kemudian setelah plaintext tersebut terenkripsi dengan menggunakan algoritma caesar, langkah selanjutnya adalah mengenkripsi plaintext yang telah terenkripsi dengan algoritma transposisi segitiga.

Plaintext : **NULSWRJUDIL EHUODSLV**

Menjadi,

				N				
			U	L	S			
		W	R	J	U	D		
	I	L	E	H	U	O	D	
S	L	V	A	B	C	D	E	F

Text Tersandi: **SILWLVUREANLJHBSUUCDODDEF**

Selanjutnya proses pengenkripsian dilakukan menggunakan algoritma vigenere.

Plaintext : **SILWLVUREANLJHBSUUCDODDEF**

Kunci : **VIGENERE**

Menjadi,

Plain	18	8	11	22	11	21	20	17	4
Kunci	21	8	6	4	13	4	17	4	21
Hasil	14	16	17	1	24	25	12	21	25
Ciphertext	O	Q	R	B	Y	Z	M	V	Z

Plain	0	13	11	9	7	1	18	20	20
Kunci	8	6	4	13	4	17	4	21	8
Hasil	8	19	15	22	11	18	22	16	3
Ciphertext	I	T	P	W	L	S	W	Q	D

Plain	2	3	14	3	3	4	5
Kunci	6	4	13	4	17	4	21
Hasil	8	7	2	7	20	8	1
Ciphertext	I	H	A	H	U	I	B

Ciphertext : **OQRBYZMVZITPWLSWQDIHAHUIB**

Selanjutnya proses pengenkripsian dilakukan menggunakan algoritma block chiper.

Plaintext : **OQRBYZMVZITPWLSWQDIHAHUIB**

Menjadi,

Plain	O	Q	R	B	Y	Z	M	V	Z
Binner	100 1111	101 0001	101 0010	100 0010	101 1001	101 1010	100 1101	101 0110	101 1010
Kunci	101 0110	100 1001	100 0111	100 0101	100 1110	100 0101	101 0010	100 0101	101 0110
Chipertext	001 1001	001 1000	001 0101	000 0111	001 0111	001 1111	001 1111	001 0011	000 1100
Konversi	19	18	15	7	17	1F	1F	13	C

Plain	I	T	P	W	L	S	W	Q	D
Binner	100 1001	101 0100	101 0000	101 0111	100 1100	101 0011	101 0111	101 0001	100 0100
Kunci	100 1001	100 0111	100 0101	100 1110	100 0101	101 0010	100 0101	100 1001	101 0110
Ciphertext	000 0000	001 0011	001 0101	001 1001	000 1001	000 0001	001 0010	001 1000	001 0010
Konversi	0	13	15	19	9	1	12	18	12

Plain	I	H	A	H	U	I	B
Binner	100 1001	100 1000	100 0001	100 1000	101 0101	100 1001	100 0010
Kunci	100 1001	100 0111	100 0101	100 1110	100 0101	101 0010	100 0101
Ciphertext	000 0000	000 1111	000 0100	000 0110	001 0000	001 1011	000 0111
Konversi	0	F	4	6	1	1B	7

Gambar 13. *Tabel Perhitungan blok cipher*

Ciphertext:
1918157171F1F13C0131519911218120F4611B7

3. Kesimpulan

Aplikasi kriptografi ini menggunakan kombinasi empat algoritma yaitu caesar cipher, transposisi permutasi segitiga, vigenere, dan block cipher. Aplikasi dapat melakukan proses enkripsi dan dekripsi dengan menggunakan empat algoritma diatas secara berlapis di platform android.

Berdasarkan pembahasan yang telah diuraikan sebelumnya maka dapat diambil kesimpulan yaitu :

1. Penelitian ini menghasilkan aplikasi berbasis mobile yang mampu menyembunyikan data dan informasi rahasia yang dirancang dengan menggunakan UML (Unified Modeling Language).
2. Aplikasi ini dapat melakukan proses enkripsi dan dekripsi pada platform smartphone.
3. Semakin besar ukuran file yang dienkripsi maka semakin lama prosesnya dan semakin besar ukuran file yang dihasilkan.
4. Aplikasi ini dibuat melalui tahap analisis yaitu dengan menggunakan analisis kebutuhan dan analisis kelayakan, setelah itu tahap perancangan yaitu dimulai rancangan aplikasi dan rancangan interface serta implementasi dan pengujian sistem atau aplikasi.

Daftar Pustaka

[1] Munir, R. *Kriptografi* . Bandung:Informatika. 2006.
[2] Ariyus, Dony. *Pengantar Ilmu Kriptografi*. Yogyakarta: Andi, 2008.
[3] Rifki Sadikin, *Pengantar Kriptografi dan Keamanan Jaringan*, Yogyakarta: Andi Offset, 2012.
[4] Nugroho, Adi. *Rekayasa Perangkat Lunak menggunakan UML dan JAVA*. Yogyakarta: Andi Offset, 2009.
[5] Haviluddin ,*"*Memahami Penggunaan UML (Unified Modelling Language)*" Jurnal Informatika Mulawarman* Vol 6 No. 1 Febuari 2011.

Biodata Penulis

Atmaja Basuki, mahasiswa semester 5 Jurusan Teknik Informatika pada STMIK AMIKOM YOGYAKARTA.

Upik Paranita, mahasiswa semester 5 Jurusan Teknik Informatika pada STMIK AMIKOM YOGYAKARTA.

Restu Hidayat, mahasiswa semester 5 Jurusan Teknik Informatika pada STMIK AMIKOM YOGYAKARTA.