Jurnal Teknik Elektro dan Komputasi (ELKOM) ISSN : 2685-1814 (*Print*)
Volume 4 Nomor 1 Maret 2022 ‖ Hal. 91-98 ISSN : 2685-7677 (*Online*)

Pengamanan Transkrip Mahasiswa Menggunakan Kriptografi *Playfair Cipher*

Ali Muhammad Faadhil, Dadang Iskandar Mulyana, Ghofurur Nawangsah, Lerry Salasi Saptan

Teknik Informatika, Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika
Jl. Raden Inten II No.8, Duren Sawit, Kota Jakarta Timur, Indonesia
E-mail: ali21fadhil@gmail.com

Naskah Masuk: 30 Januari 2022; Diterima: 02 Maret 2022; Terbit: 25 Maret 2022

ABSTRAK

Abstrak - Jika peneliti mengkirim pesan ke orang lain, tentu pesan yang dimaksud penting dan peneliti berusaha untuk menjangkau orang yang tepat secepat mungkin. Pesan yang dikirim tentunya menjadi salah satu hal yang paling penting untuk disampaikan. Untuk memastikan bahwa pesan aman sampai orang yang tepat menerimanya, pesan tersebut harus dirahasiakan dan tidak dicurigai oleh orang lain. Kombinasi penulisan *cipher* dengan *cipher* dapat lebih meningkatkan keamanan pesan, dan teknik *cipher* yang digunakan dalam penelitian ini adalah *Playfair cipher*. Karena merupakan salah satu *cipher* susbtitusi yaitu setiap huruf pada teks awal diganti dengan huruf awal yang ditambah dengan kunci yang dikamusak. Jumlah karakter dalam kata sandi akan selalu genap. Kata sandi *Playfair* hanya dapat digunakan untuk *enkripsi* dan *dekripsi* data dalam teks alfaet karakter non-alfanumerik dapat dihindari dengan menuliskannya sebagai teks alfabet. *Enkripsi* dan *dekripsi* data menggunakan kombinasi dua huruf sehingga akan menyulitkan kriptanalis yang menggunakan analisis frekuensi untuk memecahkan sandi *Playfair*. Keyboard hanya digunakan sekali karena kemungkinan keyboard telah digunakan oleh pihak yang tidak berwenang.

Kata kunci: *Playfair, cipher, Enkripsi, Dekripsi,* substitusi

ABSTRACT

Abstract - *When we send messages to other people, of course the message is important and we try to reach the right people as quickly as possible. The message sent is certainly one of the most important things to convey. To ensure that a message is safe until the right person receives it, it must be kept secret and not suspected by others. The combination of writing ciphers with ciphers can further improve message security, and the cipher technique used in this research is Playfair cipher. Because it is a substitution cipher, that is, each letter in the plaintext is replaced with a letter from keyboard. The number of characters in the password will always be even. Playfair passwords can only be used for encryption and decryption of data in alphabetic text. Non-alphanumeric characters can be avoided by writing them as alphabetic text. Encryption and decryption of data uses a combination of two letters so that it will be difficult for cryptanalysts who use frequency analysis to crack Playfair ciphers. Keyboard is only used once because it may have been used by unauthorized parties*.

Keywords: *Playfair, cipher, Enkripsi, Dekripsi, substitution.*

1. PENDAHULUAN

Keamanan data merupkan suatu hal yang sangat penting yang digunakan untuk merahasiakan data-data tertentu yang hanya boleh untuk diketahui oleh pihak tertentu saja [1]. Dalam banyak kasus perpindahan data dari suatu tempat ke tempat lain mengalami ancaman dari pihak yang tidak bertanggung jawab untuk kepentingan sendiri maupun kepentingan kelompok lain, apabila perpindahan data tersebut menggunakan jaringan maka kemungkinan data tersebut oleh pihak lain maka sangat besar.

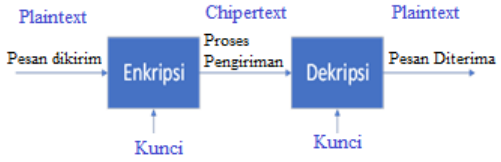
Kriptografi adalah salah satu cara untuk mengamankan data yaitu dengan cara mengubah pesan asli (*plaintext*) kedalam pesan rahasia (*ciphertext*) [2] yang dalam prosesnya melibatkan algoritama pemrograman dan kunci untuk meng*enkripsi* pesan maupun untuk mendekrip pesan agar dapat di baca oleh penerima atau mengubah plaintext dari *ciphertext*. Pada penelitian ini akan dilakukan enkripsi dengan metode *playfair*. Tujuan dari penilitian ini yaitu mengamankan data pada saat perpindahan data dari suatu

tempat ke tempat lain, Menghindari dari pesan tersebut dari kecurigaan, yang dapat dilakukan dengan proses kriptografi.

2. KAJIAN PUSTAKA

2.1. Kriptografi

Kriptografi (*cryptography*) sendiri berasal dari bahasa Yunani yakni "*cryptós*" artinya rahasia, sedangkan "gráphein" artinya tulisan [3], digabungkan menjadi "tulisan rahasia" . Saat ini kriptografi digunakan pada banyak hal terutama untuk mengamankan informasi seperti kerahasiaan/privasi (*confidentiality/privacy*), integritas data (*data integrity*), otentikasi (*authentication*),dan tanpa penyangkalan (*nonrepudiation*)yang digunakan untuk pembuktian. Kriptografi bertujuan untuk menjaga kerahasiaan (*privacy*) data, informasi, dan dokumen supaya tidak dapat diketahui oleh pihak yang tidak berhak mengetahuinya (*unauthorized person*) [4]. Berikut ini adalah bagan cara kerja dari kriptografi:



Gambar 1. Skema *enkripsi*, *ciphertext*, *dekripsi*

Istilah yang terdapat dalam kriptografi:

a. Pesan atau *Plaintext* adalah informasi atau data yang dapat dibaca dan dimengerti oleh siapapun, informasi atau datra tersebut dapat disimpan dalam semua media baik teks, citra, suara, video ataupun berkas biner dapat dikirimkan melalui saluran komunikasi, pesan yang dikirimkan mudah saja untuk dicuri kemudian digunakan oleh orang yang tidak bertanggung jawab oleh karena itu pesan yang akan dikirim kan perlu untuk disandikan agar aman. Bentuk pesan dari yang sudah di sandikan adalah *Ciphertext* atau kriptogram (*cryptogram*) dan pesan tersebuat harus dapat di ubah ke dalam plaintext dengan mudah.
b. komunikasi maka harus ada 2 objek karena jika salah satu tidak ada maka pesan tidak dapat terkirim dengan benar atau tidak akan terjadi komunikasi
c. *Enkripsi* dan *Dekripsi*. Proses menyandikan *plaintext* menjadi *ciphertext* disebut *enkripsi* (encryption) atau en*cipher*ing. *Dekripsi* adalah proses untuk mengubah *cipherteks* menjdi plainteks/data asli [5].
d. Penyadap (*eavesdropper*) ialah seorang yang berusaha mengambil pesan atau data selama proses transmisi pesan atau data sedang berlangsung. Tujuannya ialah mendapatkan informasi dengan cara memecahkan code *cipher*teks tanpa memiliki akses kunci [6].
e. Kriptanalis adalah ilmu yang digunakan untuk memecahkan kode *ciphertext* menjadi plaintext tanpa diketahui kunci yang dipakai seorang pelakunya bisa disebut kriptanalis, sedangkan kriptologi adalah ilmu studi yang mempelajari kriptografi dan kriptanalis [7].

2.2. Playfair Cipher

Seorang berwarga negara inggris yang berahli ilmu fisika yang bernama Sir Chalrles Wheastone lahir di tahun 1890 sampai 1875 ialah penemu kode *Playfair* di temukan [8], dan dipublikasikan oleh Baron Lyon *Playfair* pada 28 maret tahun 1854. *Playfair* pertama kali dipakai sebagai pengirim pesan ataupun kode berupa rahasia dalam pentempuran perang Dunia I oleh militer ingris. Meskipun *Playfair* ini sudah tidak aman dan efektif untuk digunakan pada zaman saat ini, namun *Playfair cipher* banyak dipakai dan cukup efektif pada jamannya [9].

Menurut Aftab, Chaoudhary, Vatsa *ciphertext* hasil *enkripsi* relatif mudah dipecahkan ketika kriptanalisis sudah mengetahui *ciphertext* dan tabel *cipher*-nya, walaupun kriptanalis mengetahui *cipher*text dan tidak mengetahui tabel *cipher* kriptanalis dapat menebak bigram berdasarkan huruf yang bermakna dari sebuah kata [10].

Menurut Stallings, *Playfair cipher* menggunakan papan kunci yang berbentuk bujursangkar dalam melakukan penyandian. Papan kunci ini berukuran 5 kali 5, dimana setiap bagian dalam papan kunci mewakili huruf-huruf dalam alfabet (abjad) dengan menghilangkan huruf J dari abjad [10].

Playfair Cipher adalah salah satu metode dari kriptografi yang menggunakan bentuk tabel berukuran 5 kali 5 sebagai acuan untuk melakukan proses *enkripsi* dan *dekripsi*. *Playfair Cipher* hanya

meng-*enkripsi*kan *plaintext* berupa huruf besar tanpa huruf J dan tidak berulang. *Playfair Cipher* menggunakan metode pasangan huruf (bigram) untuk meng*enkripsi*kan dan men*dekripsi* melalui kunci yang telah diinputkan pada tabel.

Khumar pada tahun 2013 dapat mengembangkan tabel *cipher* yang biasanya 5x5 menjadi 6x6 yang berisi (A-Z) dan (0-9). *Playfair* dengan tabel *cipher* 5x5 tanpa modifikasi akan membuat *cipher* mudah dipecahkan.

Nurkifli (2014) menuliskan beberapa aturan dan proses *enkripsi* maupun *dekripsi* pada *Playfair Cipher*. Berikut beberapa aturan yang perlu dipersiapkan sebelum dilakukannya *enkripsi*:

1. *Playfair Cipher* meng*enkripsi* plaintext berupa huruf besar selain huruf J. Spasi, karakter yang bukan huruf besar, dan huruf J harus dihilangkan dari plaintext.
2. Apabila terdapat huruf J pada plaintext, maka digantikan dengan huruf I.
3. *Plaintext* yang akan di*enkripsi* dituliskan dalam pasangan huruf (bigram).
4. Apabila ada huruf yang sama dalam pasangan huruf, maka disisipkan huruf X atau Z di tengahnya. Huruf yang disisipkan sebaiknya huruf X, karena kemungkinan terdapat huruf X yang sama dalam bigram sangat kecil.
5. Apabila jumlah huruf pada plaintext adalah ganjil, maka dipilih sebuah huruf sembarang untuk ditambahan di akhir plaintext.

Setelah dilakukan aturan-aturan dan didapat rangkaian kunci pada *Playfair Cipher*, rangkaian kunci tersebut diperluas. Berikut merupakan langkah-langkah *enkripsi Playfair Cipher*:

a. Apabila ada dua huruf atau angka terdapat pada baris kunci yang sama, maka setiap huruf atau angka diganti dengan atau angka di kanannya.
b. Apabila ada dua huruf atau angka terdapat pada kolom kunci yang sama, maka setiap huruf atau angka diganti dengan huruf atau di bawahnya.
c. Apabila ada dua huruf atau angka tidak pada baris atau kolom yang sama, maka huruf atau angka pertama diganti dengan dengan huruf atau angka pada perpotongan baris huruf atau angka pertama dengan kolom huruf atau angka kedua. Huruf atau angka kedua diganti dengan huruf atau angka pada titik sudut keempat dari persegi panjang yang dibentuk dari huruf atau angka yang digunakan.

Berikut merupakan langkah-langkah *dekripsi Playfair Cipher*:

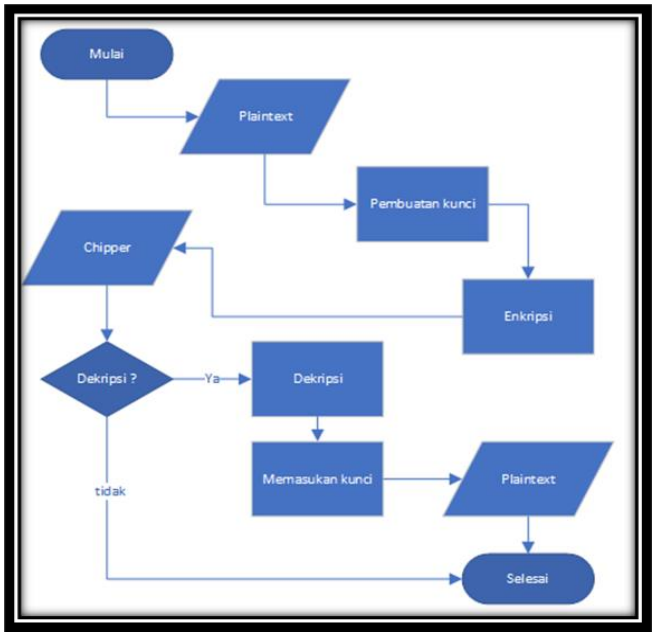
a. Apabila ada dua huruf atau angka terdapat pada baris kunci yang sama maka tiap huruf diganti dengan huruf di kirinya, begitu juga untuk angka.
b. Apabila ada dua huruf atau angka terdapat pada kolom yang sama maka tiap huruf diganti dengan huruf di atasnya, begitu juga untuk angka.
c. Jika dua huruf atau angka tidak pada baris yang sama atau kolom yang sama, maka huruf atau angka pertama diganti dengan huruf atau angka pada perpotongan baris huruf atau angka pertama dengan kolom huruf atau angka kedua. Huruf kedua diganti dengan huruf atau angka pada titik sudut keempat dari persegi panjang yang dibentuk dari huruf atau angka yang digunakan.

3. METODE PENELITIAN

Metode yang digunakan dalam penelitian ini merupakan metode penelitian kuantitatif bersifat pengumpulan data dan pengembangan, dengan cara dilakukan penerapan teknik dari metode *Playfair cipher*. pengumpulan data yang dimaksud berasal dari sumber data primer dan sumber data sekunder. Sumber data yang diambil dari nama mahasiswa dan nilai dan untuk sumber data sekunder diambil dari jurnal, artikel, makalah, dan buku referensi.

Alur dari proses enkripsi pada penelitian ini dapat dilihat pada Gamba2. Pada gambar Gambar 2 dapat ditentukan alur dari proses enkripsi sehingga teks plaintext diubah kedalam ciphertext pertama kita masukan data transkip mahasiswa kedalam program aplikasi data tersebut dapat berupa huruf maupun angka, setalah data tersebut dimasukan ke dalam program maka kita dapat menambahkan kunci untuk enkripsi, dalam kunci tersebut hanya dapat berbentuk angka dari angka 1 sampai dengan 9 dalam hal ini kunci dapat terdiri dari satu digit maupun lebih yang disesuaikan dari kebutuhannya sehingga nantinya data yang di enkripsi tidak dapat diubah kedalam data sebelum di enkripsi. Setelah memasukan kunci maka dapat menekan tombol enkripsi sehingga data akan diubah menjadi *chipertext* dan data ditampilkan menjadi data yang tidak mudah dibaca sehingga data dapat dikirimkan ke penerima. Setelah data diterima maka si penerima belum dapat mengetahui isi dari data yang dikirimkan maka perlu proses merubah *ciphertext* menjadi *plaintext* proses tersebut dinamakan dekripsi. Pada Gambar 2 juga dapat dilihat jika proses dekripsi membutuhkan kunci yang sama pada saat melakukan enkripsi jika kunci enkripsi dan dekripsi tidak sama maka proses enkripsi tidak dapat dilakukan karena hasil atau *output* dari dari data yang didekripsi tidak

sama dengan data sebelum di enkripsi oleh karena itu pengirim data atau orang yang mengenkripsi data harus menginformasikan ke penerima atau orang yang akan membaca data tersebut agar tidak ada kesalahan dalam mengdekripsikan data, lalu jika sudah memasukan kunci dapat menekan tombol dekripsi dan proses selesai data siap dibaca.



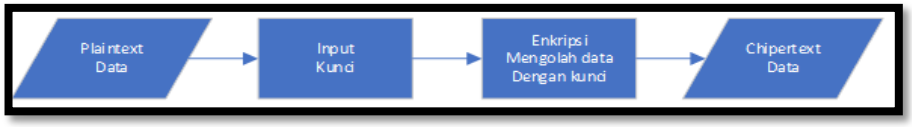
Gambar 2.Tahapan proses penelitian "*Playfair*"

Metode pengujian yang nantinya dilakukan adalah pengujian langsung ke beberapa mahasiswa yang terdaftar didalam kampus peneliti dimana nantinya yang akan diujikan dalam program ini adalah bagaimana program tersebut berjalan dengan baik atau tidak, tingkat keefektifan program untuk mengamankan data, proses pengujian ini akan dibahas secara lengkap di bab selanjutnya.

4. HASIL DAN PEMBAHASAN

Playfair cipher atau yang biasa dikenal dengan *Playfair* Square merupakan salah satu teknik *enkripsi* simetris yang termasuk dalam sistem penggantian graf berarah. *Playfair Cipher* termasuk dalam polygram *cipher*. Diciptakan oleh Sir Charles Wheatstone, tetapi dipopulerkan/dipopulerkan oleh Baron Lyon *Playfair* pada tahun 1854. *Playfair Cipher* meng*enkripsi* pasangan huruf (diagram atau digraf) alih-alih huruf individual seperti pada sandi klasik/tradisional lainnya. Tujuannya untuk mempersulit analisis frekuensi karena frekuensi kemunculan huruf dalam *cipher*text akan datar.

Dalam praktiknya, *Playfair* mengambil setiap huruf (misalnya A) dan menggantinya dengan huruf yang ditemukan setelah sejumlah posisi tertentu berdasarkan kunci yang benar. Contoh: Ambil huruf "a" dan ganti dengan huruf yang ditemukan dua tempat setelahnya, yaitu "c", dalam hal ini kuncinya adalah "2". Secara khusus, kunci yang akan peneliti gunakan tidak terdiri dari satu digit, tetapi dua digit atau lebih, jadi siapa pun yang mencoba men*dekripsi* pesan, Untuk pemahaman yang lebih baik, peneliti menjelaskan metode yang digunakan dengan sebuah contoh. Misalkan peneliti ingin meng*enkripsi* teks berikut "aaaab" (tanpa tanda kutip) menggunakan kunci 1234, hasilnya akan menjadi "bcdec



Gambar 3. Proses *enkripsi*, *Playfair*

Dalam proses plaintext memiliki sebuah kunci dari *Playfair cipher* dari ketentuan atau kalimat yang peneliti buat yang mudah di ingat sehingga membuang huruf yang berulang dari huruf yang akan diolah datanya dalam sebuah kalimat *enkripsi*.

Tabel 1. *Playfair*

Surat	Posisi Ditambahkan	Hasil
a	1	b
a	2	c
a	3	d
a	4	e
b	1	c

Karena teks yang akan di*enkripsi* lebih panjang dari kunci, peneliti hanya menambahkan tempat pada huruf "b" (huruf kelima), karena setiap kali peneliti menggunakan semua digit kunci, jika peneliti memiliki huruf lain untuk di*enkripsi*, peneliti mulai dengan digit pertama kunci. Bahkan, jika ada 'c' setelah 'b', 2 posisi ditambahkan, sehingga huruf yang di*enkripsi* menjadi 'e'.

Teks dapat berisi tanda baca seperti titik, koma, dan lain-lain karena saat menambahkan posisi ke karakter, Pembaca mengikuti urutan abjad ASCII. Dalam proses *enkripsi*-nya dapat dilihat dalam table berikut:

Tabel 2. *Enkripsi* huruf pertama

a	B	c	d
e	F	g	h
i	J	k	l
m	N	o	p
q	R	s	t

Dalam proses diatas maka huruf pertama “a” ditambah 1 huruf berikutnya sesuai dengan kunci yang pertama yaitu 1 menjadi huruf “b”

Tabel 3. *Enkripsi* huruf kedua

a	B	c	d
e	F	g	h
i	J	k	l
m	N	o	p
q	R	s	t

Untuk huruf kedua “a” ditambahkan 2 huruf berikutnya karena dikunci huruf kedua adalah 2 maka menjadi huruf “c”

Tabel 4. *Enkripsi* huruf ketiga

a	B	c	d
e	F	g	h
i	J	k	l
m	N	o	p
q	R	s	t

Untuk huruf ketiga “a” ditambahkan 3 huruf berikutnya karena dikunci huruf kedua adalah 3 maka menjadi huruf “d”

Tabel 5. *Enkripsi* huruf keempat

a	B	c	d
e	F	g	h
i	J	k	l
m	N	o	p
q	R	s	t

Untuk huruf keempat “a” ditambahkan 4 huruf berikutnya karena dikunci huruf kedua adalah 4 maka menjadi huruf “e”.

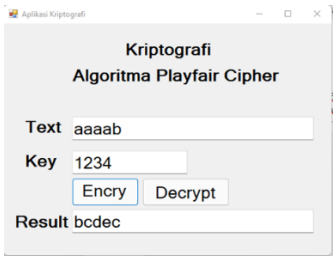
Tabel 6. *Enkripsi* huruf kelima

a	B	c	d
e	F	g	h
i	J	k	l
m	N	o	p
q	R	s	t

Untuk huruf kelima “b” ditambahkan 1 huruf karena di dalam kunci hanya terdapat 4 kunci saja maka huruf kelima Kembali ke kunci awal maka huruf “b” ditambah 1 menjadi huruf “c”

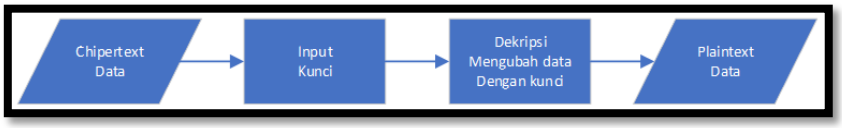
Tabel 7. *Enkripsi* huruf kelima

a	b	c	d
e	f	g	h
i	j	k	l
m	n	o	p
q	r	s	t



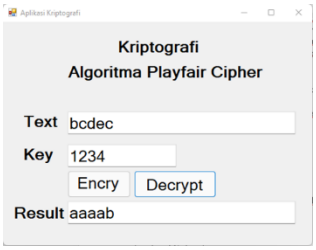
Gambar 4. Proses *enkripsi* aaaab

Setelah data di *enkripsi* dengan kunci yang sudah dipilih maka data akan dikirimkan kepada penerima melalui jaringan atau media perpindahan data lainnya. Lalu data akan dibuka oleh penerima untuk melihat data yang sebenarnya maka diperlukan kunci yang sebelumnya digunakan untuk meng*enkripsi*kan data dengan proses seperti bagan dibawah ini:



Gambar 5**.** Proses *dekripsi*

Dalam prosesnya ini maka data yang sebeumnya di *enkripsi* akan di tampilkan atau di*dekripsi* sehingga penerima data membaca. *Dekripsi* ini membutuhkan kunci yang sama dengan saat proses *enkripsi* jika tidak sama maka data yang ditampilkan nantinya tidak sesuai dengan plaintext/data sebelum di *enkripsi* dan akan terdapat kesalahan informasi karena itulah sebuah kunci dalam *enkripsi* sangat dibutuhkan. Sebagain contoh *enkripsi* sebagai berikut:



Gambar 6. Proses *dekripsi* aaaab

Data yang sebelumnya yaitu "aaaab" setelah di *enkripsi* dengan kunci 1234 menjadi "bcdec" setelah sampai kepada penerima maka akan di kembalikan menjadi plaintext agar dapat dibaca dengan benar oleh penerima maka harus dimasukan kunci yang sama juga. Prosesnya seperti berikut:

Tabel 8. *Dekripsi* huruf pertama

a	b	c	d
e	f	g	h
i	j	k	l
m	n	o	p
q	r	s	t

Huruf pertama dalam data tersebut yaitu "b" dikurangi dengan huru sebelumnya karena kunci pertama adalah 1 dan mejadi huruf "a"

Tabel 9. *Dekripsi* huruf kedua

a	b	c	d
e	f	g	h
i	j	k	l
m	n	o	p
q	r	s	t

Huruf kedua dalam data tersebut yaitu "c" dikurangi dengan huru sebelumnya karena kunci kedua adalah 2 dan mejadi huruf "a"

Tabel 10. *Dekripsi* huruf ketiga

a	b	c	d
e	f	g	h
i	j	k	l
m	n	o	p
q	r	s	t

Huruf kedua dalam data tersebut yaitu "d" dikurangi dengan huru sebelumnya karena kunci ketiga adalah 3 dan mejadi huruf "a"

Tabel 11. *Dekripsi* huruf keempat

a	b	c	d
e	f	g	h
i	j	k	l
m	n	o	p
q	r	s	t

Huruf kedua dalam data tersebut yaitu "e" dikurangi dengan huru sebelumnya karena kunci keempat adalah 4 dan mejadi huruf "a"

Tabel 12. *Dekripsi* huruf kelima

a	b	c	d
e	f	g	h
i	j	k	l
m	n	o	p
q	r	s	t

Karena hanya terdapat 4 kunci maka huruf kelima akan Kembali ke kunci pertama yaitu 1 maka huruf "c" didalam data tersebut berubah menjadi huruf "b".

Jika sudah seperti itu dapat diimplemestasikan kedalam pengamanan transkrip mahasiswa dengan data yang telah disediakan oleh pihak kampus atau perguruan tinggi dalam satu mata kuliah dan terdiri dari 5 orang mahasiswa sebagai contoh dalam transkrip tersebut terdapat NIM, nama, dan nilai supaya data taranskip mahasiswa tersebut aman maka dapat dilakukan enkripsi pada nama dan nim mahasiswa satu

persatu sebagai berikut contoh data nilai mata kuliah Pemrograman Web:

Tabel 13. Transkrip mahasiswa

NIM	Nama	Nilai
18110111012	Edi Nur Hadi	89
18110111043	Hendra Eky	85
18110111034	Muhammad Al-fath	78
18110111027	Lintang Purnama	79
18110111052	Endang Tri Handoyo	90

Setelah data tersebut didapatkan maka kita harus merubah satu persatu kedalam ciphertext agar data tersebut menjadi teks yang tidak bisa dibaca tanpa di dekripsi terlebih dahulu dan menghindari data digunakan oleh pihak yang tidak bertanggung jawab. Data tersebut akan di *enkripsi* dengan kunci "987" sehingga data menjadi seperti tabel berikut:

Tabel 14. Data *enkripsi*

NIM	Nama	Nilai
:@8:88:97::	Nlp)V|{(Ojlp	AA
:@8:88:97=;	Qmumzh)Mr,	A=
:@8:88:97<<	V}ojutjl'Jt4oi{q	@@
:@8:88:97;?	Uqu}iup(W~zujuh	@A
:@8:88:97>:	Nvkjvn)\yr(Ojvkx • v	B8

Jika data sudah di *enkripsi* seperti diatas maka data tidak akan mudah untuk diketahui oleh pihak yang tidak bertanggung jawab dan akan lebih aman untuk memindahkan data dari suatu tempat ke tempat lainnya. Pembuatan program aplikasi ini dibuat dengan menggunakan *visual studio* 2022 dan menggunakan Bahasa VB (*Visual Basic*)

5. KESIMPULAN

Setelah dilakukan uji coba maka didapatkan hasil jika suatu program yang dijalankan *cipher*text dalam meng*enkripsi*kan suatu kode yang peneliti buat dalam pemograman kriptograpi dan menganalisis kesimpulan yang dapat diambil dari Sandi *Playfair* mengkodekan pasangan huruf dengan tujuan mempersulit analisis frekuensi karena frekuensi kemunculan huruf dalam teks sandi tidak akan berubah. Implementasi ASCII juga akan membuat *cipher* yang dihasilkan lebih sulit untuk dipahami oleh pihak ketiga. Dengan menerapkan kombinasi dan kriptografi dalam mengamankan data transkrip siswa, sehingga dapat dipastikan tidak akan diketahui orang lain karena tidak akan menimbulkan kecurigaan menujukan terhadap penelitian ini.

REFERENSI

[1] M.K. Subsitusi, "95-243-1-Pb," vol. 6, no. 1, 2018.
[2] A. R. Tulloh, Y. Permanasari, dan E. Harahap, "Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen," *J. Mat. UNISBA*, vol. 2, no. 1, hal. 118–125, 2016.
[3] F.M. Ikhsan, "Kriptografi File PDF Dengan Algoritma XTEA (Algoritma Extended Tiny Encryption Algorthm)," no. January, 2019.
[4] M. A. Zainuddin dan D. I. Mulyana, "Penerapan Algoritma RSA untuk Keamanan Pesan Instan Pada Perangkat Android," *J. CKI SPOT*, vol. 9, no. 2, hal. 105–114, 2016.
[5] Y. Anggraini dan D. V. S. Y. Sakti, "Penerapan Steganografi Metode End of File (Eof) Dan *Enkripsi* Metode Data Encryption Standard (Des) Pada Aplikasi Pengamanan Data Gambar Berbasis Java," *Konf. Nas. Sist. Informasi, STMIK Dipanegara Makassar*, no. September 2016, hal. 1743–1753, 2014.
[6] M. Nahak, "Bab Ii Tinjauan Pustaka Dan Landasan Teori," *J. Chem. Inf. Model.*, vol. 53, no. 9, hal. 21–25, 2017.
[7] H. R. C. Bawono, "Kriptanalisis pada Algoritma *Cipher* Algorithm," *Skripsi*, hal. 1–123, 2015.
[8] E. Andriana, "Algoritma *Enkripsi Playfair Cipher*," *Tek. Inform.*, no. May, hal. 1–5, 2016.
[9] I. Solihin, Mesran, dan A. P. U. Siahaan, "Implementasi Algoritma Super *Playfair Cipher* Dan Two Square *Cipher* Dalam Pengamanan Pesan Teks," *KOMIK (Konferensi Nas. Teknol. Inf. dan Komputer)*, vol. 1, no. 1, hal. 195–201, 2017.
[10] R. W. Simbolon, "*Cipher* Dan Steganografi Dengan Teknik Least Significant Bit (Lsb) Protecting the Student Academic Transcript Using *Playfair Cipher* Cryptography," *J. Teknol. Inf. dan Komun.*, vol. 5, no. 1, hal. 59–70, 2016.