PENGAMANAN DATA DALAM JARINGAN LAN DENGAN MENGGUNAKAN ALGORITMA CHIPER TRANSPOSISI

Sanco Simanullang

Universitas Methodist Indonesia

sancosimanullang@methodist.ac.id

ABSTRACT

Data security is important in the implementation of information technology, especially in the field of computers, which allows thousands of people and computers around the world to be connected in a virtual world known as cyberspace or the internet. This can create new challenges and demands for the availability of a data security system that is as sophisticated as the advances in computer technology itself. In cryptography, data sent over the network will be disguised in such a way that even if the data can be read by third parties, it should not be understood by unauthorized parties. Data to be sent and has not been encrypted which produces ChipperTtext. The implementation of the transposition algorithm for securing data flowing in the Local Area Network (LAN), the transposition process changes the arrangement of letters from the source text (plaintext), with a column transposition cipher, to obtain the words in a barred manner. In the transposition cipher, the plaintext is the same, but the sequence is changed. . This algorithm transposes a series of characters in the text. Another name for this method is permutation, because transpose each character in the text is the same as permutating the characters so that this application generates encrypted data on the network stream and returns it to plaintext at the final destination. So that it can be ensured that the information and data sent to other parties is safe from unauthorized parties.

Keywords: data security, LAN, columnar transposition, cipher transposition

I. PENDAHULUAN

Perkembangan pengolahan data dan informasi yang begitu pesat saat ini, keamanan (*security*) data menjadi hal yang sangat penting untuk melakukan pengiriman data dan komunikasi data lainnya. Dalam pengiriman dan penerimaan data, sering kali pengguna baik pengirim atau penerima membutuhkan sesuatu yang dapat meyakinkan mereka bahwa data yang diperoleh adalah data yang aman dan benar. Salah satu cara yang digunakan untuk tujuan tersebut adalah kriptografi dengan mengenskripi data yang akan dikirim. Tujuan dari kriptografi adalah kerahasiaan *(Privacy/confidentially)*, integritas (*Integrity)*, Otentikasi *(Autehntication)* dan pembuktian yang tak tersangkal *(nonrepudiation)*.
Pada proses kriptografi yang pada umumnya, pesan asli (plainteks) diubah menjadi pesan yang tidak memiliki makna (cipherteks)[1], yang disebut dengan proses enkripsi. Setelah itu, cipherteks dikirim kepada penerima yang seharusnya untuk diubah kembali menjadi plainteks. Pada proses pengiriman sering terjadi penyadapan atau pencurian cipherteks asli oleh pihak yang tidak berhak. Cipherteks yang disadap tersebut, oleh penyadap memiliki berbagai kemungkinan, diantaranya isi cipherteks yang asli diubah, sehingga cipherteks yang diterima oleh penerima bukan merupakan cipherteks yang asli. Untuk meyakinkan bahwa si penerima memang menerima cipherteks yang asli, dibutuhkan sesuatu seperti tanda tangan pada surat. Dalam perkembangannya, kriptografi memiliki banyak teknik dalam mengenkripsi data, diantaranya adalah Algoritma Cipher Transposisi dan. Cipher transposisi merupakan algoritma kriptografi klasik yangdigunakan oleh tentara Sparta di Yunani pada permulaan tahun 400 SM. Mereka menggunakan alat yang namanya *scytale*. Algoritma Cipher Transposisi[2] akan digunakan untuk mengubah plainteks menjadi cipherteks. Permasalahan yang sering dihadapi adalah bagaimana cara untuk mengamankan suatu data dengan menggunakan algoritma cipher transposisi pada sebuah jaringan Local Area Network (LAN) di sebuah institusi. Sehingga dapat membantu pengguna dalam mengamankan data dan dapat memahami teknik pengamanan data dengan menggunakan kriptografi yaitu algoritma cipher transposisi. Manfaat yang diharapkan dari penelitian ini adalah tersedianya sebuah aplikasi yang dapat dipergunakan untuk melakukan enkripsi dan deskripsi data dalam LAN.

II. TINJAUAN PUSTAKA

Kriptografi

Kriptografi memiliki sejarah yang panjang dan mengagumkan.Penulisan rahasia ini dapat dilacak kembali ke 3000 tahun SM saat digunakan oleh bangsa Mesir.Mereka menggunakan *hieroglyphcs* untuk menyembunyikan tulisan dari mereka yang tidak diharapkan.Hieroglyphcs diturunkan dari bahasa Yunani hieroglyphica yang berarti ukiran rahasia. Hieroglyphs berevolusi menjadi hieratic, yaitu *stylized script* yang lebih mudah untuk digunakan. Sekitar 400 SM, kriptografi militer digunakan oleh bangsa Spartan dalam bentuk sepotong papirus atau perkamen dibungkus dengan batang kayu. Sistem ini disebut Scytale[1]. Sekitar 50 SM, Julius Caesar, kaisar Roma, menggunakan *cipher substitusi* untuk mengirim pesan ke Marcus Tullius Cicero. Pada *cipher* ini, huruf-huruf alfabet disubstitusi dengan huruf-huruf yang lain pada alfabet yang sama. Karena hanya satu alfabet yang digunakan, cipher ini merupakan substitusi monoalfabetik.*Cipher* semacam ini mencakup penggeseran alfabet dengan 3 huruf dan mensubstitusikan huruf tersebut. Substitusi ini kadang

dikenal dengan C3 (untuk Caesar menggeser 3 tempat). Secara umum sistem cipher Caesar dapat ditulis sebagai berikut :

$$Zi = Cn(Pi)$$

Dimana Zi adalah karakter-karekter ciphertext, Cn adalah transformasi substitusi alfabetik, n adalah jumlah huruf yang digeser, dan Pi adalah karakter-karakter *plaintext*. Disk mempunyai peranan penting dalam kriptografi sekitar 500 th yang lalu. Di Italia sekitar tahun 1460, Leon Battista Alberti mengembangkan disk *cipher* untuk enkripsi. Sistemnya terdiri dari dua disk konsentris. Setiap disk memiliki alfabet di sekelilingnya, dan dengan memutar satu disk berhubungan dengan yang lainnya, huruf pada satu alfabet dapat ditransformasi ke huruf pada alfabet yang lain[5][6].

Enkripsi Kunci Rahasia

Secret-key cryptography kadang disebut sebagai *symmetric cryptography* merupakan bentuk kryptografi yang lebih tradisional, dimana sebuah kunci tunggal dapat digunakan untuk mengenkrip dan mendekrip pesan. *Secret-key cryptography* tidak hanya berkaitan dengan enkripsi tetapi juga berkaitan dengan otentikasi, disebut juga *message authentication codes*. Masalah utama yang dihadapi *secret-key cryptography* adalah membuat pengirim dan penerima menyetujui kunci rahasia tanpa ada orang lain yang mengetahuinya. Ini membutuhkan metode dimana dua pihak dapat berkomunikasi tanpa takut akan disadap[7]. Kelebihan *secret-key cryptography* dari *public-key cryptography* adalah lebih cepat. Teknik yang paling umum dalam *secret-key cryptography* adalah *block ciphers*, *stream ciphers*, dan message authentication codes. Berdasarkan jenis kunci yang digunakannya, algoritma kriptografi dikelompokan menjadi dua bagian, yaitu

1. Symmetric Algorithm

Symmetric algorithm atau disebut *juga secret key algorithm* adalah algoritma yang kunci enkripsinya dapat dihitung dari kunci dekripsi dan begitu pula sebaliknya, kunci dekripsi dapat dihitung dari kunci enkripsi. Pada sebagian besar *symmetric algorithm* kunci enkripsi dan kunci dekripsi adalah sama[3]. *Symmetric algorithm* memerlukan kesepakatan antara pengirim dan penerima pesan pada suatu kunci sebelum dapat berkomunikasi secara aman.Keamanan *symmetric algorithm* tergantung pada rahasia kunci.Pemecahan kunci berarti memungkinkan setiap orang dapat mengenkripsi dan mendekripsi pesan dengan mudah.*Symmetric algorithm* dapat dikelompokkan menjadi dua jenis, yaitu *stream cipher* dan *block cipher*. *Stream cipher* beroperasi bit per bit (atau byte per byte) pada satu waktu. Sedangkan *block cipher* beroperasi per kelompokkelompok bit yang disebut blok (*block*) pada satu waktu.

2. Asymmetric Algorithm

Asymmetric algorithm atau disebut juga *public key algorithm* didesain agar memudahkan dalam distribusi kunci yang digunakan untuk enkripsi dan dekripsi.Kunci dekripsi pada *public key algorithm* secara praktis tidak dapat dihitung dari kunci enkripsi.Algoritma ini disebut "*public key*" karena kunci dapat dibuat menjadi publik.Setiap orang dapat menggunakan kunci enkripsi untuk mengenkripsi pesan, tetapi hanya orang yang memiliki kunci dekripsi yang dapat mendekripsi pesan tersebut.Pada sistem ini kunci enkripsi sering disebut kunci publik (*public key*), dan kunci dekripsi disebut kunci rahasia (*private key*). Teknik kriptografi modern yang ada saat ini dapat dikelompokkan sebagaimana ditunjukkan (*Gambar 2 Pengelompokkan enkripsi beserta contoh).*Pada bagian ini akan didiskusikan operasi-operasi penyandian dasar untuk memberikan dasar bagi pemahaman tentang evolusi metode-metode enkripsi dan usaha-usaha cryptanalysis yang berkaitan.

Substitusi

Caesar cipher adalah *cipher substitusi* yang sederhana mencakup pergeseran huruf alfabet 3 posisi ke arah kanan. Kemudian Caesar cipher merupakan subset dari cipher polialfabetik Vigenere. Pada Caesar cipher karakter-karakter pesan dan pengulangan kunci dijumlahkan bersama, modulo 26. Dalam penjumlahan modulo 26, huruf-huruf A-Z dari alfabet masing-masing memberikan nilai 0 sampai 25. Tipe *cipher* ini dapat diserang menggunakan analisis frekuensi. Dalam frekuensi analisis, digunakan karakteristik frekuensi yang tampak dalam penggunaan huruf-huruf alfabet pada bahasa tertentu. Tipe cryptanalysis ini dimungkinkan karena Caesar *cipher* adalah monoalfabetik *cipher* atau *cipher* substitusi sederhana, dimana karakter *ciphertext* disubstitusi untuk setiap karakter *plaintext*. Serangan ini dapat diatasi dengan menggunakan substitusi polialfabetik. Substitusi polialfabetik dicapai melalui penggunaan beberapa cipher substitusi. Namun substitusi ini dapat diserang dengan penemuan periode, saat substitusi berulang kembali[12][13].

Transposisi (Permutasi)

Pada *cipher* ini, huruf-huruf *plaintext* dipermutasi. Sebagai contoh, huruf-huruf plaintext I P P I C K I P D I W N dapat dipermutasi menjadi D C K I I W N I P I P P. *Cipher* transposisi kolumnar adalah *cipher* dimana *plaintext* ditulis secara horisontal pada kertas dan dibaca secara vertikal. *Cipher* transposisi dapat diserang melalui analisis frekuensi, namun *cipher* menyembunyikan properti statistik dari pasangan huruf-huruf, seperti IS dan TOO.

Contoh Permutasi :

Diketahui himpunan A(a,b,c). Tentukan banyaknya permutasi,jika

a.Diambil 2 unsur

b.Diambil semua(3unsur)

jawab :

a. Banyaknya permutasi 2 unsur dan 3 unsur

$$3P2 = \frac{3!}{(3-2)!} = \frac{3!}{1!} = \frac{3.2.1}{1} = 6$$

Permutasi dari a,b,c adalah abc,acb,bac,cab,cba

b. Banyaknya permutasi 3 unsur dan 3 unsur

$$3P2 = \frac{3!}{(3-3)!} = \frac{3!}{0!} = \frac{3.2.1}{1} = 6$$

Permutasi dari a,b,c adalah
abc,acb,bac,bca,cab,cba

Local Arena Network (LAN)

Jaringan LAN adalah sebuah jaringan komputer yang jaringannya hanya mencakup wilayah tertentu (Kecil); seperti jaringan komputer kampus, gedung, kantor, dalam rumah, sekolah atau yang lebih kecil. Saat ini, kebanyakan LAN berbasis pada teknologi IEEE 802.3 Ethernet menggunakan perangkat switch, yang mempunyai kecepatan transfer data 10, 100, atau 1000 Mbit/s. Selain teknologi Ethernet, saat ini teknologi 802.11b (atau biasa disebut *Wi-fi*) juga sering digunakan untuk membentuk LAN. Tempat-tempat yang menyediakan koneksi LAN dengan teknologi *Wi-fi* biasa disebut *hotspot*. Berbeda dengan Jaringan Area Luas atau Wide Area Network (WAN), maka LAN mempunyai karakteristik (1) mempunyai pesat data yang lebih tinggi, (2) meliputi wilayah geografi yang lebih sempit dan (3) tidak membutuhkan jalur telekomunikasi yang disewa dari operator telekomunikasi[11].

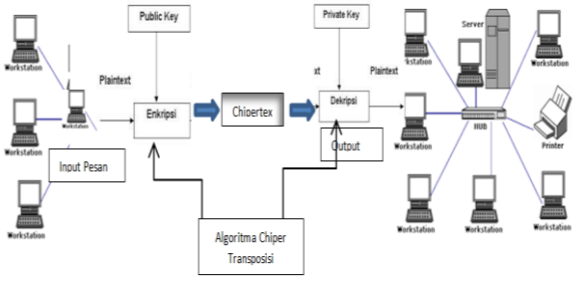
III. METODOLOGI

Metodologi yang digunakan adalah sebagai berikut :

a. Studi Literatur, pada tahap ini bertujuan memperoleh informasi dengan mengumpulkan, mempelajari dan membaca berbagai referensi baik itu dari buku-buku, jurnal, makalah, internet dan berbagai sumber lainnya yang menunjang dalam penulisan skripsi ini.
b. Analisis, pada tahap ini akan dilakukan analisis permasalahan dan kebutuhan sistem yaitu Menganalisa Algoritma Cipher Transposisi serta teknik-teknik yang digunakan.
c. Perancangan, merancang suatu aplikasi yang mengiplementasikan Algoritma Cipher
d. Pengkodean, pada tahap ini sistem yang telah dirancang diimplementasikan menggunakan bahasa pemrograman.
e. Pengujian dan Perbaikan, pada tahap ini dilakukan pengujian kinerja aplikasi yang telah dibuat dengan mencari kelemahan yang masih ada pada aplikasi tersebut, kemudian memperbaikinya.

Adapun skema proses yang dilakukan dapat digambarkan pada gambar 1 berikut ini.

Proses input dan output pesan dapat digambarkan dalam kerangka berikut ini:



Gambar 1. Skema kinerja sistem

IV. PEMBAHASAN

Analisa Transposisi

Seluruh teknik yang telah dipelajari di atas mengikutsertakan substitusi simbol cipher text untuk sebuah simbol dari plaintext. Metode yang berbeda didapat dengan adanya permutasi singkat untuk huruf-huruf plaintext.Teknik ini disebut sebagai transposition cipher.Teknik yang paling sederhana adalah teknik rail fence, dimana plaintext ditulis dengan urutan kolom dan dibaca sebagai urutan baris. Sebagai contoh untuk mengenkripsi pesan “meet me after the toga party” dengan metode rail fence dengan kedalaman 2, kita dapat menuliskan sebagai :

nenaprhpgpry

ipifipioaap

Pesan yang telah dienkripsi adalah :

NENAPRHPGPRYIPIFIPIOAAP

Metode ini cukup mudah dipecahkan.Skema yang lebih kompleks adalah dengan menuliskan pesan sebagai sebuah kotak, baris demi baris, dan membaca pesan itu kolom demi kolom, tetapi dengan permutasi dari urutan kolom. Urutan kolom kemudian menjadi kunci dari algoritma.

Key	:	4	3	1	2	5	6	7
Plaintext	:	a	t	t	a	c	k	p
		o	s	t	p	o	n	e
		d	u	n	t	i	l	T
		w	o	a	m	x	y	z
Chippertext	TTNAAPTMTSUOAODWCOIXKNLYPETZ							

Transposisi yang murni juga mudah dikenali karena mempunyai frekuensi huruf yang sama dengan plaintext. Transposition cipher dapat dibuat lebih aman secara signifikan dengan melakukan lebih dari satu level permutasi. Hasilnya adalah lebih permutasi yang lebih kompleks dan sulit untuk direkonstruksi menjadi plaintext

Key	:	4	3	1	2	5	6	7
Plaintext	:	t	t	n	a	a	p	t
		m	t	s	u	o	a	o
		d	w	c	o	i	x	k
		n	l	y	p	e	t	z
Chippertext		NSCYAUOPTTWLTMDNAOIEPAXTTOKZ						

Cipher teks diperoleh dengan mengubah posisi huruf di dalam plaintekls.

1. Dengan kata lain, algoritma ini melakukan transpose terhadap rangkaian huruf di dalam plainteks.
2. Nama lain untuk metode ini adalah permutasi, karena transpose setiap karakter di dalam teks sama dengan mempermutasikan karakter-karakter tersebut.

Contoh: Misalkan plainteks adalah

DEPARTEMEN TEKNIK INFORMATIKA ZZZ

Enkripsi:

D E P A R T
E M E N T E
K N I K I N
F O R M A T
I K A Z Z Z

Cipherteks: (baca secara vertikal)

DEKFIEMNOKPEIRAANKMZRTIAZTENTZ

atau

DEKFI EMNOK PEIRA ANKMZ RTIAZ TENTZ

Dekripsi: Bagi panjang cipherteks dengan kunci. (Pada contoh ini, 30 / 6 = 5)

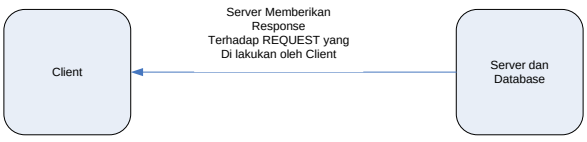
D E K F I
E M N O K
P E I R A
A N K M Z
R T I A Z
T E N T Z

Plainteks: (baca secara vertikal)

DEPARTEMEN TEKNIK INFORMATIKA ZZZ

Socket Pada Server

Socket ini di gunakan untuk komunikasi antar komputer, umumnya lewat network atau internet. Socket server ini biasa digunakan untuk pemrograman berbasis clientserver yang dapat menggunakan socket TCP/IP atau socket UDP yang berfungsi sebagai pemberi informasi pada client yang meminta layanan tersebut dan jalur pada sistem ini dapat di lihat pada diagram di bawah ini :



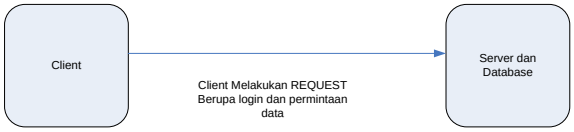
Gambar 2 : Server yang memberikan RESPONSE ke Client

Tugas-tugas dari server ini biasanya berupa :

a. Menunggu Koneksi dari Client
b. Mengirim data Permintaan Client
c. Menutup koneksi pada client tertentu
d. Menset No Port dan No IP yang akan di pergunakan di dalam jaringan
e.Mendengarkan data yang masuk

Socket Pada Client

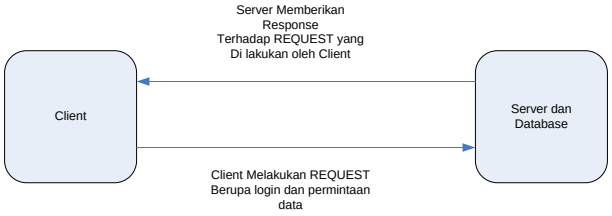
Socket ini di gunakan untuk komunikasi antar komputer, umumnya lewat network atau internet. Socket Client ini biasa digunakan untuk pemrograman berbasis client server yang dapat menggunakan socket TCP/IP atau socket UDP yang informasinya dapat di lihat dari server, sehingga client harus tergantung pada server untuk informasi yang akan di olahnya



Gambar 3 : Client yang melakukan REQUEST ke Server

Tugas-tugas dari Client ini biasanya berupa :

a. Melakukan Koneksi Ke Server
b. Mengirim data Permintaan/REQUEST ke Server
c. Menutup koneksi pada Server
d. Mendengarkan data yang masuk dari server



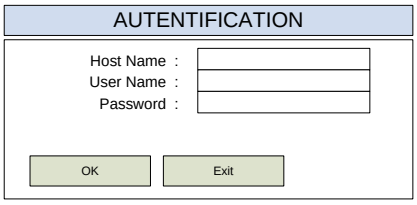
Gambar 4 : Hubungan Client dan Server

Pengiriman Data Melalui TCP/IP

Data yang dikirimkan ke server atau pun ke client mempunyai jalur melalui internet di dalam sebuah paket yang disebut dengan datagram.masing masing datagram berisi header dan payload. header berisi alamat dan port untuk setiap paket, address dan port untuk tiap paket yang masuk, sedangkan payload berisi data, sejak datagram mempunyai batasan jarak, memungkinkan sebuah paket hilang atau *corupted* ketika dikirimkan dan membutuhkan pengiriman lagi

Perancangan Interface Server

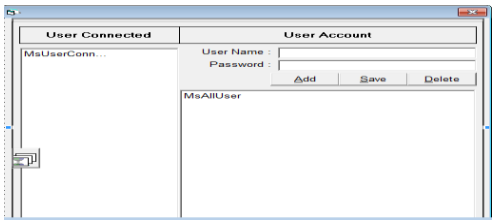
Program server ini di gunakan untuk melihat semua informasi yang datang dari client berupa siapa yang login, penambahan user id dan login ke database bagi server yg yang hostname,user name dan password sudah tersimpan dalam database server dan gambarnya dapat di lihat seperti di bawah ini :



Gambar 5 : Sistem Utama pada Server

Perancangan Interface Server untuk Penambahan dan penghapusan User.

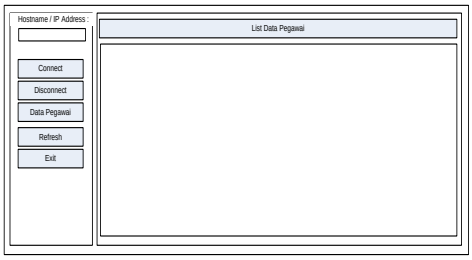
Program server ini di gunakan untuk melihat semua informasi yang datang dari client berupa siapa yang login, penambahan user id dan lain-lainnya dan gambarnya dapat di lihat seperti di bawah ini :



Gambar 6 : Rancangan Menu user Interface server

Perancangan Interface Client

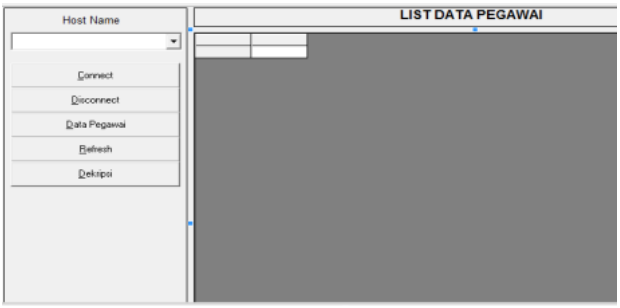
Program Client ini di gunakan untuk melihat semua informasi yang datang dari server berupa jawaban permintaan client ke server, hasil query client ke server dan list data yang di ambil dari server dan lain-lainnya dan gambarnya dapat di lihat seperti di bawah ini :



Gambar 7 : Rancangan Menu Utama Interface Client

Form Klien

Form klien merupakan form yang diakses oleh klien. Tampilan login klien dapat dilihat pada gambar 8 dibawah ini



Gambar 8. Tampilan Form Klien

V. KESIMPULAN

Dari pembahasan diatas dapat diberikan beberapa kesimpulan sebagai berikut:

1. Chiper transposisi ini memiliki berbagai macam bentuk dan algoritma, diantaranya adalah cipher transposisi itu adalah *Columnar Chiper* untuk membatasi masalah, penelitian ini hanya membahas *Columnar Transposition*. Pada Chiper Transposisi, plainteks tetap sama, tetapi urutannya diubah. Dengan kata lain, algoritma ini melakukan transpose terhadap rangkaian karakter dalam teks. Nama lain untuk metode ini adalah permutasi, karena transpose setiap karakter di dalam teks sama dengan mempermutasikan karakter-karakter tersebut.

2. Enkripsi Cipher transposisi dapat diimplementasikan dalam berkas yang dikirim melalui jaringan sehingga transfer data lebih aman.

3. Pengiriman data menjadi lebih aman karena telah dilakukan enkripsi.

DAFTAR PUSTAKA

[1]. R. Sadikin, Kriptografi untuk keamanan jaringan dan implementasinya dalam bahasa Java, Yogyakarta: Andi, 2012.
[2]. M. Tamba, Implementasi Algoritma Transposisi Cipher Dalam Sistem Pengamanan Data Pada Jaringan LAN, Jurnal Times, Volume VII No 1, Juni 2018
[3]. B.S. Hasugian, Peranan Kriptografi Sebagai Keamanan Sistem Informasi Pada Usaha Kecil Dan Menengah, Jurnal Warta,Juli 2017
[4]. Adrisatria, Yogie.2006. Study Pencarian Kolisi Pada Sha-1 oleh xiaoyun Wang dkk.
[5]. http://www.informatika.org/~rinaldi/kriptografi/2006-2007/makalah2/makalah-079.pdf.
[6]. Apriliawan,Egie. 2009. Fungsi Hash Pada Kriptografi.
[7]. http://docs.docstoc.com/orig/2220518/bf558cb1-27de-428f-baa97d1de153fab3.pdf.
[8]. Ariesanda, Boyke, 2008, Rancangan Dan Analisis Chipher Berbasis Algoritma transposisi Dengan periodisasi kunci.
[9]. http://www.informatika.org/~rinaldi/kriptografi/2006-2007/Makalah1/Makalah1-043.pdf. Diakses tanggal : 25 Maret 2018.
[10]. Ariyus, Dony. 2008. Pengantar Ilmu Kriptografi Teori, Analisi, dan Implementasi. Yogyakarta :Penerbit Andi
[11]. Melwin Syafrizal, Pengantar Jaringan Komputer, Andi Offset Yogykarta, 2005.
[12]. D. S. Nasution, "Penerapan Metode Linear Kongruen dan Algoritma Vigenere Cipher Pada Aplikasi Sistem Ujian Berbasis LAN," Jurnal Pelita Informatika Budi Darma, vol. IV, no. 1, pp. 1-10, 2013.
[13]. A. Boyke, "Rancangan Dan Analisis Cipher Berbasis Algoritma Transposisi Dengan Periodisasi Kunci," Institut Teknologi Bandung, Bandung, 2010.