ANALISA PENGAMANAN TEKS MENGGUNAKAN TEKNIK *CHARACTER CIPHER* DAN *BLOCK CIPHER*

Aida Indriani[1*] **dan Sinawati**[2]
[1]Jurusan Teknik Informatika, STMIK PPKIA Tarakanita Rahmawati
Jl. Yos Sudarso No. 8, Tarakan, Kalimantan Utara 77112.
[2]Jurusan Sistem Informasi, STMIK PPKIA Tarakanita Rahmawati
Jl. Yos Sudarso No. 8, Tarakan, Kalimantan Utara 77112.
[*]Email: aida@ppkia.ac.id

Abstrak

Kriptografi adalah salah satu cara yang digunakan untuk mengamankan teks. Pengamanan teks yang dilakukan pada kriptografi yaitu dengan cara mengubah atau melakukan penyamaran teks menjadi bentuk yang tidak mempuyai makna. Dalam kriptografi ada dua proses yang dilakukan yaitu enkripsi dan dekripsi. Enkripsi adalah proses perubahan bentuk teks asli menjadi bentuk yang tidak bermakna. Kebalikan dari enkripsi, dekripsi adalah proses perubahan bentuk teks yang tidak bermakna kembali kebentuk teks asli. Dewasa ini, pengamanan teks sangat diperlukan. Perkembangan teknologi yang semakin cepat, membuat banyaknya aplikasi-aplikasi yang dapat mengambil dokumen rahasia menjadi semakin mudah. Untuk mengatasi hal tersebut diperlukan teknik kriptografi. Seiring dengan perkembangan jaman, kriptografi terbagi atas 2 (dua) jenis yaitu kriptografi klasik dan modern. Kriptografi klasik mempunyai 2 (dua) teknik dalam hal pengamanan data yaitu teknik character cipher dan block cipher. Kriptografi tidak lepas dari cipher key yaitu kunci yang digunakan untuk proses penyandian. Cipher key terbagi atau 2 (dua) jenis yaitu kunci simetri dan asimetri. Dalam penelitian ini, penulis menganalisa pengamanan teks dengan menggunakan metode Caesar cipher yang merupakan salah satu teknik character cipher dan transposition cipher yang merupakan salah satu teknik block cipher. Kunci yang digunakan adalah kunci simetri.

Kata kunci : *block cipher, caesar cipher, character cipher, kriptografi, transposition cipher*

1. PENDAHULUAN

Seiring dengan perkembangan teknologi, banyak sekali jenis-jenis aplikasi yang dapat membaca data atau informasi pribadi yang dilakukan secara diam-diam. Untuk mencegah pencurian informasi (data), maka dilakukan beberapa cara antara lain dengan menggunakan teknik penyamaran data yang biasa disebut dengan istilah kriptografi dan teknik penyembunyian data yang biasa disebut dengan istilah steganografi.

Kriptografi adalah salah satu cara yang digunakan untuk mengamankan data. Pengamanan data yang dilakukan pada kriptografi yaitu dengan cara mengubah atau melakukan penyamaran data menjadi bentuk yang tidak mempuyai makna. Dalam kriptografi ada dua proses yang dilakukan yaitu enkripsi dan dekripsi. Enkripsi adalah proses perubahan bentuk data asli menjadi bentuk yang tidak bermakna. Kebalikan dari enkripsi, dekripsi adalah proses perubahan bentuk data yang tidak bermakna kembali kebentuk data asli.

Kriptografi dibedakan menjadi 2 (dua) jenis yaitu kriptografi klasik dan modern. Ada 2 (dua) teknik yang biasa dilakukan untuk pengamanan data yaitu teknik *character* (karakter) dan *block* (blok) cipher. Cipher karakter yaitu melakukan pengamanan data secara satu persatu terhadap huruf yang terdapat dalam data asli (plainteks). Sedangkan cipher blok yaitu dengan cara membagi plainteks sesuai dengan jumlah blok yang digunakan.

Pada kriptografi, dikenal istilah cipher key (kode kunci) yaitu kunci yang digunakan untuk melakukan proses enkripsi dan dekripsi. Terdapat 2 (dua) jenis kunci yaitu kunci simetri dan kunci asimetri. Dalam penelitian ini, penulis menganalisa pengamanan teks dengan menggunakan 2 (dua) teknik yaitu cipher karakter dan cipher blok. Untuk jenis kunci yang digunakan yaitu kunci simetri.

2. METODOLOGI

2.1. Kriptografi

Menurut Rinaldi (2006), kriptografi (*cryptography*) berasal dari Bahasa Yunani: "*cryptos*" artinya "*secret*" (rahasia), sedangkan "*graphein*" artinya "*writing*" (tulisan). Jadi, kriptografi berarti "*secret writing*" (tulisan rahasia). Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan

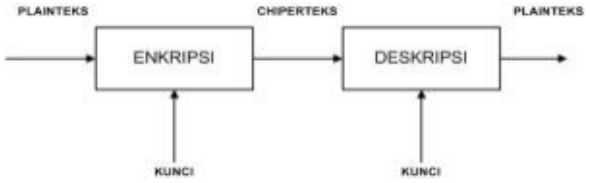
pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Saat ini kriptografi lebih dari sekadar *privacy*, tetapi juga untuk tujuan data *integrity*, *authentication*, dan *non-repudation*.

Terdapat dua konsep yang sangat penting atau utama yaitu enkripsi dan dekripsi dalam kriptografi. Enkripsi adalah proses informasi atau data yang akan dikirim diubah menjadi bentuk yang hampir tidak dikenali dengan menggunakan algoritma tertentu. Dekripsi adalah kebalikan dari enkripsi yaitu merubah kembali bentuk tersamar tersebut menjadi informasi awal (Fresly dkk., 2015).

Menurut Doni (2008), pada dasarnya komponen kriptografi terdiri dari beberapa komponen, seperti:

1. Enkripsi yaitu merupakan cara pengamanan data yang dikirimkan sehingga terjaga kerahasiaannya.
2. Dekripsi merupakan kebalikan dari enkripsi.
3. Kunci adalah kunci yang dipakai untuk melakukan enkripsi dan dekripsi. Kunci terbagi menjadi dua bagian, yaitu kunci rahasia (*private key*) dank unci umum (*public key*).
4. Cipherteks merupakan suatu pesan yang telah melalui proses enkripsi.
5. Plainteks sering disebut dengan *cleartext*. Teks-asli atau teks-biasa ini merupakan pesan yang ditulis atau diketik yang memiliki makna.
6. Pesan dapat berupa data atau informasi yang dikirim (melalui kurir, saluran komunikasi data, dsb).
7. Cryptanalysis bisa diartikan sebagai analisis kode atau suatu ilmu untuk mendapatkan teks-asli tanpa harus mengetahui kunci yang sah secara wajar.

Menurut Rinaldi (2006), proses enkripsi dan dekripsi dapat digambarkan dengan skema seperti pada gambar 1.



Gambar 1. Skema Enkrpsi dan Dekripsi

2.2. Cipher Karakter dan Cipher Blok

Ada beberapa teknik yang biasa digunakan dalam kriptografi klasik yaitu teknik cipher karakter dan teknik cipher blok.

2.2.1 Cipher Karakter

Menurut M. Miftakul (2016), kriptografi dilakukan pada jaman dahulu (sebelum adanya komputer) yaitu dengan menggunakan algoritma berbasis karakter. Terdapat beberapa algoritma kriptografi berbasis karakter, sering disebut sebagai istilah kriptografi klasik. Berikut adalah ilustrasi dari teknik cipher karakter.

Plainteks: PPKIATARAKAN

Proses enkripsi:

Huruf ke-1: P	Huruf ke-7: A
Huruf ke-2: P	Huruf ke-8: R
Huruf ke-3: K	Huruf ke-9: A
Huruf ke-4: I	Huruf ke-10: K
Huruf ke-5: A	Huruf ke-11: A
Huruf ke-6: T	Huruf ke-12: N

Untuk melakukan enkripsi, huruf demi huruf dari plainteks diolah secara satu per satu sepanjang plainteks dengan menggunakan kunci tertentu. Untuk proses dekripsi dilakukan hal yang sama terhadap Cipherteks.

ISBN 978-602-99334-9-9

2.2.2 Cipher Blok

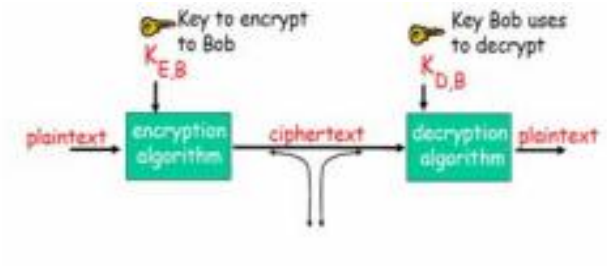
Menurut Rinaldi (2006), panjang plainteks dibagi menjadi blok-blok dengan panjang yang sama. Enkripsi dilakukan dengan menggunakan kunci yang ukurannya sama seperti panjang blok yang pada plainteks. Blok cipherteks menghasilkan ukuran blok yang sama setelah dilakukan algoritma enkripsi. Berikut adalah ilustrasi dari teknik cipher blok.

Plainteks: PPKIATARAKAN
Proses enkripsi: misalkan 1 blok berukuran 5 karakter
Blok ke-1: PPKIA
Blok ke-2: TARAK
Blok ke-3: AN

Untuk melakukan enkripsi, dibagi sesuai dengan ukuran karakter dalam 1 blok. Contoh di atas, 1 blok berisikan 5 karakter, sehingga terbentuk 3 blok yang diperoleh dari membagi jumlah seluruh karakter dengan jumlah karakter dalam 1 blok (12 / 5) = 2.4 dibulatkan menjadi 3. Dalam contoh di atas, akan terdapat beberapa karakter yang kosong pada blok terakhir. Disempurnakan dengan meletakkan karakter yang jarang digunakan seperti tanda at (@). Sehingga Blok ke-3 menjadi AN@@@.

2.3. Kriptografi Kunci Simetri

Kriptografi klasik banyak menggunakan kunci simetri. Menurut Ratih (2007), untuk proses enkripsi dan dekripsi menggunakan kunci yang sama. Tekniknya yaitu, pengirim dan penerima pesan berbagi kunci yang sama dan digunakan untuk proses enkripsi dan dekripsi. Alur proses teknik kunci simetri dapat dilihat pada gambar 2.



Gambar 2. Skema Kriptografi Simetri

Pada gambar 2, Alice akan melakukan pengiriman pesan kepada Bob. Kunci yang digunakan Alice dan Bob untuk mengenkripsi dan mendekripsi pesan adalah sama.

2.4. Caesar Cipher

Menurut Doni (2008), substitusi kode merupakan penyandian pertama yang terjadi pada pemerintahan Yulius Caesar dikenal dengan istilah kode kaisar. Cara kerja dari caesar cipher yaitu dengan mengganti posisi huruf awal dari alfabet dengan kunci yang telah ditentukan. Pada perkembangannya algoritma caesar cipher menggunakan kunci lain yang disebut *poly-alphabetic*. *Poly-alphabetic* yaitu kunci yang digunakan berupa alfabet seperti nama, alamat atau apa saja. Contoh diberikan kunci = "KUCINGSAYANG", maka pasangan alfabet plainteks dan kunci karakter dapat dilihat pada tabel 1.

Tabel 1. Alfabet Plainteks dengan Kunci Karakter

Alfabet	Kunci	Alfabet	Kunci	Alfabet	Kunci	Alfabet	Kunci
A	K	H	A	O	J	V	T
B	U	I	Y	P	L	W	V
C	C	J	B	Q	M	X	W
D	I	K	D	R	O	Y	X
E	N	L	E	S	P	Z	Z
F	G	M	F	T	Q		
G	S	N	H	U	R		

Caesar cipher dengan menggunakan kunci berupa karakter biasa disebut dengan substitusi deret campur kata kunci. Yang perlu diingat, tidak ada perulangan huruf kunci. KUCINGSAYANG menjadi KUCINGSAY.

2.5. Transposition Cipher

Menurut Rinaldi (2006), huruf-huruf di dalam plainteks pada cipher transposisi yaitu tetap sama, hanya saja urutan teks diubah. Algoritma ini melakukan transpose terhadap rangkaian karakter di dalam teks. Nama lain untuk metode ini adalah permutasi atau pengacakan (scrambling) karena transpose setiap karakter di dalam teks sama dengan mempermutasikan karakter-karakter tersebut. Berikut adalah contoh melakukan permutasi terhadap kunci yang diberikan.
Ada 6 kunci untuk melakukan permutasi kode:

1	2	3	4	5	6
3	5	1	6	4	2

Dan 6 kunci untuk inversi dari permutasi tersebut menjadi:

1	2	3	4	5	6
3	6	1	5	2	4

Menurut Doni (2008), proses enkripsi menggunakan kunci permutasi dan dekripsi menggunakan kunci inversi dari permutasi. Tahap awal dalam cipher transposisi yaitu membagi panjang plainteks dengan panjang kunci dan apabila terjadi kekurangan dari blok bisa ditambah dengan huruf yang disukai.

3. HASIL DAN PEMBAHASAN

Untuk melakukan pengamanan data dengan menggunakan 2 (dua) teknik yaitu cipher karakter dan cipher blok diawali dengan mengamankan data menggunakan teknik cipher karakter dan dilanjutkan dengan teknik cipher blok. Dalam hal ini, penulis menggunakan metode caesar cipher dan cipher tranposisi. Untuk proses dekripsi dilakukan kebalikan dari enkripsi yaitu dimulai dari teknik cipher blok dan dilanjutkan dengan teknik cipher karakter.

3.1. Enkripsi Data

Contoh plainteks yang akan disandikan yaitu “STMIK PPKIA TARAKANITA RAHMAWATI”

3.1.1. Caesar Cipher

Pada metode caesar cipher menggunakan kunci jenis *poly-alphabetic*. Dalam hal ini kunci yang digunakan yaitu “KUCINGSAYANG”. Enkripsi dilakukan dengan melihat pasangan alfabet plainteks dan kunci karakter yang telah dibuat seperti pada tabel 1. Sehingga hasil pasangan alfabet sesuai dengan plainteks dapat dilihat pada tabel 2.

Tabel 2. Alfabet Plainteks dan Cipherteks

Plainteks	Cipherteks	Plainteks	Cipherteks
S	P	A	K
T	Q	R	O
M	F	N	H
I	Y	H	A
K	D	W	V
P	L		

Pada tabel 2, cipherteks yang dihasilkan adalah “PQFYD LLDYK QKOKDKHYQK OKAFKVKQY”

3.1.2. Transposition Cipher

Pada hasil enkripsi menggunakan teknik cipher karakter yaitu caesar cipher terdapat kelemahan. Adapun kelemahannya yaitu menghasilkan cipherteks yang sama terhadap plainteks yang sama. Misalkan, huruf “P” pasti akan menjadi huruf “L”. Untuk menguatkan pengamanan data, maka dilakukan proses yang kedua yaitu menggunakan teknik cipher blok. Adapun metode yang digunakan adalah cipher transposisi. Plainteks yang digunakan yaitu cipherteks hasil dari caesar cipher “PQFYD LLDYK QKOKDKHYQK OKAFKVKQY”. Kunci yang diberikan yaitu sebanyak 6 (enam). Tahapan-tahapan dalam cipher tranposisi sebagai berikut:

ISBN 978-602-99334-9-9

a. Melakukan permutasi terhadap kunci, sehingga menjadi 3 6 1 2 4 5
b. Membagi panjang plainteks dengan jumlah kunci yang ada untuk mendapatkan jumlah blok. Adapun perhitungan pembagian sebagai berikut:
   Jumlah Blok = 32 / 6 = 5,3 = 6 blok
c. Meletakkan huruf-huruf yang terdapat pada masing-masing blok, seperti yang terlihat pada tabel 3.

Tabel 3. Alfabet Plainteks pada urutan Blok

Urutan Blok	Huruf ke -					
	1	2	3	4	5	6
Blok 1	P	Q	F	Y	D	_
Blok 2	L	L	D	Y	K	_
Blok 3	Q	K	O	K	D	K
Blok 4	H	Y	Q	K	_	O
Blok 5	K	A	F	K	V	K
Blok 6	Q	Y	@	@	@	@

Pada tabel 6, spasi (space) diganti dengan tanda garis bawah (underscore) dan blok yang tidak lengkap jumlah huruf dilengkapi dengan tanda at (@).

d. Memindahkan posisi huruf sesuai dengan kunci permutasi yang dihasilkan pada tahap pertama. Urutan alfabet plainteks dengan menggunakan kunci permutasi, ditunjukkan pada tabel 4.

Tabel 4. Alfabet Plainteks dengan Kunci Permutasi

Urutan Blok	Huruf ke -					
	1	2	3	4	5	6
Blok 1	F	Y	P	D	_	Q
Blok 2	D	Y	L	K	_	L
Blok 3	O	K	Q	D	K	K
Blok 4	Q	K	H	_	O	Y
Blok 5	F	K	K	V	K	A
Blok 6	@	@	Q	@	@	Y

Sehingga hasil enkripsi jika digabung mulai dari blok ke-1 sampai dengan ke-6 menjadi: “FYPD_Q DYLK_L OKQDKK QKH_OY FKKVKA@@Q@@Y”

3.2. Dekripsi Data

Cipherteks yang digunakan yaitu “FYPD_Q DYLK_L OKQDKK QKH_OY FKKVKA@@Q@@Y”

3.2.1. Transposition Cipher

Pada proses dekripsi, dari kunci permutasi dilakukan permutasi lagi untuk mendapatkan kunci inversi sehingga menjadi 3 4 1 5 6 2. Kemudian dilakukan proses dekripsi dengan menggunakan kunci inversi, sehingga menghasilkan urutan cipherteks seperti yang ditunjukkan pada tabel 5.

Tabel 5. Alfabet Cipherteks dengan Kunci Inversi

Urutan Blok	Huruf ke -					
	1	2	3	4	5	6
Blok 1	P	Q	F	Y	D	_
Blok 2	L	L	D	Y	K	_
Blok 3	Q	K	O	K	D	K
Blok 4	H	Y	Q	K	_	O
Blok 5	K	A	F	K	V	K
Blok 6	Q	Y	@	@	@	@

3.2.2.

3.2.3. Caesar Cipher

Pada proses dekripsi dan dengan menggunakan kunci yang sama pada saat enkripsi yaitu "KUCINGSAYANG". Pasangan kunci karakter dengan alfabet plainteks dapat dilihat pada tabel 1. Sehingga hasil pasangan alfabet sesuai yang sesuai dengan cipherteks dapat dilihat pada tabel 6.

Tabel 6. Alfabet Cipherteks dan Plainteks

Cipherteks	Plainteks	Cipherteks	Plainteks
P	S	K	A
Q	T	O	R
F	M	H	N
Y	I	A	H
D	K	V	W
L	P		

Pada tabel 6, plainteks yang dihasilkan adalah "STMIK PPKIA TARAKANITA RAHMAWATI".

4. KESIMPULAN

Setelah melakukan analisa pengamanan data dengan metode Caesar Cipher dan Transposition Cipher dapat ditarik kesimpulan sebagai berikut:

1. Metode caesar cipher dan cipher transposisi termasuk jenis kriptografi klasik dimana caesar cipher menggunakan teknik cipher karakter dan cipher transposisi menggunakan teknik cipher blok dan keduanya merupakan algoritma kunci simetri.
2. Pengamanan data yang dilakukan hanya menggunakan teknik cipher karakter terdapat kelemahan yaitu hasil enkrispi akan menghasilkan huruf yang sama terhadap plainteks yang sama.
3. Kombinasi pengamanan data dengan menggunakan 2 (dua) teknik dari kriptografi klasik dapat meningkatkan pengamanan data.
4. Diharapkan penelitian yang dilakukan dapat dikembangkan lagi dengan menggunakan metode-metode kriptografi klasik lainnya dan bisa juga menggunakan kriptografi modern, serta dapat menggunakan algoritma kunci asimetri agar pengamanan data lebih kuat.

DAFTAR PUSTAKA

Fresly, N.P., Indah, F.A., Awang, H.K., (2015), Implementasi Kriptografi Pengamanan Data pada Pesan Teks, Isi File Dokumen, dan File Dokumen menggunakan Algoritma *Advanced Encryption Standard*, Jurnal Informatika Mulawarman Vol. 10 No. 1, pp. 20-31.

M. Miftakul, A., (2016), Implementasi Kriptografi Klasik pada Komunikasi berbasis Teks, Jurnal Pseudocode Vol. III No. 2, pp. 129-136.

Doni, A., (2008), Pengantar Ilmu Kriptografi: Teori, Analisa, dan Implementasi, Andi Yogyakarta, Yogyakarta, pp. 10-11, 50-54, 75-76.

Rinaldi, M., (2006), Kriptografi, Informatika Bandung, Bandung, pp. 2, 6, 69, 116.

Ratih, (2007), Studi dan Perbandingan Penggunaan Kriptografi Kunci Simetri dan Asimetri pada Telepon Selular, Makalah Program Studi Teknik Informatika, Institut Teknologi Bandung, Bandung.

ISBN 978-602-99334-9-9