METODE BARU ALGORITMA KRIPTOGRAFI KE DALAM ENKRIPSI DAN DEKRIPSI CIPHER BERLAPIS

Antoni1, Solly Aryza2, Bonar Harahap3, Mahrani Arfah4, Azmi Rizki Lubis5

[1,3,4,5]Fakultas Teknik Universitas Islam Sumatera Utara
antonigtg@ft.uisu.ac.id
Fakultas Sains & Teknologi, Universitas Panca Budi
Sollysryzalubis@gmail.com

ABSTRAK

Enkripsi merupakan salah satu metode yang digunakan untuk melindungi atau memelihara data. Data yang telah dienkripsi akan dijaga kerahasiaannya dimana isi dari data tersebut diubah, sehingga tidak sesuai dengan data yang sebenarnya. Untuk dapat membaca data yang telah dienkripsi sebelumnya diperlukan suatu proses yang disebut dekripsi. Dalam ilmu kriptografi, data yang akan diamankan terdiri dari tiga komponen utama, yaitu pesan yang akan dibaca (plaintext), kunci untuk melakukan teknik kriptografi (Key), dan sinyal acak yang tidak dapat dibaca (ciphertext). Pengujian dilakukan dengan mengirimkan data berupa kata atau kalimat dengan menggunakan kunci rahasia. Hasil analisis data dari pengujian yang dilakukan menunjukkan bahwa dengan penggabungan beberapa algoritma berlapis kerahasiaan informasi dapat lebih aman karena membutuhkan beberapa tahapan yang berbeda untuk memecahkannya.

Kata KunciS : Algoritma, Kriptografi, Dekripsi, Enkripsi

1. Ringkasan

Dengan pesatnya perkembangan dunia komunikasi khususnya di bidang informasi seperti data, gambar, audio atau video, maka diperlukan suatu sistem yang dapat menjaga kerahasiaan informasi tersebut. Keamanan merupakan persyaratan standar dan menjadi esensial, kerahasiaan data memerlukan mekanisme keamanan yang dapat menangani kerahasiaan informasi tersebut.(Solly Aryza dkk., 2018).

Enkripsi adalah proses metode pengacakan atau cara mengamankan informasi untuk membuat informasi tersebut tidak dapat dibaca tanpa pengetahuan khusus. Enkripsi dapat digunakan untuk tujuan keamanan, tetapi teknik lain masih diperlukan untuk membuat komunikasi aman, terutama untuk memastikan integritas dan otentikasi pesan. Penelitian ini dilakukan untuk menganalisis suatu metode enkripsi-dekripsi sehingga menjadi password yang berlapis-lapis yang bertujuan untuk meningkatkan keamanan informasi.(Aryza dkk., 2018).

2. Kriptografi

Kriptografi adalah ilmu yang mempelajari bagaimana menjaga agar data atau pesan tetap aman saat dikirimkan dari pemancar ke penerima tanpa gangguan dari pihak ketiga. Menurut Bruce Scheiner dalam bukunya "Applied Cryptography", kriptografi adalah ilmu dan seni menjaga pendistribusian pesan agar tetap aman atau terlindungi.

Selain istilah-istilah tersebut, ada pula pengertian lain bahwa kriptografi adalah ilmu yang mempelajari teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, validitas data, integritas data, dan otentikasi data.(Ikhwan & Rahim, 2016)Awal mula kriptografi dipahami sebagai ilmu menyembunyikan pesan(Aspan & Aryza, 2018)Namun seiring perkembangan zaman hingga saat ini, pengertian kriptografi berkembang menjadi ilmu teknik matematika yang digunakan untuk memecahkan masalah keamanan seperti privasi dan otentikasi.(Indar Sugiarto, Thiang Thiang, & Timothy Joy Siswanto, 2008).

Ada empat tujuan mendasar dari ilmu kriptografi yang juga aspek keamanan informasi, yaitu:

• Confidentiality adalah layanan yang digunakan untuk menyimpan isi data siapa pun kecuali yang memiliki kewenangan atau kunci rahasia untuk membuka informasi yang telah dikodekan.

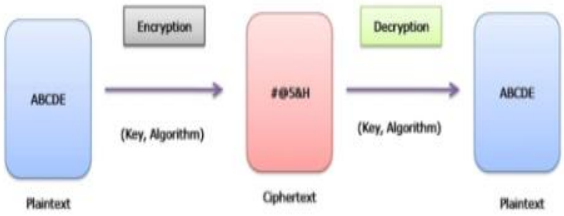
• Integritas data dikaitkan dengan pelestarian perubahan data yang tidak sah. Untuk menjaga integritas data sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak yang tidak berhak atas penyisipan, penghapusan, dan pemasukan data lainnya ke dalam data yang sebenarnya.

• Otentikasi dikaitkan dengan identifikasi atau pengenalan, baik sebagai keseluruhan sistem atau informasi itu sendiri. Dua pihak yang berkomunikasi harus memperkenalkan diri. Informasi yang dikirim melalui kanal harus diotentikasi keaslian isi data, waktu pengiriman, dan lain-lain.

• Non-repudiation atau non-denial adalah upaya untuk mencegah penolakan penyampaian atau pembuatan informasi oleh pihak yang mengirim atau membuat informasi tersebut.

2.1 Proses utama dalam Kriptografi

- Enkripsi adalah proses di mana informasi atau data sebelum ditransmisikan, diubah menjadi bentuk yang hampir tidak dapat dikenali sebagai informasi yang awalnya menggunakan algoritma tertentu.
- Deskripsi adalah kebalikan dari enkripsi yang membentuk kembali penyamaran sebagai informasi awal..



Gambar 1. Ilustrasi Dasar Kriptografi

2.2 Istilah dalam Kriptografi

Berikut adalah istilah-istilah yang digunakan dalam kriptografi:

- Plaintext (M) adalah pesan yang akan dikirim (berisi data asli).
- Ciphertext (C) adalah pesan terenkripsi (encrypted) yang merupakan hasil enkripsi.
- Enkripsi (Fungsi E) adalah proses mengubah plainteks menjadi cipherteks.
- Dekripsi (Fungsi D) adalah proses pengubahan ciphertext menjadi plaintext, sehingga menjadi data awal atau data asli.
- Kunci adalah nomor rahasia, yang digunakan dalam proses enkripsi dan dekripsi.

3. Pengantar Jenis Kriptografi

3.1Jenis Kriptografi Menurut Perkembangannya

Algoritma kriptografi dapat diklasifikasikan menjadi dua jenis berdasarkan perkembangannya, yaitu kriptografi klasik dan kriptografi modern.

- **Algoritma Kriptografi Klasik**

Algoritma ini digunakan sejak sebelum era komputerisasi dan kebanyakan menggunakan teknik kunci simetris. Cara menyembunyikan pesan adalah dengan menggunakan teknik substitusi atau transposisi atau keduanya [4]. Teknik substitusi adalah mengganti karakter pada plainteks menjadi karakter lain yang hasilnya berupa cipherteks. Sedangkan transposisi adalah teknik mengubah plainteks menjadi cipherteks dengan cara permutasi karakter. Ini adalah kombinasi kompleks dari keduanya yang mendasari pembentukan berbagai algoritma kriptografi modern(Hesari & Sistani, 2017).

- **Algoritma Kriptografi Modern**

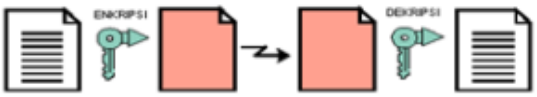
Algoritma ini memiliki tingkat kesulitan yang lebih kompleks [2], dan kekuatannya ada di kunci [5]. Algoritma ini menggunakan simbol biner karena mengikuti operasi pemrosesan komputer digital. Sehingga diperlukan suatu bentuk dasar pengetahuan matematika untuk menguasainya [4].

3.2 Jenis Kriptografi Menurut Kuncinya

Algoritma kriptografi dapat diklasifikasikan menjadi dua jenis berdasarkan kuncinya, yaitu algoritma simetris dan algoritma asimetris [2].

3.2.1 Algoritma Simetris

Algoritma ini disebut simetris karena memiliki kunci yang sama dalam proses enkripsi dan dekripsi sehingga algoritma ini juga sering disebut algoritma kunci tunggal atau algoritma satu kunci. Kunci pada algoritma ini bersifat rahasia atau private sehingga algoritma ini disebut juga dengan algoritma kunci rahasia [2].



Gambar 2. Ilustrasi Algoritma Simetris

- **Kelebihan Algoritma Simetris**

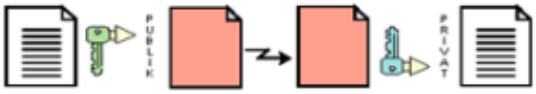
Kecepatan operasi lebih tinggi jika dibandingkan dengan algoritma asimetris, karena kecepatannya cukup tinggi, dapat digunakan dalam sistem waktu nyata.

- **Kelemahan Algoritma Simetris**

Untuk setiap pengiriman pesan dengan pengguna yang berbeda membutuhkan kunci yang berbeda pula, sehingga akan terjadi kesulitan dalam pengelolaan kunci, yang biasa disebut dengan masalah distribusi kunci.

3.2.2 AAlgoritma simetris

Algoritma ini disebut asimetris karena kunci yang digunakan untuk enkripsi berbeda dengan kunci yang digunakan untuk dekripsi. Kunci yang digunakan untuk enkripsi adalah kunci publik sehingga algoritma ini disebut juga dengan algoritma kunci publik. Sedangkan kunci untuk dekripsi menggunakan kunci rahasia atau private key [2].



Gambar 3. Ilustrasi Algoritma Asimetris

Keuntungan Algoritma Asimetris:
- Masalah keamanan pada distribusi kunci bisa lebih baik.
- Masalah manajemen kunci lebih baik karena jumlah kunci lebih sedikit.

Kelemahan Algoritma Asimetris:
- Kecepatannya lebih rendah jika dibandingkan dengan algoritma simetris.
- Untuk tingkat keamanan yang sama, kunci yang digunakan lebih panjang dari algoritma simetris.

4. Metode Pengujian

Pada awalnya pengamanan data dengan kriptografi yang menggunakan algoritma kriptografi klasik masih berbasis karakter, menggunakan pena dan kertas saja, tanpa komputer. Algoritma kriptografi klasik termasuk dalam kriptografi kunci simetris.
Algoritma kriptografi klasik:
- Cipher Pergantian
- Cipher Transposisi

Dalam penelitian ini penulis hanya akan membahas tentang Substitusi Cipher.

4.1 Cipher Pergantian

Substitusi cipher mengubah satu huruf atau karakter dalam pesan (plaintext), sesuai dengan aturan kunci (key), menjadi karakter lain dalam sandi rahasia (ciphertext). Berikut adalah bagian dari Pergantian Chipers :

4.1.1 Caesar Cipher

Contoh paling sederhana dari cipher substitusi adalah cipher Caesar. Caesar Cipher adalah cipher substitusi yang menggunakan panjang kunci 1 karakter (karakter yang diambil dari alfabet). Biasanya para pihak sudah sepakat dan sama-sama tahu bahwa mereka akan menggunakan Caesar Cipher dengan karakter tertentu untuk bertukar pesan rahasia.
Pengirim pesan: memiliki pesan asli, tahu kuncinya, tahu cara menggunakan Caesar Cipher. Dia menggunakan Caesar Cipher untuk menghasilkan kata sandi rahasia.
Penerima pesan: tahu kuncinya, tahu cara menggunakan Caesar Cipher, tahu kata sandi rahasianya. Dia menggunakan kata sandi untuk memecahkan kode rahasia untuk mendapatkan pesan asli.

A	B	C	D	E	F	G	H	I	J
0	1	2	3	4	5	6	7	8	9

K	L	M	N	O	P	Q	R	S	T
10	11	12	13	14	15	16	17	18	19

U	V	W	X	Y	Z
20	21	22	23	24	25

Gambar.5 Indeks Urutan Abjad

Alfabet yang digunakan untuk membangun pesan (plaintext) diberi nomor indeks seperti gambar di atas. Karakter yang digunakan sebagai kunci juga diambil dari alfabet. Kunci akan "ditambahkan" atau membuat karakter "geser" dari pesan asli untuk membuat kata sandi. Jika ketika ditambahkan atau digeser menghasilkan indeks lebih dari 25, urutan indeks akan kembali ke 0, Dari Z kembali ke A.

4.1.2 Cipher Atbash

Contoh klasik lainnya adalah Atbash Cipher. Atbash Cipher ini mengubah huruf dari depan ke belakang jadi dari belakang ke depan seperti gambar di bawah ini:

```
Pesan: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Sandi: ZYXWVUTSRQPONMLKJIHGFEDCBA
```

Dengan menggunakan password Atbash, pesan ZENIUS akan menjadi password AVMRFH. Penerima hanya perlu menukar urutan huruf di belakangnya. Nama Atbash berasal dari penggunaan pertama dalam huruf Ibrani, Aleph-Tav-Shin-Beth, yang pertama, terakhir, kedua dan kedua dari belakang dalam bahasa Ibrani. Jika nama dalam huruf romawi atau kurang akan Azby [7].

4.1.3 Cipher Polialpabetik

Vigenere Cipher termasuk dalam substitusion cipher polialpabetik. Algoritma baru yang dikenal luas 200 tahun kemudian oleh penemu cipher ini kemudian disebut Vigenere Cipher.
Vigenere Vigenere Cipher digunakan untuk mengenkripsi Square, setiap baris di dalam square menyatakan ciphertext huruf yang diperoleh Caesar Cipher.
Contoh penerapan Vigenere Cipher

teks biasa :TEKS PLAINT INI
Kunci :sonysonysonysCiphertext: LVVQ HZNGFHRVL

Jika panjang kunci lebih pendek dari panjang plainteks, maka kunci diulang secara berkala. Dalam hal ini kunci "sony" diulang selama plaintext-nya.
Pada dasarnya setiap huruf adalah enkripsi Caesar cipher dengan kunci yang berbeda.
c('T') = ('T' + 's') mod 26 = LT = 20 dan s= 19◊(20+19)%26=13◊Lc('H') = ('H' + 'o') mod 26 = V, dll

5. Analisis Hasil Tes

Dalam hal ini saya mencoba memasukkan beberapa kata sandi untuk membuat kata sandi yang juga disebut kata sandi beruntun, misalnya, setelah melakukan Atbash Cipher kemudian dienkripsi lagi dengan Polyalphabetic Cipher.

5.1 Proses Enkripsi

Data yang disampaikan berikut hasil pengujian yang dilakukan:

HAFIZHATUL AHLA

Pesan ini terdiri dari 14 karakter.

Langkah 1: Menggunakan Atbash Cipher, itu akan diperoleh
Teks Biasa : HAFIZHATUL AHLA

Teks sandi : SZURASZGFO ZSOZ

Langkah 2 : Menggunakan Caesar Cipher, dimana cipher text pada langkah 1 akan menjadi teks biasa pada langkah 2. Teks chiper pada langkah 2 diperoleh dengan menggunakan kunci E.

Tabel 1. Kunci Teks E dan Chiper

plain text	S	Z	U	R	A	S	Z	G	F	O		Z	S	O	Z
	18	25	20	17	0	18	25	6	5	14		25	18	14	25
key, E = 5	5	5	5	5	5	5	5	5	5	5		5	5	5	5
	23	30	25	22	5	23	30	11	10	19		30	23	19	30
chiper text	X	E	Z	W	F	X	E	L	K	T		E	X	T	E

asil Pengujian Caesar Cipher

Maksud dari kunci, E = 5 adalah nilai numerik setiap huruf dalam karakter teks biasa dijumlahkan dengan 5. Jika ketika ditambahkan atau digeser menghasilkan indeks lebih dari 25, indeks urutan harus kembali ke 0.

Langkah 3: adalah langkah terakhir dari proses menggunakan Polyalphabetic Cipher, dimana cipher teks pada langkah 2 akan menjadi teks biasa, cipher teks diperoleh dengan menggunakan kunci SUN.

Tabel 2. Teks Chiper Menggunakan Key Sun

plain text	X	E	Z	W	F	X	E	L	K	T		E	X	T	E
	23	4	25	22	5	23	4	11	10	19		4	23	19	4
key, SUN	S	U	N	S	U	N	S	U	N	S		U	N	S	U
	18	20	13	18	20	13	18	20	13	18		20	13	18	20
	23	4	25	22	5	23	4	11	10	19		4	23	19	4
	18	20	13	18	20	13	18	20	13	18		20	13	18	20
	41	24	38	40	25	36	22	31	23	37		24	36	37	24
back to the index 0, minus 26	15	24	4	14	25	10	22	5	23	11		24	10	11	24
Chiper Text	P	Y	E	O	Z	K	W	F	X	L		Y	K	L	Y

PolyalphabeticHasil Pengujian

ini sama dengan Caesar Cipher, yaitu dengan menjumlahkan
erdiri dari tiga karakter, sedangkan pesan (XezwfxeLkt exte) terdiri dari 14 karakter, kita dapat mengulang kunci sehingga panjang karakter kunci = panjang karakter pesan. Ini berlaku untuk semua kasus, di mana panjang karakter kunci tidak sama dengan panjang karakter pesan.

5.2 Proses Dekripsi

Dekripsi dilakukan dengan membalik proses enkripsi dengan tahapan sebagai berikut:

Langkah 1: ciphertext didekripsi dengan cara dikurangkan dengan kunci (SUN), sehingga hasilnya akan menunjukkan plain text.

Tabel 3.Hasil Dekripsi Cipher Polyalphabetic

Cipher Text	P	Y	E	O	Z	K	W	F	X	L		Y	K	L	Y
	15	24	4	14	25	10	22	5	23	11		24	10	11	24
Plus 26	15	24	4	14	25	10	22	5	23	11		24	10	11	24
Key, SUN	18	20	13	18	20	13	18	20	13	18		20	13	18	20
	23	4	25	22	5	23	4	11	10	19		4	23	19	4
Plain Text	X	E	Z	W	F	X	E	L	K	T		E	X	T	E

Langkah 2: Gunakan teks biasa pada langkah 1 sebagai teks sandi Caesar Cipher dan kemudian dekripsi dengan kunci E = 5. Hasil Dekripsi sebagai berikut:

Tabel 4. Hasil Dekripsi Caesar Cipher

cipher text	X	E	Z	W	F	X	E	L	K	T		E	X	T	E
key, E = 5	23	4	25	22	5	23	4	11	10	19		4	23	19	4
	5	5	5	5	5	5	5	5	5	5		5	5	5	5
back to the index 25	18	-1	20	17	0	18	-1	6	5	14		-1	18	14	-1
plain text	18	25	20	17	0	18	25	6	5	14		25	18	14	25
	S	Z	U	R	A	S	Z	G	F	O		Z	S	O	Z

Langkah 3 merupakan tahap akhir dari proses dekripsi, dengan menggunakan plain text pada Caesar Cipher sebagai ciphertext dan dengan menggunakan Atbash Cipher akan diperoleh :

Teks Chiper :SZURASZGFO ZSOZ

Teks Biasa : HAFIZHATUL AHLA

6. Kesimpulan

Kesimpulan yang dapat diambil dari penelitian ini adalah :

1. Sedangkan dengan menggabungkan beberapa informasi algoritma kerahasiaan berlapis mungkin lebih aman karena membutuhkan beberapa tahapan yang berbeda untuk diselesaikan.

2. Algoritma kriptografi klasik berfokus pada kekuatan kerahasiaan. Dengan algoritma maksud yang digunakan (artinya jika algoritma yang digunakan diketahui maka pesannya jelas "bocor" dan dapat diketahui isinya oleh siapa saja yang mengetahui algoritma tersebut).

3. Kriptografi adalah ilmu yang mempelajari bagaimana menjaga agar data atau pesan tetap aman saat dikirimkan dari pengirim ke penerima tanpa gangguan dari pihak ketiga.

4. Enkripsi adalah proses dimana informasi atau data yang akan ditransmisikan, diubah menjadi bentuk yang hampir tidak dapat dikenali sebagai informasi yang awalnya menggunakan algoritma tertentu..

5. Dekripsi adalah proses mengembalikan data asli sehingga dapat dibaca atau dipahami kembali.

7. Referensi

[1] Diffie, Whitfield, Martin E Hellman. 1976. Arah Baru dalam Kriptografi. IEEE Trans. Info. Teori IT-22.

[2] Prayudi, Yudi, Idham Halik. 2005. Studi Analisis Algoritma Rivest Code 6 (RC6) Dalam Enkripsi/Dekripsi Data. Seminar Nasional Aplikasi Teknologi Informasi 2005 (SNATI 2005), Yogyakarta.

[3] Rizal, Ansar, Suharto. 2011. Implementasi Algoritma RC4 untuk Keamanan Login Pada Sistem Pembayaran Uang Sekolah. Dielektrika, ISSN 2086-9487 Vol. 2 No.2.

[4] Sadikin, Rifki. 2012. Kriptografi untuk Keamanan Jaringan dan Implementasinya dalam Bahasa Java. Penerbit Andi, Yogyakarta.

[5] Wirdasari, Dian. 2008. Prinsip Kerja Kriptografi dalam Mengamankan Informasi, Jurnal SAINTIKOM Vol.5 No.2.

[6]https://shineofscience.wordpress.com/tag/konsep-kriptografi/

[7]https://www.zenius.net/blog/7095/kriptografi-enkripsi-dekripsi

[8]Aryza, S., Irwanto, M., Lubis, Z., Siahaan, APU, Rahim, R., & Furqan, M. (2018). Sebuah Desain Baru Meminimalkan Kerugian Listrik Dalam Drive Mesin Induksi Vektor Terkendali. Seri Konferensi IOP: Ilmu dan Teknik Material, 300(1), 12067. Diperoleh dari http://stacks.iop.org/1757-899X/300/i=1/a=012067

[9] Aspan, H., & Aryza, S. (2018). Dear Sir/Madam, Elpina, Henry Aspan, Solly Aryza Dengan ini kami informasikan kepada Anda bahwa setelah proses peninjauan yang ketat, panel peninjau kami telah mengambil

keputusan tentang makalah Anda! “, (Januari), 76318.
[10] Hesari, S., & Sistani, MBN (2017). Peningkatan efisiensi motor induksi menggunakan algoritma fuzzy-genetic. Konferensi Sistem Tenaga ke-30, PSC 2015, (Mei 2016), 210–216. https://doi.org/10.1109/IPSC.2015.7827750
[11] Ikhwan, A., & Rahim, R. (2016). Implementasi Algoritma Modified Median Filtering untuk Pengurangan Noise Salt & Pepper pada Citra. Jurnal Internasional Sains & Teknologi, 4(11), 2321–2919. Diperoleh dari www.theijst.com
[12] Indar Sugiarto, Thiang Thiang, & Timothy Joy Siswanto. (2008). Disain dan Implementasi Modul Akuisisi Data sebagai Alternatif Modul DAQ LabVIEW. Jurnal Teknik Elektro, 8(1), 30–37. Diperoleh dari http://puslit2.petra.ac.id/ejournal/index.php/elk/article/view/17353