Jurnal JTIK (Jurnal Teknologi Informasi dan Komunikasi)

Journal Homepage: http://journal.lembagakita.org/index.php/jtik

Pengamanan Basis Data Kasus Kekerasan pada Perempuan dan Anak Menggunakan Algoritma *Vigenere Cipher* dan Base64

Fenny Fitria Oktaviany [1*], Eka Ardhianto [2]

[1,2] Program Studi Teknik Informatika, Fakultas Teknologi Informasi dan Industri, Universitas Stikubank Semarang, Kota Semarang, Provinsi Jawa Tengah, Indonesia.*

a r t i c l e i n f o

Article history:
Received 21 June 2023
Received in revised form
24 November 2023
Accepted 3 December 2023
Available *online* January 2024

DOI:
https://doi.org/10.35870/jtik.v8i1.1311.

Keywords:
Base64; Cryptography; Encryption; Vigenere.

Kata Kunci:
Base64; Enkripsi; Kriptografi; Vigenere.

a b s t r a c t

Cases of violence against children and women that occur in Indonesia are still a serious problem that must be addressed immediately. The official website of the Ministry of Women's Empowerment and Child Protection shows that in the last 3 years these cases have increased significantly. One of the efforts that have been made is to form Integrated Service Centers that spread across various cities as a forum for complaints. The complaint data must be secured to prevent misuse by unauthorized parties. The purpose of this study is to secure these data using the Vigenere Cipher and Base64 algorithms and a combination of the two algorithms. The entropy value is used as a test performance metric for each algorithm. From this test, the level of information security obtained was 72.77% on data encrypted using a combination of the Base64 and Vigenere Cipher algorithms.

a b s t r a k

Kasus kekerasan pada anak dan perempuan yang terjadi di Indonesia masih menjadi masalah serius yang harus segera ditangani. Dilansir dari laman resmi milik Kementrian Pemberdayaan Perempuan dan Perlindungan Anak, dalam 3 tahun terakhir kasus-kasus tersebut terus mengalami peningkatan yang signifikan. Salah satu upaya yang dilakukan oleh Kementrian Pemberdayaan Perempuan ialah membentuk Pusat Pelayanan Terpadu yang tersebar di berbagai kota sebagai wadah pengaduan. Data hasil pengaduan tersebut tentunya harus diamankan agar tidak disalahgunakan. Penelitian ini bertujuan untuk mengamankan data-data digital tersebut menggunakan algoritma Vigenere Cipher dan Base64 serta kombinasi kedua algortima tersebut. Nilai entropi digunakan sebagai metrik performa setiap algoritma yang diujikan. Hasilnya diperoleh capaian level keamanan informasi sebesar 72,77% pada penggunaan kombinasi algoritam Base64 dan Vigenere Cipher.

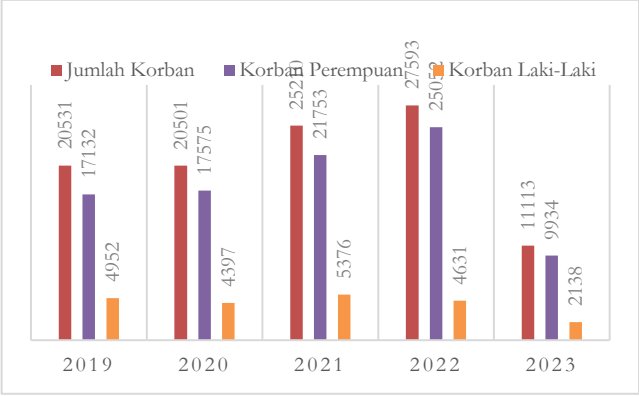
Corresponding Author. Email: fennyoktaviany19@gmail.com [1].

ACM Computing Classification System (CCS)
EBSCOhost
Communication and Mass Media Complete (CMMC)

© E-ISSN: 2580-1643.

1. Latar Belakang

Kasus kekerasan pada anak dan perempuan yang terjadi di Indonesia masih menjadi masalah serius yang harus segera ditangani. Dilansir dari laman resmi milik Kementrian Pemberdayaan Perempuan dan Perlindungan Anak, sejak awal tahun 2023 sudah ada sebanyak 11.113 kasus kekerasan terhadap anak dan perempuan dengan korban perempuan sebanyak 9.934 dan korban laki–laki sebanyak 2.138. Angka ini tentu saja bukan jumlah yang sedikit, bisa jadi masih banyak kasus di luar sana yang belum bahkan tidak dilaporkan.



Gambar 1. Kasus Kekerasan di Indonesia

Berdasarakan Gambar 1 di atas, kasus kekerasan perempuan dan anak yang terjadi mengalami kenaikan yang amat signifikan pada tahun 2021, yaitu sebanyak 4.709 kasus, dibanding tahun 2020. Pada tahun 2021 ke tahun 2022 pun terdapat kenaikan sebanyak 2.383 kasus, dari 25.210 kasus menjadi 27.593 kasus. Untuk mengatasi peningkatan kasus yang terjadi, Kementrian Pemberdayaan Perempuan dan Perlindungan Anak telah mengerahkan berbagai macam upaya, salah satunya dengan mendirikan Pusat Pelayanan Terpadu yang khusus menangani kasus kekerasan terhadap anak dan perempuan. Pusat Pelayanan Terpadu yang ada akan dibagi lagi ke tiap–tiap kota agar dapat menangani laporan tidak kekerasan dengan lebih cepat dan akurat, seperti Pusat Pelayanan Terpadu yang ada di Kota A (untuk selanjutnya akan disebut Pusat Pelayanan Terpadu DEF atau PPT DEF).

Visi dari Pusat Pelayanan Terpadu DEF adalah tercapainya keterpaduan pelayanan penanganan kekerasan terhadap perempuan dan anak yang berbasis gender, guna terwujudnya penghapusan kekerasan terhadap perempuan dan anak serta *human trafficking* (perekrutan, pemindahan, penyembunyian, penipuan manusia dengan tujuan mengambil keuntungan). Salah satu tujuan dari Pusat Pelayanan Terpadu DEF adalah menyediakan tempat pengaduan, pencatatan administrasi, membuat kronologis kasus dan melaksanakan rapat kasus untuk penyelesaian kasus, memberikan layanan untuk Rumah Aman/Shelter bagi korban yang terancam jiwa maupun raganya.

Pengaduan kepada Pusat Pelayanan Terpadu DEF dilakukan dengan beberapa cara, pelapor bisa langsung mendatangi kantor Pusat Pelayanan Terpadu DEF, melaui telepon, atau dengan mengisi form pengaduan di web yang telah disediakan. Isi dari form pengaduan ini antara lain adalah identitas pelapor, seperti nama, alamat, nomor handphone, email, serta status pelapor (apakah pelapor adalah korban atau orang terdekat). Ada pula jenis kasus yaitu kekerasan terhadap anak, kekerasan dalam rumah tangga, anak berhadapan dengan hukum, kekerasan dalam pacaran, kekerasan terhadap perempuan dan *human trafficking*. Selanjutnya identitas korban, data ini biasanya berisikan nama korban, jenis kelamin, apakah korban termasuk golongan disabilitas atau bukan, usia korban saat kejadian, pendidikan, pekerjaan, dan status perkawinan. Yang terakhir adalah identitas pelaku, isi data pelaku hampir sama dengan korban, hanya saja terdapat tambahan hubungan dengan korban dan kewarganegaraan.

Data–data tersebut tentunya perlu dijaga kerahasiaannya demi menjaga keamanan orang–orang yang terlibat, terutama bila pelapor, korban atau pelaku masih anak–anak. Apabila data tersebut sampai bocor kepada pihak yang salah, tentu akan berakibat fatal. Beberapa hal yang pernah terjadi sebagai akibat dari kebocoran data tersebut adalah korban atau pelaku mendapatkan pembullyan dari masyarakat, korban dan keluarganya diterror oleh pelaku, keluarga (baik korban maupun pelaku) dikucilkan dari lingkungan sekitar, pada kasus *human trafficking* korban diburu oleh pelaku untuk kembali dimanfaatkan atau diancam untuk tutup mulut agar pelaku tetap bisa menjalankan aksi jahatnya tersebut.

Sistem pencatat administrasi yang digunakan oleh Pusat Pelayanan Terpadu DEF saat ini sudah menerapkan pengamanan di mana *user* harus *login*

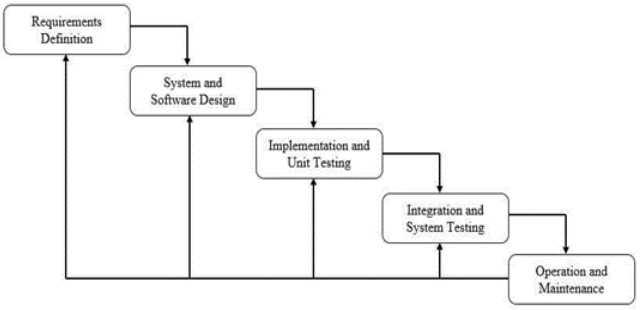
menggunakan *username* dan *password* yang sudah terdaftar untuk bisa mengakses data. Namun kedua hal tersebut masih belum cukup untuk menjaga data yang ada. Pengamanan yang ada perlu ditingkatkan lagi untuk mengantisipasi apabila *username* dan *password* tersebar ke pihak–pihak yang tidak berkepentingan atau memiliki niat buruk. Untuk menjaga kerahasiaan data tersebut, diperlukan mekanisme pengamanan khusus saat menyimpan data pada sistem basis data. Salah satu algoritma yang bertujuan untuk mengamanakan basis data dikenal dengan nama Kriptografi. Menurut Ahamed & Krishnamoorthy (2020) proses kriptografi menghasilkan teks sandi (*ciphertext*) dari informasi teks biasa (*plaintext*) dengan menggunakan kunci (*key*), sehingga informasi yang sebelumnya dapat dibaca menjadi tidak bisa dipahami setelah melalui proses penyandian [1]. Terdapat dua macam kriptografi, yaitu kriptografi klasik dan kriptografi modern [2]. Kriptografi klasik kebanyakan menggunakan kunci simetris, metode penyandiannya menggunakan teknik substitusi atau transposisi atau menggabungkan kedua teknik tersebut. Teknik substitusi bekerja dengan cara menggantikan *plaintext* dengan karakter lain sehingga menghasilkan *ciphertext*. Teknik transposisi bekerja dengan mengubah *plaintext* menjadi *ciphertext* melalui penyusunan kembali karakter dengan urutan yang berbeda dari urutan aslinya (permutasi). Sedangkan pada kriptografi modern, metode penyandiaannya bersifat lebih kompleks karena menggunakan pengolahan simbol biner mengikuti operasi komputer digital, sehingga membutuhkan pengetahuan matematika dasar untuk menguasainya. Algoritma klasik dibagi lagi menjadi beberapa macam algoritma, salah satu yang masih berkembang sampai saat ini adalah algoritma Vigenere Cipher. Vigenere Cipher menggunakan metode substitusi poli alfabetik yang bersifat simetris pada proses penyadiannya, yang berarti kunci yang digunakan pada penyandian adalah sama [3]. Proses penyadian pada kriptografi terdiri dari proses Enkripsi dan proses Dekripsi. Enkripsi adalah proses mengubah *plaintext* menjadi *ciphertext*, sedangkan Dekripsi adalah proses mengembalikan *ciphertext* menjadi *plaintext* [2].

Agar keamanan basis data lebih kuat lagi, beberapa penelitian menyarankan untuk mengkombinasikan beberapa model algoritma enkripsi, seperti kombinasi antara algoritma Vigenere Cipher dan AES 128 bit yang diterapkan oleh Denny Eka Erlianto dan Painem (2018) dalam Aplikasi Kriptografi Pengamanan Database Menggunakan Metode AES dan Vigenere Berbasis Desktop pada Divisi Pencegahan dan Penanggulangan HIV AIDS Yayasan Kapeta [4], ada pula kombinasi algoritma Blowfish dan Base64 pada Implementasi Kriptografi Menggunakan Metode Blowfish dan Base 64 untuk Mengamankan Database Informasi Akademik pada Kampus Akademi Telekomunikasi Bogor Berbasis Web-Based oleh Annas Rifa'i dan Lilis Cucu Sumartini (2019) [5], juga kombinasi algoritma RC4 dan Base64 pada Sistem Keamanan Basis Data Klien PT. Infokes Menggunakan Kriptografi Kombinasi RC4 dan Base64 yang dibuat oleh Irawan Afrianto dan Nurhikmah Taliasih (2020) [6]. Keunggulan dari sistem keamanan basis data yang menggunakan kriptografi kombinasi antara lain tidak mudah dipecahkan oleh kriptanalis karena memiliki tingkat kesulitan yang berlapis untuk mengamankan *plaintext* [7], hasil dari enkripsi dan dekripsinya juga tidak mengubah isi dari *plaintext* yang ada, selain itu dengan kriptografi kombinasi kelebihan pada masing–masing algoritma juga ikut dikombinasikan sehingga dapat mengatasi kekurangan masing–masing algoritma. Penelitian ini bertujuan untuk meningkatkan keamanan sistem basis data di Pusat Pelayanan Terpadu DEF. Basis data akan diamankan dengan menggunakan algoritma kriptografi secara berlapis. Algoritma kriptografi yang digunakan adalah algoritma Vigenere Cipher dan Base64.

2. Metode Penelitian

Metode Pengembangan Sistem

Metode pengembangan sistem yang digunakan dalam penelitian ini adalah metode *waterfall*. Metode *waterfall* merupakan metode pengembangan sistem yang dilakukan secara berurutan dalam linier mode, dimana tahapan–tahapannya saling terkait satu sama lain [8]. Metode *waterfall* terdiri dari 5 langkah, yaitu analisa kebutuhan sistem, desain sistem, implementasi desain, pengujian sistem, dan terakhir pemeliharaan sistem [9]. Untuk lebih jelasnya dapat dilihat pada Gambar 2 di bawah ini.



Gambar 2. Metode Waterfall

Uji Coba Performa Sistem

Pada uji coba performa sistem, metrik yang digunakan ialah nilai entropi. Nilai entropi dihitung dari ciphertext yang dihasilkan. Nilai ideal entropi adalah 8, semakin tinggi nilai entropi maka semakin sulit ciphertext dipecahkan [10]. Nilai entropi dihitung menggunakan persamaan 1.

$$E = -\sum_{r=0}^{R=255} c_{(r)} \log_2\left(c_{(r)}\right) \qquad (1)$$

Dari persamaan 1 di atas,
E = nilai entropi
R = rentang kode ASCII
$c_{(r)}$ = probabilitas simbol pada ciphertext

Base64

Algoritma Bas64 merupakan sebuah algoritma untuk melakukan *encoding* dan *decoding* sebuah data dengan mengubahnya ke dalam format ASCII berdasarkan bilangan dasar 64 terhadap data binary [11]. Karakter yang dihasilkan dari Base64 terdiri dari huruf A sampai Z, a sampai z, angka 0 sampai 9, ditambah dengan dua karakter terakhir bersimbol + dan /, dan satu buah karakter = yang digunakan untuk menggenapkan data binari.

Index (6 bit data)	Char *Encoding* Base64	Index (6 bit data)	Char *Encoding* Base64	Index (6 bit data)	Char *Encoding* Base64	Index (6 bit data)	Char *Encoding* Base64
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/
						pad	=

Gambar 3. Index Base64

Vigenere Cipher

Vigenere Cipher dikembangkan oleh seorang ahli matematikan Prancis Bernama Blaise de Vigenere [12]. Cipher sendiri merupakan fungsi matemaatika yang dapat mengdnkripsi dan mendekripsi data [13]. Vigenere Cipher termasuk dalam *polyalphabetic substitution cipher* dan merupakan pengembangan dari Caesar cipher. Algoritma Vigenere Cipher sulit dipecahkan karena frekuensi kemunculan huruf yang sama berkurang, dalam Vigenere Cipher satu huruf dapat berubah menjadi beberapa huruf yang berbeda tergantung kuncinya [14]. Proses enkripsi dan dekripsi Vigenere Cipher dapat dilakukan dengan dua cara.

Menggunakan Tabula Recta

Tabula recta (bujur sangkar vigenere) merupakan cara pertama untuk menerapkan Vigenere Cipher. Tabel mendatar menunjukan digunakan untuk merujuk *plaintext* dan tabel menurun digunakan untuk merujuk pada kunci. Pertemuan antara kedua tabel tersebut nantinya akan menjadi *ciphertext*.

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

Gambar 4. Tabula Recta

Melakukan Perhitungan Matematis

Perhitungan matematis dilakukan dengan menggunakan dua persamaan [15].

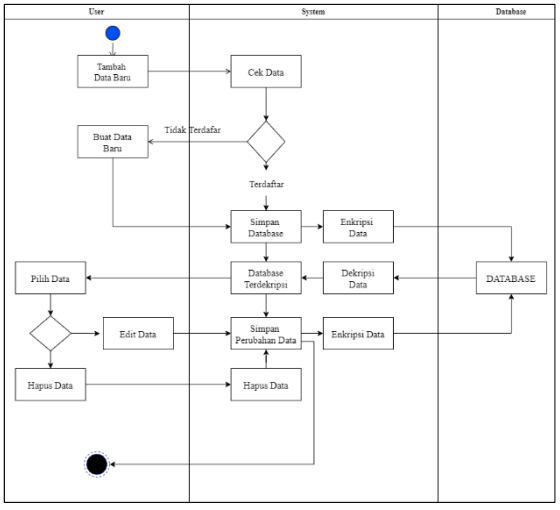
$$C_i \equiv (P_i + K_i) \bmod 26 \qquad (2)$$

$$P_i \equiv (C_i - K_i) \bmod 26 \qquad (3)$$

Persamaan (2) digunakan untuk proses enkripsi, sedangkan persamaan (3) digunakan untuk proses dekripsi, di mana c sebagai *ciphertext*, p sebagai *plaintext*, k sebagai kunci, dan mod atau *modulo* merupakan sisa.

Activity Diagram CURD Data

Saat *user* akan menambah data baru, sistem akan mengecek terlebih dahulu apakah data tersebut sudah terdaftar. Jika sudah terdaftar, *user* dapat melakukan perubahan pada data yang ada. Jika belum, *user* akan diminta untuk menambahkan data. Setelah data berhasil ditambah atau diubah, sistem akan melakukan enkripsi sesuai dengan algoritma yang dipilih *user* sebelum data tersebut disimpan di *database*. Ketika *user* akan melakukan perubahan pada data yang sudah ada, sistem akan melakukan dekripsi terlebih dahulu agar data dapat dibaca oleh *user*.



Gambar 5. Activity Diagram CRUD

3. Hasil dan Pembahasan

Algoritma Vigenere Cipher

Algoritma Vigenere Cipher merupakan salah satu metode kriptografi klasik yang digunakan untuk mengamankan data dengan menggunakan teknik substitusi polialfabetik. Dalam algoritma ini, terdapat dua fungsi utama, yaitu encrypt dan decrypt. Fungsi encrypt bertanggung jawab untuk mengubah plaintext menjadi ciphertext dengan menggunakan sebuah kunci. Kunci ini biasanya terdiri dari serangkaian karakter yang dibuat secara acak, dalam penelitian ini terdiri dari 10 karakter yang dihasilkan secara otomatis. Proses encrypt pada algoritma Vigenere Cipher dilakukan dengan menggeser setiap karakter plaintext sesuai dengan karakter kunci yang sesuai. Sedangkan fungsi decrypt akan melakukan proses kebalikannya, yaitu mengembalikan ciphertext menjadi plaintext dengan menggunakan kunci yang sama. Dengan menggunakan algoritma ini, keamanan data dapat ditingkatkan karena setiap karakter plaintext akan dienkripsi menjadi beberapa karakter ciphertext yang berbeda, tergantung pada karakter kunci yang digunakan.

```
function encrypt($pswd, $text){
    $pswd = strtolower($pswd);

    $code = "";
    $ki = 0;
    $kl = strlen($pswd);
    $length = strlen($text);

    for ($i = 0; $i < $length; $i++){
        if (ctype_alpha($text[$i])){
            if (ctype_upper($text[$i])){
                $text[$i] = chr(((ord($pswd[$ki]) - ord("a") + ord($text[$i]) - ord("A")) % 26) + ord("A"));
            }else{
                $text[$i] = chr(((ord($pswd[$ki]) - ord("a") + ord($text[$i]) - ord("a")) % 26) + ord("a"));
            }
            $ki++;
            if ($ki >= $kl) {
                $ki = 0;
            }
        }
    }
    return $text;
}
```

Gambar 6. Enkripsi Vigenere Cipher

Sedangkan fungsi decrypt akan melakukan kebalikannya. Fungsi ini akan mengubah ciphertext menjadi plain text dengan kunci yang telah ada.

```
function decrypt($pswd, $text){
    $pswd = strtolower($pswd);
    $code = "";
    $ki = 0;
    $kl = strlen($pswd);
    $length = strlen($text);
    for ($i = 0; $i < $length; $i++){
        if (ctype_alpha($text[$i])){
            if (ctype_upper($text[$i])){
                $x = (ord($text[$i]) - ord("A")) - (ord($pswd[$ki]) - ord("a"));
                if ($x < 0){
                    $x += 26;
                }
                $x = $x + ord("A");
                $text[$i] = chr($x);
            }else{
                $x = (ord($text[$i]) - ord("a")) - (ord($pswd[$ki]) - ord("a"));
                if ($x < 0){
                    $x += 26;
                }
                $x = $x + ord("a");
                $text[$i] = chr($x);
            }$ki++;
            if ($ki >= $kl){
                $ki = 0;
            }
        }
    }return $text;
}
```

Gambar 7. Dekripsi Vigenere Cipher

Algoritma Base64

Algoritma Base64 adalah sebuah metode encoding yang digunakan untuk mengubah data biner menjadi teks ASCII. Fungsi utama dari algoritma ini adalah encode dan decode. Fungsi encode bertugas untuk mengonversi plaintext menjadi ciphertext melalui beberapa tahapan. Pertama, plaintext dipecah menjadi blok-blok data dengan panjang tertentu. Kemudian, setiap blok data tersebut diubah menjadi nilai numerik dalam bentuk bilangan desimal. Tahap terakhir dari

proses encode adalah mengubah bilangan desimal tersebut ke dalam bentuk karakter ASCII menggunakan indeks dari tabel karakter Base64. Implementasi dari proses encode ini dapat dilihat pada gambar 8 dan gambar 9 dalam penelitian ini. Proses decode pada algoritma Base64 adalah kebalikan dari proses encode. Decode bertugas untuk mengembalikan ciphertext ke plaintext. Caranya adalah dengan mengonversi setiap karakter dalam ciphertext kembali menjadi bilangan desimal menggunakan indeks dari tabel karakter Base64. Setelah itu, bilangan desimal tersebut diubah kembali menjadi blok data biner, dan akhirnya disusun kembali menjadi plaintext. Dengan demikian, algoritma Base64 memungkinkan penggunaan data biner dalam format teks ASCII yang dapat dengan mudah ditransmisikan melalui berbagai jenis media komunikasi.

```
}else if ($_POST['jenis']==2){
    $nama = Base64Url::encode($_POST['nama']);
    $tgllhr = $_POST['tgllhr'];
    $hp = Base64Url::encode($_POST['hp']);
    $email = Base64Url::encode($_POST['email']);
    $alamat = Base64Url::encode($_POST['alamat']);
    $pekerjaan = Base64Url::encode($_POST['pekerjaan']);
```

Gambar 8. Encoding Base64

```
}else if ($o['jenis']==2){
  $nama = Base64Url::decode($o['nama']);
  //$tgllhr = Base64Url::decode($o['tgllhr']);
  $tgllhr = $o['tgllhr'];
  $hp = Base64Url::decode($o['hp']);
  $email = Base64Url::decode($o['email']);
  $alamat = Base64Url::decode($o['alamat']);
  $pekerjaan = Base64Url::decode($o['pekerjaan']);
```

Gambar 9. Decoding Base64

Kombinasi Algoritma Vigenere Cipher dan Base64

Pada kombinasi algoritma Vigenere Cipher dan Base64, data akan dienkripsi dulu menggunakan algoritma Vigenere Cipher. Kemudian hasil enkripsi tersebut akan di*encoding* menggunakan algoritma Base64. Setelah selesai di*encoding*, data baru akan masuk ke dalam database. Di proses dekripsi, data yang ada di dalam database akan *didecoding* terlebih dahulu. Apabila data sudah selesai *didecoding*, data tersebut akan didekripsi. Ketika data selesai didekripsi, data baru akan ditampilkan kepada *user*.

Kombinasi Algoritma Base64 dan Vigenere Cipher

Kebalikan dari kombinasi algoritma Vigenere Cipher dan Base64, pada kombinasi algoritma Base64 dan Vigenere Cipher data yang diinput akan diencoding terlebih dahulu menggunakan Base64 untuk selanjutnya dienkripsi menggunakan Vigenere Cipher

Uji Performa Sistem

Sistem yang telah selesai dibangun akan diuji performanya menggunakan analisis nilai entropi, dengan nilai ideal 8. Jika nilai entropi yang dihasilkan semakin mendekati angka 8 maka pengamanan pada database tersebut juga semakin kuat. Pengujian dilakukan pada tiap tabel yang ada yaitu tabel pelapor, tabel pelaku, tabel korban, dan tabel kasus. Masing – masing tabel akan memiliki 20 data set berbeda yang nantinya akan dienkripsi menggunakan algoritma Vigenere Cipher, algoritma Base64, kombinasi algoritma Vigenere Cipher dan Base64, serta kombinasi algoritma Base64 dan Vigenere Cipher. Hasil pengujian terhadap 4 tabel tersebut dapat dilihat pada tabel 1 di bawah ini.

Tabel 1. Nilai Entropi

Tabel	Nilai Entropi			
	Vigenere Cipher	Base64	Vigenere Cipher dan Base64	Base64 dan Vigenere Cipher
Pelapor	5,7609	5,6194	5,7076	5,8617
Pelaku	5,6094	5,5592	5,6640	5,8393
Korban	5,6620	5,5592	5,6866	5,8528
Kasus	5,8001	5,4452	5,5899	5,7331

Bersumber dari tabel Nilai Entropi di atas, tabel yang dienkripsi menggunakan algoritma Base64 menghasilkan nilai entropi yang paling kecil. Selanjutnya ada pada tabel yang dienkripsi dengan menggunakan algoritma kombinasi Vigenere Cipher dan Base64, yang nilai entropi tabel Korbannya ada pada urutan kedua setelah algoritma kombinasi Algoritma Base64 dan Vigenere Cipher. Nilai entropi terbesar terdapat pada tabel yang dienkripsi menggunakan algoritma Vigenere Cipher dan kombinasi Algoritma Base64 dan Vigenere Cipher. Algoritma Vigenere Cipher mendapatkan hasil nilai terbesar pada 1 tabel, yaitu tabel Kasus. Sedangkan kombinasi Algoritma Base64 dan Vigenere Cipher mendapat hasil nilai terbesar pada tabel Pelapor, Pelaku, dan Korban.

Karena algoritma Vigenere Cipher dan algoritma kombinasi Algoritma Base64 dan Vigenere Cipher menghasilkan nilai entropi tertinggi pada tabel yang berbeda, perlu dianalisa kembali algoritma mana yang memperoleh hasil entropi paling besar. Selanjutnya

akan dihitung rata–rata nilai entropi pada tiap algoritma sehingga diperoleh nilai rata–rata entropi sebagai berikut :

Tabel 2. Rata-Rata Nilai Entropi

	Vigenere Cipher	Base64	Vigenere Cipher dan Base64	Base64 dan Vigenere Cipher
Rata-Rata	5,7081	5,5458	5,6620	5,8217

Berdasarkan pada tabel 2 Rata – Rata Hasil Entropi, diperoleh persentase rata – rata nilai entropi sebagai berikut.

Tabel 3. Persentase Rata-Rata Nilai Entropi

	Vigenere Cipher	Base64	Vigenere Cipher dan Base64	Base64 dan Vigenere Cipher
Rata–Rata (%)	71,35	69,32	70,78	72,77

Dengan persentase rata-rata nilai entropi sebesar 72,77%, kombinasi algoritma Base64 dan Vigenere Cipher merupakan algoritma yang paling tepat digunakan untuk mengamankan *database* di Pusat Pelayanan Terpadu DEF.

4. Kesimpulan

Setelah melakukan penelitian yang menghasilkan sistem pengamanan database dengan menggunakan algoritma Vigenere Cipher dan Base64, diperoleh simpulan sebagai berikut :

1) Algoritma yang menggunakan kunci untuk proses enkripsi dan dekripsi (Vigenere Cipher) memiliki tingkat keamanan lebih tinggi dari pada algoritma yang tidak menggunakan kunci (Base64).
2) Kombinasi algoritma Base64 dan Vigenere Cipher memiliki tingkat keamanan lebih tinggi dengan rata – rata nilai entropi 5,8217 dibandingkan dengan kombinasi algoritma Vigenere Cipher dan Base64 yang menghasilkan nilai entropi 5,6620.

5. Daftar Pustaka

[1] Ahamed, B.B. and Krishnamoorthy, M., 2020. SMS encryption and decryption using modified vigenere cipher algorithm. *Journal of the Operations Research Society of China*, pp.1-14. DOI: https://doi.org/10.1007/s40305-020-00320-x.

[2] Ziaurrahman, M., Utami, E. and Wibowo, F.W., 2019. Modifikasi Kriptografi Klasik Vigenere Cipher Menggunakan One Time Pad Dengan Enkripsi Berlanjut. *Informasi Interaktif*, *4*(2), pp.63-68.

[3] Ardhianto, E., Handoko, W.T., Supriyanto, E. and Murti, H., 2021. Evolusi Cipher Vigenere dalam Peningkatan Pengamanan Informasi. *Jurnal Informatika UPGRIS*, *7*(2), pp. 23-27. DOI: https://doi.org/10.26877/jiu.v7i2.9333.

[4] Erlianto, D.E. and Painem, P., 2018. Aplikasi Kriptografi Pengamanan Database Menggunakan Metode Aes Dan Vigenere Berbasis Desktop Pada Pada Divisi Pencegahan Dan Penanggulangan Hiv Aids Yayasan Kapeta. *SKANIKA: Sistem Komputer dan Teknik Informatika*, *1*(2), pp.773-779.

[5] Rifaâ, A. and Sumartini, L.C., 2019. Implementasi Kriptografi Menggunakan Metode Blowfish Dan Base64 Untuk Mengamankan Database Informasi Akademik Pada Kampus Akademi Telekomunikasi Bogor Berbasis Web-Based. *Jurnal E-Komtek*, *3*(2), pp.87-96. DOI: https://doi.org/10.37339/e-komtek.v3i2.133.

[6] Taliasih, N. and Afrianto, I., 2020. Sistem Keamanan Basis Data Klien PT Infokes Menggunakan Kriptografi Kombinasi RC4 Dan Base64. *Jurnal Nasional Teknologi dan Sistem Informasi*, *6*(01), pp.9-18.

[7] Haris, C.A. and Ariyus, D., 2020. Kombinasi dan Modifikasi Vigenere Cipher dan Hill Cipher Menggunakan Metode Hybrid Kode Pos, Trigonometri, dan Konversi Suhu Sebagai Pengamanan Pesan. *Inform. Mulawarman J. Ilm. Ilmu Komput*, *15*(2), p.90-96.

[8] Cahyono, T., Setianingsih, S. and Iskandar, D., 2022. Implementation Of The Waterfall Method In The Design Of A Website-Based Book Lending System. *Jurnal Teknik Informatika (Jutif)*, *3*(3), pp.723-730. DOI: https://doi.org/10.20884/1.jutif.2022.3.3.285

[9] Irsandi, J.S., Fitri, I., Nathasia, N.D. and Kunci, K., 2020. Sistem Informasi Pemasaran dengan Penerapan CRM (Customer Relationship Management) Berbasis Website menggunakan Metode Waterfall dan Agile. *J. JTIK (Jurnal Teknol. Inf. dan Komunikasi)*, *5*(4), p.346. DOI: https://doi.org/10.35870/jtik.v5i4.192.

[10] Supriyanto, E., Handoko, W.T., Wibowo, S.A. and Ardhianto, E., 2022. Peningkatan Ketahanan Algoritma Vigenere menggunakan Generator kunci Tiga Lapis. *JURNAL MAHAJANA INFORMASI*, *7*(1), pp.24-33. DOI: https://doi.org/10.51544/jurnalmi.v7i1.2894.

[11] Aulia, R., Zakir, A. and Purwanto, D.A., 2018. Penerapan Kombinasi Algoritma Base64 Dan Rot47 Untuk Enkripsi Database Pasien Rumah Sakit Jiwa Prof. Dr. Muhammad Ildrem. *InfoTekJar: Jurnal Nasional Informatika dan Teknologi Jaringan*, *2*(2), pp.146-151. DOI: https://doi.org/10.30743/infotekjar.v2i2.300.

[12] Hameed, T.H. and Sadeeq, H.T., 2022. Modified Vigenère cipher algorithm based on new key generation method. *Indonesian Journal of Electrical Engineering and Computer Science*, *28*(2), pp.954-961.

[13] Milian, Y.C. and Sulistyo, W., 2023. Model Pengembangan Keamanan Data dengan Algoritma ROT 13 Extended Vernam Cipher dan Stream Cipher. *Jurnal JTIK (Jurnal Teknologi Informasi dan Komunikasi)*, *7*(2), pp.208-216. DOI: https://doi.org/10.35870/jtik.v7i2.716.

[14] Junikhah, A., 2022. Implementasi Vigenere Cipher Pada Aplikasi Myprichat End-To-End Encrypted Sms Berbasis Android. *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, *7*(3), pp.680-691. DOI: https://doi.org/10.29100/jipi.v7i3.3012.

[15] Alasi, T.S. and Siahaan, A.T.A.A., 2020. Algoritma Vigenere Cipher Untuk Penyandian Record Informasi Pada Database. *Jurnal Informasi Komputer Logika*, *1*(4).