JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol. VII No. 1, Dec 2020, hlm. 33 – 38 ISSN 2550-0201 (Online)
DOI: https://doi.org/10.33330/jurteksi.v7i1.896
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

PENGAMANAN DATABASE MENGGUNAKAN KOMBINASI ALGORITMA (CEST CRYPTOGRAPHY) DAN ALGORTIMA BASE64

Cendra Wadisman[1*], Irohito Nozomi[1], Sri Rahmawati[1]
[1]Sistem Informasi, Universitas Putra Indonesia YPTK Padang
email: *cendra_wadisman@upiyptk.ac.id

Abstract: Combined algorithm (Cest Cryptography) is a combination of 3 algorithms such as Merklee-Hellman, Discrete Logarithm and ASCII Modification, using Base64 to hide 2 public keys and 2 private keys. Combination algorithms are used because of the increasing number of techniques in cryptography, making it easier to combine each other algorithms in order to get more complicated encryption that won't even be cracked in the near future. On large sites there has been database theft, if the stolen database has been encrypted it will be difficult for data thieves to take advantage of it, but if it is not encrypted it is very easy to use the data so that it creates huge losses, especially user trust from the site.

Keywords: algorithm combination; ascii modification; base64; merklee-hellman; discrete logarithm

Abstrak: Kombinasi algoritma (Cest Cryptography) merupakan kombinasi 3 algoritma seperti Merklee-Hellman, Logaritma Diskrit dan Modifikasi ASCII, menggunakan Base64 untuk menyembunyikan 2 kunci public dan 2 kunci private.. Kombinasi algoritma digunakan karena semakin banyaknya teknik-teknik dalam kriptografi sehingga mempermudah untuk saling mengkombinasikan algoritma agar mendapatkan enkripsi yang lebih rumit dan bahkan tidak bisa dipecahkan dalam jangka waktu dekat. Pada situs-situs besar telah terjadi pencurian database, jika database yang dicuri telah terenkripsi maka akan mempersulit pencuri data untuk memanfaatkannya tetapi jika tidak terenkripsi maka sangat mudah data tersebut di manfaatkannya sehingga membuat kerugian yang sangat besar terutama kepercayaan pengguna dari situs tersebut.

Kata kunci: kombinasi algoritma; modifikasi ascii; base64; merklee-hellman;logaritma diskrit

PENDAHULUAN

Pada saat ini banyak blog yang membahas cara membobol sistem, karena setiap orang memiliki gadget sehingga dengan mudah mengakses situs web yang mengulas tentang cara membobol sistem. Kita tidak tau siapa yang belajar dan megerti dari ulasan tersebut. Jumlah kejahatan komputer terutama yang berhubungan dengan sistem informasi terus meningkat. Untuk itu keamanan sistem terutama web harus lebih diperhatikan karena semua orang bisa mengakses diseluruh dunia. Jika data yang kita miliki menarik perhatian orang banyak maka website kita bisa menjadi target serangan. Ada artikel yang mengulas tentang mengamankan url dengan base64 agar tidak diserang *SQL Inejction* [1]. Algo-

JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol. VII No. 1, Dec 2020, hlm. 33 – 38 ISSN 2550-0201 (Online)
DOI: https://doi.org/10.33330/jurteksi.v7i1.896
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

ritma base64 merupakan salah satu algoritma untuk *encoding* dan *decoding* suatu data kedalam format ASCII. Dengan menerapkan *base64* dapat mengurangi resiko terkena serangan *SQL Injection*. Pada penelitian lain *base64* juga diterapkan untuk mengamankan *sourcode* suatu sistem[2], sehingga jika seseorang berhasil mendapatkan *sourcecode* tetapi tidak bisa digunakan karena *sourcecode* berupa karakter ASCII. Teknik kriptografi juga dapat diterapkan pada file gambar [3]. Dengan semakin banyaknya teknik kriptografi sehingga memudahkan dalam memilih teknik yang akan digunakan dan mengkombinasikan antara teknik yang satu dengan yang lainnya seperti yang diterapkan pada rumah sakit dalam enkripsi database [4]. Untuk pengenkripsian dokumen juga sudah diterapkan menggunakan kriptograpi [5]. Didunia perbankan juga sudah menerapkan kriptografi dalam sistem keamanan anjungan tunai [6]

Penerapan kriptografi bukan membuat sistem menjadi tidak bisa dibobol karena tidak ada sistem yang sempurna, hanya saja akan menjadi lebih sulit untuk dibobol. Syarat dari keamanan sistem yaitu pencegahan, yaitu memperkecil peluang pembobolan oleh pemakai yang tak diotorisasi [7]. Algoritma Merkle-Hellman menggunakan algoritma asimetris dan memiliki 2 kunci utama yaitu kunci *private* dan kunci *public* [8]. Logaritma diskrit yang digunakan berdasarkan konsep algoritma RSA, jadi semua properti yang ada di logaritma diskrit tersebut sama dengan properti dari RSA. [9]. Pada tahun 1984 shamir menyatakan algoritma Merkle-Hellman tidak aman, sehingga diperlukan kombinasi dengan algoritma kriptografi lainnya. Transformasi base64 merupakan salah satu algoritma untuk *encoding* dan *decoding* suatu data ke dalam format ASCII, yang didasarkan pada bilangan dasar 64 atau bisa dikatakan sebagai salah satu metode yang digunakan untuk melakukan *encoding* (penyandian) terhadap data *binary*. [10]

METODE

Mekanisme dari kombinasi algoritma ini terdapat 2 kunci *private* dan 2 *kunci* public. Beberapa mekanisme dari kombinasi algoritma knapsack dan logaritma diskrit adalah sebagai berikut :

1. Menentukan urutan superincreasing di mana setiap elemen dalam urutan harus lebih besar dari jumlah elemen sebelumnya. Urutan superincreasing ini digunakan sebagai kunci *private* pertama
2. Memilih bilangan prima m dengan syarat harus lebih besar dari unsur terakhir deret pertambahan
3. Pilih bilangan n, di mana bilangan prima relatif terhadap m .
4. Menghasilkan kunci *public* pertama dengan persamaan (1)
   a. $pi = si * n \ mod$ m *(1)*
5. Pilih bilangan prima p dan q .
6. Menghitung nilai n_rsa = p * q
7. Menghitung nilai ϕ (n) = (p-1) (q-1)
8. Pilih bilangan e dengan syarat (e, ϕ (n) = 1). angka e digunakan sebagai kunci *public* kedua
9. Menghitung nilai d dengan syarat *d * e mod (ϕ(n)) = 1*.
10. Nilai d ini digunakan sebagai private key kedua
11. Melakukan proses enkripsi pertama dengan persamaan (2)

a. $c=b1*p1+b2*p2+. . +bn*pn$ (2)

12. Melakukan proses enkripsi kedua dengan persamaan (3)
13. $c = m^{e} \ mod \ n_rs$a (3)
14. Variabel m pada persa-

JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol. VII No. 1, Dec 2020, hlm. 33 – 38 ISSN 2550-0201 (Online)
DOI: https://doi.org/10.33330/jurteksi.v7i1.896
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

maan (3) merupakan hasil dari proses persamaan (2). Artinya, proses enkripsi dilakukan dua kali pada persamaan (2) dan persamaan (3)

15. Hasil enkripsi persamaan 3 dimodifikasi menggunakan modifikasi ASCII dan menjadi enkripsi ketiga.

Tabel 1. Modifikasi ASCII

No	Karakter
0	a
1	b
2	c
3	D
4	e
5	F
6	g
7	h
8	i
9	j

16. Hasil enkripsi ketiga pada modifikasi ascii dilakukan dekripsi pertama sesuai table 1.
17. Melakukan proses dekripsi kedua dengan persamaan (4)

a. $e = m^{c} mod\ n\_rsa$ (4)

18. Melakukan proses dekripsi pertama menggunakan persamaan (5).

b. $c * n^{-1}\ mod$ m (5)

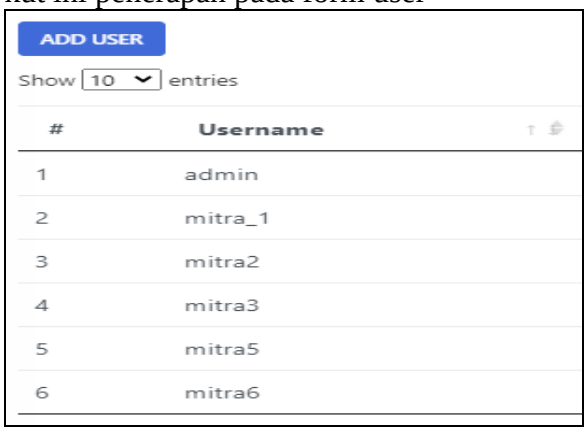
HASIL DAN PEMBAHASAN

Pada aplikasi jasa pengangkutan sampah, kombinasi algoritma diterapkan pada field-field yang dianggap penting dan sangat rentan jika diketahui oleh orang banyak. Seperti pada username dan password, saat ini jika username sudah diketahui oleh orang banyak maka semakin mudah orang-orang yang ingin menjebol sistem tersebut untuk mengujinya dengan menggunakan teknik *brute force attack*, sehingga username juga perlu di amankan.

Aplikasi ini menggunakan codeignither sehingga kunci *private* maupun kunci *private* bisa disimpan di dalam config. Untuk meningkatkan keamanan kunci tersebut maka di gunakan algoritma base64 [2], seperti pada gambar 1.

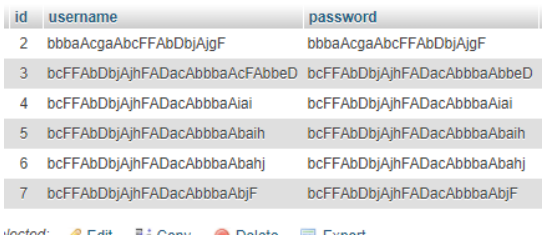
Gambar 1 base_config

Kombinasi algortima Merkle-Hellman dan Logaritma Diskrit sebelumnya juga sudah pernah diterapkan pada aplikasi chat[9]. Pada gambar 2 berikut ini penerapan pada form user



Gambar 2 Tampilan User

Jika dilihat pada tampilan user hanya seperti biasa, tetapi pada database sudah terenkripsi, seperti pada gambar 3.



id	username	password
2	bbbaAcgaAbcFFAbDbjAjgF	bbbaAcgaAbcFFAbDbjAjgF
3	bcFFAbDbjAjhFADacAbbbaAcFAbbeD	bcFFAbDbjAjhFADacAbbbaAbbeD
4	bcFFAbDbjAjhFADacAbbbaAiai	bcFFAbDbjAjhFADacAbbbaAiai
5	bcFFAbDbjAjhFADacAbbbaAbaih	bcFFAbDbjAjhFADacAbbbaAbaih
6	bcFFAbDbjAjhFADacAbbbaAbahj	bcFFAbDbjAjhFADacAbbbaAbahj
7	bcFFAbDbjAjhFADacAbbbaAbjF	bcFFAbDbjAjhFADacAbbbaAbjF

Gambar 3 Data User Tersimpan

JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol. VII No. 1, Dec 2020, hlm. 33 – 38 ISSN 2550-0201 (Online)
DOI: https://doi.org/10.33330/jurteksi.v7i1.896
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

Agar perhitungan mudah dilakukan, nilai-nilai yang akan digunakan dapat dilihat pada tabel 2

Tabel 2. Melengkapi Nilai

No	Keterangan	Karakter
1	Superincreasing	(1,2,4,8,16,32,64,128)
2	m	251
3	n	11
4	p	33
5	q	41
6	nrsa	1353
7	ϕ (n)	1280
5	e	7
6	d	183
7	n^{-1}	137

Untuk mendapatkan kunci *public* dapat menggunakan persamaan 1, untuk hasil persamaan 1 dapat dilihat pada tabel 3.

Tabel 3. Kunci *Public*

No	Kunci *Private*	Kunci *Public*
1	1	11
2	2	22
3	3	44
4	4	88
4	16	176
5	32	101
6	64	202
7	127	153

Untuk memulai menggunakan kombinasi algoritma, tentukan *plaintext* dan dapatkan nilai ascii dari *plaintext* tersebut ubah menjadi biner dengan 8 bit., dapat dilihat pada table 4.

Tabel 4. *Plaintext* "ces" dan nilai Ascii

No	Kunci *Public*	c	e	s
1	11	0	0	0
2	22	1	1	1
3	44	1	1	1
4	88	0	0	1
5	176	0	0	0
6	101	0	1	0
7	202	1	0	1
8	153	1	1	1
ASCII		99	101	115

Hasil enkripsi pertama dapat dilihat pada tabel 5 dengan menggunakan persamaan 2

Tabel 5. Enkripsi pertama

No	Kunci Publik	c	e	s
1	11	0	0	0
2	22	22	22	22
3	44	44	44	44
4	88	0	0	88
5	176	0	0	0
6	101	0	101	0
7	202	202	0	202
8	153	153	153	153
Enkripsi		420	320	509

.

Pada table 6 untuk mendapatkan hasil enkripsi kedua digunakan digunakan persamaan (6) dan untuk mendapatkan enkripsi ketiga itu menggunakan tabel 1 modifikasi ascii sesuai nilai yang didapatkan pada enkripsi kedua.

Tabel 6. Enkripsi Kedua dan ketiga

No	Enkripsi	c	E	s
1	Pertama	420	320	509
2	Kedua	691	1310	218
3	Ketiga	gjb	bDba	cbi

Untuk melakukan proses dekripsi dilakukan 3 tahap, pertama dekripsi pada modifikasi ascii sesuai pada tabel 1 dan dekripsi kedua menggunakan persamaan (4)

Dari persamaan (4) didapatkan hasil seperti tabel 7

Tabel 7. Dekripsi Pertama dan kedua

No	Dekripsi	gjb	bDba	cbi
1	Pertama	691	1310	218
2	Kedua	420	320	509

JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol. VII No. 1, Dec 2020, hlm. 33 – 38 ISSN 2550-0201 (Online)
DOI: https://doi.org/10.33330/jurteksi.v7i1.896
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

Untuk mendapatkan proses dekripsi ketiga menggunakan persamaan (5)

Dari persamaan (5) didapatkan hasil dekripsi seperti pada tabel 8

Tabel 8. Dekripsi Ketiga

No	Dekripsi	gjb	bDba	cbi
1	Ketiga	198	166	206

Setelah mendapatkan nilai dari dekripsi ketiga, langkah selanjutnya membentuk nilai biner berdasarkan kunci *private* yang terbesar yang dimulai dari kunci *private*.

Tabel 9. Nilai Biner

No	Kunci *Private*	198	166	206
1	128	1	1	1
2	64	1	0	1
3	32	0	1	0
4	16	0	0	0
4	8	0	0	1
5	4	1	1	1
6	2	1	1	1
7	1	0	0	0

Setelah mendapatkan hasil dari tabel 9, maka disusun dari kunci paling terkecil agar bisa mendapatkan nilai awal.

Tabel 9. Biner Awal

No	Biner	ascii	Karakter
1	01100011	99	c
2	01100101	101	e
3	01110011	115	s

SIMPULAN

Kombinasi algoritma (CEST Cryptography) dapat diterapkan pada database sebuah sistem untuk meningkatkan keamanan dari database tersebut. Database tersebut terlindungi karena beberapa data yang penting sudah dienkripsi dengan 2 kunci *private* dan 2 kunci *public* agar tidak mudah dibaca oleh orang yang tidak berhak sehingga data menjadi lebih aman. Karena memimiliki 2 kunci *private* dan *public* yang tidak boleh diketahui oleh orang lain maka perlu menerapkan algoritma *base64* untuk melakukan *encode* sebuah *sourcecode* yang memuat informasi mengenai kunci tersebut. Penerapan kombinasi algoritma pada sebuah sistem membutuhkan waktu akses lebih lama dibandingkan tidak menggunakannya karena saat menggunakan kombinasi algoritma membutuhkan 3 kali proses enkripsi dan 3 kali proses dekripsi, jika ingin menerapkan pada sebuah sistem diharapkan pada data yang sangat penting saja agar kecepatan akses tidak terlalu lama.

UCAPAN TERIMA KASIH

Terimakasih kepada Universitas Putra Indonesia YPTK Padang yang telah mendanai penelitian ini.

DAFTAR PUSTAKA

[1] E. Gunadhi and A. P. Nugraha, “Penerapan Kriptografi Base64 Untuk Keamanan URL (Uniform Resource Locator) Website Dari Serangan SQL Injection,” *J. Algoritm.*, 2017, doi: 10.33364/algoritma/v.13-2.391.

[2] C. Saefudin, G. Abdillah, and A. Maspupah, “PENGAMANAN SOURCE CODE PROGRAM MENGGUNAKAN ALGORITMA ADVANCED ENCRYPTION STANDARD

JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol. VII No. 1, Dec 2020, hlm. 33 – 38 ISSN 2550-0201 (Online)
DOI: https://doi.org/10.33330/jurteksi.v7i1.896
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

DAN ALGORITMA BASE64," *Semin. Nas. Apl. Teknol. Inf.*, 2019.

[3] D. Rizal, T. Sutojo, and Y. Rahayu, "Implementasi Kriptografi Gambar Menggunakan Kombinasi Algoritma Elgamal Dan Mode Operasi Ecb (Electronic Code Book)," *Techno.COM*, 2016.

[4] R. Aulia, A. Zakir, and D. A. Purwanto, "PENERAPAN KOMBINASI ALGORITMA BASE64 DAN ROT47 UNTUK ENKRIPSI DATABASE PASIEN RUMAH SAKIT JIWA PROF. DR. MUHAMMAD ILDREM," *InfoTekJar (Jurnal Nas. Inform. dan Teknol. Jaringan)*, 2018, doi: 10.30743/infotekjar.v2i2.300.

[5] F. N. Pabokory, I. F. Astuti, and A. H. Kridalaksana, "Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard," *Inform. Mulawarman J. Ilm. Ilmu Komput.*, 2016, doi: 10.30872/jim.v10i1.23.

[6] F. Efendi and N. P. Dewanti, "Implementasi Kriptografi dalam Sistem Keamanan Anjungan Tunai Mandiri," *J. Inform. Upgris*, 2019, doi: 10.26877/jiu.v5i1.3212.

[7] N. Fahriani, P. A. R. Devi, and D. Aditama, "Alternatif Penanganan Jenis Serangan Pencurian Data Pada Jaringan Komputer," *Pros. Semin. Nas. Teknol. dan Rekayasa Inf. Tahun 2017*, 2017.

[8] M. Fadlan and H. Hadriansa, "Rekayasa Aplikasi Kriptografi dengan Penerapan Kombinasi Algoritma Knapsack Merkle Hellman dan Affine Cipher," *J. Teknol. Inf. dan Ilmu Komput.*, 2017, doi: 10.25126/jtiik.201744468.

[9] A. Aminudin, A. F. Helmi, and S. Arifianto, "Analisa Kombinasi Algoritma Merkle-Hellman Knapscak dan Logaritma Diskrit pada Aplikasi Chat," *J. Teknol. Inf. dan Ilmu Komput.*, 2018, doi: 10.25126/jtiik.201853844.

[10] S. Supiyandi, H. Hermansyah, and K. A. P. Sembiring, "Implementasi dan Penggunaan Algoritma Base64 dalam Pengamanan File Video," *J. MEDIA Inform. BUDIDARMA*, 2020, doi: 10.30865/mib.v4i2.2042.