Rekayasa Hijau: Jurnal Teknologi Ramah Lingkungan Volume 8 | Nomor 2
ISSN [e]: 2579-4264 | DOI: https://doi.org/10.26760/jrh.V8i2.162-171 Juli 2024

Peningkatan Keamanan Basis Data menggunakan Kombinasi Algoritma RC4 dan SHA3-512

Asep Rizal Nurjaman[1], Sofia Umaroh[2]
[1]Institut Teknologi Nasional, Kota Bandung, Indonesia
[2]Institut Teknologi Nasional, Kota Bandung, Indonesia
Email: aseprizal@itenas.ac.id[1], sofia.umaroh@itenas.ac.id[2]

Received 25 Apil 2024 | Revised 2 Mei 2024 | Accepted 10 Mei 2024

ABSTRAK

Perkembangan teknologi yang pesat membuat banyak sistem menjadi terdigitalisasi dan terintegrasi. Banyak sistem yang memuat data-data yang penting seperti profil pengguna, no handphone, e-mail, nomor kependudukan, bahkan hingga file-file dokumen yang bersifat rahasia. Dalam dunia maya, banyak kejahatan yang terjadi, dengan digitalisasi menyebabkan kejahatan seperti pencurian data, perubahan data atau bahkan pengambil alihan akun yang menyebabkan pemilik aslinya tidak dapat masuk ke dalam sistem disebabkan akun yang dimiliki telah diambil alih oleh hacker. Penelitian ini bertujuan untuk mengamankan informasi-informasi penting milik pengguna dengan menggunakan kombinasi RC4 dan SHA3-512 pada kunci agar saat sebuah sistem diretas dan masuk ke basis data, attacker tidak dapat langsung mendapatkan informasinya namun harus memecahkan informasi yang terenkripsi tersebut. Hal ini membuat attacker membutuhkan waktu untuk memecahkan informasi-informasi pengguna.

***Kata kunci**: SHA3-512, Enkripsi, Dekripsi, Hashing, RC4, Algoritma*

ABSTRACT

Rapid technological developments mean that many systems are becoming digitalized and integrated. Many systems contain important data such as user profiles, cellphone numbers, e-mails, population numbers, and even confidential document files. In cyberspace, many crimes occur, with digitalization causing crimes such as data theft, changing data or even taking over accounts which cause the original owner to not be able to enter the system because his account has been taken over by hackers. This research aims to secure the user's important information by using a combination of RC4 and SHA3-512 in the key so that when a system is hacked and entered into the database, the attacker cannot immediately get the information but must crack the encrypted information. This makes the attacker need time to decipher user information.

***Keywords:** SHA3-512, Encryption, Decryption, Hashing, RC4, Algorithm*

1. PENDAHULUAN

Perkembangan teknologi yang pesat membuat banyak sistem menjadi ter digitalisasi. Banyak sistem yang memuat data-data yang penting seperti profil pengguna, no. handphone, *e-mail*, nomor kependudukan, bahkan hingga *file* dokumen yang bersifat rahasia. Dalam dunia maya, banyak kejahatan yang terjadi, dengan digitalisasi pun menyebabkan kejahatan seperti pencurian data, perubahan data atau bahkan pengambil alihan akun yang menyebabkan pemilik aslinya tidak dapat membuka atau masuk ke dalam sistem disebabkan akun yang dimiliki nya telah diambil alih oleh *hacker*.

Pada tahun 2023 data penduduk Indonesia di retas lewat aplikasi kpu.go.id [6]. Pada Mei 2021 BPJS mengalami pembobolan data, diduga sebanyak 279 juta data penduduk Indonesia yang berasal dari BPJS kesehatan bocor dan dijual di forum peretas [8]. Semakin besar peluang seorang peretas untuk mendapatkan informasi yang akurat dari banyaknya data yang tersimpan dalam sebuah basis data. Sehingga dibutuhkan cara untuk menjaga integritas dan keamanan basis data dalam menjaga kerahasiaan dan keaslian data. Salah satu ilmu yang mempelajari tentang keamanan dan integritas data adalah kriptografi, kriptografi merupakan seni untuk menyandikan pesan [1].

Penelitian tentang pengaman basis data dengan teknik kriptografi sudah dilakukan sebelumnya, pada tahun 2018 Lutfi telah melakukan penelitian dengan judul "Pengamanan Tabel Database menggunakan Kriptografi Algoritma RSA" dan menghasilkan sebuah kesimpulan bahwa sistem pengamanan basis data yang dibangun membuat proses pertukaran informasi dan penyimpanan data lebih aman dengan waktu proses enkripsi dan dekripsi tabel yang berbanding lurus dengan ukuran dari tabel basis data [8]. Di tahun 2018 juga dilakukan penelitian terkait pengamanan pesan teks dengan modifikasi RC4 berhasil dilakukan oleh Dani [9]. Di tahun 2021 Annisa telah melakukan penelitian dengan judul "Implementasi Kriptografi untuk Keamanan Data dan Jaringan menggunakan Algoritma DES" dan menghasilkan sebuah kesimpulan bahwa algoritma kriptografi DES dapat mengamankan data dan juga jaringan dengan proses kerjanya sehingga sebelum sampai ke penerima bentuk pesannya masih berbentuk *ciphertext*, dari sisi penerima dapat membaca dengan mengubah *ciphertext* ke *plaintext* menggunakan aplikasi tertentu [5]. Pada tahun 2022 Nurmi telah melakukan penelitian dengan judul "Penerapan Keamanan Basis Data Dengan Menggunakan Kombinasi Teknik Enkripsi SHA Dan Knapsack" dan menghasilkan sebuah kesimpulan bahwa penelitiannya berhasil menerapkan kombinasi teknik enkripsi SHA dan Knapsack dan memanfaatkan CrypTool 2.1 untuk mengetahui hasil pengujian dari kombinasi SHA1 dan Knapsack tidak berhasil dideskripsi atau di-decode seperti teks asli [4]. Dari penelitian-penelitian sebelumnya telah dicoba pengamanan basis data dengan menggunakan algoritma RSA, Knapsack, SHA, DES, dan RC4.

Berdasarkan penelitian sebelumnya, maka peneliti mencoba untuk mengombinasikan algoritma RC4 dan SHA3-512 untuk mengamankan informasi-informasi penting pada profil pengguna seperti nik, tempat & tanggal lahir, unit kerja, nomor handphone, e-mail, dan alamat akan aman dari pencurian data dan membutuhkan waktu bagi peretas untuk mendapatkan data aslinya, namun tidak sulit bagi pengguna dan admin aplikasi karena diberikan akses. RC4 memiliki proses enkripsi dan dekripsi yang relatif cepat juga dibantu oleh SHA3-512 untuk men-*generate* kunci yang digunakan sehinnga hanya pengguna yang sah yang mengetahui kunci dan dapat dengan mudah melakukan enkripsi-dekripsi datanya.

2. METODOLOGI

2.1 Keamanan Komputer

Teknologi yang semakin canggih dan perkembangan sistem informasi yang pesat berdampak positif dan memudahkan masyarakat dalam melakukan pekerjaan seiring dengan dampak positif yang dirasakan maka harus diimbangi dengan peningkatan keamanan baik dari sisi perangkat (komputer) dan juga dari sisi sistem / aplikasi. Salah satu dampak negatif yang akan ditimbulkan jika tidak dibarengi dengan peningkatan keamanan adalah maraknya pencurian data atau munculnya penipuan dengan memanfaatkan teknologi komputer. Salah satu cara untuk menyolusikan dampak negatif tersebut dengan meningkatkan keamanan komputer sehingga data-data yang ada tidak dapat dicuri dengan mudah atau tidak rusak [11]. Cara untuk meningkatkan keamanan komputer salah satunya dengan mengimplementasikan metode-metode yang ada pada ilmu kriptografi. Salah satunya dengan menggunakan algoritma RC4 dan SHA3-512 untuk menjaga keamanan dan kerahasiaan data yang ada pada komputer kita dari hal–hal yang dapat mengancam keamanan komputer.

2.2 Data

Baik data maupun informasi merupakan suatu rangkaian kesatuan, dimana informasi akan didapatkan dari data, dan data yang diolah akan menghasilkan sebuah informasi. Namun ada beberapa perbedaan antara data dan informasi, sebelum membahas mengenai perbedaan antara keduanya, maka ada baiknya kita membahas mengenai pengertian masing-masing terlebih dahulu [8]. Basis Data merupakan data yang terintegrasi, yang diorganisasi untuk memenuhi kebutuhan para pemakai di dalam suatu organisasi [3], basis data merupakan data yang dapat didesain dan berintegrasi dan dapat memenuhi kebutuhan *user* dalam perusahaan atau organisasi.

2.3 Kriptografi

Kriptografi merupakan ilmu untuk menyandikan pesan, dengan kata lain kriptografi adalah tulisan yang tersembunyi sehingga orang-orang yang tidak mengetahui bagaimana tulisan tersebut disembunyikan tidak akan mengetahui bagaimana cara membaca maupun menerjemahkan tulisan tersebut. Kriptografi sebagai "*the art and science of keeping messages secure*" [1].

Kriptografi merupakan salah satu dasar bagi keamanan komputer dan jaringan karena berisi data atau informasi. Keamanan komputer atau lebih dikenal cyber secutity merupakan penerapan pengamanan informasi pada komputer dan jaringan. Tujuannya membantu mencegah pengguna agar terhindar dari penipuan, mendeteksi adanya usaha penipuan dan mengamankan datanya dari penipu dalam sebuah sistem yang berbasis informasi [8].

2.4 RC4

RC4 adalah jenis *stream-cipher* dimana proses penyandian dilakukan per karakter 1 *byte* dalam satu kali operasi. Algoritma kriptografi Rivest Code 4 (RC4) merupakan satu dari banyaknya algoritma kunci simetris yang dibuat oleh RSA *Data Security Inc* (RSADSI) [1].

Tahun 1987 algoritma RC4 ditemukan oleh Ronald Rivest yang menjadi simbol keamanan dari algortima RSA. Untuk menginisialisasikan tabel sepanjang 256 *byte* algoritma ini menggunakan panjang kunci dari 1 sampai 256 *byte*. Terdapat dua buah *Substitution Box (S-Box)* yang digunakan pada algoritma ini, yang pertama merupakan *array* dengan panjang 256 yang berisi permutasi dari bilangan 0 sampai 255, yang kedua *S-Box* berisi permutasi yang merupakan fungsi dari kunci dengan panjang variabel.

Algoritma RC4 bekerja dengan menginisialisasi *S-Box* diawal, S[0], S[1], …….., S[255], dengan bilangan 0 sampai 255. pada proses ini dilakukan pengisian data secara berurutan S[0]=0, S[1]=1, …., S[255]=255. Selanjutnya inisialisasi *array / S-Box* lain misalkan *array* K dengan panjang 256. Isi *array* K dengan kunci diulangi sampai seluruh array K[0], K[1], ……., K[255] terisi.

a. Proses inisialisasi *S-Box* (*Array* S) dapat dilihat pada persamaan 1.

```
for a=0 to 255
    s[a] = a                                    (1).
```

b. Proses inisialisasi *S-Box* (*Array* K)
Kunci berbentuk array yang dapat dilihat pada persamaan 2.

```
for a=0 to 255
    K[a] = Kunci[i mod length]                  (2).
```

c. Proses *S-Box* yang diacak dapat dilihat pada persaman 3.

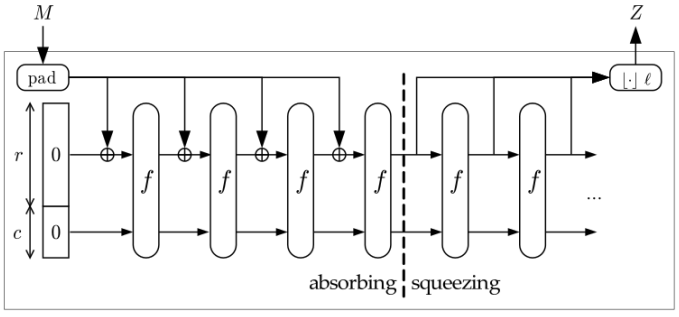
```
a=0
b=0
for a=0 to 255
    b=(b+s[a]+K[a]) % length
        Swap s[a] dan s[b]) mod length          (3).
```

d. Proses pembuatan pseudo random byte yang dapat dilihat pada persaman 4.

```
i=(i+1) % 255
j=(j+s[i]) % 255)
Swap s[i] dan s[j])
 t=(s[i]+s[j]) % 255
K = s[t]                                        (4).
```

2.5 SHA3-512

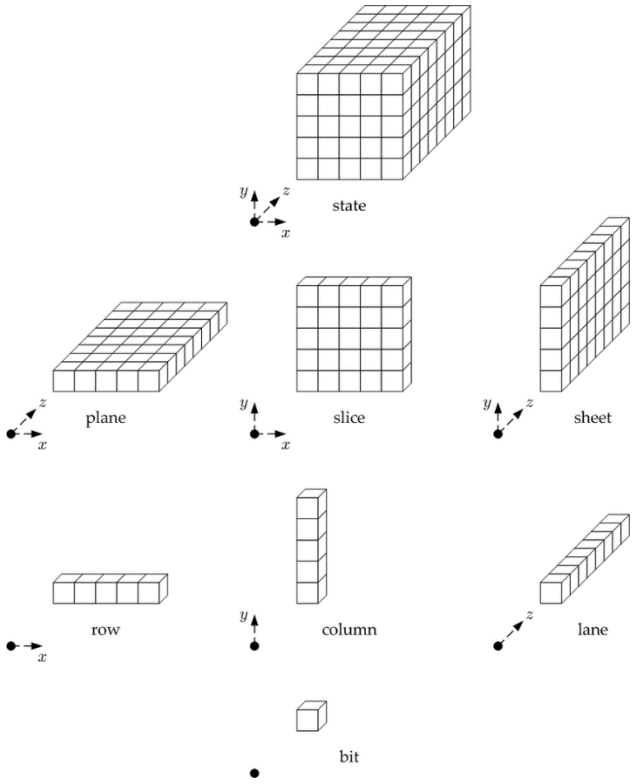
SHA3-512 merupakan salah satu jenis algoritma dari fungsi *hash keccak* yang digunakan untuk membuat integritas pesan terjaga. Fungsi *hash keccak* merupakan salah satu fungsi hash kriptografi yang mempunyai masuukan dan panjang luaran yang berubah-ubah. *Keccak* menggunakan konstruksi spons (*sponge construction*) sebagai dasar desainnya. Konstruksi spons memiliki dua fase yaitu menyerap (*absorbing*) dan memeras (*sequeezing*) [2][10], fungsi *hash keccak* ditunjukkan pada Gambar 1.



Gambar 1. Fungsi hash Keccak [2][10]

Absorbing [2][10] adalah suatu proses dimana input akan di-*xor* kan dengan *bitrate* (*r)* dan diteruskan ke fungsi. 5 tahapan operasi pada fungsi *f* yaitu: *diffusion (θ)*, *inter-slice dispersion (ρ)*, *disturbing the horizontal / vertical alignment (π), non-linierity (X)*, dan *break symetric (i). Sequeezing* [2][10] merupakan fase untuk mendapatkan output dimana penggabungan digunakan untuk menghasilkan nilai *hash* dengan panjang sama dengan total bit dari *capacity (c).*

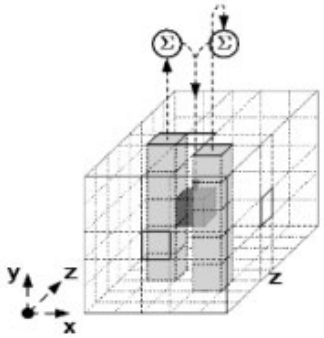
State pada *keccak* adalah bit-bit yang dapat dilihat sebagai bit *array* dengan bentuk tiga dimensi [2][10]. Setiap sumbu dari *array* di representasikan dengan sumbu x, y dan z. x*y merupakan potongan dari *state* dan z adalah sumbu dari *lane state* Jumlah dari bit-bit untuk setiap *slice* dari state pasti 5*5 atau 25 bit. Sementara ukuran dari tiap *lane* untuk *state* adalah 1, 2, 4, 8, 16, 32 atau 64. *State* dari keccak ditunjukkan pada Gambar 2.



Gambar 2. *State* pada *Keccak* [2][10]

a. Diffusion (θ)

Merupakan sebuah proses untuk meng-*xor* kan setiap bit pada *state* dengan *parity* dari dua kolom pada array. Luaran dari *diffusion* adalah perubahan kolom yang akan digunakan pada proses *inter-slice dispersion (ρ).* ilustrasi dari proses *diffusion* ada pada Gambar 3.

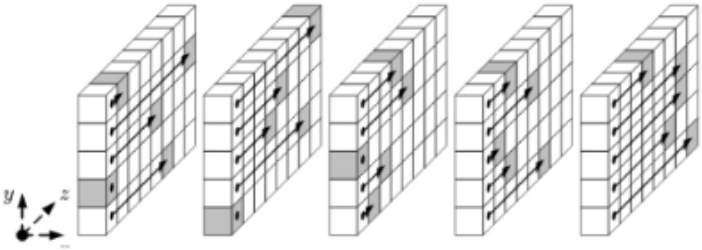


Gambar 3. Ilustrasi proses *diffusion* pada *single* bit [2][10]

b. *Inter-slice dispersion (ρ)*

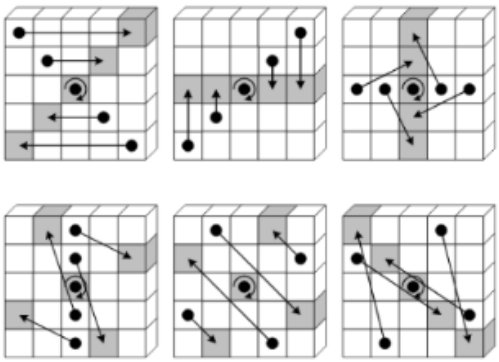
*Inter-slice dispersion m*erupaka sebuah proses untuk memutar bit-bit pada setiap *lane* berdasarkan panjangnya, yang disebut *offset,* berdasarkan koordinat x dan y dari tiap *lane.* Luarannya akan digunakan

oleh *disturbing the horizontal / vertical alignment (π).* Ilustrasi dari i*nter-slice dispersion (ρ)* ditunjukkan pada Gambar 4.



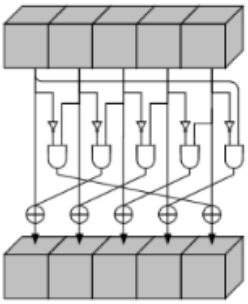
Gambar 4. Ilustrasi dari proses *inter-slice dispersion* [2][10]

c. Disturbing the horizontal / vertical alignment (π)
Disturbing the horizontal / vertical alignment merupakan proses untuk mengatur ulang posisi dari *lane,* koordinat x dan y akan berubah. Luarannya akan digunakan pada pada tahap selanjutnya. Ilustrasi dari *Disturbing the horizontal / vertical alignment* ditunjukkan pada Gambar 5.



Gambar 5. Ilustrasi dari proses *disturbing the horizontal / vertical alignment* [10]

d. Non-linierity (X)
Non-linierity merupakan sebuah proses untuk operasi-*xor* kan setiap bit dengan fungsi *non-linear* dari dua bit lainnya dalam sebuah baris. Alur proses *Non-Linierity* dapat dilihat pada Gambar 6.



Gambar 6. Alur dari *proses non-linierity [10]*

e. Break symetric (i)
Break symetric merupakan sebuah proses untuk mengubah beberapa bit dari *Lane(0,0)* berdasarkan putaran index i_r. Urutan *lane* 24 tidak terpengaruh oleh *break symetric.*

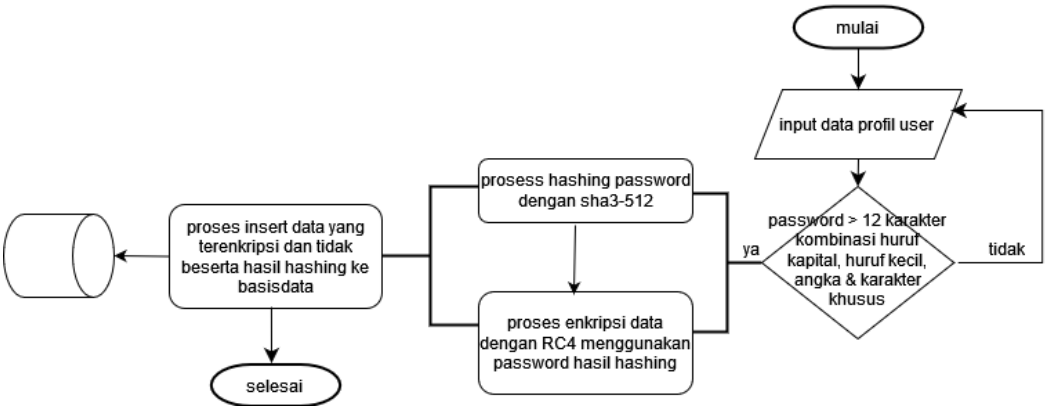
3. HASIL DAN PEMBAHASAN

3.1 Perancangan Skema Desain Sistem

Skema Desain Sistem yang dirancang membuat data terenkripsi saat tersimpan di basis data dan hanya dapat dibuka oleh pengguna yang terautentikasi. Perancangan Skema Desain Sistem terdiri dari :

a. Perancangan Desain Sistem Saat Registrasi (Enkripsi)

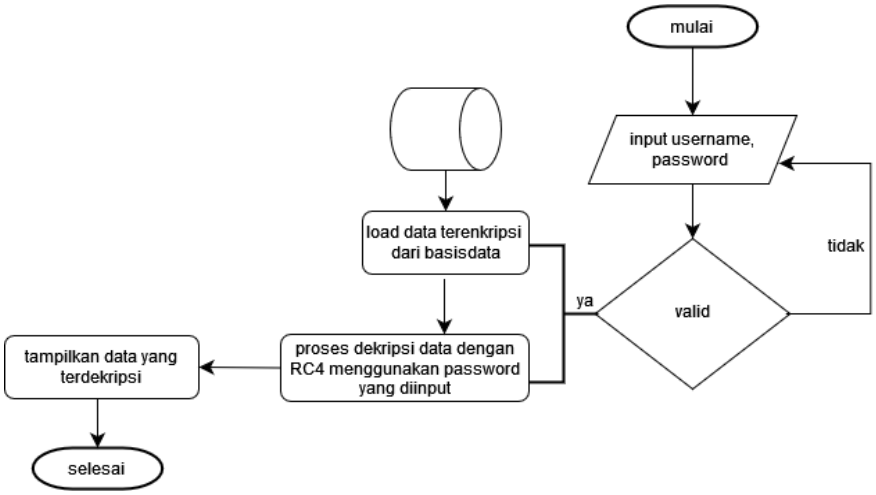
Saat registrasi data yang di masukkan adalah : *username, password,* email, alamat, tempat_lahir, tanggal_lahir, nik, nama_lengkap, alamat_tinggal, *gender*, no_hp, tempat bekerja. Proses enkripsi dengan menggunakan *password* dan hasil *hashing password* disimpan untuk autentikasi pengguna ke basis data beserta semua data profil pengguna. Alur proses enkripsi dapat dilihat pada Gambar 7.



Gambar 7. Perancangan Desain Sistem Saat Registrasi (Enkripsi)

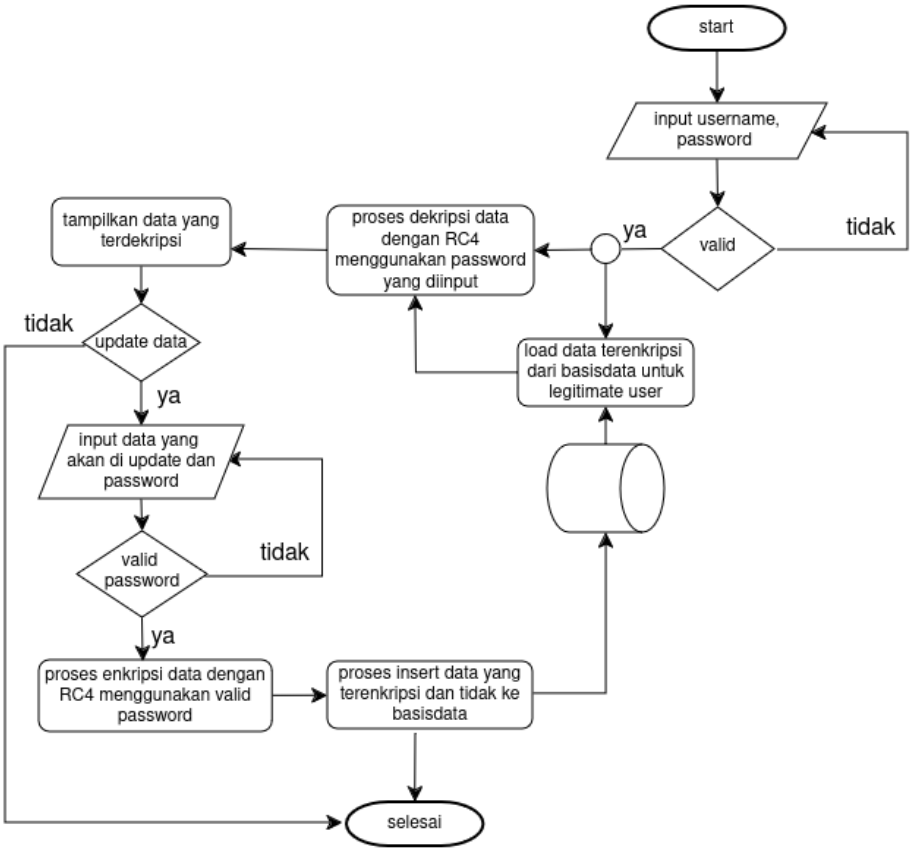
b. Perancangan Desain Sistem Setelah *login* (Dekripsi)

Proses dekripsi dilakukan setelah pengguna ter-autentikasi, maka data profil pengguna yang ada dalam basis data diambil dan didekripsi dengan kunci *password* yang digunakan saat *login*. Alur proses dekripsi dapat dilihat pada Gambar 8.



Gambar 8. Perancangan Desain Sistem Setelah Login (Dekripsi)

c. Perancangan Desain Sistem Saat Perubahan Data (Enkripsi/Dekripsi)



Gambar 9. Perancangan Desain Sistem saat Perubahan Profil Pengguna (Enkripsi/Dekripsi)

Pada Gambar 9 menjelaskan rancangan proses enkripsi dan dekripsi dimana pengguna harus memasukkan *password* pengguna saat akan mengubah data profilnya. Sehingga data yang diubah diyakini oleh pengguna yang sah dan memiliki akses pada datanya.

3.2 Hasil Pengujian

Pada Tabel 2 ditunjukkan hasil pengujian dari penerapan kombinasi algoritma RC4 dan SHA3-512 pada basis data yang memberikan hasil yang signifikan dari pada basis data standar. Luaran dari basis data dengan informasi yang diamankan akan menyulitkan penyerang untuk melihat, mengubah dan atau memanipulasi informasi yang ada. Hasil luaran dari enkripsi basis data menghasilkan panjang luaran yang sama dengan teks aslinya dengan hasil luaran berupa heksadesimal.

Tabel 1. Perbandingan Kunci Asli dan Hasil Hashing SHA3-512

Kunci Asli	Hasil Hashing SHA3-512
pwd123!@#$	7dba6ca3dd9d467739d027c3ef18306b5c3b883b529dd7ba2875576741f5915b5de91f eb687023449cd8d70fccb5d4fe8f311a09a8dfbbf8dbd069693a52483e
Password	e9a75486736a550af4fea861e2378305c4a555a05094dee1dca2f68afea49cc3a50e8de6 ea131ea521311f4d6fb054a146e8282f8e35ff2e6368c1a62e909716
Pas30rd12!@#	2bef868a8b3702e7b83501171d0d6bcece8f7f791bd8850ad0a721b07d338e920b0dea 4c7486d2ebdbe40b8e71fa1108f0b7fdf4d8711f4e0a3b397177a1744a

Tabel 2. Perbandingan Basis data standar dan basis data terenkripsi

Informasi	Basis data standar	Basis data terenkripsi
NIK	320634123456789012	0xca0xf40xca0x5f0x490x8a0x520xcb0x3d0x110xd90xbc 0x910x9a0x930x4a0xdf0x6b
Tempat Lahir	tasikmalaya	0x8d0xa70x890x00x110xd30x20x950x6f0x5c0x8d
Tanggal Lahir	1997-01-01	0xc80xff0xc30x5e0x570x8e0x520xd40x3e0x14
Unit Kerja	bandung	0x9b0xa70x940xd0xf0xd00x4
No Handphone	082320123456	0xc90xfe0xc80x5a0x480x8e0x520xcb0x3d0x110xd90xbc
Email	coba@gmail.com	0x9a0xa90x980x80x3a0xd90xe0x980x670x490xc20xe90 xc90xcf
Alamat	Jl. Pesantren dalam, rt05 rw11	0x930xaa0xd40x490xa0xd60xb0xd90x630x500x9f0xfe0x c70xc40xcb0x5a0x8c0x380x880x790xc70x1d0xf6

Hasil pengujian kekuatan algoritma, baik dari penelitian yang sudah ada dan juga yang akan diajukan dapat dilihat pada tabel 3, pada penelitian yang diajukan, kompleksitas untuk memecahkan informasi lebih sulit dibandingkan dengan algoritma RC4 dan DES.

Tabel 3. Perbandingan Algoritma untuk Pengamanan Basis Data

Algoritma	Probabilitas terpecahkan satu informasi dalam satu baris	Probabilitas terpecahkan informasi dari satu baris
RC4	$1/2^{256}$	$1/2^{256}$
DES	$1/2^{64}$	$1/2^{64}$
RC4+SHA3-512 (Diajukan)	$1/2^{256}$	$1/2^{256} * 1/2^{256}$

4. KESIMPULAN

Dengan menggunakan RC4 dan SHA3-512 membuat informasi penting pengguna pada basis data dapat diamankan dan tidak mudah terbaca oleh orang selain yang diberi hak akses. Kekuatan pada rc4 ini berada pada panjang kunci maksimal di 256 bit, sementara SHA3-512 ini memiliki kekuatan pada panjang luaran maksimal dibagi 2 sebagai batas *collision*, sehingga kemungkinan dapat terpecahkan informasi setiap baris adalah $1/2^{256}$. Jika penyerang mencoba menebak informasi tanpa menebak kunci maka probabilitas terpecahkannya $1/2^{256}$ dengan konsekuensi penyerang mencoba memecahkan satu persatu informasi dari setip baris. Jika penyerang mencoba memecahkan dengan cara menebak kunci lalu mencoba memecahkan salah satu informasi dalam baris maka kemungkinan terpecahkannya $1/2^{256} * 1/2^{256}$. Saran untuk penelitian selanjutnya diimplementasi dan diujikan pada *Mobile device* mengingat saat ini pengguna aplikasi atau sistem berbentuk *Mobile* juga mulai banyak digunakan. Yang perlu diperhatikan adalah waktu enkripsi dan dekripsi serta ukuran informasi hasil enkripsinya agar proses waktunya tidak melambat.

DAFTAR PUSTAKA

[1] Stallings, W. (2013). "Cryptography and Network Security: Principles and Practice". New Jersey: Prentice Hall Press.

[2] J. Kelsey, S. Change, dan R. Perlner, (2016). "SHA-3 derived functions: cSHAKE, KMAC, TupleHash and ParallelHash," Gaithersburg, MD, Des 2016. doi: 10.6028/NIST.SP.800-185.

[3] ayanti, Ni Ketut Dewi Ari & Sumiari, Ni Kadek. Teori Basis Data. Yogyakarta : Penerbit ANDI, 2018.

[4] Hidayasari, N dkk. (2022). "Penerapan Keamanan Basis Data Dengan Menggunakan Kombinasi Teknik Enkripsi SHA Dan Knapsack". *Seminar Nasional Industri dan Teknologi*, 5, pp. 40-48.

[5] Thahara, A dan Siregar, T. (2021). "Implementasi Kriptografi untuk Keamanan Data dan Jaringan menggunakan Algoritma DES". *JURTI,* 5(1), pp. 31-38.

[6] Ysl, (2024, Jan 11). KPU Dibobol Hacker, Data Pribadi 204 Juta Penduduk Indonesia Dijual Rp 1,2 Miliar. Retrieved from https://www.liputan6.com/tekno/read/5467318/kpu-dibobol-hacker-data-pribadi-204-juta-penduduk-indonesia-dijual-rp-12-miliar?page=5

[7] Ayp. (2021, Sep 3). Rentetan Kasus Dugaan Kebocoran Data Kesehatan Pemerintah. Retrieved from https://www.cnnindonesia.com/teknologi/20210903142047-185-689370/rentetan-kasus-dugaan-kebocoran-data-kesehatan-pemerintah

[8] Irwansyah, D. (2018). "Pengamanan Data Teks dengan Algoritma Modifikasi RC4". *Jurnal Pelita Informatika,* 6(3), pp. 309-312.

[9] Pratama, L dan Subandi. (2018). "Pengamanan Tabel Database menggunakan Kriptografi Algoritma RSA". *SKANIKA*, 1(3), pp. 925-930.

[10] M. J. Dworkin, (2015). "SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions," Gaithersburg, MD, Jul 2015. doi: 10.6028/NIST.FIPS.202.

[11] N, Syahputri. (2019). "Rancang Bangun Aplikasi Kriptografi Pengamanan Transmisi Data Multimedia Menggunakan Algoritma Data Encryption Standard". Maj. Ilm. Methoda, vol. 9, no. 2, pp. 57–63.

[12] Kurniawan, F., Kusyanti, A. & Nurwarsito, H., (2017), Analisis dan Implementasi Algoritme SHA-1 dan SHA-3 pada Sistem Autentikasi Garuda Training Cost, 1, 9, 803–812.