Perancangan Sistem keamanan Database Menggunakan Super Encryption dengan Algoritma Kriptografi Diffie Hellman dan Blowfish

1st Septya Andini Putri
Program Studi Teknik Informatika
Fakultas Informatika
Telkom University Purwokerto
Purwokerto, Indonesia
septyaandiniputri@student.telkomuniversity.ac.id

2nd Wahyu Adi Prwbowo
Program Studi Teknik Informatika
Fakultas Informatika
Telkom University Purwokerto
Purwokerto, Indonesia
wahyup@telkomuniversity.ac.id

line 1: 3rd Trihastuti Yuniati
Program Studi Teknik Informatika
Fakultas Informatika
Telkom University Purwokerto
Purwokerto, Indonesia
trihastutiy@telkomuniversity.ac.id

***Abstrak* — Meningkatnya penggunaan data digital dalam berbagai sektor menuntut sistem keamanan basis data yang mampu melindungi informasi sensitif dari ancaman siber. Penelitian ini bertujuan merancang sistem keamanan database berbasis web menggunakan pendekatan super encryption, yaitu kombinasi algoritma Diffie Hellman untuk pertukaran kunci dan Blowfish untuk proses enkripsi serta dekripsi data. Sistem dikembangkan menggunakan PHP native dan MySQL serta diimplementasikan pada web hosting daring. Hasil pengujian menunjukkan bahwa sistem mampu mengenkripsi dan mendekripsi data dengan baik secara manual, serta efektif mencegah serangan SQL Injection karena data tersimpan dalam bentuk ciphertext. Dengan demikian, sistem yang dirancang terbukti efektif dalam meningkatkan keamanan data pada basis data berbasis web.**

***Kata kunci*— kriptografi, database, super encryption, blowfish, diffie hellman**

I. PENDAHULUAN

Kemajuan teknologi informasi telah mendorong transformasi besar dalam pengelolaan data digital oleh berbagai institusi, termasuk sektor pemerintahan, Pendidikan, dan keuangan. Namun, peningkatan konektivitas digital juga memperbesar risiko terhadap kebocoran dan penyalahgunaan data sensitif. Serangan seperti SQL Injection dan *Cross-Site Scripting* (XSS) merupakan ancaman serius yang mengeksploitasi celah keamanan dalam aplikasi web untuk mengakses data secara ilegal [1].

Beberapa kasus kebocoran data skala besar di Indonesia memperkuat urgensi pengamanan database. Pada tahun 2021, sebanyak 297 juta data peserta BPJS Kesehatan dilaporkan bocor dan diperjualbelikan secara daring [2]. Di tahun yang sama, peretas LockBit mengklaim mencuri 1,5 Tb data Bank Syariah Indonesia. Kasus-kasus ini menunjukkan lemahnya system pengamanan database yang masih banyak menyimpan data dalam bentuk *plaintext*.

Untuk mengatasi tantangan tersebut, kriptografi menjadi Solusi utama dalam melindungi data. Salah satu pendekatan yang menjanjikan adalah *super encryption*, yaitu penggabungan dua algoritma kriptografi dengan fungsi berbeda. Dalam penelitian ini digunakan algoritma Diffie Hellman untuk proses pertukaran kunci seacara aman dan Blowfish untuk proses enkripsi dan dekripsi data. Diffie Hellman memungkinkan pembentukan *shared key* tanpa perlu mengirimkan kunci secara langsung, sedangkan Blowfish dikenal sebgai algoritma blok yang efisien dan ringan.

Penelitian terdahulu oleh Rizka (2021) telah mengimplementasikan kombinasi Diffie Hellman dan Blowfish pada pengamanan dokumen berbasis desktop. Namun, belum banyak studi yang menerapkannya secara manual dalam sistem database berbasis web. Maka dari itu, penelitian ini mengembangkan dan menguji sistem keamanan database berbasis web dengan pendekatan *super encryption* yang dirancang dan diimplementasikan secara manual tanpa library eksternal.

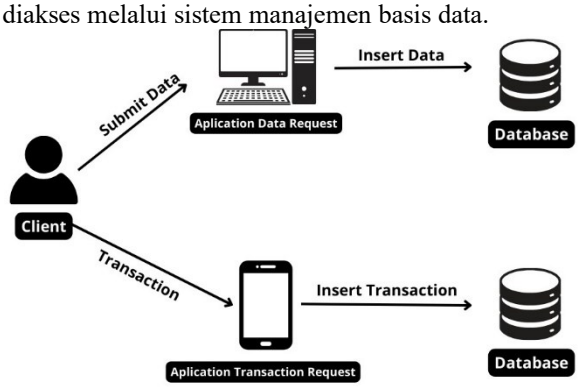
Tujuan dari penelitian ini adalah untuk merancang sistem keamanan database dengan mengombinasikan algoritma Diffie Hellman dan Blowfish, serta menguji efektivitasnya dalam menjaga kerahasiaan data terhadap serangan seperti SQL Injection. Sistem diimplementasikan menggunakan PHP Native dan MySQL, dengan pengujian pada data pribadi seperti tempat dan tanggal lahir, NIM, nomor rekening, dan nomor handphone, untuk membuktikan efektivitas metode super encryption dalam konteks aplikasi web nyata.

II. KAJIAN TEORI

A. Keamanan *Database*

Basis data atau *database* didefinisikan sebagai sistem yang dirancang untuk mengatur, menyimpan, dan mengambil data dengan cara yang terstruktur. Menurut penelitian lain, *database* didefinisikan sebagai kumpulan data yang saling berhubungan dan dirancang untuk memenuhi kebutuhan informasi suatu organisasi. Basis data disimpan secara teratur dalam komputer sehingga dapat diakses dan dianalisis menggunakan program komputer untuk memperoleh informasi yang diperlukan. Gambar 1 menunjukkan ilustrasi

database yang merepresentasikan bagaimana data disimpan dan diakses melalui sistem manajemen basis data.



GAMBAR 1
(ILUSTRASI DATABASE)

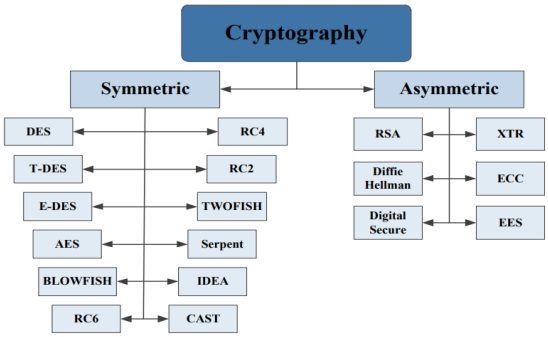
Database berfungsi sebagai tempat penyimpanan data yang terhubung dalam sebuah sistem informasi. Sistem database juga memudahkan akses, memungkinkan administrator untuk dengan mudah Melakukan operasi CRUD (Create, Read, Update, Delete) pada database. Selain itu, database juga berfungsi sebagai penyimpanan data aplikasi, di mana banyak aplikasi saat ini memanfaatkan database untuk menyimpan data. Dari segi manajemen, pengelompokan data dalam sistem database memudahkan administrator dalam mengelola semua data yang tersimpan.

Di sisi lain, di tengah kemudahan dan peran penting database dalam sistem informasi, aspek keamanan menjadi faktor krusial yang tidak dapat diabaikan. Seiring dengan meningkatnya ketergantungan terhadap teknologi informasi, ancaman terhadap keamanan database juga semakin kompleks [3]. Keamanan database didefinisikan sebagai langkah krusial untuk menjamin bahwa data yang tersimpan dalam basis data tetap aman dan selalu dapat diakses sesuai kebutuhan. Upaya ini mencakup berbagai tindakan yang bertujuan untuk memastikan bahwa hanya pengguna yang memiliki otorisasi yang dapat mengakses data, serta mencegah akses dari pihak yang tidak berwenang. Ruang lingkup keamanan database meliputi penerapan kebijakan perlindungan data, pengelolaan hak akses, penggunaan enkripsi, pelaksanaan prosedur pencadangan dan pemulihan data, serta pemantauan dan pengawasan sistem secara berkala [4].

B. Kriptografi

Kriptografi adalah ilmu yang mempelajari teknik pengamanan informasi dengan cara mengubah data asli (*plaintext*) menjadi bentuk terenkripsi (*ciphertext*) agar tidak dapat dibaca tanpa kunci tertentu [5]. Kriptografi memiliki dua proses utama, yaitu enkripsi dan dekripsi [6]. Berdasarkan jenis kuncinya, kriptografi terbagi menjadi dua:

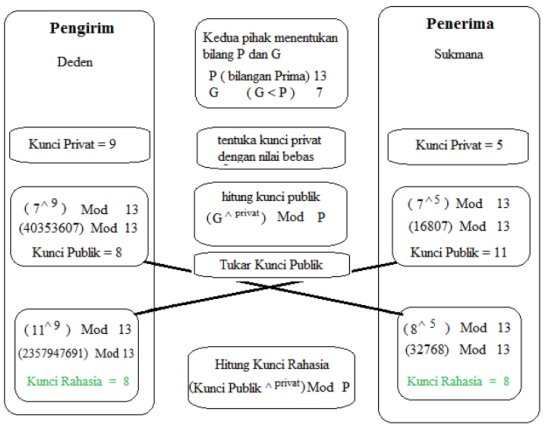
- **Simetris**, yang menggunakan satu kunci untuk enkripsi dan dekripsi.
- **Asimetris**, yang menggunakan pasangan kunci publik dan privat, dengan keunggulan dalam pertukaran kunci yang lebih aman.



GAMBAR 2
(KLASIFIKASI KRIPTOGRAFI)

C. Algoritma Diffie-Hellman

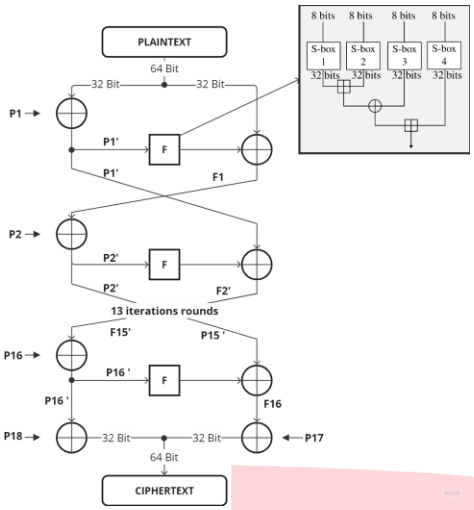
Algoritma Diffie-Hellman merupakan salah satu bentuk kriptografi asimetris yang digunakan untuk melakukan pertukaran kunci secara aman. Proses pertukaran kunci dilakukan menggunakan operasi eksponensial dalam modular matematika, di mana dua pihak dapat menghasilkan kunci bersama tanpa mentransmisikan kunci secara langsung melalui jaringan [7]. Hal ini meningkatkan keamanan karena kunci rahasia tidak pernah dikirimkan secara eksplisit. Algoritma ini efektif sebagai tahap awal dalam sistem enkripsi ganda, seperti super encryption [8].



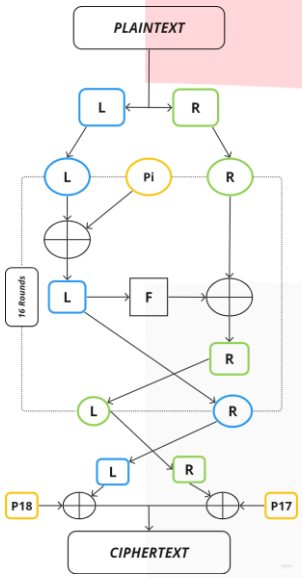
GAMBAR 3
(ILUSTRASI PERTUKARAN KUNCI DIFFIE HELLMAN)

D. Blowfish

Blowfish merupakan algoritma kriptografi blok simetris yang dirancang oleh Bruce Schneier sebagai alternatif dari DES. Algoritma ini menggunakan blok 64-bit dan mendukung panjang kunci antara 32 hingga 448 bit. Blowfish memiliki struktur 16 ronde jaringan Feistel dan dikenal karena efisiensinya dalam proses enkripsi dan dekripsi, terutama pada perangkat lunak [9]. Proses enkripsi Blowfish diawali dengan ekspansi kunci yang menghasilkan P-array dan S-box sebagai subkunci [10]. Dalam penelitian ini, Blowfish digunakan untuk mengamankan data dalam database setelah memperoleh kunci dari algoritma Diffie-Hellman.



GAMBAR 4
(DIAGRAM ALUR ENKRIPSI ALGORITMA BLOWFISH)



GAMBAR 5
(SKEMA ALUR ALGORITMA BLOWFISH)

E. Super Encryption

Super encryption adalah metode pengamanan berlapis yang menggabungkan dua atau lebih algoritma kriptografi secara berurutan untuk meningkatkan kekuatan sistem keamanan. Pendekatan ini sering memanfaatkan keunggulan dari algoritma asimetris dan simetris secara bersamaan. Beberapa penelitian menunjukkan bahwa super encryption dapat meningkatkan ketahanan terhadap serangan kriptanalisis dibandingkan penerapan satu algoritma tunggal [11]. Dalam konteks penelitian ini, super encryption diimplementasikan melalui kombinasi algoritma Diffie-Hellman untuk pertukaran kunci dan Blowfish untuk enkripsi data.

F. SQL Injection

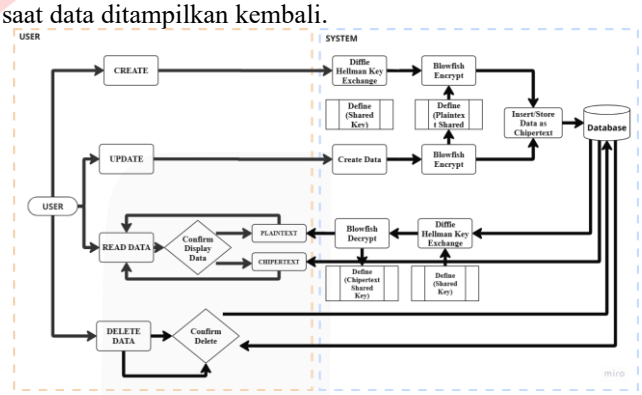
SQL Injection merupakan teknik serangan yang mengeksploitasi kelemahan input pada aplikasi web untuk menyisipkan perintah SQL berbahaya. Serangan ini memungkinkan penyerang untuk mengakses, memanipulasi, atau bahkan menghapus data dalam database secara ilegal [12]. SQL Injection sering terjadi karena kurangnya validasi input dari sisi server. Implementasi enkripsi pada tingkat kolom database, seperti yang dilakukan dalam penelitian ini, menjadi salah satu solusi mitigasi serangan tersebut [13].

III. METODE

Penelitian ini menggunakan pendekatan rekayasa perangkat lunak dengan tahapan analisis kebutuhan, perancangan sistem, implementasi algoritma, dan pengujian keamanan database berbasis web. Sistem dikembangkan menggunakan bahasa pemrograman PHP Native dan MySQL sebagai basis data. Proses pengujian keamanan dilakukan melalui simulasi serangan SQL Injection menggunakan SQLMap.

A. Arsitektur Sistem

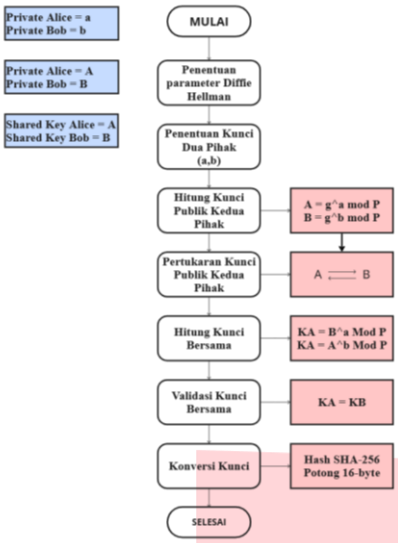
Sistem keamanan database dirancang menggunakan pendekatan *super encryption* dengan mengintegrasikan dua algoritma kriptografi: Diffie-Hellman untuk pertukaran kunci dan Blowfish untuk enkripsi serta dekripsi data. Gambar 1 menunjukkan arsitektur sistem yang terdiri dari proses input, enkripsi, penyimpanan data terenkripsi, dan proses dekripsi saat data ditampilkan kembali.



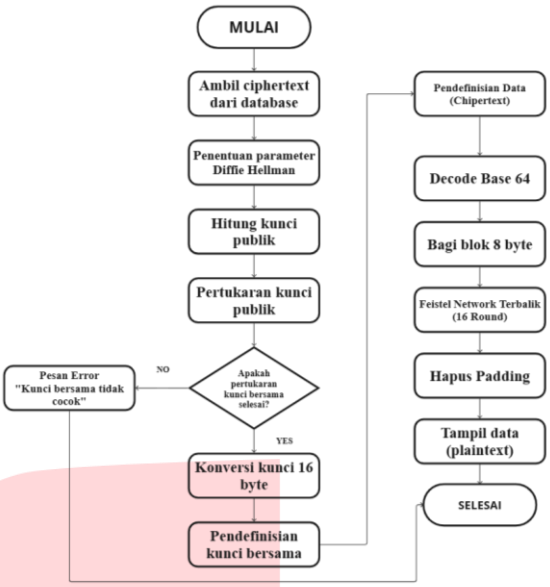
GAMBAR 6
ARSITEKTUR SISTEM

B. Proses Pertukaran Kunci Diffie Helman

Pertukaran kunci dilakukan menggunakan algoritma Diffie-Hellman. Algoritma ini memungkinkan dua pihak (client-server) menghasilkan kunci simetris bersama (*shared key*) tanpa perlu mengirimkan kunci secara eksplisit. Kunci hasil pertukaran kemudian di-hash menggunakan SHA-256 dan dipotong menjadi 16 byte agar sesuai dengan kebutuhan kunci Blowfish.



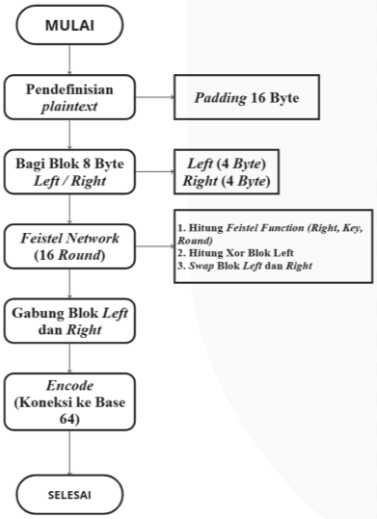
GAMBAR 7
(PROSES PERTUKARAN KUNCI DIFFIE HELMAN)



GAMBAR 9
(PENGINTEGRASIAN MODEL ENKRIPSI)

C. Proses Enkripsi dan Dekripsi Blowfish

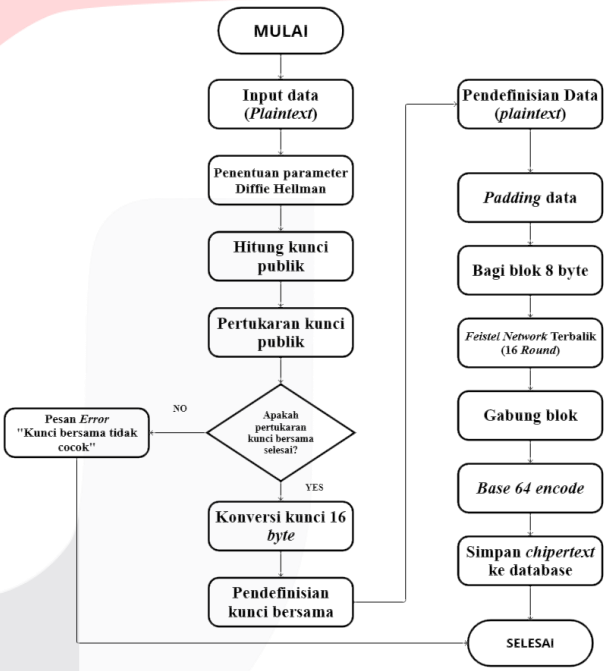
Proses enkripsi menggunakan algoritma Blowfish dilakukan terhadap data sensitif seperti NIM, tempat lahir, tanggal lahir, nomor rekening, dan nomor telepon. Data ini dienkripsi sebelum disimpan ke dalam database. Dekripsi dilakukan saat data akan ditampilkan kembali dalam bentuk plaintext.



GAMBAR 8
(MODEL ENKRIPSI BLOWFISH)

D. Integrasi Sistem

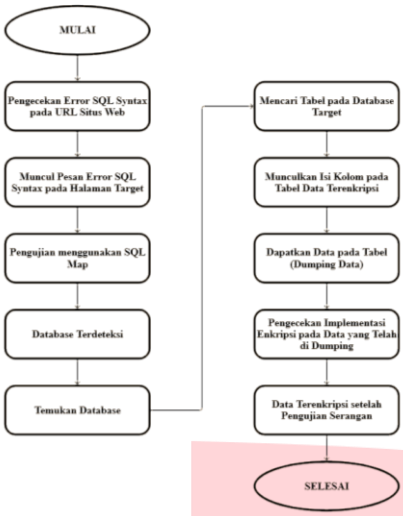
Sistem mengintegrasikan fungsi Diffie-Hellman dan Blowfish dalam proses create (tambah data), update, dan read (tampilkan data). Kunci yang dihasilkan digunakan secara dinamis untuk setiap proses enkripsi dan dekripsi, tanpa disimpan secara eksplisit.



GAMBAR 10
(PENGINTEGRASIAN MODEL DEKRIPSI)

E. Pengujian Sistem

Pengujian sistem dilakukan dengan menyerang sistem menggunakan SQL Injection melalui tools *SQLMap*. Tujuannya untuk memastikan bahwa data yang disimpan dalam bentuk terenkripsi tidak dapat dibaca atau dimanipulasi oleh pihak yang tidak berwenang. Keberhasilan diuji dari ketidakmampuan SQLMap membaca data terenkripsi.



GAMBAR 11
(ALUR SKEMA PENGUJIAN SISTEM)

IV. HASIL DAN PEMBAHASAN

A. Hasil Perancangan Sistem

Hasil implementasi menunjukkan bahwa sistem berhasil mengintegrasikan algoritma Diffie-Hellman dan Blowfish dalam proses super encryption untuk keamanan database. Proses pertukaran kunci menggunakan Diffie-Hellman menghasilkan shared key yang identik pada sisi pengirim dan penerima, yang kemudian digunakan sebagai input untuk proses enkripsi dan dekripsi Blowfish.

```php
function modExp($base, $exp, $mod): int
{
    $result = 1;
    $base = $base % $mod;
    while ($exp > 0) {
        if ($exp % 2 == 1) {
            $result = ($result * $base) % $mod;
        }
        $exp = floor(num: $exp / 2);
        $base = ($base * $base) % $mod;
    }
    return $result;
}
```

GAMBAR 12
(HASIL IMPLEMENTASI PERTUKARAN KUNCI DIFFIE-HELLMAN)

1. Hasil Enkripsi dan Dekripsi Blowfish

Hasil implementasi algoritma Blowfish menunjukkan bahwa data sensitif seperti NIM, tempat lahir, tanggal lahir, dan nomor rekening berhasil dienkripsi dan disimpan dalam bentuk ciphertext di dalam database.

```php
function blowfishEncrypt($key, $data): string
{
    $blockSize = 8;
    $data = addPadding(data: $data, blockSize: $blockSize); //
    Tambahkan padding
    $n = strlen(string: $data);
    $encrypted = '';

    for ($i = 0; $i < $n; $i += $blockSize) {
        $block = substr(string: $data, offset: $i,
        length: $blockSize);
        $left = substr(string: $block, offset: 0,
        length: $blockSize / 2);
        $right = substr(string: $block, offset: $blockSize / 2);

        // 16 Putaran Feistel
        for ($round = 0; $round < 16; $round++) {
            $temp = $right;
            $right = stringXOR(string: $left,
            intValue: feistelFunction(block: $right, key: $key,
            round: $round));
            $left = $temp;
        }

        $encrypted .= $right . $left;
    }

    return base64_encode(string: $encrypted); // Encode dalam
    Base64
}
```

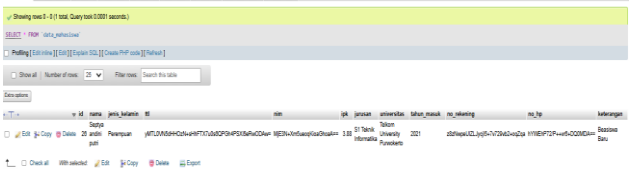
GAMBAR 13
(HASIL ENKRIPSI BLOWFISH)

```php
function blowfishDecrypt($key, $data): string
{
    $blockSize = 8;
    $data = base64_decode(string: $data); // Decode dari Base64
    $n = strlen(string: $data);
    $decrypted = '';

    for ($i = 0; $i < $n; $i += $blockSize) {
        $block = substr(string: $data, offset: $i,
        length: $blockSize);
        $right = substr(string: $block, offset: 0,
        length: $blockSize / 2);
        $left = substr(string: $block, offset: $blockSize / 2);

        // 16 Putaran Feistel (dibalik)
        for ($round = 15; $round >= 0; $round--) {
            $temp = $left;
            $left = stringXOR(string: $right,
            intValue: feistelFunction(block: $left, key: $key,
            round: $round));
            $right = $temp;
        }

        $decrypted .= $left . $right;
    }

    return removePadding(data: $decrypted); // Hapus padding
}
```

GAMBAR 14
(HASIL DEKRIPSI BLOWFISH)

2. Integrasi Super Encryption pada CRUD

Integrasi super encryption ke dalam proses CRUD (Create, Read, Update, Delete) berhasil dilakukan. Data yang dienkripsi menggunakan kunci hasil Diffie-Hellman dapat diakses dan ditampilkan kembali melalui proses dekripsi saat dilakukan pembacaan (*read*). Sistem tidak menyimpan kunci secara eksplisit di dalam database, sehingga menambah lapisan keamanan.

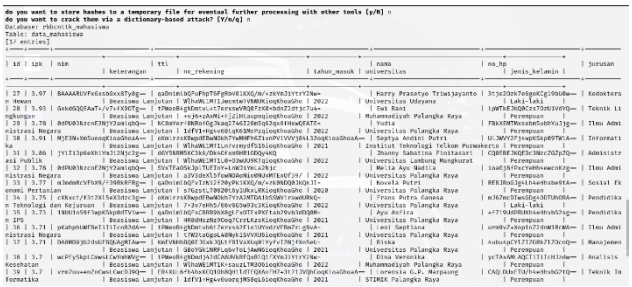


GAMBAR 15
(HASIL ENKRIPSI DATA)

3. Pengujian Sistem terhadap SQL Injection

Pengujian dilakukan menggunakan tools SQLMap dengan teknik *union-based* dan *error-based* SQL Injection. Hasil pengujian menunjukkan bahwa data yang telah dienkripsi tidak dapat dimengerti oleh attacker karena yang berhasil diperoleh hanyalah ciphertext tanpa makna.

GAMBAR 16
(PROSES SQL INJECTION)



GAMBAR 16
(PROSES SQL INJECTION)
GAMBAR 17
(HASIL *SQL INJECTION* PADA TABEL 'DATA_MAHASISWA' 1)

GAMBAR 17
HASIL *SQL INJECTION* PADA TABEL 'DATA_MAHASISWA' 2

V. KESIMPULAN

Integrasi super encryption ke dalam proses CRUD (Create, Read, Update, Delete) berhasil dilakukan. Data yang dienkripsi menggunakan kunci hasil Diffie-Hellman dapat diakses dan ditampilkan kembali melalui proses dekripsi saat dilakukan pembacaan (*read*). Sistem tidak menyimpan kunci secara eksplisit di dalam database, sehingga menambah lapisan keamanan. Proses dekripsi berhasil mengembalikan ciphertext ke bentuk plaintext dengan akurat menggunakan shared key yang sama.

REFERENSI

[1] "Sntik 2015."

[2] Cnn Indonesia, "Data Bpjs Kesehatan Diduga Bocor, Kominfo Turun Tangan," Cnnindonesia.Com, 2021."

[3] W. Andrian And D. P. Kristiadi, "Pengembangan Manajemen Keamanan Informasi Database Dan Aplikasi Dengan Optimasi Keamanan Website," *Jurnal Sistem Informasi Dan Teknologi (S I N T E K)*, 2022, [Online]. Available: Https://Sintek.Stmikku.Ac.Id/Index.Php/Home

[4] A. P. E. Daulay, V. Febriana, A. D. A. Kita, S. Gunawan, And Nurbaiti, "Keamanan Dalam Sistem Database Sebagai Sumber Informasi Manajemen Terhadap Perlindungan Data," 2023.

[5] R. Munir, "Kriptografi Kuliah Pengantar," 2019.

[6] A. Amrulloh And E. Ujianto, "Kriptografi Simetris Menggunakan Algoritma Vigenere Cipher," *Jurnal Coreit*, Vol. 5, No. 2, 2019, [Online]. Available: Https://Program.Arfianhidayat.Com/Kriptografi/Vig

[7] Intech, "Jurnal Ilmiah Intech," 2020.

[8] J. N. Situmoran, E. Nainggolan, A. S. Loi, A. W. Hutablian, A. F. Hutasoit, And J. N. Situmorang, "Security Analysis Of Diffie-Hellman Algorithm In Cryptographic Key Exchange," 2023. [Online]. Available: Https://Jurnal.Seaninstitute.Or.Id/Index.Php/Juti

[9] J. Thakur And N. Kumar, "Des, Aes And Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis," Dec. 2011. [Online]. Available: Www.Tropsoft.Com

[10] S. Khan And S. H. Abbas, "Enhancing Cloud Data Security Using A Hybrid Cryptographic Model: A Combination Of Advanced Encryption Standard And Elliptic Curve Cryptography," 2024. [Online]. Available: Https://Www.Jisem-Journal.Com/

[11] L. B. Handoko And C. Umam, "A Super Encryption Approach For Enhancing Digital Security Using Column Transposition - Hill Cipher For 3d Image Protection," *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, And Control*, Jun. 2024, Doi: 10.22219/Kinetik.V9i3.1984.

[12] N. Yulias And S. R. Widianto, "Prediction Of Drinking Water Facility Conditions Using The Naive Bayes Algorithm," 2021. [Online]. Available: Https://Iocscience.Org/Ejournal/Index.Php/Mantik