Bulletin of Data Science
ISSN 2745-7966 (Media Online)
Vol 3, No 3, June 2024
Hal 243-250
https://ejurnal.seminar-id.com/index.php/bulletinds

Implementasi Teknik Enkripsi Menggunakan Algoritma XXTEA (Corrected Block Tiny Encryption Algorithm) Untuk Penyandian Record Data Pada Database

Cici Rahmadani

Fakultas Ilmu Komputer dan Teknologi Informasi, Program Studi Teknik Informatika, Universitas Budi Darma
Jl. Sisingamangaraja No.338, Siti Rejo I, Kec. Medan Kota, Kota Medan, Sumatera Utara, Indonesia
Email: ciciramadani958@gmail.com

Abstrak− Zaman serba komputer seperti sekarang ini banyak dari sekolah yang masih memberlakukan sistem ujian konvensional atau ujian menggunakan selebaran kepada siswanya tidak sedikit pula dari bapak dan ibu guru tersebut masih membuat kunci jawaban mereka dengan menggunakan kertas atau dimasukkan kedalam file tentu ini akan sangat rentan dari kebocoran dan siapa saja akan dengan mudah mengetahuinya. Melihat dari rentannya kunci jawaban tersebut pihak sekolah atau bapak ibu guru harus bertindak agar tidak ada kejadian yang tidak diinginkan maka dari itu lembaran kunci jawaban yang mudah diketahui tersebut harus segera diamakan dari orang-orang yang tidak bertanggung jawab dengan menggunakan teknik kriptografi. Teknik pengamanan menggunakan kriptografi sangat tepat untuk hal ini, karena kriptografi merupakan ilmu atau seni untuk pengamanan didalam kriptografi terdapat banyak algoritma yang mampu mengubah teks terang menjadi chipertext atau pesan tersandi yang hanya diketahui oleh orang tertentu agar kunci jawaban tidak terbaca dengan mudah oleh orang-orang yang tidak bertanggung jawab.

Kata Kunci: Kriptografi, XXTEA, Record, Kunci Jawaban

Abstract− In this computer era, many schools still implement conventional exam systems or exams using leaflets for their students, not a few of the teachers still make their answer keys using paper or put them in files, of course this will be very vulnerable to leaks and anyone will easily find out. Seeing the vulnerability of the answer key, the school or teachers must act so that there are no unwanted incidents, therefore the answer key sheets that are easy to find out must be immediately secured from irresponsible people by using cryptography techniques. Security techniques using cryptography are very appropriate for this, because cryptography is the science or art of security in cryptography there are many algorithms that can change clear text into ciphertext or encrypted messages that are only known by certain people so that the answer key cannot be easily read by irresponsible people.

Keywords: Cryptography, XXTEA, Record, Answer Key

1. PENDAHULUAN

Teknologi komputer saat ini semakin berkembang hampir di setiap aktivitas masyarakat tidak terlepas dengan yang namanya komputer, didalam komputer terdapat informasi atau data yang tersimpan secara sistematis. Basis data atau didalam bahasa inggris yaitu database mempunyai hubungan yang sangat erat terhadap perangkat komputer salah satu fungsi penting. Database adalah menjaga kerahasiaan data dan informasi melihat dari banyaknya jumlah kejahatan atau ciber yang banyak dibicarakan dimedia massa para pelaku memanfaatkan celah keamanan dalam database untuk dimasuki dan dimanipulasi data-data penting didalamnya[1][2]. Kerahasiaan data dan informasi merupakan hal yang sangat penting bagi beberapa kalangan seperti perusahaan, organisasi, lembaga pendidikan dan lain sebagainya maka dari itu sangat penting untuk menjaga keamanan database agar data penting terjaga keamanan dan kerahasiaannya[3][4].

Pemanfaatan aplikasi komputer dalam suatu perusahaan, organisasi, lembaga pendidikan dan di bidang pekerjaan lainnya sudah menjadi kebutuhan, seperti halnya lembaga pendidikan tidak sedikit dari sekolah yang sudah menerapkan ujian berbasis komputer dan tidak sedikut pula sekolah yang masih menggunakan ujian konvensional (tradional) dimana ujian konvensional guru-guru masih menggunakan lembaran untuk membuat kunci jawabannya dimana ini sangat rentan dari kebocoran. Teknik pengamanan menggunakan enkripsi bisa kurang tepat apabila penggunaannya tidak maksimal teknik pengacakan menjadi chipertext merupakan salah satu teknik yang bisa dilakukan agar informasi di dalamnya tidak dibaca dan dibocorkan oleh penyusup.

Kriptografi adalah disiplin ilmu yang mempelajari bagaimana cara menjaga data atau pesan tetap aman sehingga terhindar dari tindakan kejahatan yang dilakukan kriptanalisis[5][6]. Salah satu algoritma dari kriptografi adalah XXTEA atau corrected block tiny encryption algorithm adalah algoritma sederhana tapi kuat yang diciptakan oleh roger m. Needham dan david j. Wheeler. Pada penelitian yang dilakukan oleh yuricha, tursina, helfi nasution yang menyatakan bahwa algoritma kriptografi xxtea meningkatkan sekuritas pada aplikasi online test dengan di ujikan pada server secara online mengunakan aplikasi yang dipilih. Selain itu ada juga penelitian yang di lakukan oleh khandar wiliam yang memaparkan mengenai tea,xtea, dan turunannya yaitu xxtea serta sejarah perkembangan sehingga menjadikan xxtea sebagai pilihan utama dan yang terbaik. Pada penelitian yang dilakukan oleh kinasih nur azizah dengan menyatakan bahwa implementasi algoritma xxtea pada aplikasi surat elektronik berbasis web berhasil dilakukan dengan cara enkripsi dan dekripsi pada pengiriman dan pengambilan pesan menggunakan algoritma xxtea.

Corrected block tiny encryption algorithm atau xxtea dirancang berupa program kecil yang dapat berjalan pada banyak mesin dan mengekripsi dengan aman. Xxtea merupakan turunan dari block tea dan xtea terdapat ada kelemahan dalam proses dekripsi xtea sehingga xxtea dikeluarkan pada tahun 1998. Pada penelitian yang dilakukan oleh arif rahman dan khoirul dalam mengenkripsi short message servis atau sms memaparkan bahwa algoritma ini dapat dilakukan enkripsi parsing teks serta juga dapat berjalan pada platform android. Penelitian juga di lakukan oleh oris krianto, khairuddin

Bulletin of Data Science
ISSN 2745-7966 (Media Online)
Vol 3, No 3, June 2024
Hal 243-250
https://ejurnal.seminar-id.com/index.php/bulletinds

nasution dan satria yudha menjelaskan bahwa metode xxtea dalam menginplementasikan enkripsi surat elektronik dapat digunakan untuk menyamarkan isi pesan asli yang akan dikirimkan melalui e-mail sehingga menjaga kerahasiaan isi pesan tersebut.

Berdasarkan penjelasan yang sudah dipaparkan diatas maka penulis mengangkat judul tentang "implementasi teknik enkripsi menggunakan algoritma xxtea (corrected block tiny encryption algorithm) untuk penyandian record data pada database".

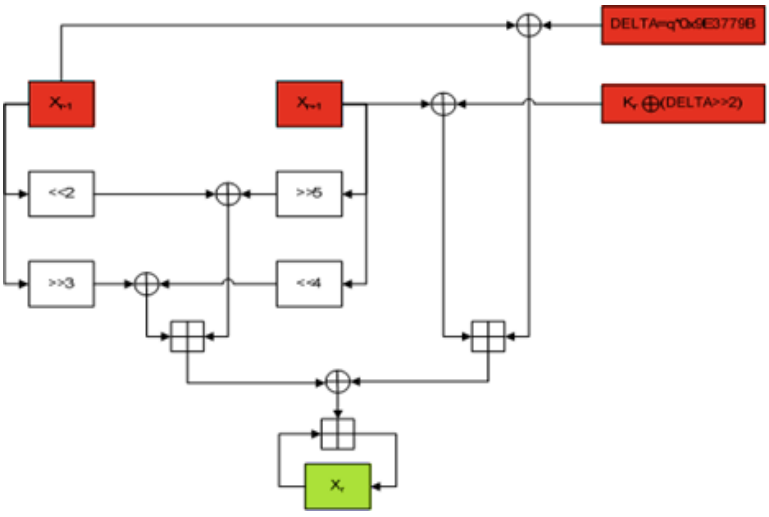
2. METODOLOGI PENELITIAN

2.1 Kriptografi

Kriptografi (cryptography) adalah ilmu dan juga suatu seni yang mempelajari bagaimana menjaga dan menyembunyikan data, pesan atau informasi dengan melakukan penyandian kedalam suatu bentuk sehingga makna aslinya tidak dapat diketahui[7]. Secara etimologis, kata Kriptografi berasal dari bahasa Yunani yang mana terdiri dari dua suku kata yaitu Crypto dan Graphia, kata Crypto yang artinya adalah "rahasia" sedangkan kata Graphia memiliki arti yaitu "tulisan" sehingga kriptografi dapat didefinisikan sebagai tulisan yang bersifat rahasia[8][9][10]. Pengertian lain dari kriptografi ialah ilmu yang mempelajari atau berfokus pada teknik matematika yang berhubungan dengan aspek keamanan informasi, kerahasian, integritas data serta otentikasi begitu pentingnya kriptografi untuk keamanan dan kerahasiaan dari suatu pesan maupun informasi, sehingga kriptografi tidak bisa di pisahkan jika berbicara mengenai keamanan data, pesan, dan informasi dari pengguna komputer[11][12]. Cryptanalysis merupakan sebuah ilmu untuk memecahkan teks bersandi menjadi plaintext serta orang yang memahaminya disebut crypnalyst. dan juga cabang matematika yang meliputi kriptografi dan cryptanalysis disebut cryptology, sedangkan orang yang menguasai ilmu tersebut dinamakan cryptologi[13][14].

2.2 Algoritma XXTEA

Corrected Block Tiny Encryption Algorithm atau yang lebih dikenal algoritma XXTEA. algoritma ini merupakan turunan dari algoritma XTEA dan TEA ketiga algoritma ini tergolong algoritma block chiper karena menggunakan jaringan feistel sebagai dasar dari algoritmanya diciptakan oleh David J Wheeler dan Roger M. Needhem. XXTEA beroperasi pada block panjang variable yang berukuran 32 bit algoritma ini menggunakan lebih banyak fungsi pengacakan yang menggunakan dua blok tetangganya dalam pemrosesan setiap kata dalam blok, berikut akan dijelaskan proses pengacakan yang terjadi pada satu iterasi[15][16][17][18].



Gambar 1. Proses Pengacakan Satu Iterasi

Keterangan Simbol pada gambar:

1. Xr, X_{r-1} ,X_{r+1} : blok *plaintex*t, di mana r adalah urutan blok yang sedang diacak
2. q : jumlah iterasi yang sedang dilakukan.
3. DELTA : q dikalikan dengan konstanta yang bernilai 0x9E3779B
4. Kr : blok kata kunci ke-r dimana r sama dengan keterangan diatas
5. << n : pergeseran bit ke kiri sebanyak n kali.
6. >> n : pergeseran bit ke kanan sebanyak n kali.
7. $\oplus$: operasi XOR
8. $\boxplus$: operasi penambahan

Keterangan warna pada Gambar :

1. Kotak merah : input user.
2. Kotak hijau : output program.

Bulletin of Data Science
ISSN 2745-7966 (Media Online)
Vol 3, No 3, June 2024
Hal 243-250
https://ejurnal.seminar-id.com/index.php/bulletinds

Proses Pengacakan yang dilakukan dalam satu iterasi adalah sebagai berikut:

1. Algoritma XXTEA akan mengacak blok ke – r dari plaintext
2. Proses Pengambilan Xr-1, Xr+1, DELTA dan kata kunci sebagai input
3. Pengacakan pertama yaitu Xr-1 << 2 di- XOR – kan dengan Xr+1 >> 5
4. Proses pengacakan kedua yaitu Xr-1 >>3 di- XOR – kan dengan Xr+1 >> 4
5. Hasil yang didapat dari tahap 3 dan 4 lalu ditambahkan
6. Pengacakan ketiga yaitu Xr-1 di – XOR- kan dengan DELTA yang merupakan perkalian antara konstanta DELTA yang bernilai 0x9e3779b dengan jumlah iterasi pertama yang telah dilakukan
7. Pengacakan ke empat yaitu Xr+1 di –XOR- kan dengan salah satu blok kata kunci ke – r yang sebelumnya telah di – XOR- kan dengan DELTA>>2AND3
8. Hasil yang didapat dari tahap 6 dan 7 ditambahkan
9. Hasil dari tahap 5 dan 8 di XOR kan
10. Hasil yang didapat pada tahap 9 ditamhakan ke blok plaintext ke- r

2.3 Kerangka Kerja Penelitian

Kerangka kerja penelitian merupakan sebuah tahapan-tahapan yang akan dilaksanakan dalam menyelesaikan masalah yang sedang di bahas, yang bertujuan agar proses penelitian sesuai dengan yang diharapkan, dalam pengimplementasiannya penelitian ini menggunakan algoritma XXTEA, Adapun tahapan-tahapan kerangka kerja penelitian yang akan dilakukan adalah sebagai berikut:

Gambar 2. Kerangka Kerja Penelitian

Pada gambar 2 dapat dilihat tahapan penelitian yang akan dilakukan berikut ini adalah penjelasan mengenai dari tahapan tersebut yaitu sebagai berikut:

1. Identifikasi Masalah
   Dapat di definisikan sebagai langkah awal untuk menjelaskan masalah dan membuat penjelasannya terukur
2. Mengumpulkan Data
   Pengumpulan data yang digunakan pada penelitian ini adalah dokumentasi
3. Analisis
   Proses menganalisa enkripsi record untuk di ubah ke bentuk yang tidak bisa di pahami begitu juga pada proses dekripsi
4. Penerapan
   Adalah sebuah proses penerapan dari sebuah teknik yang telah ditentukan

Bulletin of Data Science
ISSN 2745-7966 (Media Online)
Vol 3, No 3, June 2024
Hal 243-250
https://ejurnal.seminar-id.com/index.php/bulletinds

5. Perancangan
   Pada tahap ini terdapat sebuah proses pendefinisian dan perkembangan sistem baru atau sebuah sistem yang akan dibekuk
6. Pengujian
   Proses pengujian yang dilakukan melalui perhitungan dan perancangan dengan aplikasi apakah hasil yang diperolah sesuai dengan maksud dan tujuan penelitian

3. HASIL DAN PEMBAHASAN

3.1 Sampel Data

Sampel data yang digunakan pada penelitian ini berupa database dan sampel record yang diambil dari kolom jawaban, berikut adalah sampel data yang di gunakan:

soal

Soal	Jawaban
1. Yang dimaksud dengan Manajemen keselamatan adalah	C.ISM Code
2. Sifat dan ISM code	C.Wajib
3. Elemen persyaratan ISM Code untuk kapal (Auditee) adalah	A.16 Elemen
4. Elemen persyaratan ISM Code untuk pemeriksaan (Audotor) adala	D.16 Elemen
5. Legalitas ISM Code	B.Solas 1974 Chapter IX
6. Hal penting dalam penerapan ISM Code	B.Buat prosedur tertulis dan laksanakan
7. DOC diberikan kepada	B.Syahbandar
8. SMC diberikan kepada	C.Kapal
9.Yang dimaksud dengan Non Conformity adalah	A.Tidak sesuai dengan persyaratan ISM-Code
10.Yang mengeluarkan sertifikat SMC dan DOC	C.Adpel

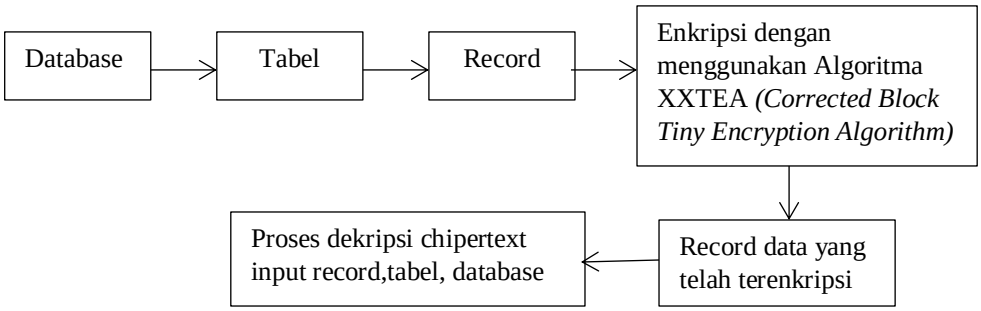
Gambar 3. Sampel Data

Dari banyaknya record yang ada, maka diambil sampel lagi untuk dilakukan proses enkripsi, sampel record yang diambil adalah “B.Syahbandar”.

3.2 Analisa dan Penerapan Metode

Analisa yang dilakukan dalam penelitian ini adalah dengan menerapkan algoritma XXTEA yang digunakan untuk mengenkripsi file database, algoritma ini terbilang sederhana namun kuat. Algoritma XXTEA pada proses enkripsi menggunakan lebih banyak fungsi pengacakan yang menggunakan kedua blok tetangganya dalam pemrosesan setiap kata dalam blok yang sedang diacak begitu juga dengan proses dekripsi yang dilakukan kebalikannya algoritma ini dapat mengenkripsi keseluruhan pesan atau file sekaligus pada implementasinya. Algoritma XXTEA dapat digunakan dengan mode operasi untuk file-file yang berukuran besar serta mampu mengubah sekitar setengah dari plaintext tanpa meninggalkan jejak dan dari mana awal perubahan itu dilakukan.

Pada penelitian ini pengamanan record database dimulai dengan membuka file database yang akan di enkripsikan setelahnya memilih salah satu tabel kemudian dienkripsikan berdasarkan algoritma kriptografi yang telah ditentukan dan menghasilkan record database yang telah berubah dalam bentuk sandi yang tidak dapat dipahami lagi. Pada proses dekripsi terjadi pengaksesan ulang dimana dimulai dengan memanggil database dan dicocokkan pada chiper yang telah tersimpan didalam databasenya.



Gambar 4. Prosedur Enkripsi dan Dekripsi

3.3 Contoh Kasus

Pada contoh kasus ini terdapat 2 (dua) bagian proses yaitu enkripsi dan dekripsi kedua proses tersebut yaitu:

Bulletin of Data Science
ISSN 2745-7966 (Media Online)
Vol 3, No 3, June 2024
Hal 243-250
https://ejurnal.seminar-id.com/index.php/bulletinds

1. Proses Enkripsi
   Analisa proses enkripsi *file database* menggunakan algoritma XXTEA terdapat beberapa tahapan dalam proses ini antara lain iyalah sebagai berikut:
   a. Mencari nilai Karakter
      Sampel data yang digunakan pada contoh kasus disini diambil dari record database kunci jawaban dan juga menggunakan kata kunci untuk dienkripsikan, berikut adalah nilai bit dari karakter tersebut:

Tabel 1. Nilai Desimal Plaintext

Plaintext	B	.	S	y	a	h	b	a	n	d	a	r
Desimal	66	46	83	121	97	104	98	97	110	100	97	114

Pada tabel 1 diatas merupakan tabel nilai ascii kode dari karakter "B.Syahbandar" pada proses pengenkripsiannya terdapat pula kata kunci berikut nilai bit Ascii dari kata kunci tersebut:

Tabel 2. Nilai Desimal Kata Kunci

Kata Kunci	R	A	H	M	A	D	H	A	N	I
Desimal	82	65	72	77	65	68	72	65	78	72

Pada tabel 2 merupakan kode ascii dari karakter kata kunci "RAHMADHANI" yang akan dienkeripsikan langkah awal dengan mengambil nilai binary dari deret kode tersebut, dengan rumus (r+n-1) mod n dan (r+1) mod n, sehingga diperoleh hasilnya yaitu sebagai berikut:

$$X_{r-1} = Binary\ (X(1+11)\ mod\ 24)$$
$$= Binary\ \big(X(12)\big)$$
$$= 01110010$$
$$X_{r+1} = Binary\ (X(1+1)\ mod\ 24)$$
$$= Binary\ \big(X(2)\big)$$
$$= 00101110$$

   b. Setelah diketahui nilai binarynya melalui proses hitungan (r+n-1) mod n dan (r+1) mod n maka selanjutnya dilakukan proses pengacakan yang kedua dengan menghitung Xr-1<<2 XOR Xr+1>>5 yaitu sebagai berikut:

$$Y_1 = X_{r-1} \ll 2\ XOR\ X_{r+1} \gg 5$$
$$= 01011100 \text{ XOR } 10111000$$
$$= 11100100$$

   c. Setelah diketahui hasil dari pengacakan sebelumnya maka selanjutnya akan dilakukan proses pengacakan berikutnya dengan menghitung Xr-1>>3 XOR Xr+1 <<4 yaitu sebagai berikut:

$$Y_2 = X_{r-1} \ll 3\ XOR\ X_{r+1} \gg 4$$
$$= 01001110 \text{ XOR } 11100010$$
$$= 10101100$$

   d. Pada pengacakan yang pertama yaitu Y1 dan pengacakan yang kedua yaitu Y2 telah diketahui hasilnya, maka selanjutnya penambahan dari proses pengacakan tersebut seperti berikut:

$$Z_1 = Y_1 + Y_2$$
$$= 11100100\ XOR\ 10101100$$
$$= 01001000$$

   e. Setelah dikethui hasil dari penambahan dari proses pengacakan sebelumnya lalu selanjutnya menghitung Xr-1 XOR D dimana D bernilai binary dari Delta (0x9E3779B)

$$D = 2654435769$$
$$= 10011110001101110111100110111001$$
$$Y_3 = X_{r-1}\ XOR\ D$$
$$= 01110010\ XOR\ 10011110001101110111100110111001$$
$$= 10011110001101110111100111001011$$

Bulletin of Data Science
ISSN 2745-7966 (Media Online)
Vol 3, No 3, June 2024
Hal 243-250
https://ejurnal.seminar-id.com/index.php/bulletinds

f. Lakukan pengacakan dengan mengitung Xr-1 XOR binary dari K(E) adalah nilai desimal dari D>>2 AND 3 sehingga diperoleh hasil sebagai berikut:

$$E = Desimal\ (D \gg 2\ AND\ 3)$$
$$= (10100111100011011101111001001110\ AND\ 3)$$
$$= Desimal\ (00000010)$$
$$= 2$$
$$Y_4 = X_{r+1}\ XOR\ binary\ \big(K(2)\big)$$
$$= 00101110\ XOR\ Binary\ (65)$$
$$= 01100001\ \text{XOR}\ 01000001$$
$$= 00100000$$

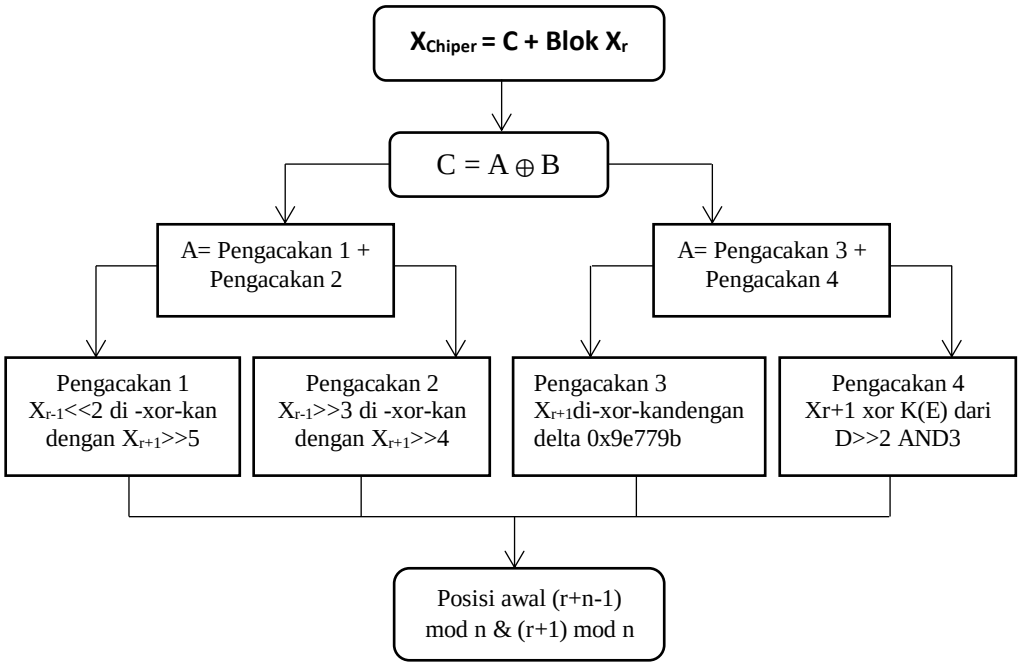
g. Berikutnya dilakukan proses penjumlahan Y3 dan Y4 dari proses sebelumnya sehingga diperoleh hasil sebagai berikut:

$$Z_2 = Y_3 + Y_4$$
$$= 10011110001101110111100111001011\ +\ 00100000$$
$$= 10011110001101110111100111101011$$

h. (Z1 XOR Z2) merupakan perhitungan atau proses terakhir dari pengenkripsian XXTEA hasilnya merupakan chipertext atau pesan yang berhasil di sandikan berikut ini adalah prosesnya

$$C1 = Desimal\ (Z_1\ XOR\ Z_2)$$
$$= Desimal\ (01001000\ \text{XOR}\ 10011110001101110111100111101011)$$
$$= 10011110001101110111100110100011$$
$$= 2654435747$$

2. Proses Deskripsi
Pada algoritma XXTEA dalam proses dekripsi merupakan proses yang sama dengan enkripsi tetapi berbeda dengan proses enkripsi pada proses ini dimulai dari byte terakhir dari deret byte hingga pada posisi yang di awal atau pertama. berikut adalah alur dari dekripsi pada contoh kasus ini.

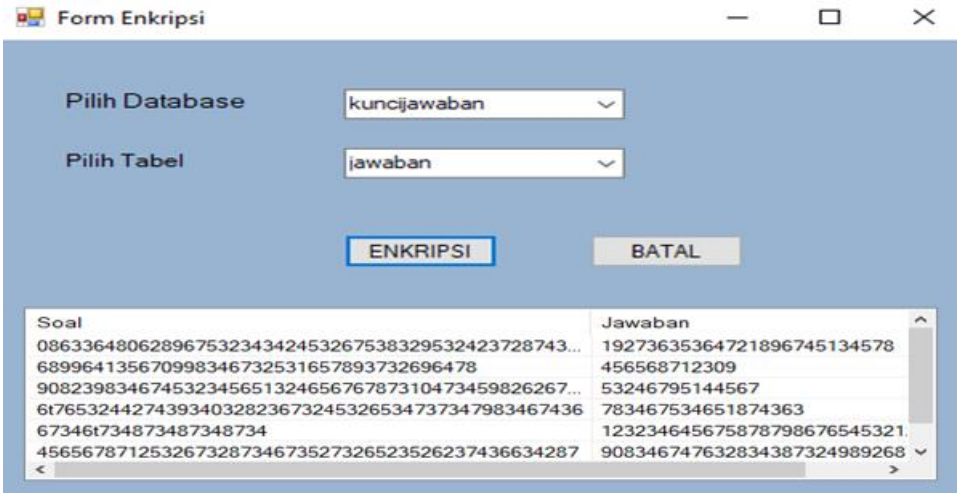


Gambar 5. Alur Proses Dekripsi

3.4 Hasil Pengujian Program

Hasil dari pengujian ini akan meliputi hasil *software* yang dibuat berupa *printscreen*, tampilannya meliputi tentang *form* enkripsi dan dekripsi, berikut adalah tampilan dari *form* enkripsi dan dekripsi tersebut:

1. Form Enkripsi
   Form ini merupakan *form* yang digunakan untuk proses enkripsi dimana harus terlebih dahulu memilih *file database* yang akan dienkripsikan berikut gambar dari proses enkripsi tersebut:



Gambar 6. Tampilan Form Hasil Enkripsi

2. Form Dekripsi
   Form ini merupakan form yang digunakan untuk proses dekripsi yang mengharuskan terlebih dahulu memilih file database yang akan didekripsikan berikut gambar dari proses dekripsi tersebut:

Gambar 7. Tampilan Form Hasil Dekripsi

4. KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan yang telah dilakukan, maka dapat diambil kesimpulan sebagai berikut: prosedur enkripsi *record database* menggunakan algoritma *Corrected Block Tiny Encryption Algorithm* atau XXTEA telah dilakukan dengan menggunakan teknik yang sudah ditentukan. Algoritma XXTEA mampu mengamankan *record* kunci jawaban dengan mengubahnya menjadi *chipertext*. Aplikasi untuk mengenkripsi *file record* telah dirancang menggunakan *Microsoft Visual Studio* 2010.

REFERENCES

[1] H. Zhao *et al.*, "NPASS database update 2023: quantitative natural product activity and species source database for biomedical research," *Nucleic Acids Res*, vol. 51, no. D1, pp. D621–D628, 2023.

[2] Y. Zhou *et al.*, "Therapeutic target database update 2022: facilitating drug discovery with enriched comparative data of targeted agents," *Nucleic Acids Res*, vol. 50, no. D1, pp. D1398–D1407, 2022, doi: 10.1093/nar/gkab953.

[3] K. 'Afiifah, Z. F. Azzahra, and A. D. Anggoro, "Analisis Teknik Entity-Relationship Diagram dalam Perancangan Database Sebuah Literature Review," *INTECH (Informatika dan Teknologi)*, vol. 3, no. 1, pp. 8–11, 2022, doi: 10.54895/intech.v3i1.1261.

[4] E. Setyawati, H. Wijoyo, and N. Soeharmoko, *Relational Database Management System (RDBMS)*. Thesis Commons, 2020. doi: 10.31237/osf.io/wuk6q.

[5] N. W. Hidayatulloh, M. Tahir, H. Amalia, N. A. Basyar, A. F. Prianggara, and M. Yasin, "Mengenal Advance Encryption Standard (AES) sebagai Algoritma Kriptografi dalam Mengamankan Data," *Digital Transformation Technology*, vol. 3, no. 1, pp. 1–10, 2023, doi: 10.47709/digitech.v3i1.2293.

[6] R. Oktafiani, E. I. H. Ujianto, and R. Rianto, "Kombinasi Algoritma Kriptografi Vigenere Cipher dan SHA256 untuk Keamanan Basis Data," *Jurnal Sistem Komputer dan Informatika (JSON)*, vol. 4, no. 3, pp. 433–442, 2023, doi: 10.30865/json.v4i3.5583.

[7] M. Azhari, D. I. Mulyana, F. J. Perwitosari, and F. Ali, "Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES)," *Jurnal Pendidikan Sains dan Komputer*, vol. 2, no. 01, pp. 163–171, 2022, doi: 10.47709/jpsk.v2i01.1390.

[8] K. Andrea, A. Wardana, B. S. Wanandi, and A. Ikhwan, "Penerapan Kriptografi Caesar Cipher Pada Fitur Aplikasi Chatting Whatsapp," *Jurnal Penelitian Dan Pengkajian Ilmiah Eksakta*, vol. 2, no. 1, pp. 6–11, 2023, doi: 10.47233/jppie.v2i1.660.

[9] W. Wahyudi, D. Hartama, I. O. Kirana, S. Sumarno, and I. Gunawan, "Implementasi Algoritma Kriptografi Rivest Shamir Adlemen untuk Mengamankan Data Ijazah pada SMK Swasta Prama Artha Kab. Simalungun," *Jurnal Ilmu Komputer dan Informatika*, vol. 2, no. 1, pp. 57–66, 2022, doi: 10.54082/jiki.19.

[10] A. Ariska and W. Wahyuddin, "Penerapan Kriptografi Menggunakan Algoritma Des (Data Encryption Standard)," *Jurnal Sintaks Logika*, vol. 2, no. 2, pp. 9–19, 2022, doi: 10.31850/jsilog.v2i2.1734.

[11] I. Riadi, A. Fadlil, and F. A. Tsani, "Pengamanan Citra Digital Berbasis Kriptografi Menggunakan Algoritma Vigenere Cipher," *JISKA (Jurnal Informatika Sunan Kalijaga)*, vol. 7, no. 1, pp. 33–45, 2022, doi: 10.14421/jiska.2022.7.1.33-45.

[12] W. R. Maya, A. Azanuddin, and E. Elfitriani, "Implementasi Kriptografi Pengamanan Data Nilai Siswa Menggunakan Algoritma DES," *Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer)*, vol. 21, no. 1, pp. 1–9, 2022, doi: 10.53513/jis.v21i1.4764.

[13] M. Hidayat, M. Tahir, A. Sukriyadi, and A. Sulton, "Penerapan Kriptografi Caesar Chiper dalam Pengamanan Data," *Jurnal Ilmiah Multidisiplin*, vol. 2, no. 03, pp. 35–41, 2023, doi: 10.56127/jukim.v2i03.619.

[14] P. G. Pamungkas and A. H. Muhammad, "Modifikasi Algoritma Kriptografi Caesar Chiper pada Deretan Simbol dan Huruf di Smarphone dan Laptop," *Journal of Information Technology*, vol. 2, no. 1, pp. 1–5, 2022, doi: 10.46229/jifotech.v2i1.234.

[15] E. M. Galas and B. D. Gerardo, "Implementing randomized salt on round key for corrected block tiny encryption algorithm (XXTEA)," in *2019 IEEE 11th International Conference on Communication Software and Networks (ICCSN)*, IEEE, 2019, pp. 795–799. doi: 10.1109/ICCSN.2019.8905270.

[16] H. P. H. Pandiangan, "Implementasi Algoritma Xtea (Extended Tyni Encryption Algoritma) Dalam Pengamanan Data File Dokumen Teks," *Bulletin of Information Technology (BIT)*, vol. 1, no. 3, pp. 122–133, 2020.

[17] N. Anwar, S. Sinurat, and I. Saputra, "Penerapan Algoritma Xtea Dengan Metode Pembangkitan Kunci Linear Congruential Generator Untuk Pengamanan Teks Rahasia," *RESOLUSI: Rekayasa Teknik Informatika dan Informasi*, vol. 2, no. 3, pp. 96–105, 2022, doi: 10.30865/resolusi.v2i3.272.

[18] B. O. Sinaga, S. Sinurat, and T. Zebua, "Modifikasi Algoritma XTEA dengan Pembangkitan Kunci Menggunakan Metode Linear Congruential Untuk Pengamanan File Dokumen," *Journal of Informatics Management and Information Technology*, vol. 1, no. 4, pp. 144–152, 2021, doi: 10.47065/jimat.v1i4.130.