Implementasi Block Cipher Electronic Codebook (ECB) untuk Pengamanan Data Pegawai

Implementation Of Block Cipher Electronic Codebook (ECB) For Employee Data Security

Wahyu Ariandi*[1], Susi Widyastuti[2], Lutfi Haris[3]
[1,2,3] *Program Studi Teknik Informatika, STIKOM Poltek Cirebon*
e-mail: *[1]wahyuariandi@mail.ugm.ac.id, [2]susi.widyastuti@stikompoltek.ac.id,
[3]luthfihazis28@gmail.com

Abstrak

Data pegawai adalah satu data penting dan basic pada PDAM Tirta Sanita Sumber, dimana data ini akan terhubung keberbagai system seperti kenaikkan pangkat, penggajian, pelaporan dan tanggungjawab pekerjaan. Untuk melindungi kerahasiaan data pegawai dari orang-orang yang tidak berhak, maka pengelola system informasi dapat melakukan pengamanan data melalui Teknik kriptografi, pada penelitian ini peneliti menggunakan algoritma Electronic Codebook (ECB) untuk mengamankan data pegawai. Berdasarkan hasil penelitian didapatkan hasil bahwa algoritma ECB mampu melakukan enkripsi dan deskripsi data pegawai pada PDAM Tirta Sanita Sumber dengan baik, sehingga data pegawai dapat terlindungi dari orang-orang yang tidak berhak mengetahui. Melalui hasil uji pada 50 data pengujian, didapatkan ketepatan proses enkripsi dan deskripsi sebesar 96%, hal ini didukung oleh tingkat prosentase kepuasan user terhadap kinerja enkripsi dan dekripsi aplikasi sebesar 82%. Sedangkan dari sisi pengujian fungsionalitas keseluruhan aplikasi secara blackbox didapatkan bahwa aplikasi sudah mampu memenuhi segala kebutuhan fungsionalitasnya dengan prosentase sebesar 100% benar

Kata kunci*—Kriptografi, ECB, Blackbox, data pegawai*

Abstract

One of the most important data in PDAM Tirta Sanita Sumber is employee data. This data will connected and associated with several part of organization system like employee promotion, salary, reporting, and job desk. To keep confidentiality of employee data from people who don't have access right , cryptography can be used for protecting this data. This research used Electronic Codebook (ECB) Algorithm to apply cryptography technique. This research found that ECB Algorithm can encrypt and decrypt employee data of PDAM Tirta Sanita Sumber. From testing process of 50 data, we discovered that this algorithm produced 96% accuracy of encryption and decryption process and 82% customer satisfaction from this algorithm performance. While, from black box testing to conduct test of system functionality, this system can satisfy customer needs with 100% success.

Keywords*—3-5 keywords, Algorithm A, B algorithms, complexity*

PENDAHULUAN

Masalah keamanan merupakan salah satu aspek penting dari suatu sistem, namun sayangnya masalah keamanan ini masih kurang mendapat perhatian khusus dari para pemilik dan pengelola *system* informasi. Saat ini semua pengolahan data pada Perusahaan Daerah Air Minum (PDAM) Tirta Jati Sumber, Kabupaten Cirebon sudah terkomputerisasi dengan baik dan saling berhubungan satu sama lain ke setiap divisinya. Salah satunya adalah *system* kenaikkan pangkat, *system* penggajian, *system* pelaporan dan *system* pelayanan yang semuanya terhubung dengan data pegawai yang ada di *database* perusahaan. Berdasarkan hal tersebut, maka dapat dikatakan bahwa data pegawai merupakan data *basic* dari PDAM Tirta Jati, dan memiliki

Informasi Artikel:
Submitted: Juni 2020, **Accepted:** Juli 2020, **Published:** November 2020
ISSN: 2685-4902 (media online), Website: http://jurnal.umus.ac.id/index.php/intech

peranan yang sangat penting. Dengan mengetahui nama seseorang dari data pegawai, maka orang lain dapat dengan mudahnya mengetahui informasi mengenai jabatan, gaji, tanggungjawab ataupun pekerjaan yang dilakukan oleh pegawai tersebut. Untuk melindungi kerahasiaan data pegawai dari orang-orang yang tidak berhak tersebut, maka pengelola *system* informasi dapat melakukan pengamanan data melalui teknik kriptografi yang akan menyamarkan data asli perusahaan menjadi data-data yang telah terenkripsi[1]. Melihat beberapa analisis permasalahan diatas, maka penelitian ini bertujuan untuk mengetahui penerapan algoritma *Electronic Codebook* (ECB) untuk mengamankan data pegawai pada PDAM Tirta Jati Sumber.

Berbagai teknik pengamanan data yang pernah dilakukan melalui pendekatan kriptografi beberapa diantaranya adalah pada penerapan algoritma *XOR* untuk mengamankan data guru pada sekolahan XYZ[2], algoritma DES yang digunakan untuk mengamankan data karyawan di CV. Sinergi Informasi Global [3], algoritma MD5 utk pengolahan data pada bagian tatausaha Lembaga Sandi Negara [4], algoritma AES untuk pengamanan data gaji karyawan di PT Capella Medan [5], serta kombinasi antara algoritma *caesar chipper* dan *vigenere cipher* untuk mengekripsi dan dekripsi data penggajian di PT. Kemasindo Cepat Nusantara [6]. Kombinasi antara Diffie – Hellman, Message-Digest 5 dan Rivest Chiper 4 juga akan menghasilkan kekuatan yang jauh lebih baik untuk proses enkripsi dan dekripsi[7]. Pengamanan data pesesrta juga pernah dilakukan dengan menggunakan AES[8]

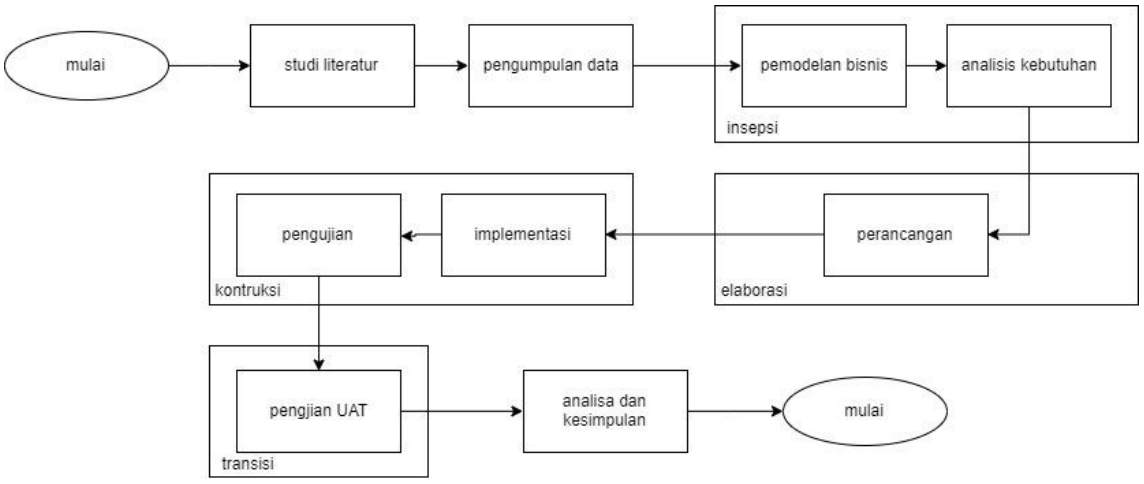
Berbeda dengan beberapa algoritma diatas, pada penelitian ini peneliti menggunakan algoritma *Electronic Codebook* (ECB) untuk mengamankan data pegawai pada PDAM Tirta Jati Sumber, algoritma *Electronic Codebook* (ECB) dipilih karena data pegawai yang akan dienkripsi bersifat acak dan hal ini memungkinkan blok *plaintext* akan dienkripsi secara independen[9]. Beberapa penelitian mengenai penerapan ECB juga pernah dilakukan dengan membandingkan antara waktu enkripsi yang dihasilkan oleh ECB dan CBC pada optimasi *blowfish*, dan hasil penelitiannya menunjukkan bahwa optimasi *blowfish* dengan ECB mampu melakukan enkripsi lebih cepat dari pada CBC[10]. ECB juga pernah dikombinasikan dengan *vigenere chipher* untuk proses pengamanan data, dimana hasilnya dapat lebih bagus tetapi memerlukan waktu yang lebih lama baik dalam mengenkripsi maupun dekripsi plainteks[11].

METODE PENELITIAN

Pada penelitian ini penulis menggunakan pendekatan secara RUP (*Rational Unified Process*) karena mampu memenuhi semua kebutuhan pihak-pihak yang berkepentingan[12]. Pendekatan RUP memiliki 4 fase dalam pendefinisiannya yaitu insepsi (akan menghasilkan analisis kebutuhan), elaborasi (menghasilkan perancangan), konstruksi (implementasi dan *testing system*), transaksi (pengujian)[13].

Penelitian ini akan dimulai dengan studi literatur mengenai berbagai macam algoritma enkripsi yang memiliki kekuatan agar tidak dengan mudah di ketahui, dari tahap studi literatur penulis memutuskan untuk menggunakan ECB sebagai algoritma yang akan digunakan, kemudian akan dilakukan pengumpulan data dimana tahapan ini merupakan mencari data *basic* yang ada di PDAM Tirta Jati Sumber yang akan menjadi fokus enkripsi. Langkah selanjutnya yaitu masuk kedalam proses RUP, pada tahap insepsi peneliti akan menganalisa proses bisnis seperti alur penggunaan data pegawai pada PDAM Tirta Jati akan digunakan untuk proses apa saja, dan hal ini terlihat bahwa data pegawai digunakan pada proses pengolahan data penggajian, kenaikan pangkat, tanggungjawab pekerjaan, dan pelaporan. Semua kebutuhan yang didapatkan pada tahap insepsi selanjutnya digambarkan dalam bentuk *usecase* dan *activity* diagram. Setelah semua kebutuhan *input* didapatkan maka langkah selanjutnya yaitu dilakukan perancangan secara *squance* diagram, GUI, dan penerapan ECB terhadap data pegawai. Pada tahap kontruksi penulis akan mengimplementasikan perancangan menjadi suatu aplikasi kemudian mengujinya melalui *validation testing*. Dan pada tahap akhir RUP akan dilakukan

kembali proses pengujian secara UAT pada tahap transisi. Rangkuman mengenai tahapan yang dilakukan pada RUP tergambar pada Gambar 1.



Gambar 1. Alur RUP pada penelitian

***Electronic Codebook* (ECB)**

Electronic codebook (ECB) merupakan salah satu mode operasi yang setiap karakteristik nilai *plaintext* nya memiliki nilai yang sama seperti *ciphertext*[10]. Secara matematis dapat dinyatakan dengan[14] :

$$C_i = E_k(P_i) \quad (1)$$

$$P_i = D_k(C_i) \quad (2)$$

Adapun proses enkripsinya adalah:
1. Ubah *plaintext* menjadi kode ASCII
2. Ubah hasil no 1 menjadi bentuk bilangan biner 8 bit
3. Ubah *key* dalam bentuk biner
4. Kombinasikan *plaintext* dengan *key*
5. Konversikan dalam bentuk *decimal*
6. Ubah hasil no 5 menjadi *cipertext*

Sedangkan proses untuk dekripsinya adalah
1. Ubah *cipertext* menjadi bilangan biner
2. Ubah bilangan *decimal* menjadi bilangan biner atau *xor* dengan kunci
3. Ubah *xor* biner menjadi bilangan decimal
4. Didapatkan *plaintext*

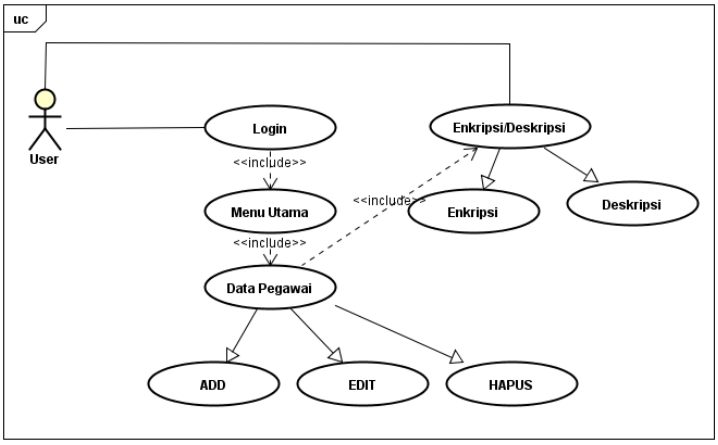
HASIL DAN PEMBAHASAN

Insepsi

Berdasarkan Gambar 1, maka pada tahap insepsi akan didapatkan analisa terhadap kebutuhan yang diperlukan serta pemodelan yang cocok, yang selanjutnya akan digambarkan menjadi *usecase* dan *activity* diagram. Adapun desain prosedur untuk enkripsi dan dekripsi yang dilakukan adalah sebagai berikut:
1. Untuk dapat melakukan enkripsi dan deskripsi data pegawai, user harus melakukan login terlebih dahulu dengan memasukan *username* dan *password* yang sudah tervalidasi.

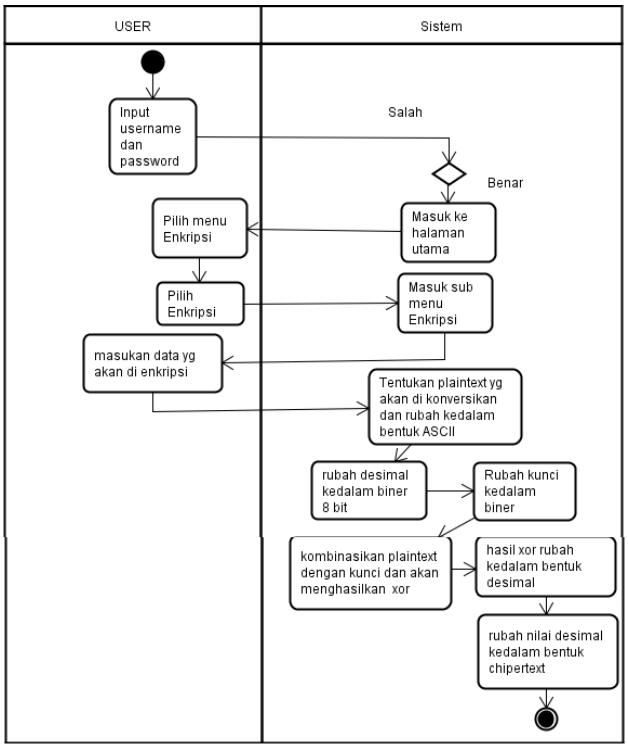
2. Setelah berhasil melakukan login, *user* dapat melakukan enkripsi atau deskripsi file pegawai.
3. Untuk melakukan enkripsi maupun dekripsi user harus mengisi terlebih dahulu data-data pegawai kedalam aplikasi.
4. Kemudian data akan di enkripsi dan deskripsi oleh database ke dalam aplikasi.
5. Setelah data terenkripsi dan terdeskripsi data akan tersimpan kedalam database.

Gambaran mengenai *usecase* diagram dan *activity* diagram tersebut terlihat pada Gambar 1 dan 2.



Gambar 1. Usecase diagram

Actor yang terlibat pada aplikasi adalah para pegawai yang login keaplikasi, dimana pegawai ini hanya dapat melakukan perubahan ataupun penghapusan data dirinya. Untuk *activity* diagram yang terbentuk berdasarkan Gambar 1 adalah 6 buah *activity* diagram diantaranya adalah *activity* login, *activity* menu input, *activity* menu edit, *activity* menu hapus, *activity* enkripsi, *activity* deskripsi. Gambar 2 merupakan *activity* diagram untuk enkripsi yang dilakukan oleh aplikasi.



Gambar 2. Activity diagram enkripsi

Elaborasi

Pada penelitian ini, penulis akan menggunakan data pegawai sebagai fokus enkripsi dan dekripsi kerahasiaan data yang akan dilakukan. Pada tahapan ini akan dilakukan penerapan algoritma ECB terhadap data pegawai seperti berikut:

Enkripsi Block Chipper

Sedangkan untuk prosedur enkripsi *block chipper* yang dilakukan adalah sebagai berikut:

1. Langkah pertama pada tahap ini mengubah pesan atau *plaintext* di konversikan dengan cara konversi menggunakan kode ASCII. Tabel 1 adalah bentuk konversi *plaintext* LUTFI kedalam kode ASCII.

Table 1. Konversi plaintext kedalam ASCII

Plaintext	L	U	T	F	I
Desimal	76	85	84	70	73

2. Setelah mendapatkan hasil bilangan *decimal* dari plainteks selanjutnya akan mengubah bilangan ke *decimal* kedalam bentuk biner 8 bit dengan cara:
   a. Buatlah deret bilangan 2 pangkat yang dimulai dari 2^0. Penulisan dimulai dari sebelah kanan. Batas bilangan harus kurang dari atau sama dengan (<=) nilai ASCII. Pada nilai 76 berarti kita menuliskan $2^6\ 2^5\quad 2^4\ 2^3\ 2^2\ 2^1\ 2^0$. Sehingga kalau kita tuliskan jumlah perpangkatannya, akan kita temukan bilangan, Sehingga kalau kita tuliskan jumlah perpangkatannya, akan kita temukan bilangan 64, 32, 16, 8, 4, 2, 1
   b. Kemudian kurangi 76 dengan 64. Karena 76 bisa dikurangi dengan 64 maka kita tuliskan 1. 76 – 64 = 12. Kemudian hasil 12 dikurangkan dengan 32. Karena 12 tidak bisa dikurangi dengan 32, maka kita tuliskan 0. Kemudian 9 – 16. Dan karena tidak bisa lagi kita tuliskan 0. Dan begitulah seterusnya sampai 1 sehingga dari nilai 76 akan terbentuk bilangan 1001100. Karena hanya ada 7 bilangan maka kita tambahkan 0 di depan menjadi 01001100. Sehingga kita sudah menemukan biner 8 bit dari L. Lakukan hal yang sama untuk mencari binner 8 bit dari teks selanjutnya UTFI. Hasil perubahan ini terdapat pada Tabel 2.

Table 2. konversi ASCII kedalam biner 8 bit

ASCII	76	85	84	70	73
Biner 8 bit	01001100	01010101	01010100	01000110	01001001

3. Pada tahap ini melakukan perubahan *key* atau kunci kedalam bentuk biner. Kunci yang akan digunakan adalah YOxKa, hasil perubahan key menjadi biner terdapat pada Tabel 3.

Table 3. Konversi key menjadi biner

Kunci	Y	O	x	K	a
Biner	01111001	01101111	01111000	01101011	01100001

4. Langkah selanjutnya pada tahap ini dilakukan kombinasi Antara *plaintext* dengan kunci. Hasil kombinasi antara *plaintext* dengan *key* terdapat pada Tabel 4

Table 4. Hasil kombinasi plaintext dengan kunci

Plaintext	01001100	01001100	01010100	01000110	01001001
Key	01111001	01101111	01111000	01101011	01100001
XOR	00110101	00100011	00101100	00101101	00101000

5. Tahap kelima pada tahap ini hasil yang sudah di dapat di konversikan kedalam bentuk desimal. Table 5 merupakan hasil konversi poin 4 menjadi desimal.

Table 5. Hasil konversi XOR ke desimal

XOR	00110101	00100011	00101100	00101101	00101000
Decimal	53	58	44	45	40

6. Tahap terakhir ubah nilai decimal kedalam *chipertext*. Hasil perubahan *decimal* kedalam *chipertext* terdapat pada Tabel 6.

Table 6. Hasil konversi decimal menjadi chipertext

Decimal	53	58	44	45	40
Chipertext	5	:	,	-	(

Prosedur *Deskripsi Block Cipher* Mode ECB

1. Langkah pertama proses deskripsi, pada tahap ini hasil yang sudah di dapatkan *chipertext* lalu di konversikan kedalam biner. Hasil konversi ini terdapat pada Tabel 7.

Table 7. Konversi chipertext kedalam biner

CHIPERTEXT	5	:	,	-	(
Decimal	53	58	44	45	40

2. Langkah selanjutnya ubah bilangan *decimal* menjadi bilangan biner dan xor dengan kunci. Hasil konversi ini terdapat pada Tabel 8.

Tabel 8. Hasil konversi chipertext dengan kunci

Chipertext	00110101	00111010	00101100	00101101	00101000
Kunci	01111001	01101111	01111000	01101011	01100001
Xor	01001100	01010101	01010100	01000110	01001001

3. Ubah hasil xor biner menjadi bilangan decimal. Hasil konversi xor menjadi decimal terdapat pada Tabel 9.

Table 9. Hasil konversi chipertext ke desimal

Chipertext biner	01001100	01010101	01010100	01000110	01001001
Desimal	76	85	84	70	73

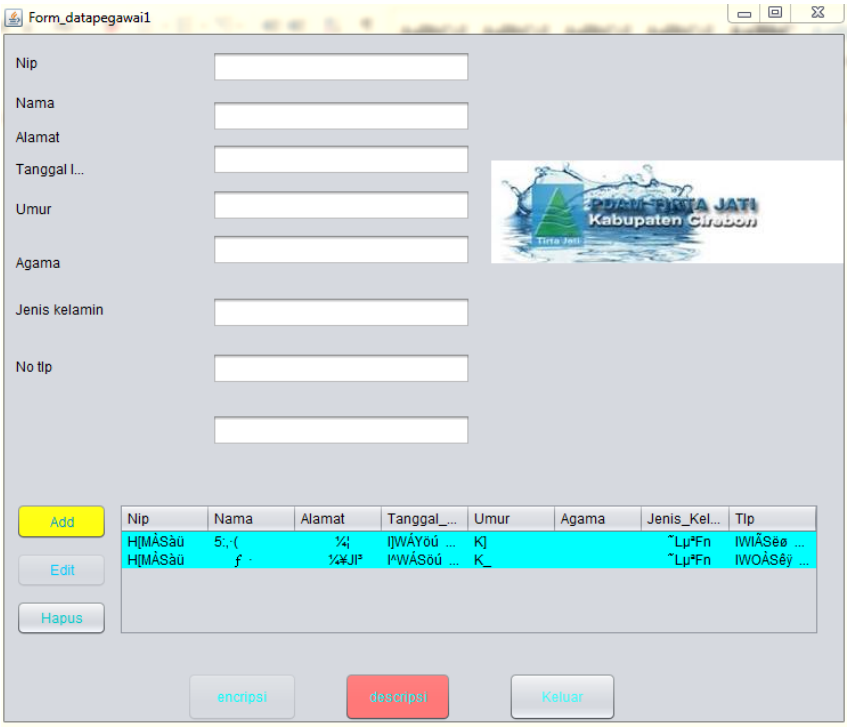
4. Tahap terakhir sudah menjadi karakter. Hasilnya adalah pada Tabel 10.

Table 10. Hasil dekripsi

L	U	T	F	I

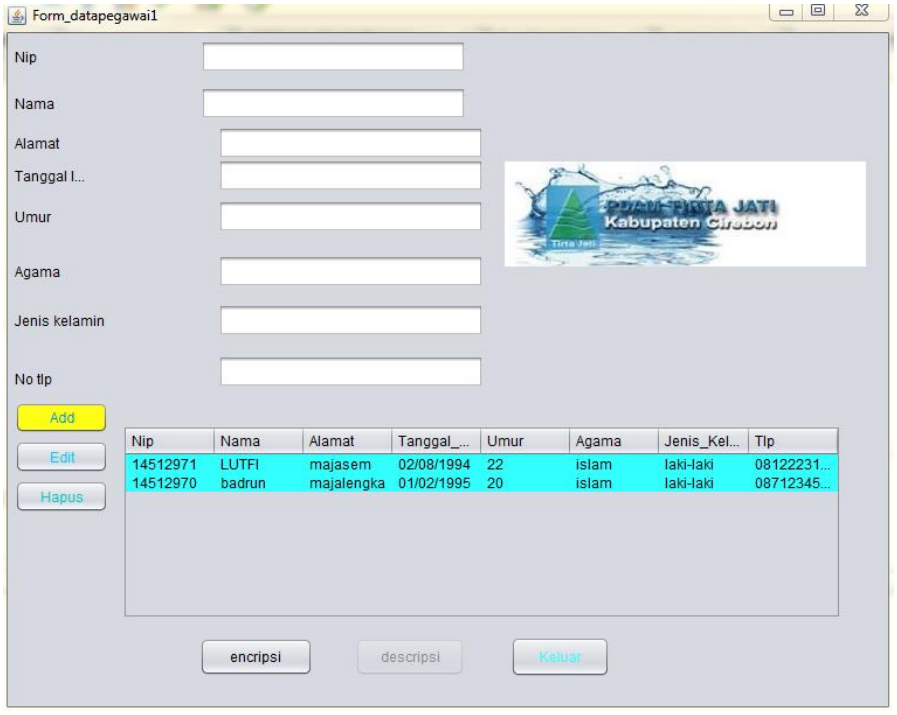
Konstruksi

Pada tahap ini akan dilakukan pengimplementasian perancangan algoritma ECB menjadi suatu aplikasi. Gambar 3 dan 4 merupakan tampilan untuk enkripsi dan dekripsi yang dihasilkan.



Gambar 2. Tampilan Menu Utama Deskripsi

Berdasarkan Gambar 2 *button* enkripsi berfungsi untuk mengenkripsi data, untuk mengenkripsi data pilih *button* enkripsi maka data pada database akan otomatis terenkripsi data tidak dapat diedit. Sedangkan pada Gambar 3 *button* deskripsi untuk mengdeskripsi data, untuk mengdeskripsi data pilih button deskripsi maka data pada database akan otomatis terdeskripsi dan button deskripsi akan di non aktifkan.



Gambar 3. Tampilan Menu Utama Deskripsi

Aplikasi yang dibangun memiliki 6 form yaitu form login, tambah data pegawai, edit data pegawai, hapus data pegawai, enkripsi, deskripsi. Untuk memastikan bahwa semua form tersebut sudah bekerja dengan baik sesuai fungsionalitasnya maka akan dilakukan pengujian menggunakan *blackbox*. Hasil pengujian tersebut terangkum pada Tabel 11.

Table 11. Hasil pengujian *blackbox*

No	Jenis Pengujian	Deskripsi	Hasil Yang Diharapkan	Hasil pengamatan	Kesimpulan
1	Form login	*User* memasukkan *username* dan *password* benar	Pengecekkan kedalam database, dan *system* berhasil membawa *user* ke halaman pegawai	Database berhasil mengenali *username* dan *password* dan membawa user kehalaman pegawai	Sesuai
2	Form login	*User* memasukkan *username* dan *password* salah	Pengecekkan kedalam database, dan *system* akan menolah *username* yang dimasukkan	Database berhasil tidak mengenali *username* dan *password* dan menampilkan pesan	Sesuai
3	Edit data pegawai	*User* memasukkan data nama pegawai yang akan diedit	Aplikasi akan mengecek ejaan nama pegawai yang diedit jika huruf semua maka data akan disimpan dalam *table*	Aplikasi berhasil menyimpan data pegawai yang namanya dirubah	Sesuai
4	Edit data pegawai	*User* memasukkan data nama pegawai dengan kombinasi huruf dan angka	Aplikasi akan menampilkan pesan bahwa nama pegawai tidak boleh kombinasi antara huruf dan angka	Aplikasi menampilkan pesan	Sesuai
5	Hapus data pegawai	*User* akan menghapus salah satu nama pegawai berdasarkan id / nama pegawai tersebut	Aplikasi akan menampilkan pesan dan jika *user* mengklik *button* hapus maka data akan terhapus dari *table*	Aplikasi berhasil menampilkan pesan konfirmasi dan data terhapus dari table	Sesuai
6	Enkripsi	*User* akan mengklik button enkripsi data pegawai yang akan diamankan	Aplikasi akan melakukan enkripsi dan menampilkan hasil enkripsinya pada gridview	Aplikasi menampilkan hasil enkripsi pada *gridview*	Sesuai
7	Dekripsi	*User* akan mengklik *button* deskripsi data pegawai yang akan diamankan	Aplikasi akan melakukan deskripsi dan menampilkan hasil dekripsinya pada *text field* pegawai	Aplikasi menampilkan hasil deskripsi pada *textfiled*	Sesuai

Sedangkan untuk tingkat kesalahan dari 50 uji coba data pegawai didapatkan hasil bahwa:

$$hasil\ pengujian = \frac{jumlah\ benar}{jumlah\ data}\ x\ 100\%$$

$$hasil\ pengujian = \frac{48}{50}\ x\ 100\%$$

$$hasil\ pengujian = 96\%$$

Transisi

Pada tahap pengujian UAT, penulis akan menyediakan jawaban terhadap pertanyaan-pertanyaan yang akan dijawab oleh responden, rangkuman mengenai jawaban tersebut terangkum pada Tabel 12.

Tabel 12. Pilihan jawaban

Nilai	Keterangan
A	Sangat : mudah / bagus / sesuai / jelas
B	Mudah / bagus / sesuai / jelas
C	Netral
D	Cukup : sulit / bagus / sesuai / jelas
E	Sangat : sulit / jelek / tidak sesuai / tidak jelas

Sedangkan untuk bobot dari masing-masing jawaban yang akan dijawab terangkum pada Tabel 13.

Table 13. Bobot jawaban

Jawaban	Bobot
A: Sangat : mudah / bagus / sesuai / jelas	5
B: Mudah / bagus / sesuai / jelas	4
C: Netral	3
D: Cukup : sulit / bagus / sesuai / jelas	2
E: Sangat : sulit / jelek / tidak sesuai / tidak jelas	1

Sedangkan daftar pertanyaan dan hasil respon *user* untuk pertanyaan-pertanyaan yang diajukan terangkum pada Tabel 14.

Tabel 14. Hasil respon user

No	Pertanyaan	Nilai				Jumlah
		A	B	C	D	
1	apakah tampilan dari aplikasi ini mudah dipahami?	40	24	6	2	72
2	apakah kombinasi warna pada aplikasi sudah sesuai?	2	0	20	15	37
3	apakah tombol-tombol pada aplikasi ini mudah dipahami	35	22	12	0	69
4	apakah hasil enkripsi membantu mengamankan data	40	20	10	1	71
5	apakah hasil dekripsi sama dengan plaintext	40	20	0	0	60

Berdasarkan Tabel 14, diketahui bahwa untuk pertanyaan pertama *prosentase* kepuasan user dari tampilan aplikasi masih rendah yaitu hanyalah 71%, pengaturan warna dan tataletak tombol juga juga sekitar 72%, namun *user* merasa puas terhadap proses enrkipsi dan dekripsi data yang dilakukan oleh aplikasi yaitu yang mencapai 82%.

KESIMPULAN

Berdasarkan hasil penelitian didapatkan hasil bahwa algoritma ECB mampu melakukan enkripsi dan deskripsi data pegawai pada PDAM Tirta Sanita Sumber dengan baik, sehingga data pegawai dapat terlindungi dari orang-orang yang tidak berhak mengetahui. Melalui hasil uji pada 50 data pengujian, didapatkan ketepatan proses enkripsi dan deskripsi sebesar 96%, hal ini didukung oleh tingkat prosentase kepuasan user terhadap kinerja enkripsi dan dekripsi aplikasi sebesar 82%. Sedangkan dari sisi pengujian fungsionalitas keseluruhan aplikasi secara *blackbox*

didapatkan bahwa aplikasi sudah mampu memenuhi segala kebutuhan fungsionalitasnya dengan prosentase sebesar 100% benar.

DAFTAR PUSTAKA

[1] 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)*, vol. 2, no. 2, pp. 146–151, 2018, doi: 10.30743/infotekjar.v2i2.300.

[2] A. A and D. Dasril, "Perancangan Aplikasi Pengamanan Data Menggunakan Algoritma XOR," *J. IT*, vol. 8, no. 1, pp. 61–69, 2017.

[3] S. Hanadwiputra, "Implementasi Enkripsi Dalam Pengamanan File Data Karyawan Dengan Metode Algoritma DES (Data Encryption Standard) Pada CV. Sinergi Informasi Global," *J. Gema Kampus*, vol. 13, no. 2, pp. 61–69, 2018.

[4] N. KUSTIAN, "Sistem Informasi Pengamanan Basis Data Menggunakan Teknik Enkripsi Bagian Tata Usaha Lembaga Sandi Negara," *Fakt. Exacta*, vol. 7, no. 2, pp. 188–199, 2015, doi: 10.30998/FAKTOREXACTA.V7I2.259.

[5] J. Prayudha, S. Saniman, and I. Ishak, "Implementasi Keamanan Data Gaji Karyawan Pada PT . Capella Medan Menggunakan Metode Advanced Encryption Standard (AES)," *Sains dan Komput.*, vol. 18, no. 2, 2019.

[6] I. A. Susanto and A. Solichin, "Enkripsi Data Penggajian Dengan Algoritma Caesar Cipher dan Vigenere Cipher Pada PT. Kemasindo Cepet Nusantara," *Skainika*, vol. 1, no. 1, pp. 399–404, 2018.

[7] S. F. Rodiasyah, T. Wahyuni, and D. Sukmana, "Kombinasi Kriptografi Diffie-Hillman, Message-Digest 5 dan Rivest Chiper 4," *J. Ilm. Intech Informatioan Technol. J. UMUS*, vol. 2, no. 01, pp. 1–10, 2020, doi: https://doi.org/10.46772/intech.v2i01.180.

[8] S. Widyastuti, W. Ariandi, and V. Sulistiono, "Implementasi Kriptograsi Aes Dalam Pengamanan Data Seleksi Peserta Jamkesmas," *J. Ilm. Intech Informatioan Technol. J. UMUS*, vol. 1, no. 02, 2019, doi: https://doi.org/10.46772/intech.v1i02.66.

[9] A. P. Sidik and N. Mayasari, "Rancangan Model Algoritma Hybrid Teknik Enkripsi Xor Dengan Kombinasi Mode Block Cipher CBC - ECB 512 Bits dan Algoritme RSA," *J. Tek. dan Inform.*, vol. 6, no. 2, 2019.

[10] I. A. W. Arnawa, P. E. W. C, and A. A. G. B. Putra, "Perbandingan Waktu Enkripsi Antara Metode Electronic Codebook (ECB) dan Chipher Block Chaining (CBC) Dalam Algoritma Blowfish," *J. Ilmu Komput. Indones.*, vol. 5, no. 1, pp. 50–54, 2020, doi: https://doi.org/10.23887/jik.v5i1.3056.

[11] A. Widarma, H. F. Siregar, and M. D. Irawan, "Teknik Keamanan Data Menggunakan Vigenere Cipher Dan Electronic Code Book (ECB)," *J-SAKTI (Jurnal Sains Komput. dan Inform.*, vol. 3, no. 2, p. 393, 2019, doi: 10.30645/j-sakti.v3i2.157.

[12] D. J. Hutahaean, N. H. Wardani, and W. Purnomo, "Pengembangan Sistem Informasi Penyewaan Gedung Berbasis Web dengan Metode Rational Unified Process (RUP) (Studi Kasus: Wisma Rata Medan)," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 3, no. Vol. 3, No. 6, Juni, pp. 5789–5798, 2019.

[13] F. Mubarok, H. Harliana, and I. Hadijah, "Perbandingan Antara Metode RUP dan Prototype Dalam Aplikasi Penerimaan Siswa Baru Berbasis Web," *Creat. Inf. Technol. J. (CITEC JOURNAL)*, vol. 2, no. 2, pp. 114–127, 2015, doi: https://doi.org/10.24076/citec.2015v2i2.42.

[14] F. Zuli and A. Irawan, "Implementasi Kriptografi Dengan Algoritma Blowfish Dan Riverst Shamir Adleman (Rsa) Untuk Proteksi File," *J. Ilm. FIFO*, vol. 9, no. 1, p. 5, 2017, doi: 10.22441/fifo.v9i1.1437.