

Sistem Keamanan Dokumen Data Pegawai pada PT. Nirwana Anugerah Lestari Menggunakan Metode RC4 dengan Cloud Firestore Berbasis Android

Employee Data Document Security System at PT. Nirwana Anugerah Lestari Using the RC4 Method with Android-Based Cloud Firestore

Nico Syahputra¹, Ria Eka Sari²

^aProgram Studi Informatika Universitas Potensi Utama, Jl.K.L Yos Sudarso KM 6.5 Tj.Mulia, Medan, 20241, Indonesia

^bProgram Studi Informatika Universitas Potensi Utama, Jl.K.L Yos Sudarso KM 6.5 Tj.Mulia, Medan, 20241, Indonesia

E-mail: syahputranico92@gmail.com¹, ladiespure@gmail.com²

ABSTRAK

Keamanan data merupakan aspek penting dalam pengelolaan dokumen digital, terutama pada sistem yang menyimpan informasi sensitif seperti data pegawai. PT. Nirwana Anugerah Lestari membutuhkan sistem yang mampu menjaga kerahasiaan dan integritas dokumen pegawai dari potensi akses tidak sah. Penelitian ini bertujuan untuk membangun sistem keamanan dokumen data pegawai berbasis aplikasi Android dengan menerapkan algoritma kriptografi RC4 serta penyimpanan cloud menggunakan Cloud Firestore. Metode RC4 digunakan untuk mengenkripsi dan mendekripsi dokumen, sehingga hanya pengguna yang memiliki kunci yang tepat yang dapat mengakses data. Cloud Firestore dipilih karena kemampuannya dalam menyediakan penyimpanan real-time dan aman. Hasil pengujian menunjukkan bahwa sistem mampu mengenkripsi dan menyimpan dokumen dengan aman, serta dapat mendekripsi data dengan cepat dan tepat saat dibutuhkan. Dengan penerapan metode ini, diharapkan keamanan data pegawai di PT. Nirwana Anugerah Lestari dapat ditingkatkan secara signifikan.

Kata Kunci : Keamanan data, RC4, Cloud Firestore, Android, enkripsi dokumen.

ABSTRACT

Data security is a critical aspect of managing digital documents, especially in systems that store sensitive information such as employee data. PT. Nirwana Anugerah Lestari requires a system capable of safeguarding the confidentiality and integrity of employee documents from unauthorized access. This study aims to develop a document security system for employee data through an Android-based application by implementing the RC4 cryptographic algorithm and cloud storage using Cloud Firestore. RC4 is used to encrypt and decrypt documents, ensuring that only users with the correct key can access the data. Cloud Firestore is chosen for its ability to provide secure and real-time storage. The test results show that the system successfully encrypts and stores documents securely, and can decrypt data quickly and accurately when needed. The implementation of this method is expected to significantly enhance the security of employee data at PT. Nirwana Anugerah Lestari.

Keywords : Data security, RC4, Cloud Firestore, Android, document encryption

Disubmit:

Direview:

Diterima :

Copyright © 2025 - Journal UPU. All rights reserved.

1. PENDAHULUAN

Di era digital yang semakin berkembang pesat, kebutuhan akan sistem pengelolaan data yang cepat, akurat, dan aman menjadi sangat penting, khususnya dalam lingkungan perusahaan. PT. Nirwana Anugerah Lestari merupakan salah satu perusahaan yang bergerak dalam bidang biro jasa. PT. Nirwana Anugerah Lestari sebagai salah satu perusahaan yang terus berkembang di bidangnya, memiliki berbagai data penting dan sensitif, terutama terkait data pegawai. Informasi seperti identitas pribadi, riwayat pekerjaan, serta dokumen administrasi lainnya perlu dikelola secara efisien dan dilindungi dari risiko kebocoran, manipulasi, ataupun akses tidak sah [1].

Saat ini, sebagian besar perusahaan sudah mulai beralih ke sistem berbasis digital untuk menyimpan dan mengelola data karyawan. Namun, tidak semua sistem memiliki mekanisme keamanan yang memadai. Banyak sistem yang hanya fokus pada kemudahan akses tanpa memperhatikan aspek kerahasiaan dan integritas data. Hal ini menjadi celah yang berpotensi dimanfaatkan oleh pihak yang tidak bertanggung jawab. Oleh karena itu, pengembangan sistem keamanan data yang andal sangat diperlukan, terlebih jika data disimpan di cloud atau diakses melalui perangkat mobile seperti Android [2].

Salah satu pendekatan dalam meningkatkan keamanan data adalah dengan menerapkan algoritma kriptografi. Algoritma RC4 (Rivest Cipher 4) merupakan salah satu algoritma stream cipher yang cukup ringan dan cepat dalam proses enkripsi maupun dekripsi [3]. Meskipun ada berbagai algoritma enkripsi yang lebih kompleks, RC4 tetap relevan untuk sistem yang memerlukan proses enkripsi real-time dengan keterbatasan resource seperti pada aplikasi mobile [4].

Algoritma dari metode RC4 *stream cipher* ini terdiri dari dua bagian, yaitu: *key setup* dan *stream generation*. Pada *key setup* terdapat tiga tahapan proses di dalamnya, yaitu Inisialisasi S-Box, menyimpan *key* dalam *key byte array*, dan permutasi pada S-Box [5]. Pada *stream generation* akan menghasilkan nilai *pseudorandom* yang akan dikenakan operasi XOR untuk menghasilkan *ciphertext* ataupun sebaliknya yaitu menghasilkan *plaintext* [6]. Penerapan metode RC4 dapat mengamankan data pegawai dengan baik dengan menggunakan aplikasi berbasis android. Pihak PT. Nirwana Anugerah Lestari akan lebih mudah menjaga kerahasiaan data pegawai dan pembuatan laporan pegawai.

Selain itu, penggunaan *Cloud Firestore* sebagai media penyimpanan berbasis cloud menawarkan fleksibilitas tinggi, skalabilitas, dan kemampuan sinkronisasi data secara real-time [7]. Dengan integrasi antara *Cloud Firestore* dan platform Android, sistem dapat diakses secara mobile dengan tetap menjaga performa dan efisiensi [8]. Namun demikian, *Cloud Firestore* sendiri belum memberikan lapisan enkripsi data end-to-end secara default, sehingga dibutuhkan sistem tambahan untuk mengenkripsi data sebelum disimpan ke cloud.

Melihat kebutuhan tersebut, maka dibutuhkan sebuah sistem keamanan dokumen data pegawai yang tidak hanya menyediakan kemudahan akses dan manajemen data, tetapi juga mampu melindungi kerahasiaan data dengan menerapkan metode enkripsi RC4 sebelum data disimpan ke *Cloud Firestore*. Sistem ini dirancang berbasis Android agar dapat memberikan kemudahan bagi admin atau pihak yang berwenang dalam mengelola data kapan pun dan di mana pun dengan perangkat mobile [9].

Dengan adanya penelitian ini, diharapkan dapat membantu PT. Nirwana Anugerah Lestari dalam meningkatkan keamanan dan efisiensi pengelolaan data pegawai, serta menjadi solusi inovatif dalam perlindungan data pada sistem berbasis mobile dan cloud.

Penelitian lain yang dilakukan oleh [10] Dengan menerapkan RC4, perusahaan dapat memastikan bahwa data yang dikirimkan antara perangkat mereka terlindungi dan tidak dapat diakses oleh pihak yang tidak berwenang. Berdasarkan penelitian dan pengujian program, aplikasi ini berhasil mengatasi kebocoran, pencurian dan perubahan dokumen penting pada perusahaan dengan memanfaatkan enkripsi dan dekripsi metode RC 4

Penelitian lain yang dilakukan oleh [11] Dalam perancangannya aplikasi akan dibuat menggunakan teknik dengan cara proses enkripsi. Aplikasi ini diimplementasikan dengan menggunakan bahasa pemrograman PHP.

Pada aplikasi ini, data yang dienkripsi hanya berupa dokumen perusahaan yang bersifat rahasia dan hanya orang tertentu pada perusahaan tersebut yang dapat mengakses aplikasi ini [12]. Penelitian lain yang dilakukan oleh [13] Kriptografi merupakan seni dan ilmu untuk memproteksi pengiriman data dengan mengubahnya menjadi kode tertentu dan hanya ditujukan untuk orang yang mempunyai kunci untuk mengubah kode itu Kembali yang berfungsi untuk menjaga kerahasiaan data atau pesan. Algoritma RC4 adalah algoritma yang membangkitkan keystream yang kemudian di-XOR-kan dengan plaintext pada waktu enkripsi atau di-XOR-kan dengan bit-bit ciphertext pada waktu dekripsi. Hasil penelitian, aplikasi ini dapat mengamankan database yang berisikan data pasien dan file penting [14].

Penelitian lain yang dilakukan oleh [15] Dengan aplikasi kriptografi dengan menggunakan metode RC4 dan BASE64 ini diharapkan informasi data yang disimpan kedalam aplikasi sekolah SDN

Grogol Utara 10 akan aman dan tidak bocor kepada penyadap ataupun pihak yang tidak bertanggung jawab. Pada aplikasi ini, informasi yang di enkripsi adalah data siswa, data guru, mata pelajaran dan nilai. Berdasarkan implementasi ataupun pengujian program, dapat disimpulkan bahwa aplikasi ini mudah digunakan dan juga dapat melindungi kerahasiaan data ataupun informasi. Serta bermanfaat untuk guru sekolah SDN Grogol Utara 10 dalam menjalankan tugas pokok dan fungsi.

2. METODE

Pada tahap ini dilakukan dengan mempelajari teori dasar yang mendukung penelitian, pencarian dan pengumpulan data-data yang dibutuhkan. Untuk mengumpulkan data yang dibutuhkan, maka penulis menggunakan beberapa teknik.

A. Penelitian Lapangan

Pada proses penelitian ini penulis melakukan penelitian lapangan dengan proses sebagai berikut :

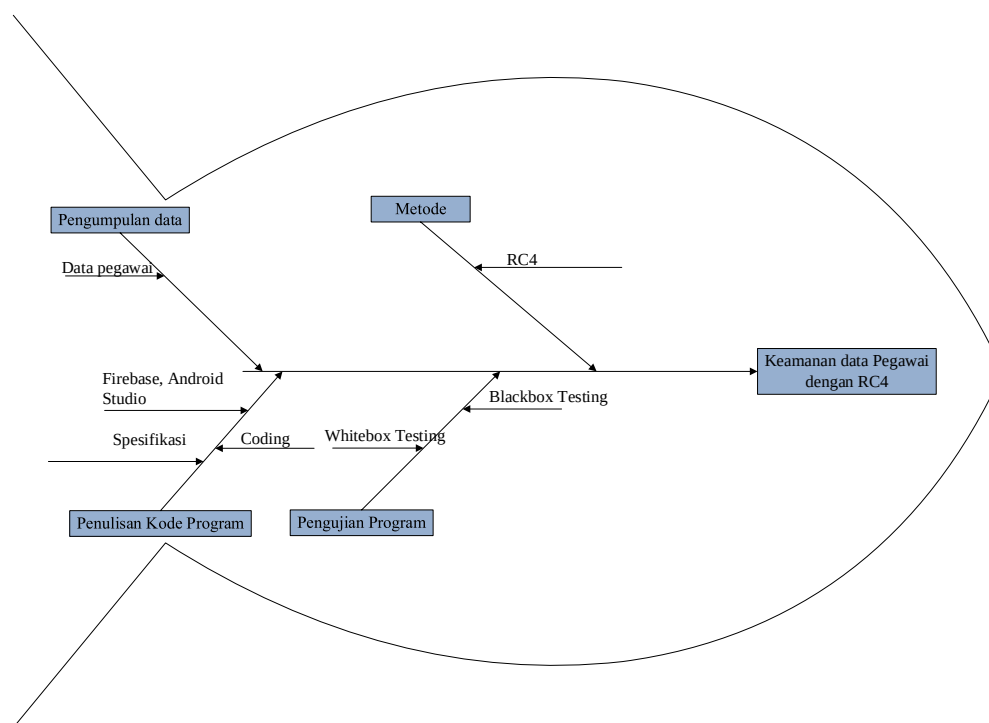
1. Pengamatan Langsung (*Observation*)
Peneliti melakukan pengamatan secara langsung pada PT. Nirwana Anugerah Lestari untuk mendapatkan data yang berkaitan dengan penelitian tentang keamanan data pegawai.
2. Wawancara (*Interview*)
Peneliti secara langsung bertatap muka dengan HRD pada PT. Nirwana Anugerah Lestari untuk mendapatkan data-data yang lebih lengkap tentang Implementasi Algoritma RC4 Dalam Keamanan data pegawai Pada PT. Nirwana Anugerah Lestari Berbasis Android.
3. *Sampling*
Peneliti memilih data-data yang tersedia dan sesuai dengan penelitian yaitu aplikasi penelitian terdahulu dan skripsi penelitian terdahulu untuk dijadikan sampel pada penelitian ini berupa data pegawai.

B. Penelitian Kepustakaan (*Library Research*)

Pada metode ini penulis mengutip dari beberapa bacaan yang berkaitan dengan pelaksanaan skripsi yang dikutip dari buku dan jurnal karya ilmiah. Literatur yang berkaitan dengan penelitian adalah kriptografi, pegawai dan metode RC4.

C. Metodologi Penelitian

Penelitian ini akan melalui beberapa tahapan. Tahapan dalam penelitian ini dapat di modelkan pada diagram *Fishbone*. Adapun beberapa tahapan yang digunakan dalam penelitian ini adalah sebagai berikut :

Gambar 1. Diagram *Fishbone*

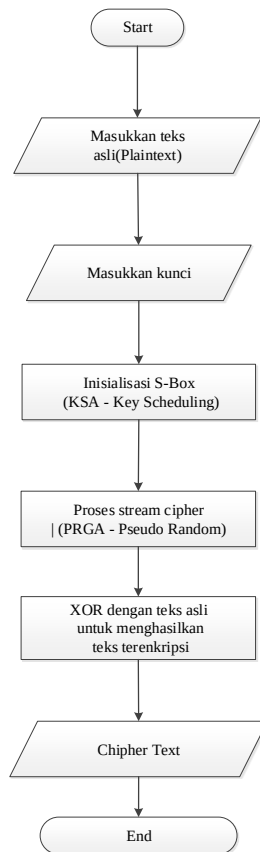
Keterangan :

1. Pengumpulan Data
Pada tahap ini adalah menganalisis sistem yang sedang berjalan sesuai dengan data-data khususnya data pegawai pada PT. Nirwana Anugerah Lestari yang telah diperoleh dari penelitian ini.
2. Metode
Pada tahap ini dilakukan perancangan system dengan menggunakan metode RC4 yang diusulkan dalam keamanan data pegawai pada PT. Nirwana Anugerah Lestari Dalam melakukan design penulis menggunakan diagram UML, dimana bukan hanya sekedar diagram tetapi juga menceritakan konteksnya.
3. Penulisan Kode Program
Merupakan penerjemah data atau pemecahan masalah *software* yang telah dirancang dalam bahasa pemrograman yang sudah ditentukan dan digunakan, dalam tahap pengkodean diimplementasikan kedalam bahasa pemrograman yang digunakan untuk membangun sistem pembuatan sistem menggunakan Android studio dan Firebase.
4. Pengujian Program
Berisi langkah-langkah yang dilakukan dalam pembuatan alat serta tahapan-tahapan pengujian yang dilakukan untuk masing-masing blok peralatan yang dirancang yaitu menganalisis beberapa kesalahan yang ada pada sistem yang lama dan melakukan pengujian aplikasi yang baru untuk meminimalisir kesalahan yang ada.
5. Hasil
Dengan selesainya melakukan pengujian program, dapat di jalan sesuai dengan yang diharapkan, maka program akan menampilkan aplikasi berbasis android dari program yang telah dibuat seperti keamanan data pegawai pada PT. Nirwana Anugerah Lestari.

3. HASIL DAN PEMBAHASAN

3.1. Pembahasan

Langkah yang harus dilakukan dalam proses enkripsi dengan menggunakan metode RC4 digambarkan dalam flowchart berikut :

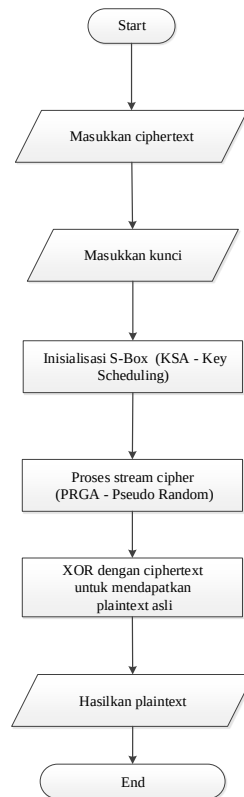


Gambar 2. Flowchart Enkripsi

Adapun penjelasan dari flowchart enkripsi diatas adalah sebagai berikut :

1. Mulai
Proses enkripsi dimulai.
2. Masukkan Teks Asli (Plaintext)
Data yang ingin dienkripsi dimasukkan.
3. Masukkan Kunci (Key)
Pengguna memasukkan kunci yang digunakan untuk enkripsi.
4. Inisialisasi S-Box (KSA - Key Scheduling Algorithm)
RC4 memiliki array S-Box (256 byte) yang diinisialisasi dengan nilai 0 hingga 255. Kemudian, elemen-elemen dalam S-Box diacak berdasarkan kunci.
5. Proses Stream Cipher (PRGA - Pseudo Random Generation Algorithm)
Menghasilkan stream kunci pseudo-random yang akan digunakan untuk enkripsi.
6. XOR dengan Plaintext
Setiap byte teks asli di-XOR dengan byte dari stream kunci untuk mendapatkan ciphertext.
7. Hasilkan Ciphertext
Hasil dari proses XOR adalah teks terenkripsi.
8. Selesai
Proses enkripsi selesai.

Langkah yang harus dilakukan dalam proses Dekripsi dengan menggunakan metode RC4 digambarkan dalam flowchart berikut :

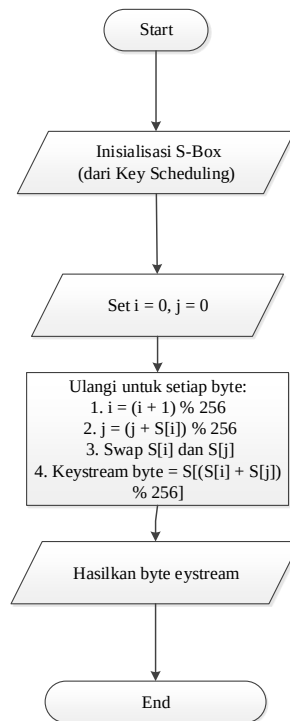


Gambar 3. Flowchart Dekripsi

Keterangan Langkah-langkah dalam Flowchart dekripsi diatas adalah sebagai berikut :

1. Mulai
Proses dekripsi dimulai.
2. Masukkan Ciphertext
Data yang telah dienkripsi dimasukkan.
3. Masukkan Kunci (Key)
Kunci yang sama dengan yang digunakan saat enkripsi harus dimasukkan.
4. Inisialisasi S-Box (KSA - Key Scheduling Algorithm)
Array S-Box diinisialisasi dengan nilai 0 hingga 255 dan diacak berdasarkan kunci.
5. Proses Stream Cipher (PRGA - Pseudo Random Generation Algorithm)
Menghasilkan keystream pseudo-random yang akan digunakan untuk dekripsi.
6. XOR dengan Ciphertext
Setiap byte dari ciphertext di-XOR dengan keystream untuk mendapatkan kembali plaintext asli.
7. Hasilkan Plaintext
Output plaintext yang telah berhasil didekripsi.
8. Selesai
Proses dekripsi selesai.

Langkah yang harus dilakukan dalam Proses Pseudo Random dengan menggunakan metode RC4 digambarkan dalam flowchart berikut :



Gambar 4. Flowchart Proses Pseudo Random

Langkah-langkah dalam PRGA (sesuai flowchart):

1. Mulai
Algoritma mulai dijalankan.
2. Inisialisasi S-Box
S-Box yang telah dibuat dalam tahap Key Scheduling Algorithm (KSA) digunakan.
3. Set nilai awal $i = 0, j = 0$
Indeks i dan j diatur ke nol sebelum loop PRGA berjalan.
4. Loop untuk setiap byte keystream
 - a. i bertambah ($i = (i + 1) \% 256$)
 - b. j dihitung berdasarkan nilai dalam S-Box ($j = (j + S[i]) \% 256$)
 - c. Swap nilai $S[i]$ dan $S[j]$ untuk memperbarui S-Box.
 - d. Byte keystream diambil dari indeks $(S[i] + S[j]) \% 256$ dalam S-Box.
5. Hasilkan byte keystream
Byte ini digunakan dalam operasi XOR untuk enkripsi atau dekripsi.
6. Selesai
Setelah cukup banyak byte keystream dihasilkan, proses berhenti.

Studi kasus

Algoritma RC4 menggunakan mode 4byte untuk mengenkripsikan file pegawai dengan format excel "DATA_PEGAWAI.xlsx" dengan kunci enkripsi RC4.

Maka berikut ini merupakan hasil RC4 mengenkripsi data dengan operasi XOR antara setiap byte plaintext dan keystream.

Tabel 1.Plaintext, Keystream dan Ciphertext (40 Byte Pertama)

Byte Index	Plaintext (P)	Keystream (K)	XOR ($P \oplus K$) $\rightarrow$ Ciphertext (C)
1	80 (P)	17 (K)	$80 \oplus 17 = 65$
2	75	232	$75 \oplus 232 = 163$
3	3	137	$3 \oplus 137 = 138$
4	4	161	$4 \oplus 161 = 165$

Byte Index	Plaintext (P)	Keystream (K)	XOR ($P \oplus K$) → Ciphertext (C)
5	20	235	$20 \oplus 235 = 255$
6	0	101	$0 \oplus 101 = 101$
7	6	113	$6 \oplus 113 = 119$
8	0	182	$0 \oplus 182 = 182$
9	8	153	$8 \oplus 153 = 145$
10	0	98	$0 \oplus 98 = 98$
11	0	105	$0 \oplus 105 = 105$
12	0	179	$0 \oplus 179 = 179$
13	33	221	$33 \oplus 221 = 252$
14	0	50	$0 \oplus 50 = 50$
15	59	123	$59 \oplus 123 = 64$
16	195	194	$195 \oplus 194 = 1$
17	224	229	$224 \oplus 229 = 5$
18	6	127	$6 \oplus 127 = 121$
19	168	102	$168 \oplus 102 = 202$
20	1	246	$1 \oplus 246 = 247$
21	0	8	$0 \oplus 8 = 8$
22	0	35	$0 \oplus 35 = 35$
23	214	4	$214 \oplus 4 = 210$
24	10	114	$10 \oplus 114 = 120$
25	0	219	$0 \oplus 219 = 219$
26	0	116	$0 \oplus 116 = 116$
27	19	194	$19 \oplus 194 = 209$
28	0	232	$0 \oplus 232 = 232$
29	8	252	$8 \oplus 252 = 244$
30	2	222	$2 \oplus 222 = 220$
31	91	184	$91 \oplus 184 = 227$
32	67	199	$67 \oplus 199 = 132$
33	111	202	$111 \oplus 202 = 165$
34	110	198	$110 \oplus 198 = 168$
35	116	46	$116 \oplus 46 = 90$
36	101	207	$101 \oplus 207 = 170$
37	110	58	$110 \oplus 58 = 84$
38	116	137	$116 \oplus 137 = 249$
39	95	138	$95 \oplus 138 = 213$
40	84	91	$84 \oplus 91 = 15$

Maka diperoleh hasil enkripsi (ciphertext) dalam desimal sebagai berikut :

[65, 163, 138, 165, 255, 101, 119, 182, 145, 98, 105, 179, 252, 50, 64, 1, 5, 121, 202, 247, 8, 35, 210, 120, 219, 116, 209, 232, 244, 220, 227, 132, 165, 168, 90, 170, 84, 249, 213, 15]

RC4 bersifat simetris, sehingga untuk mendekripsi, hanya perlu melakukan XOR ulang ciphertext dengan keystream.

Tabel 2. Proses Dekripsi (XOR Ulang dengan Keystream)

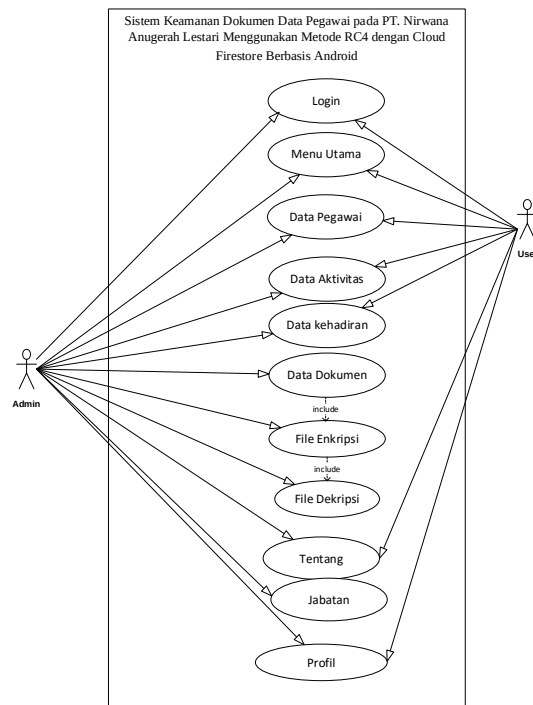
Byte Index	Ciphertext (C)	Keystream (K)	XOR ($C \oplus K$) → Plaintext (P)
1	65	17	$65 \oplus 17 = 80$
2	163	232	$163 \oplus 232 = 75$
3	138	137	$138 \oplus 137 = 3$
4	165	161	$165 \oplus 161 = 4$
5	255	235	$255 \oplus 235 = 20$

6	101	101	$101 \oplus 101 = 0$
7	119	113	$119 \oplus 113 = 6$
8	182	182	$182 \oplus 182 = 0$
9	145	153	$145 \oplus 153 = 8$
10	98	98	$98 \oplus 98 = 0$
11	105	105	$105 \oplus 105 = 0$
12	179	179	$179 \oplus 179 = 0$
13	252	221	$252 \oplus 221 = 33$
14	50	50	$50 \oplus 50 = 0$
15	64	123	$64 \oplus 123 = 59$
16	1	194	$1 \oplus 194 = 195$
17	5	229	$5 \oplus 229 = 224$
18	121	127	$121 \oplus 127 = 6$
19	202	102	$202 \oplus 102 = 168$
20	247	246	$247 \oplus 246 = 1$
21	8	8	$8 \oplus 8 = 0$
22	35	35	$35 \oplus 35 = 0$
23	210	4	$210 \oplus 4 = 214$
24	120	114	$120 \oplus 114 = 10$
25	219	219	$219 \oplus 219 = 0$
26	116	116	$116 \oplus 116 = 0$
27	209	194	$209 \oplus 194 = 19$
28	232	232	$232 \oplus 232 = 0$
29	244	252	$244 \oplus 252 = 8$
30	220	222	$220 \oplus 222 = 2$
31	227	184	$227 \oplus 184 = 91$
32	132	199	$132 \oplus 199 = 67$
33	165	202	$165 \oplus 202 = 111$
34	168	198	$168 \oplus 198 = 110$
35	90	46	$90 \oplus 46 = 116$
36	170	207	$170 \oplus 207 = 101$
37	84	58	$84 \oplus 58 = 110$
38	249	137	$249 \oplus 137 = 116$
39	213	138	$213 \oplus 138 = 95$
40	15	91	$15 \oplus 91 = 84$

Hasil Dekripsi (Plaintext) dalam Desimal:

[80, 75, 3, 4, 20, 0, 6, 0, 8, 0, 0, 0, 33, 0, 59, 195, 224, 6, 168, 1,

Sebuah *use case* digambarkan sebagai elips horizontal dalam suatu diagram UML *use case*, dapat dilihat pada gambar 5:



Gambar 5. Use Case Diagram

3.2. Hasil

1. Tampilan Menu *Login*

Tampilan *Login* merupakan tampilan yang pertama kali muncul ketika program dijalankan. Berfungsi sebagai *form input email* dan *password* admin program. Adapun gambar tampilan *login* dapat ditunjukkan pada gambar 6:

Gambar 6. Tampilan *Form Login*

2. Tampilan *Input Form* Menu Utama

Tampilan *input form* menu utama berfungsi untuk menampilkan tampilan utama dari *Pengguna interface*. Adapun gambar tampilan *input form* menu utama dapat ditunjukkan pada gambar 7



Gambar 7. Tampilan *Input Form* Menu Utama

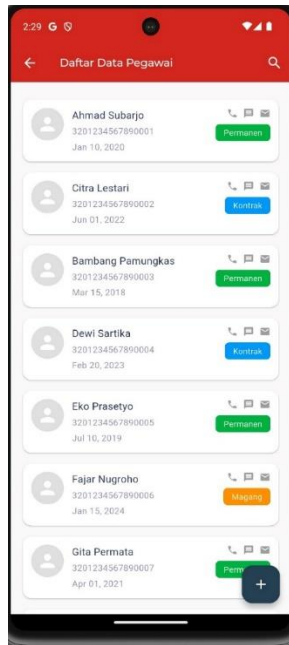
3. Tampilan *Form* Input Data Pegawai

Tampilan form ini menampilkan pilihan data input data pegawai, ketika memilih data input data pegawai maka program akan menampilkan data input data pegawai. dan form untuk penyimpanan data-data input data pegawai. Adapun gambar tampilan *form* input data pegawai dapat ditunjukkan pada gambar 8

Gambar 8. Tampilan *Form* Input Data Pegawai

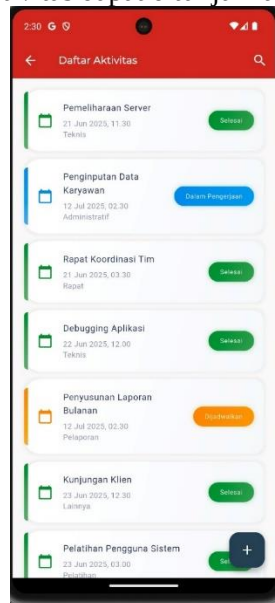
4. Tampilan *Form* Data Pegawai

Tampilan form ini menampilkan pilihan data data pegawai, ketika memilih data input data pegawai maka program akan menampilkan data data pegawai dan form untuk penyimpanan data pegawai. Adapun gambar tampilan *form* data pegawai dapat ditunjukkan pada gambar 9

Gambar 9. Tampilan *Form* Data Pegawai

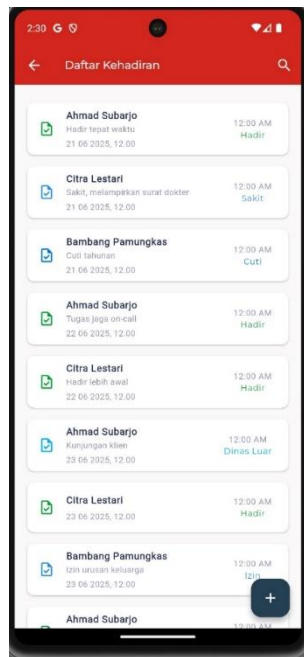
5. Tampilan *Form* Data Aktivitas

Tampilan *input form* data aktivitas ini menampilkan untuk penyimpanan data-data aktivitas. Adapun gambar tampilan *form input* aktivitas dapat ditunjukkan pada gambar 10

Gambar 10.. Tampilan *Form* Aktivitas

2. Tampilan *Form* data Kehadiran

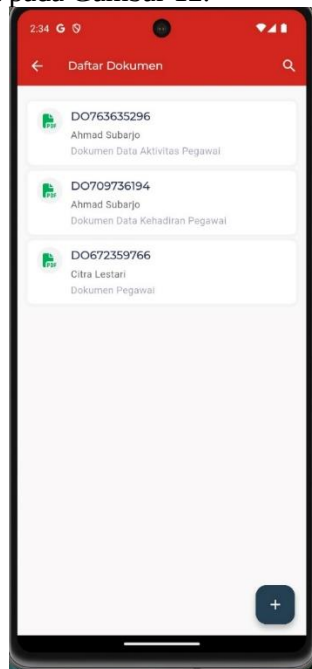
Tampilan *form* data data kehadiran merupakan form untuk penyimpanan data-data kehadiran. Adapun bentuk tampilan *form* data kehadiran dapat dilihat pada Gambar 11:



Gambar 11. Tampilan *Form* Data Kehadiran

3. Tampilan *Form* data dokumen

Tampilan *form* dokumen merupakan form untuk penyimpanan data-data dokumen. Adapun bentuk tampilan *form* dokumen dapat dilihat pada Gambar 12:



Gambar 12. Tampilan *Form* Dokumen

4. Tampilan *Form* keamanan data pegawai

Tampilan *form* keamanan data pegawai merupakan form untuk penyimpanan data-data keamanan data pegawai. Adapun bentuk *form* keamanan data pegawai dapat dilihat pada Gambar 13:



Gambar 13. Tampilan *Form* Keamanan Data Pegawai

4. KESIMPULAN

Berdasarkan hasil pembahasan dan uji coba yang telah dilakukan yaitu Sistem Keamanan Dokumen Data Pegawai pada PT. Nirwana Anugerah Lestari Menggunakan Metode RC4 dengan Cloud Firestore Berbasis Android, dapat disimpulkan :

1. Dengan menggunakan aplikasi ini user dan HRD dapat melakukan proses enkrip dan dekrip data dokumen data pegawai berupa data pegawai, data aktivitas pegawai serta data kehadiran dan melakukan generate kunci RC4 dalam proses enkripsi data.
2. Penerapan metode RC4 dalam proses kerahasiaan data dokumen data pegawai diimplementasikan untuk file xls.
3. Dengan menggunakan aplikasi yang dibangun dapat memudahkan PT. Nirwana Anugerah Lestari dalam menjaga kerahasiaan data pegawai dari pihak yang tidak berwenang.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Universitas Potensi Utama yang telah banyak memberikan masukan dan saran dalam penyelesaian penelitian ini.

REFERENSI

- [1] Azhari, M., Mulyana, D. I., Perwitosari, F. J., & Ali, F. (2022). Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES). *Jurnal Pendidikan Sains Dan Komputer*, 2(01), 163–171. <https://doi.org/10.47709/jpsk.v2i01.1390>
- [2] Darmawan, R., Teknik, F., Informatika, T., & Pamulang, U. (2023). *Perancangan Aplikasi Kriptografi Menggunakan Algoritma RC4 (Rivest Code 4) Untuk Mengamankan Pesan Email di PT CREATIFACTORY*. 2(3), 740–753.
- [3] Dian Kusuma Wardani, U. K. N. Q. (2020). Exact Papers in Compilation. *Exact Papers in Compilation*, 2(1), 211–218.
- [4] Haris Hrp, M., Nugroho, N. B., & Ginting, R. I. (2020). Implementasi Keamanan Data Gaji Pada Dinas Komunikasi Dan Persandian Kabupaten Aceh Tamiang Menggunakan Algoritma RC4. *Jurnal CyberTech*,

- x, 1–10. <https://ojs.trigunadharma.ac.id/>
- [5] Hiuredhy, D. K., & Beeh, Y. R. (2022). Rancang Bangun Aplikasi Pemesanan Desain Jersey Berbasis Android Dengan Menggunakan Teknologi Firebase (Studi Kasus : Konfeksi Minister). *JATISI (Jurnal Teknik Informatika Dan Sistem Informasi)*, 9(3), 1739–1751.
- [6] Hulu, S. (2024). Implementasi Algoritma Kriptografi Simetris Dalam Pengamanan Data Absensi Guru Dan Pegawai Pada Website Sekolah Smk Dharma Caraka Teluk Dalam Menggunakan RC4 Chiper. 01(04), 1–7.
- [7] Janis, J. W., Mamahit, D. J., Sugiarso, B. A., Rumagit, A. M., Elektro, T., Sam, U., & Manado, R. (2020). Rancang Bangun Aplikasi Online Sistem Pemesanan Jasa Tukang Bangunan Berbasis Lokasi. *Jurnal Teknik Informatika*, 15(1), 1–12. <https://doi.org/10.35793/jti.15.1.2020.29023>
- [8] Jihad, F., Lubis, D. R. P., & Lubis, A. H. (2023). Perancangan Sistem Informasi Jadwal Kegiatan Pegawai Berbasis Web. *Simtek: Jurnal Sistem Informasi Dan Teknik Komputer*, 8(1), 24–29. <https://doi.org/10.51876/simtek.v8i1.173>
- [9] Maulana, R., & Simanjorang, R. M. (2021). Implementasi Kriptografi Pengamanan Data Pribadi Siswa SMA Swasta Jaya Krama Beringin Dengan Algoritma RC4. *Jurnal Nasional Komputasi Dan Teknologi Informasi (JNKTI)*, 4(6), 377–383. <https://doi.org/10.32672/jnkti.v4i6.3533>
- [10] Notaris Susanto, K., & Muid Maulana, M. (2020). PENGAMANAN DATA SURAT-SURAT BERTHARGA di MENGGUNAKAN KRIPTOGRAFI dengan METODE RIVES CODE 4 (RC4). *Jurnal CyberTech*, September.
- [11] Rahmawati, M., & Yaumaidzinnaimah, Y. (2021). Sistem Informasi Penggajian Karyawan Berbasis Java Desktop. *INOVTEK Polbeng - Seri Informatika*, 6(1), 51. <https://doi.org/10.35314/isi.v6i1.1856>
- [12] Rohman, A., & Ramdhani, Y. A. (2022). Implementasi Algoritma AES Untuk Meningkatkan Keamanan Data Karyawan Pada PT PNM Cabang Karawang Barat Menggunakan PHP. *Jurnal Cahaya Mandalika*, 3(3), 169–174. <https://ojs.cahayamandalika.com/index.php/JCM/article/view/1132%0Ahttps://ojs.cahayamandalika.com/index.php/JCM/article/download/1132/965>
- [13] Siregar, S. J., Nugroho, N. B., & Sigalingging, H. (2023). Implementasi Algoritma Kriptografi RSA (Rivest Shamir Adleman) Dalam Pengamanan Data Gaji Karyawan Di Kantor BSPJI. *Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika Dan Komputer)*, 22(2), 528. <https://doi.org/10.53513/jis.v22i2.9409>
- [14] Sumiah, A., & Hakim, R. R. (2020). Implementasi Metode Linear Congruential Generator Pada Game Puzzle Berbasis Android. *JEJARING: Jurnal Teknologi Dan Manajemen Informatika*, 5(1), 1–10. <https://doi.org/10.25134/jejaring.v5i1.6748>
- [15] Tambunan, H. S., Gunawan, I., Novica Aswita, R. S., Nasution, Z. M., & Sumarno, S. (2021). Implementasi Algoritma Aes & Rc4 Terhadap Keamanan Data Produk Benih Sayuran di PT. Ewindo. *Jurnal Sosial Sains*, 1(6), 461–468. <https://doi.org/10.59188/jurnalsosains.v1i6.126>