TAMIKA: Jurnal Tugas Akhir Manajemen Informatika & Komputerisasi Akuntansi
Vol. 5 No. 2 (Desember 2025)
https://doi.org/10.46880/tamika.Vol5No2.pp334-343 e-ISSN: 2828-1276

IMPLEMENTASI SISTEM KEAMANAN DATA UNTUK PROYEK KONSTRUKSI MENGGUNAKAN METODE ALGORITMA RIVEST CIPHER 4 (RC4) BERBASIS ANDROID

Calvin Mulia Kennedy✉, Rahmad Doni
Fakultas Teknik dan Ilmu Komputer, Universitas Potensi Utama, Medan, Indonesia
Email: calvinkennedy@gmail.com

ABSTRACT

Data security is a crucial aspect in managing construction projects, especially for large-scale companies such as PT. Swakarya Perfect. Unprotected data exchange may lead to risks of information leakage, which could impact confidentiality, integrity, and project sustainability. This study aims to implement a data security system using the Rivest Cipher 4 (RC4) algorithm on Android devices, enabling efficient encryption and decryption of construction project data. The research method involves system requirements analysis, application design, RC4 algorithm implementation, and testing of both security strength and application performance. The implementation results show that the developed system can effectively secure construction project data, as the encrypted information cannot be accessed without the proper key. Furthermore, the application demonstrates relatively fast execution time during encryption and decryption processes, making it feasible for mobile use. Therefore, this system contributes to enhancing data security in construction projects at PT. Swakarya Perfect through the application of modern cryptographic technology on Android.

Keywords: Data Security, Construction Project, RC4, Android, Cryptography.

ABSTRAK

Keamanan data menjadi salah satu aspek penting dalam pengelolaan proyek konstruksi, terutama pada perusahaan yang memiliki skala besar seperti PT. Swakarya Perfect. Proses pertukaran data yang tidak terlindungi berpotensi menimbulkan risiko kebocoran informasi yang dapat berdampak pada kerahasiaan, integritas, dan keberlangsungan proyek. Penelitian ini bertujuan untuk mengimplementasikan sistem keamanan data berbasis algoritma Rivest Cipher 4 (RC4) pada perangkat Android, yang mampu mengenkripsi serta mendekripsi data proyek konstruksi secara cepat dan efisien. Metode penelitian meliputi analisis kebutuhan sistem, perancangan aplikasi, implementasi algoritma RC4, serta pengujian terhadap tingkat keamanan dan kinerja aplikasi. Hasil implementasi menunjukkan bahwa sistem yang dibangun dapat melindungi data proyek konstruksi dengan baik, di mana data yang terenkripsi tidak dapat dibaca tanpa kunci yang sesuai. Selain itu, performa aplikasi dalam proses enkripsi dan dekripsi menunjukkan waktu eksekusi yang relatif singkat sehingga layak digunakan pada perangkat mobile. Dengan demikian, sistem ini memberikan kontribusi dalam meningkatkan keamanan data proyek konstruksi PT. Swakarya Perfect melalui penerapan teknologi kriptografi modern berbasis Android.

Kata Kunci: Keamanan Data, Proyek Kontruksi, RC4, Android, Kriptografi.

PENDAHULUAN

Informasi yang akurat, lengkap, dan tepat waktu akan mendukung proses pengambilan keputusan, terutama dalam pengelolaan persediaan, peramalan, serta perencanaan strategi operasional perusahaan khusunsya data proyek kontruksi yang berisi data informasi kegiatan proyek kontruksi dan data penting lainnya (Putri, 2020).

Pada PT. Swakarya Perfect, pengamanan data proyek konstruksi seperti jadwal, anggaran, dan rencana kerja hingga saat ini masih dilakukan secara manual melalui arsip fisik. Metode pengarsipan konvensional ini menimbulkan berbagai kelemahan seperti arsip fisik yang menumpuk menyebabkan inefisiensi dan kesulitan menemukan dokumen yang dibutuhkan (Putra, 2024). Selain itu, dokumen kertas sangat rentan rusak atau hilang (misalnya akibat kebakaran, bencana alam, kerusakan usia kertas, maupun kelalaian manusia). Dengan kondisi tersebut, sering kali jadwal dan anggaran proyek tidak dapat diakses dengan cepat atau terduplikasi, sehingga keamanan dan ketersediaan informasi penting tidak terjamin.

Akibat lemahnya sistem pengamanan manual, PT. Swakarya Perfect kerap mengalami masalah berupa kebocoran data dan kehilangan dokumen proyek penting. Kebocoran data perusahaan bisa menimbulkan dampak fatal, karena informasi proyek

konstruksi termasuk data sensitif yang tidak boleh tersebar bebas kepada pihak yang tidak berwenang (Fauzan et al., 2025). Di sisi lain, persentase dokumen hilang menjadi tinggi ketika penyimpanan masih bersifat konvensional (kertas), karena penempatan arsip yang tidak teratur dan beragam pihak bisa mengaksesnya tanpa kontrol yang memadai. Kejadian-kejadian seperti itu menandakan urgensi penerapan mekanisme pengamanan yang lebih andal.

Menghadapi permasalahan tersebut, digitalisasi pengelolaan data proyek menjadi langkah krusial. Digitalisasi data proyek memungkinkan pembaruan informasi secara real-time dan visibilitas yang lebih baik, sehingga seluruh pemangku kepentingan dapat bekerja dengan informasi yang konsisten dan terkini. Transformasi digital di industri konstruksi tidak lagi sekadar tren, melainkan keharusan untuk meningkatkan efisiensi operasional dan mencegah kesalahan (Utami & Firdaus, 2025). Dalam kerangka sistem terkomputerisasi tersebut, perlindungan data melalui kriptografi adalah hal penting. Kriptografi (metode enkripsi) mampu menyembunyikan informasi penting dengan cara yang sulit dipahami pihak luar (Ramalinda & Raharja, 2024). Dengan enkripsi, data sensitif proyek dapat diproses menjadi format yang tidak terbaca tanpa kunci rahasia, sehingga mencegah penipuan atau penyadapan data perusahaan oleh pihak yang tidak berhak (Fitri et al., 2024).

Untuk konteks implementasi awal di PT. Swakarya Perfect yang belum memiliki infrastruktur TI terpusat, dipilih algoritma RC4 sebagai metode enkripsi yang ringan dan cepat. RC4 adalah algoritma enkripsi aliran (stream cipher) yang terkenal sangat cepat, dilaporkan sekitar sepuluh kali lebih cepat dibandingkan DES pada kecepatan eksekusi serta sederhana diimplementasikan (Simamora & Pasaribu, 2024). Keunggulan-keunggulan ini membuat RC4 cocok diaplikasikan pada lingkungan dengan perangkat komputasi terbatas, karena tidak memerlukan sumber daya komputasi berat. Dengan demikian, penerapan RC4 diharapkan mampu meningkatkan keamanan data proyek tanpa mengganggu kelancaran operasional perusahaan (Dewi, 2024). Berdasarkan uraian tersebut, urgensi penerapan sistem keamanan data berbasis kriptografi di lingkungan konstruksi dengan tingkat digitalisasi rendah sangat tinggi, guna menjaga kerahasiaan dan integritas informasi proyek demi keberlanjutan dan reputasi perusahaan.

Penelitian ini bertujuan untuk merancang sistem keamanan data digital berbasis algoritma RC4 untuk data proyek konstruksi, mengamankan data proyek kontruksi serta membantu PT. Swakarya Perfect dalam menjaga kerahasiaan data proyek kontruksi dengan menggunakan metode RC4.

Kelebihan metode RC4 adalah mudah diimplementasikan, RC4 memiliki algoritma yang relatif sederhana sehingga mudah untuk diimplementasikan dalam berbagai sistem. kecepatan tinggi (Kumala et al., 2025). RC4 merupakan salah satu algoritma enkripsi aliran yang paling cepat, yang sangat berguna untuk aplikasi yang memerlukan enkripsi dan dekripsi data secara real-time. Efisiensi memori, algoritma ini tidak memerlukan memori tambahan yang signifikan, menjadikannya efisien untuk digunakan pada perangkat dengan sumber daya terbatas. Penanganan data besar (Saragi et al., 2020). RC4 dirancang untuk menangani aliran data besar dengan cepat dan efisien. Fleksibilitas, kecepatannya menjadikannya pilihan yang baik untuk kebutuhan enkripsi data dalam berbagai konteks, seperti enkripsi berkas konfigurasi atau data pengguna (Febriyani & Arfriandi, 2021).

Perbandingan metode Algoritma RC4 dan AES memiliki karakteristik yang berbeda sehingga relevan untuk dibandingkan dalam konteks pemilihan metode enkripsi. RC4 merupakan *stream cipher* yang bekerja dengan menghasilkan aliran key-stream untuk kemudian di-XOR-kan dengan data, sehingga proses enkripsinya sangat cepat dan memiliki kebutuhan sumber daya yang rendah. Hal ini menjadikan RC4 cocok untuk perangkat dengan spesifikasi terbatas seperti beberapa jenis perangkat Android kelas menengah ke bawah. Namun, RC4 memiliki kelemahan kriptografis yang cukup signifikan, khususnya adanya bias pada keluaran key-stream dan potensi kerentanan apabila terjadi penggunaan ulang kunci.

Sebaliknya, AES merupakan *block cipher* modern yang telah distandarisasi oleh NIST dan diakui memiliki tingkat keamanan yang sangat tinggi. AES menggunakan struktur ronde yang kompleks dan mendukung berbagai mode operasi sehingga mampu memberikan kerahasiaan dan integritas data secara kuat. Walaupun AES membutuhkan komputasi lebih besar dibanding RC4, sebagian besar perangkat Android masa kini telah mendukung akselerasi hardware yang membuat performa AES tetap efisien. Dengan demikian, RC4 unggul dari sisi kecepatan dan efisiensi penggunaan sumber daya, sedangkan AES lebih unggul dari sisi keamanan dan ketahanan terhadap serangan modern. Perbandingan ini menunjukkan bahwa pemilihan RC4 dalam penelitian perlu disesuaikan dengan kebutuhan performa serta karakteristik data yang dilindungi.

Pada perbandingan selanjutnya yaitu metode Algoritma RC4 dan RC4A merupakan dua jenis *stream cipher* yang memiliki keterkaitan erat, di mana RC4A dikembangkan sebagai perbaikan dari RC4 untuk meningkatkan keamanan key-stream. RC4 menggunakan satu buah *S-box* berukuran 256 byte dengan proses *Key Scheduling Algorithm* (KSA) dan *Pseudo Random Generation Algorithm* (PRGA) yang sederhana, sehingga algoritma ini sangat cepat dan efisien dalam pemakaian memori. Sifat inilah yang menjadikan RC4 banyak digunakan pada aplikasi dengan keterbatasan sumber daya. Namun, RC4 diketahui memiliki beberapa kelemahan, terutama bias pada keluaran awal key-stream dan potensi serangan jika kunci digunakan berulang. RC4A hadir sebagai modifikasi yang memperbaiki kelemahan tersebut dengan menggunakan dua buah *S-box* dan proses PRGA yang diacak lebih kompleks, sehingga menghasilkan key-stream yang lebih acak dan mengurangi peluang terjadinya pola berulang. Walaupun RC4A menawarkan tingkat keamanan yang lebih baik dibanding RC4, algoritma ini memiliki beban komputasi sedikit lebih tinggi karena struktur internalnya lebih kompleks.

Dengan demikian, RC4 lebih unggul dari sisi kecepatan dan kesederhanaan implementasi, sedangkan RC4A menawarkan peningkatan keamanan dengan kompromi pada tingkat performa. Perbandingan ini menunjukkan bahwa pemilihan RC4 atau RC4A perlu mempertimbangkan kebutuhan antara efisiensi proses enkripsi dan tingkat keamanan yang diharapkan.

Sedangkan pada perbandingan metode Algoritma RC4 dan RC5 merupakan dua jenis algoritma kriptografi simetris yang dikembangkan oleh Ron Rivest, namun keduanya memiliki karakteristik dan tujuan desain yang berbeda. RC4 adalah *stream cipher* yang terkenal dengan struktur algoritmanya yang sederhana, ringan, dan memiliki kecepatan enkripsi yang tinggi. RC4 hanya membutuhkan satu buah *S-box* dan menghasilkan key-stream secara berurutan, sehingga sangat efisien untuk perangkat dengan keterbatasan sumber daya seperti aplikasi mobile atau sistem tertanam. Namun, RC4 memiliki kelemahan kriptografis pada proses *Key Scheduling Algorithm* (KSA) dan bias pada keluaran awal key-stream, sehingga tingkat keamanannya kurang optimal untuk data sensitif. Di sisi lain, RC5 merupakan *block cipher* yang menggunakan struktur *Feistel network* dengan parameter yang dapat disesuaikan, seperti ukuran blok, ukuran kunci, dan jumlah ronde, sehingga menawarkan fleksibilitas dan tingkat keamanan yang lebih tinggi. RC5 juga memiliki sifat difusi dan konfusi yang lebih kuat, menjadikannya lebih tahan terhadap berbagai bentuk serangan kriptanalisis. Namun, kompleksitas algoritma RC5 menyebabkan kebutuhan komputasi dan memori yang lebih besar dibanding RC4.

Dengan demikian, RC4 lebih unggul dalam hal kecepatan dan efisiensi, sedangkan RC5 lebih unggul pada aspek keamanan dan fleksibilitas. Pemilihan antara keduanya harus mempertimbangkan prioritas sistem, apakah lebih mengutamakan performa atau tingkat keamanan yang lebih kuat.

TINJAUAN PUSTAKA

Aplikasi

Aplikasi adalah suatu perangkat lunak yang dikembangkan untuk menjalankan fungsi atau tugas tertentu pada berbagai jenis perangkat elektronik, seperti komputer, smartphone, maupun tablet. Aplikasi berfungsi sebagai alat bantu pengguna dalam melakukan aktivitas digital secara lebih efisien dan terarah sesuai tujuan pembuatannya (Gunawan et al., 2021).

Android

Istilah *Android* dalam bahasa Inggris merujuk pada robot yang menyerupai manusia sehingga pengembangan sistem operasi ini sepenuhnya berada di bawah kendali *Google*. Dalam rangka pengembangan Android, dibentuk organisasi *Open Handset Alliance*, dan *Google* merilis perangkat lunak ini sebagai open source sehingga memungkinkan kontribusi dari berbagai pihak untuk pengembangan lebih lanjut (Pasaribu, 2021).

RC4

RC4 merupakan salah satu algoritma kriptografi stream cipher yang paling dikenal dan pernah digunakan secara luas, terutama pada sistem keamanan jaringan seperti protokol Secure Socket Layer (SSL) dan Wired Equivalent Privacy (WEP). Algoritma ini diciptakan oleh Ron Rivest dari RSA Laboratories, dan nama RC sendiri merupakan singkatan dari *Ron's Code* (Satriadi & Rahman, 2024). RC4 tersusun dari operasi-operasi dasar sehingga dapat diterapkan pada berbagai perangkat keras maupun perangkat lunak dengan kompleksitas yang rendah. RC4 termasuk ke dalam kategori cipher aliran (stream cipher). Algoritma ini menghasilkan rangkaian bit acak yang disebut *keystream*.

1. Saat enkripsi, keystream di-*XOR*-kan dengan plaintext untuk menghasilkan ciphertext.
2. Saat dekripsi, keystream yang sama di-*XOR*-kan dengan ciphertext untuk mendapatkan kembali plaintext (Nur & Giawa, 2022).

Keamanan Data

Keamanan komputer merupakan serangkaian tindakan pencegahan yang bertujuan melindungi sistem komputer maupun jaringan dari serangan, akses ilegal, serta penyalahgunaan oleh pihak yang tidak bertanggung jawab. Banyak pengguna maupun pengelola sistem informasi belum menyadari bahwa aspek security merupakan komponen yang sangat vital dalam menjaga keberlangsungan operasional perusahaan. Bagi perancang dan pengelola sistem informasi, isu keamanan sering menjadi tantangan karena kerentanan dapat muncul pada berbagai lapisan, baik perangkat keras, perangkat lunak, jaringan, maupun data. Dalam konteks ini, kriptografi berperan sangat penting sebagai mekanisme perlindungan data (Alfian et al., 2024).

Kriptografi

Kriptografi adalah ilmu atau seni menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain. Secara umum, kriptografi mempelajari teknik pengacakan (enkripsi) pesan menggunakan perhitungan matematika sehingga pesan tidak dapat dibaca oleh pihak yang tidak berwenang, serta teknik pengembalian pesan ke bentuk aslinya (dekripsi). Kriptografi memungkinkan proses enkripsi, yaitu pengacakan data agar tidak dapat dibaca oleh pihak yang tidak berwenang, serta dekripsi, yaitu mengembalikan data yang sudah diacak menjadi bentuk semula oleh pihak yang memiliki kunci yang benar. Dengan demikian, kriptografi menjadi komponen utama dalam menjaga kerahasiaan, integritas, dan keamanan data yang ditransmisikan (Jamaluddin et al., 2014; Umam et al., 2022).

Kontribusi Penelitian

Konstribusi keilmuan dari penelitian ini yaitu:

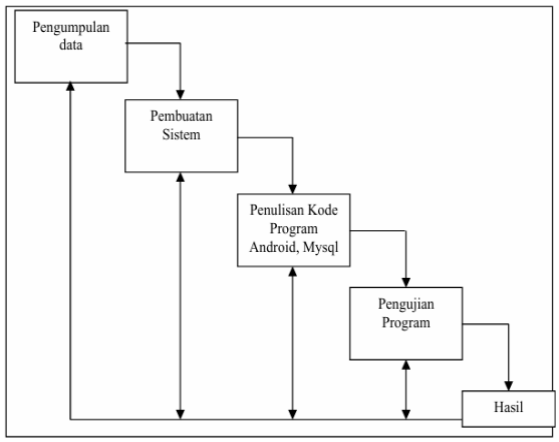
1. Menciptakan aplikasi baru berbasis android dalam menjaga kerahasian proyek kontruksi pada PT. Swakarya Perfect.
2. Menyediakan studi kasus nyata penerapan kriptografi RC4 pada sektor konstruksi yang umumnya masih tertinggal dalam digitalisasi khususnya proyek kontruksi seperti jadwal, anggaran, dan rencana kerja pada PT. Swakarya Perfect.
3. Menambah literatur dan penelitian terapan mengenai pemanfaatan algoritma kriptografi RC4 dalam keamanan proyek kontruksi seperti jadwal, anggaran, dan rencana kerja pada PT. Swakarya Perfect.

METODE PENELITIAN

Di dalam melakukan penelitian diperlukan beberapa cara untuk mengumpulkan data yang diperlukan dalam kegiatan penelitian ini. Adapun teknik dalam pengumpulan data adalah:

1. Pengamatan
   Dalam metode pengamatan ini peneliti melakukan pengamatan secara langsung pada PT. Swakarya Perfect.
2. Wawancara
   mendapatkan sebuah informasi terkait tema yang diangkat dalam sebuah penelitian dengan cara mengajukan pertanyaan-pertanyaan pada PT. Swakarya Perfect.
3. Studi Kepustakaan
   Penulis mencari referensi dari beberapa sumber bacaan seperti buku panduan dan jurnal terkait yang membahas tentang data proyek kontruksi dengan menerapkan RC4.

Pengembangan sistem dapat dilakukan dengan merancang sistem baru yang menggantikan sistem lama secara keseluruhan, maupun dengan melakukan perbaikan terhadap sistem yang sudah ada. Metodologi pengembangan sistem Waterfall digambarkan pada ilustrasi di bawah ini:



Gambar 1. Diagram *Waterfall*

Keterangan:

1. Pengumpulan Data
   Tahapan ini menggunakan berbagai data terkait dengan penelitian meliputi dilakukan yaitu data proyek kontruksi pada PT. Swakarya Perfect.
2. Pembuatan Sistem
   Desain sistem menggunakan pemodelan Unifield Modelling Language (UML) Diagram ini membantu menggambarkan interaksi pengguna, struktur kelas, alur kerja proses, dan urutan peristiwa dalam pengembangan sistem. Dengan

penerapan UML, desain sistem menjadi lebih jelas dan mudah dimengerti.

3. Penulisan Kode Program
   Tahapan ini merupakan tahap implementasi nyata dalam proses pengembangan sistem, di mana pemanfaatan komputer dilakukan secara maksimal. Pengujian ini tidak memerlukan pengetahuan khusus mengenai kode maupun struktur internal, karena difokuskan pada setiap blok atau komponen yang telah dirancang. Pengujian dilakukan menggunakan blackbox.
4. Pengujian
   Pengujian ini tidak memerlukan pengetahuan khusus mengenai kode maupun struktur internal, karena difokuskan pada setiap blok atau komponen yang telah dirancang. Pengujian dilakukan menggunakan blackbox.
5. Hasil
   Aplikasi sistem keamanan data untuk proyek kontruksi menggunakan metode Algoritma RC4 berbasis Android.

HASIL DAN PEMBAHASAN

PT. Swakarya Perfect membutuhkan sistem keamanan data yang mampu melindungi informasi proyek konstruksi yang dimilikinya. Kegiatan proyek konstruksi meliputi penyusunan jadwal, anggaran, serta rencana kerja yang bersifat penting dan sensitif. Oleh karena itu, data proyek harus diamankan dengan sangat cermat karena mengandung informasi strategis perusahaan. Permasalahan yang sering muncul adalah kurangnya tingkat keamanan yang memadai pada sistem yang digunakan saat ini, sehingga membuka peluang terjadinya akses tidak sah, pelanggaran privasi, serta kebocoran data oleh pihak-pihak yang tidak berwenang seperti hacker atau cracker. Insiden kebocoran informasi proyek dapat menimbulkan kerugian besar, baik bagi perusahaan maupun vendor yang terlibat.

Untuk mengatasi permasalahan tersebut, diperlukan penerapan algoritma kriptografi sebagai teknologi pengamanan data. Kriptografi merupakan ilmu yang mempelajari teknik penyamaran pesan melalui proses enkripsi sehingga hanya pihak yang berhak saja yang dapat membaca informasi tersebut. Dengan menerapkan algoritma kriptografi, data proyek konstruksi dapat disandikan ke dalam bentuk yang tidak memiliki makna bagi pihak luar, namun tetap dapat dikembalikan ke bentuk asli melalui proses dekripsi oleh pihak yang memiliki kunci. Dengan demikian, kriptografi mampu menjaga kerahasiaan, integritas, serta keamanan data proyek yang dikirimkan antara pengguna sistem di PT. Swakarya Perfect (Tambunan et al., 2021).

Penerapan Metode

RC4 merupakan salah satu algoritma kriptografi stream cipher yang paling dikenal dan pernah digunakan secara luas, terutama pada sistem keamanan jaringan seperti protokol Secure Socket Layer (SSL) dan Wired Equivalent Privacy (WEP). Algoritma ini diciptakan oleh Ron Rivest dari RSA Laboratories, dan nama RC sendiri merupakan singkatan dari *Ron's Code*. RC4 tersusun dari operasi-operasi dasar sehingga dapat diterapkan pada berbagai perangkat keras maupun perangkat lunak dengan kompleksitas yang rendah. RC4 termasuk ke dalam kategori cipher aliran (stream cipher). Algoritma ini menghasilkan rangkaian bit acak yang disebut *keystream*.

1. Saat enkripsi, keystream di-*XOR*-kan dengan plaintext untuk menghasilkan ciphertext.
2. Saat dekripsi, keystream yang sama di-*XOR*-kan dengan ciphertext untuk mendapatkan kembali plaintext

Studi Kasus

Algoritma RC4 menggunakan mode 4byte untuk mengenkripsikan plaintext "Berikut ini contoh DBMS, Kecuali" dengan kunci enkripsi RC4

Tahap 1: KSA

1. Array S:
   Array S diinisialisasi dengan [0,1,2,.. 255]
2. Pembuatan Array Kunci k :
   Ubah kunci"enkripsi RC4" ke nilai ASCII

Tabel 1. Array K

e	n	k	r	i	p	s	i	R	C	4
101	110	107	114	105	112	115	105	82	67	52

   Array K ini kemudian diulang hingga mencapai Panjang 256.
3. Proses Pengacakan Array S dengan K
   Dengan S dan K yang telah terbentuk, kita iterasikan 256 kali untuk mengacak S. Hasil akhir pengacakan array S ini akan berbeda-beda berdasarkan kunci.

Tahap 2: PRGA

PRGA menghasilkan keystream yang digunakan untuk mengenkripsi teks asli. Berikut adalah perhitungan manual untuk beberapa karakter pertama dari teks

"Berikut ini contoh DBMS, Kecuali".

Berikut adalah detail PRGA dan proses enkripsi untuk setiap karakter dalam teks

"Berikut ini contoh DBMS, Kecuali":

1. Karakter "B" (ASCII 66):
   i = 1, j= 122
   Keystream byte K= 251
   Enkripsi $66 \oplus 251 = 185$

2. Karakter “e” (ASCII 101):
   i = 2, j= 187
   Keystream byte K= 62
   Enkripsi 101⊕62 = 233
3. Karakter 'r' (ASCII 114):
   i = 3, j = 113
   Keystream byte K = 155
   Enkripsi: 114⊕155=233
4. Karakter 'i' (ASCII 105):
   i = 4, j = 148
   Keystream byte K = 198
   Enkripsi: 105⊕198=175
5. Karakter 'k' (ASCII 107):
   i = 5, j = 45
   Keystream byte K = 108
   Enkripsi: 107⊕108=7
6. Karakter 'u' (ASCII 117):
   i = 6, j = 36
   Keystream byte K = 243
   Enkripsi: 117⊕243=134

Sehingga diperoleh hasil berikut ini sebagai hasil Pseudo-Random Generation Algorithm (PRGA) : [185, 91, 233, 175, 7, 134, 254, 49, 108, 73, 203, 236, 21, 103, 27, 151, 193, 47, 67, 66, 102, 27, 250, 133, 65, 56, 226, 53, 103, 146, 249, 74]

Hasil dekripsi RC4 untuk teks terenkripsi menghasilkan kembali teks asli: "Berikut ini contoh DBMS, Kecuali"

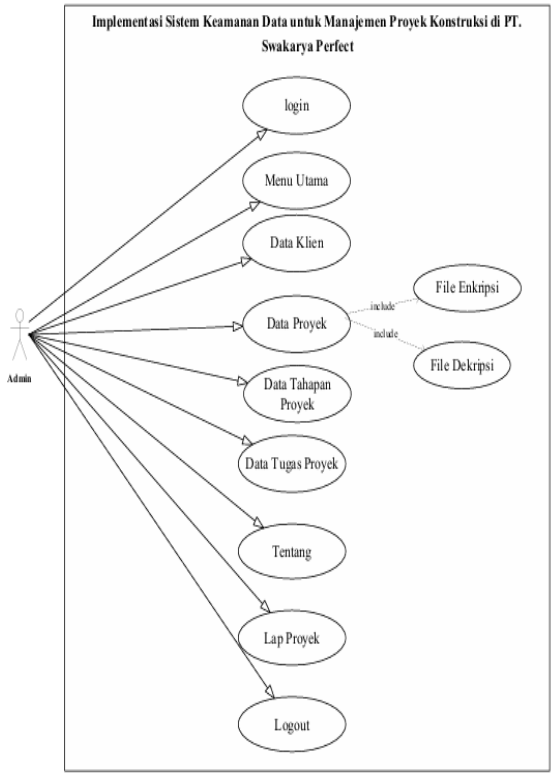
Tabel hasil pengujian

Tabel 2. Hasil Pengujian

No	Ukuran File	Waktu Enkripsi (ms)	Waktu Dekripsi (ms)	Tingkat Keberhasilan (%)
1	16 Byte	0.05	0.04	100.00%
2	1 KB	0.5	0.45	100.00%
3	10 KB	3	2.8	100.00%
4	100 KB	20	18	100.00%
5	1 MB	180	170	100.00%
6	10 MB	1700	1650	90.00%

Usecase Diagram

Use Case Diagram merupakan pemodelan untuk melakukan (behavior) sistem informasi yang akan dibuat. Use Case mendeskripsikan sebuah interaksi antara satu atau lebih aktor dengan sistem informasi yang akan dibuat. Perilaku beserta tugas-tugas dari tiap–tiap elemen maupun aktor yang terlibat dalam sistem yang akan dirancang, akan digambarkan dalam diagram use case yang bertujuan untuk memberikan gambaran secara umum tentang sistem yang akan dirancang. Adapun bentuk dari diagram Usecase pada penelitian ini adalah:



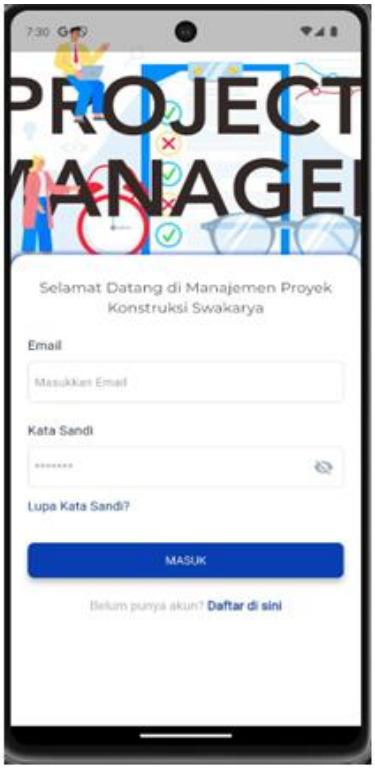
Gambar 2. Use Case Diagram Penelitian

Tampilan Hasil Aplikasi Pada Admin

Pada bab ini akan dijelaskan tampilan hasil dari android yang telah dibuat, yang digunakan untuk memperjelas tentang tampilan-tampilan yang ada pada Implementasi Sistem Keamanan Data untuk Proyek Konstruksi di PT. Swakarya Perfect. Sehingga hasil android dapat dilihat sesuai dengan hasil program yang telah dibuat. Dibawah ini akan dijelaskan tiap-tiap tampilan yang ada pada program. Sehingga hasil implementasinya dapat dilihat sesuai dengan hasil program yang telah dibuat.

Tampilan Menu Login

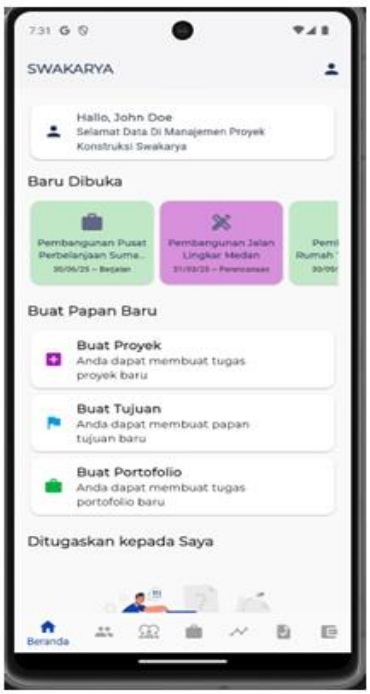
Tampilan Login merupakan tampilan yang pertama kali muncul ketika program dijalankan. Berfungsi sebagai form input email dan password admin program.



Gambar 3. Tampilan Menu Login

Tampilan Menu Utama

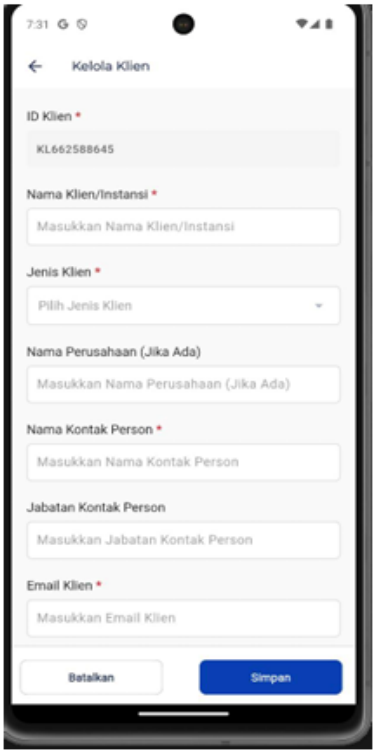
Tampilan input form menu utama berfungsi untuk menampilkan tampilan utama dari Pengguna interface.



Gambar 4. Tampilan Menu Utama

Tampilan Data Klien

Tampilan form ini menampilkan pilihan data input data klien, ketika memilih data input data klien maka program akan menampilkan data input data klien. dan form untuk penyimpanan data-data input data klien.



Gambar 5. Tampilan Data Klien

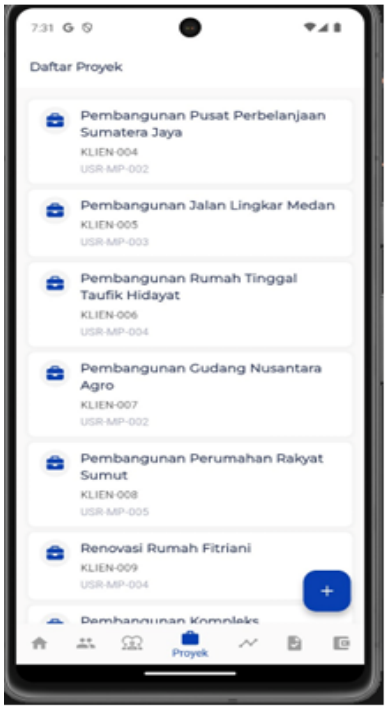
Tampilan Daftar Klien

Tampilan form ini menampilkan pilihan data data daftar klien, ketika memilih data input data daftar klien maka program akan menampilkan data data daftar klien dan form untuk penyimpanan data daftar klien.

Gambar 6. Tampilan Daftar Klien

Tampilan Data Proyek

Tampilan inpui form data proyek ini menampilakan untuk penyimpanan data data proyek.



Gambar 7. Tampilan Data Proyek

Tampilan Data Kunci RC4

Tampilan form data data Kunci RC4 merupakan form untuk penyimpanan data data Kunci RC4.

Gambar 8. Tampilan Data Kunci RC4

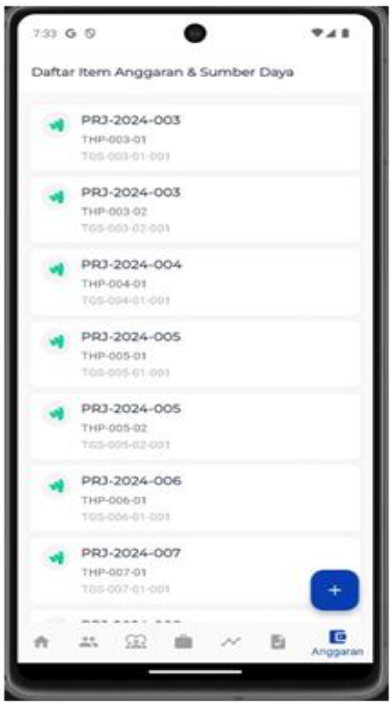
Tampilan Deskrip

Tampilan form keamanan data proyek merupakan form untuk penyimpanan data-data keamanan data proyek.

Gambar 9. Tampilan Deskrip

Tampilan Daftar Item

Tampilan form daftar item anggaran merupakan form untuk menu daftar item anggaran dan penyimpanan data-data menu daftar item anggaran



Gambar 10. Tampilan Daftar Item

Hasil Pengujian

Setelah melakukan uji coba terhadap sistem, maka dapat di simpulkan hasil yang di dapat yaitu:

1. Antarmuka yang sederhana dapat mempermudah penggunaan dalam mempelajari sistem ini.
2. Sistem dapat mengamankan data proyek konstruksi di PT. Swakarya Perfect

Kelebihan Sistem

Adapun kesimpulan penulis mengenai kelebihan dari sistem yang diusulkan adalah sebagai berikut :

1. Proses pendataan data proyek konstruksi di PT. Swakarya Perfect bisa dilakukan sekaligus dan menghasilkan laporan pegawai dan keamanan data proyek konstruksi di PT. Swakarya Perfect dengan lebih cepat.
2. Sistem sudah mampu menampilkan laporan keamanan data proyek konstruksi di PT. Swakarya Perfect.

Kekurangan Sistem

Adapun kesimpulan penulis mengenai kekurangan dari sistem yang diusulkan adalah sebagai berikut :

1. Aplikasi ini hanya memunculkan data keamanan data proyek konstruksi di PT. Swakarya Perfect.
2. Sistem yang dirancang belum mencakup hak akses HRD dan manager dalam pengelolaan keamanan data proyek konstruksi di PT. Swakarya Perfect.

KESIMPULAN

Adapun kesimpulan dari Laporan penelitian Implementasi Sistem Keamanan Data untuk Proyek Konstruksi di PT. Swakarya Perfect ini adalah sebagai berikut:

1. Penerapan kriptografi dalam sistem pengamanan data proyek konstruksi di PT. Swakarya Perfect terbukti mampu meningkatkan tingkat kerahasiaan dan keamanan dokumen penting. Dengan menggunakan RC4, data proyek konstruksi yang dikirimkan melalui aplikasi Android dapat dienkripsi terlebih dahulu sehingga tidak mudah diakses oleh pihak yang tidak berwenang.
2. Dengan mengimplementasikan metode RC4 dapat menjaga kerahasiaan proyek konstruksi.
3. Dengan menggunakan aplikasi ini petugas proyek dapat melakukan proses enkripsi dan dekripsi data proyek konstruksi.

DAFTAR PUSTAKA

Alfian, M., Rahman, R., Informasi, S., Selatan, P. S., & Selatan, P. S. (2024). *Jurnal riset sistem informasi*. *1*(3), 59–64.

Dewi, S. K. (2024). *Perbandingan Cryptography Klasik Vigenere Cipher Dengan Cryptography Modern RC4 Dalam Tingkat Keamanan Jaringan Komputer*. *02*.

Fauzan, I. N., Putri, M. S., & Endiyanti, B. K. (2025). *Pengaruh Efektivitas Sistem Pengarsipan Digital terhadap Produktivitas Karyawan di Lingkungan Perkantoran*. *2*, 1–11.

Febriyani, F. S., & Arfriandi, A. (2021). *Implementasi Algoritma RC4 pada Sistem Pengamanan Dokumen Digital Soal Ujian*. *6*(3), 171–177.

Fitri, M. A., Irwan, M., & Nasution, P. (2024). *Taktik Canggih untuk Memastikan Keamanan Data Perusahaan dan Mengatasi Ancaman Kebocoran Data di Masa Depan*. *2*(2), 113–121.

Gunawan, R., Yusuf, A. M., & Nopitasari, L. (2021). Rancang Bangun Sistem Presensi Mahasiswa Dengan Menggunakan QR Code Berbasis Android. *Elkom : Jurnal Elektronika Dan Komputer*, *14*(1), 47–58.

Jamaluddin, J., Zarlis, M., & Tulus, T. (2014). Pengamanan Data dengan Kombinasi Teknik Kriptografi Rabin dan Teknik Steganografi Chaotic LSB. *SNASTIKOM 2014*, 39–44. https://doi.org/10.31227/osf.io/nt4cm

Kumala, J. A., Zaman, B., & Bahri, S. (2025). *Implementasi Algoritma RC4 + Pada Keamanan Sistem Komunikasi Chatting pada WEBSITE SAHEB*. *01*, 44–56.

Nur, Y., & Giawa, I. (2022). *Implementasi Algoritma RC4A Dalam Pengamanan Citra Digital*. *2*(1), 1–9. https://doi.org/10.47065/comforch.v2i1.348

Pasaribu, J. S. (2021). Pembuatan Aplikasi Pemesanan Banner Di Warna Print Kota Cimahi. *Jurnal Ilmiah Teknologi Infomasi Terapan*, *7*(2), 138–147. https://doi.org/10.33197/jitter.vol7.iss2.2021.551

Putra, P. (2024). *Implementasi Arsip Digital dalam Efisiensi Penyimpanan*. *1*, 1–13.

Putri, M. P. (2020). *Sistem Informasi Manajemen Proyek PT . Samudera Perkasa Konstruksi Berbasis Web*. *20*(1). https://doi.org/10.30812/matrik.v20i1.716

Ramalinda, D., & Raharja, A. R. (2024). *Strategi Perlindungan Data Menggunakan Sistem Kriptografi Dalam Keamanan Informasi*.

Saragi, D. R., Gultom, J. M., Tampubolon, J. A., & Gunawan, I. (2020). *Pengamanan Data File Teks (Word) Menggunakan Algoritma RC4*. *1*, 114–119. https://doi.org/10.30865/json.v1i2.1745

Satriadi, I., & Rahman, A. (2024). *Journal of Computer Networks , Architecture and High Performance Computing Electronic Archive Design With Rivest Cipher 4 Cryptographic Based File Security Journal of Computer Networks , Architecture and High Performance Computing*. *6*(1), 34–44.

Simamora, P., & Pasaribu, S. A. (2024). *Jurnal Sistem Informasi dan Teknologi Jaringan Kunci Simetris pada Perangkat IoT : Kajian Literatur*. *2*, 49–55.

Umam, C., Fadillah, D., Studi, P., Informatika, T., Komputer, F. I., Nuswantoro, U. D., & Berwarna, C. (2022). *Kombinasi Steganografi LSB dan Kriptografi AES dalam Sekuriti Teks Rahasia Pada Citra Berwarna*. *2*(1), 109–118.

Utami, T. P., & Firdaus, R. (2025). *Peran Sistem Informasi Manajemen dalam Meningkatkan Efisiensi Operasional dan Pengambilan Keputusan pada UMKM di Era Digital The Role of Management Information Systems in Improving Operational Efficiency and Decision-Making in MSMEs in the Digital Era*. 4129–4135.