

Keamanan data *Database* Pasien Klinik Pada Klinik Nehemia Dengan Metode RC4 berbasis Android

Jacob Chandra Sinaga¹, Ratih Puspasari²

^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: jacobbisa123@gmail.com

ABSTRAK

Klinik Nehemia adalah suatu instansi pelayanan kesehatan yang beralamat di Jl. Pelita IV No.1, Sidorame Tim., Kec. Medan Perjuangan, Kota Medan, Sumatera Utara 20236. Masalah keamanan informasi seringkali kurang mendapat perhatian dari pemilik dan pengelola sistem informasi, seperti sistem informasi untuk Klinik Nehemia, padahal masalah keamanan informasi memegang peranan penting dalam sistem informasi seiring dengan kemajuan teknologi. Masalah keamanan informasi merupakan salah satu aspek penting dari sistem informasi. Akibatnya, administrator dan pemilik sistem informasi harus memprioritaskan masalah keamanan ini dan memikirkan solusinya. Salah satu aspek keamanan data yang kurang mendapat perhatian adalah keamanan data pada sistem informasi pasien. Informasi pribadi pasien dirahasiakan dan tidak dapat diakses oleh orang lain. Di Klinik Nehemia, tidak ada keamanan data untuk melindungi dari masalah yang mungkin timbul karena hal ini menimbulkan ketidakpastian sistem *database* untuk mencegah pencurian data dan perubahan *database* yang berisi sistem informasi. Namun, terdapat banyak kerentanan di Klinik Nehemia yang dapat dimanfaatkan untuk mengubah hak akses database, seperti serangan URL dan teknik injeksi SQL, ancaman keamanan dan serangan siber, kebocoran data pasien, kehilangan data karena human error dan serangan insider (pegawai yang menyalahgunakan aksesnya).

Kata Kunci : Pasien, Keamanan data, Android, RC4

ABSTRACT

Nehemia Clinic is a health service institution located at Jl. Pelita IV No.1, Sidorame Tim., Kec. Medan Perjuangan, Medan City, North Sumatra 20236. Information security issues often receive less attention from owners and managers of information systems, such as the system for Nehemia Clinic, even though information security issues play an important role in information systems along with technological advances. Information security issues are one of the important aspects of information systems. As a result, administrators and owners of information systems must prioritize this security issue and think about solutions. One aspect of data security that receives less attention is data security in patient information systems. Patient personal information is kept confidential and cannot be accessed by others. At Nehemia Clinic, there is no data security to protect against problems that may arise because this causes intimidation of the database system to prevent data theft and changes to the database containing the information system. However, there are many vulnerabilities in Nehemia Clinic that can be exploited to change database access rights, such as URL attacks and SQL injection techniques, security threats and cyber attacks, patient data leaks, data loss due to human error and insider attacks (employees who abuse their access).

Keywords : Patients, Data security, Android, RC4

Info Artikel :

Disubmit: 12 Juni 2025

Direview: 05 Juli 2025

Diterima : 21 Agustus 2025

Copyright © 2025 – Journal UPU. All rights reserved.

1. PENDAHULUAN

Dalam kemajuan teknologi yang sangat cepat dan akurat telah mengalami perkembangan setiap informasi dalam bidang pendidikan untuk terus berusaha meningkatkan kemampuan dalam mengelola suatu data-data dan informasi yang aman dan efisien karena sangat dibutuhkan dalam bidang pendidikan. Penulisan sebuah informasi saat ini juga tidak lepas dari teknologi-teknologi kecanggihan yang ada pada

saat ini. Hal ini masih banyak dari pihak instansi yang belum menggunakan atau mengelola teknologi secara maksimal, yang dimana teknologi ini sangat berguna untuk memudahkan pihak sekolah dalam mengamankan data dan pasien, sehingga memudahkan pengurus dan petugas di Klinik Nehemia.

Klinik Nehemia adalah suatu instansi pelayanan kesehatan yang beralamat di Jl. Pelita IV No.1, Sidorame Tim., Kec. Medan Perjuangan, Kota Medan, Sumatera Utara 20236. Masalah keamanan informasi seringkali kurang mendapat perhatian dari pemilik dan pengelola sistem informasi, seperti sistem informasi untuk Klinik Nehemia, padahal masalah keamanan informasi memegang peranan penting dalam sistem informasi seiring dengan kemajuan teknologi. Setidaknya satu pengguna dan informasi dalam sistem ini harus dipahami oleh setidaknya satu orang agar selalu *up to date* agar terhindar dari berbagai resiko dan mencegah penyalahgunaan data oleh pihak yang tidak bertanggung jawab.

Masalah keamanan informasi merupakan salah satu aspek penting dari sistem informasi. Akibatnya, administrator dan pemilik sistem informasi harus memprioritaskan masalah keamanan ini dan memikirkan solusinya. Salah satu aspek keamanan data yang kurang mendapat perhatian adalah keamanan data pada sistem informasi pasien. Informasi pribadi pasien dirahasiakan dan tidak dapat diakses oleh orang lain. Di Klinik Nehemia, tidak ada keamanan data untuk melindungi dari masalah yang mungkin timbul karena hal ini menimbulkan ketidakpastian sistem *database* untuk mencegah pencurian data dan perubahan *database* yang berisi sistem informasi. Namun, terdapat banyak kerentanan di Klinik Nehemia yang dapat dimanfaatkan untuk mengubah hak akses database, seperti serangan URL dan teknik injeksi SQL, ancaman keamanan dan serangan siber, kebocoran data pasien, kehilangan data karena human error dan serangan insider (pegawai yang menyalahgunakan aksesnya). Penyerang dapat menambahkan pernyataan SQL sebagai bagian dari input, sumber data database, dan data harus diproses untuk membuat data dalam *database* lebih aman jika data langsung masuk ke *database* dan disaring dengan benar secara tidak langsung.

Keamanan komputer merupakan tindakan pencegahan dari serangan pengguna komputer atau pengakses jaringan yang tidak bertanggung jawab. Banyak yang belum mengetahui bahwa keamanan (*security*) merupakan sebuah komponen yang sangat penting. Bagi perancang dan pengelola sistem informasi, masalah keamanan sering menjadi masalah. (Abdul Kodir : 2021).

Diperlukan teknik untuk mengamankan data-data penting agar akses terhadap data tersebut dibatasi hanya kepada pihak yang berkepentingan. Berdasarkan cara kerjanya, algoritma kriptografi RC4 merupakan jenis stream cipher. Kelebihannya adalah dengan menggunakan cara ini enkripsi algoritma RC4 dapat dilakukan pada data dengan panjang yang beragam. Algoritma RC4 dinilai sangat cepat dalam prosesnya, kurang lebih 10 kali lebih cepat dari DES. Algoritma dari metode RC4 stream cipher ini terdiri dari dua bagian, yaitu: *key setup* dan *stream generation* (Muhammad Muid Maulana : 2020).

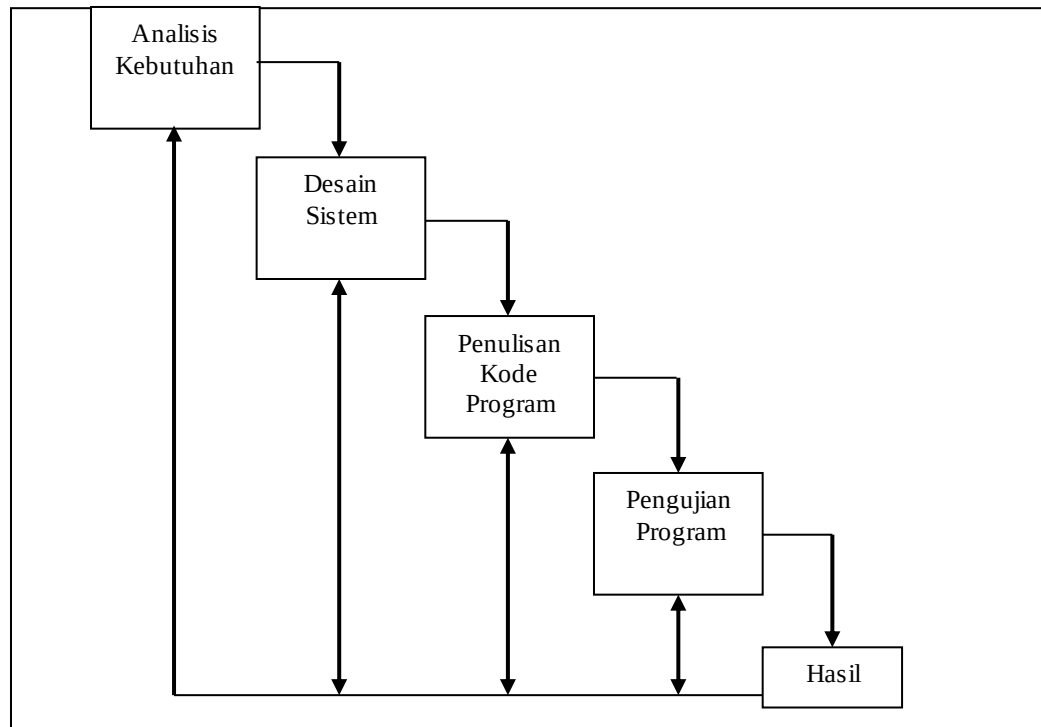
2. METODE

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

1. Pengamatan Langsung (*Observation*)
Peneliti melakukan pengamatan secara langsung pada Klinik Nehemia untuk mendapatkan data yang berkaitan dengan penelitian.
2. Wawancara (*Interview*)
Peneliti secara langsung bertatap muka dengan Personaloa Klinik Nehemia untuk mendapatkan data-data yang lebih lengkap tentang Implementasi Algoritma RC4 Dalam Keamanan data pasien klinik Pada Klinik Nehemia 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 yaitu data pasien klinik Andhika Medan.

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



Gambar 1. Diagram *Waterfall*

Keterangan :

1. Analisis Kebutuhan

Pada tahapan ini merupakan analisa terhadap kebutuhan yang diperlukan untuk mencapai tujuan penelitian yang akan dilakukan yaitu data pasien klinik pada Klinik Nehemia.

2. Desain Sistem

Desain sistem yang digunakan dalam teori adalah pemodelan UML yaitu *use case diagram*, *class diagram*, *activity diagram* dan *sequence diagram*.

3. Tools

Pada tahapan ini peneliti menggunakan *Android* dengan menggunakan *Android Studio*. Peneliti menggunakan *hardware* komputer/laptop. *Database* yang digunakan adalah *MySQL*.

4. Pengujian

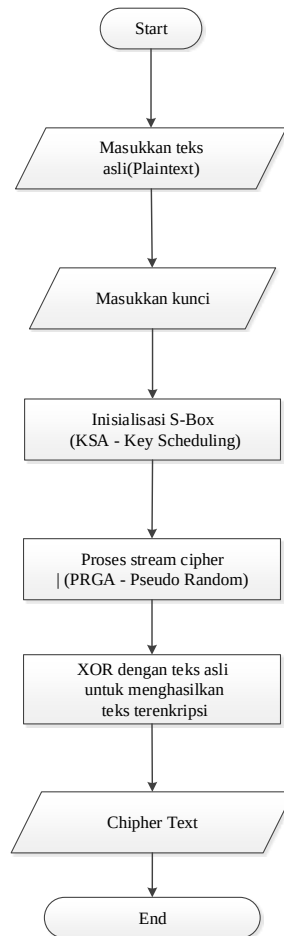
Pada tahapan ini peneliti menguji sistem yang telah dibuat menggunakan pengujian teori dan praktek. Pengujian teori peneliti menggunakan *blackbox testing*.

5. Hasil

Pada tahapan ini penelitian sudah selesai dibuat, hasil dari penelitian ini yaitu Algoritma RC4 Dalam Keamanan pasien klinik pada Klinik Nehemia Berbasis *Android*.

3. HASIL DAN PEMBAHASAN

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

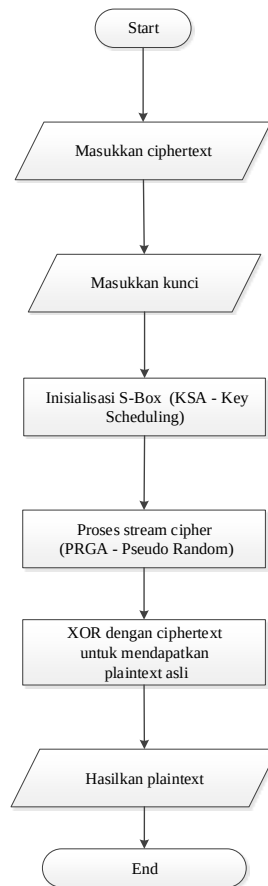


Gambar 2. Flowchart Enkripsi

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 :

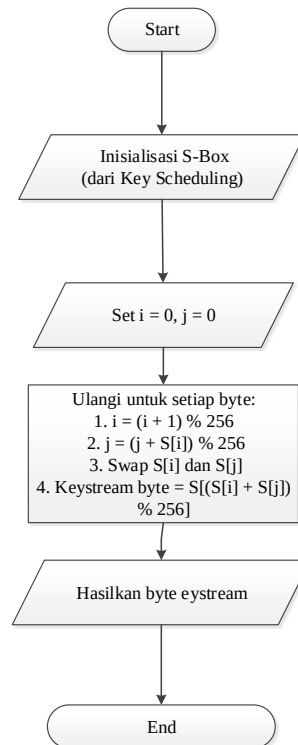


Gambar 3. Flowchart Dekripsi

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_PASIEN.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	$4 \oplus 161 = 165$
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.

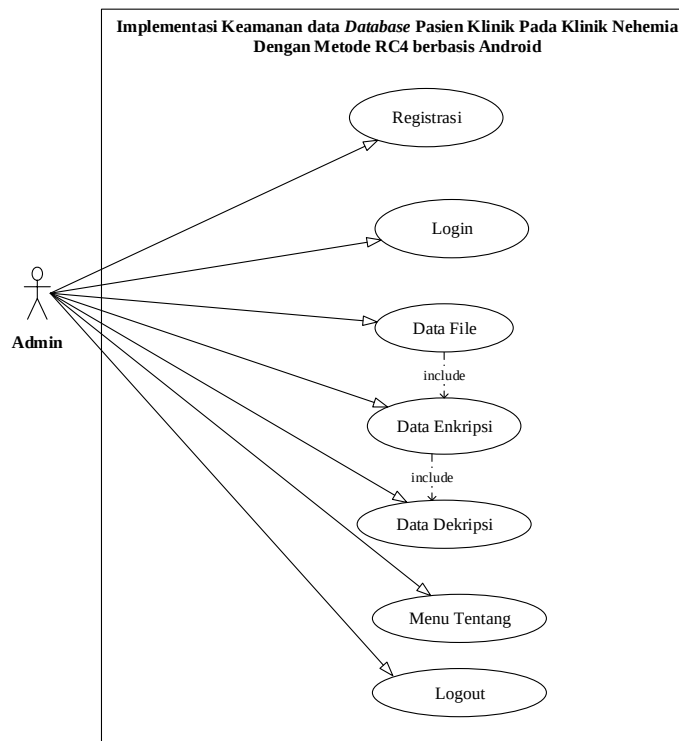
Tabel 2. Proses Dekripsi (XOR Ulang dengan Keystream)

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, 0, 0, 214, 10, 0, 0, 19, 0, 8, 2, 91, 67, 111, 110, 116, 101, 110, 116, 95, 84]

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 username* dan *password admin* program. Gambar tampilan *login* dapat ditunjukkan pada gambar 6 :



Gambar 6 Tampilan *Form Login*

2. Tampilan *Form* Data Menu utama

Form ini menampilkan pilihan data menu utama, ketika memilih data menu utama maka program akan menampilkan data menu utama. Gambar tampilan *form* data menu utama dapat pada gambar 7



Gambar 7. Tampilan *Form* Menu Utama

3. Tampilan *Form* Analisa metode

Tampilan ini merupakan tampilan *form* analisa metode yang berfungsi untuk mengisi data-data analisa metode. Berikut gambar *form* antrian ditunjukkan pada gambar 8:

Gambar 8. Tampilan *Form* Analisa Metode

4. Tampilan *Form* Pasien menu tentang

Tampilan ini merupakan tampilan *form* menu tentang yang berfungsi untuk mengisi data-data menu tentang. Berikut gambar *form* menu tentang ditunjukkan pada gambar 9 :



Gambar 9. Tampilan *Form* Menu Tentang

4. KESIMPULAN

Berdasarkan hasil pembahasan dan uji coba yang telah dilakukan yaitu Implementasi Keamanan data *Database* Pasien Klinik Pada Klinik Nehemia Dengan Metode RC4 berbasis Android, dapat disimpulkan :

1. Aplikasi Telah dibangun dan dapat menjaga keamanan data *database* pasien klinik pada Klinik Nehemia dengan system penyandian Metode RC4.
2. Sistem yang dibangun sudah mampu melakukan enkripsi dan dekripsi terhadap *database* pasien klinik pada Klinik Nehemia sehingga dapat Melindungi *database* pasien klinik pada Klinik Nehemia.
3. Sistem yang dibangun mempunyai tampilan yang sangat sederhana dan mudah digunakan oleh *user*.

UCAPAN TERIMA KASIH

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

REFERENSI

- [1] Anwar, B., Azanuddin, A., Nugroho, N. B., & Siregar, R. (2020). Aplikasi Pengamanan Dokumen Penjualan Tiket Pesawat Di Pt. Benua Raya Jaya Tour And Travel Menggunakan Metode Advanced Encryption Standard (AES). *J-SISKO TECH (Jurnal Teknologi Sistem Informasi Dan Sistem Komputer TGD)*, 3(1), 96. <https://doi.org/10.53513/jsk.v3i1.200>
- [2] Maulana, R., & Simanjorang, R. M. (2021). Implementasi Kriptografi Untuk Pengamanan Data Pribadi Siswa SMA Swasta Jaya Krama Beringin Dengan Algoritma RC4. *Jurnal Nasional Komputasi dan Teknologi Informasi*, 4(6), 377-383.

- [3] Maulana, M. M. I. (2022). KRIPTOGRAFI PENGAMANAN DATA CALON PENERIMA BANTUAN PADA KANTOR CAMAT, KECAMATAN KEDAI DURIAN DENGAN METODE RC4. *Jurnal Cyber Tech*, 2(12).
- [4] Hrp, M. H., Nugroho, N. B., & Ginting, R. I. (2022). Implementasi Keamanan Data Gaji Pada Dinas Komunikasi Dan Persandian Kabupaten Aceh Tamiang Menggunakan Algoritma RC4. *Jurnal Cyber Tech*, 1(4).
- [5] Adnan, M. R., & Fatimah, T. (2022, September). Pengamanan Data Laporan Keuangan Menggunakan Metode RC4 Pada Reddog Cabang Gading Serpong. In *Prosiding Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)* (Vol. 1, No. 1, pp. 230-239).
- [6] Efranda, N., Rusdiyanto, R., & Irvai, M. (2022). PERANCANGAN SISTEM INFORMASI PENGOLAHAN DATA NILAI SMPN PURWODADI BERBASIS WEB MOBILE DENGAN ENKRIPSI RC4. *Jurnal Teknologi Informasi Mura*, 14(1), 28-37.
- [7] Hermiati, R., Asnawati, A., & Kanedi, I. (2021). Pembuatan E-Commerce Pada Sistem Komputer Menggunakan Bahasa Pemrograman Php Dan Database Mysql. *Jurnal Media Infotek*, 1(1), 54–66. <https://doi.org/10.37676/jmi.v1i1.1317>
- [8] Janis, J. W., Mamahit, D. J., Sugiarto, 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>
- [9] Kadek, N., Dewi, C., Bagus, I., Anandita, G., Atmaja, K. J., Aditama, P. W., & Magister, P. S. (2020). Rancang Bangun Aplikasi Mobile Siska Berbasis Android. In *SINTECH Journal | 100 SINTECH JOURNAL* (Vol. 1, Issue 2). Online. <http://jurnal.stiki-indonesia.ac.id/index.php/sintechjournal>
- [10] Listianto, F., Fauzi, Irviani, R., Kasmi, & Garaika. (2020). Konveksi Seragam Drumband Di Pekon Klaten Gadingrejo Kabupaten Pringsewu Program Studi Manajemen , STIE Trisna Negara , OKU Timur. *Jurnal TAM(Technology Acceptance Model)*, 8(2), 146–152.
- [11] Suparman, B. (2022). Aplikasi Pengamanan Data Menggunakan Kriptografi Dengan Metode Wake dan Algoritma Des Bebasis Java Desktop. *OKTAL: Jurnal Ilmu Komputer Dan Sains*, 1(07), 808–817. <https://journal.mediapublikasi.id/index.php/oktal/article/view/777%0Ahttps://journal.mediapublikasi.id/index.php/oktal/article/download/777/304>