JURNAL NUANSA INFORMATIKA p-ISSN : 1858-3911, e-ISSN : 2614-5405
Volume 15 Nomor 1, Januari 2021 https://journal.uniku.ac.id/index.php/ilkom

IMPLEMENTATION OF THE RSA CRYPTOGRAPHIC ALGORITHM IN THE QR-CODE ANDROID-BASED BUILDING PERMIT CHECKING APPLICATION

Darsanto[1], Rio Andriyat Krisdiawan[2], Dias Eka Prayuda[3]
[1]Teknik Komputer Fakultas Teknik Universitas Wiralodra
[23]Teknik Informatika Fakultas Ilmu Komputer Universitas Kuningan
[1]Jln. Ir. H. Juanda Km.3 Indramayu
[23]Jln. Cut Nyak Dhien No.36A, Cijoho, Kuningan, Jawa Barat 45513
Email: [1]shantost.ft@unwir.ac.id, [2]rioandriyat@uniku.ac.id, [3]prayudadias20@gmail.com

Abstrak

Dinas penanaman modal dan pelayanan terpadu satu pintu (DPMPTSP) kabupaten Kuningan mengeluarkan berbagai macam izin, salah satu izin bangunan adalah izin mendirikan bangunan (IMB) yang di keluarkan oleh dinas penanaman modal dan pelayanan terpadu satu pintu pada pihak pemohon. Penelitian dilatarbelakangi oleh rawannya pemalsuan izin yang sudah di berikan dinas penanaman modal dan pelayanan terpadu satu pintu. Tujuan dari penelitian ini yaitu membuat sistem atau teknologi informasi yang dapat membantu untuk mempermudah pengecekan izin bangunan, salah satunya dengan menggunakan teknologi *QR-Code*. Sistem ini dapat memindai kode yang telah dienkripsi dengan algoritma RSA sehingga kode yang di buat tidak mudah di palsukan atau di baca dengan aplikasi sejenisnya. Algoritma Kriprografi RSA, Algoritma yang digunakan untuk mengenkripsi dan mendekripsi data. Algoritma RSA itu sendiri merupakan algoritma asimetris, sehingga memiliki kunci public dan kunci privat. RSA memiliki dasar proses enkripsi dan dekripsinya pada konsep bilangan prima dan aritmatika modulo. Kunci dekripsi dan enkripsi keduanya merupakan bilangan bulat. Kunci enkripsi tidak dirahasiakan dan diketahui oleh umum sehingga kunci enkripsi biasa disebut juga dengan kunci publik, namun kunci untuk dekripsi bersifat rahasia.

Kata Kunci : DPMPTSP, QR-Code, Algoritma Kriptrografi RSA

Abstract

The investment office and one-stop integrated service (DPMPTSP) of Kuningan regency issues various kinds of permits, one of which is a building permit (IMB) issued by the investment office and one-stop integrated service on the applicant's side. Research is motivated by the vulnerability of counterfeiting permits that have been granted by the investment service and one-stop integrated services. The purpose of this research is to create a system or information technology that can help to make it easier to check building permits, one of which is by using QR-Code technology. This system can scan code that has been encrypted with the RSA algorithm so that the code created is not easily faked or read with similar applications. RSA Cryptography Algorithm, an algorithm used to encrypt and decrypt data. The RSA algorithm itself is an asymmetric algorithm, so it has a public key and a private key. RSA has a basic encryption and decryption process in the concepts of prime numbers and modulo arithmetic. The decryption and encryption keys are both integers. The encryption key is not kept secret and is known to the public so that the encryption key is also known as the public key, but the key for decryption is secret.

Keywords*: DPMPTSP, QR-Code, RSA Cryptrographic Algorithm*

p-ISSN : 1858-3911, e-ISSN : 2614-5405
https://journal.uniku.ac.id/index.php/ilkom

1. PENDAHULUAN

Seiring kemajuan teknologi yang semakin pesat diberbagai bidang, termasuk bidang elektronika, kebutuhan akan kemudahan dan kenyamanan dalam pengontrolan atau pengecekan yang akan dilakukan oleh petugas agar lebih mudah, khusunya pengontrolan dan pengecekan ijin pada bangunan.

Untuk izin di Kabupaten Kuningan di atur dalam Peraturan Bupati Kuningan Nomor 14 Tahun 2018 yang mengatur tentang Pendelegasian Sebagian Kewenangan di Bidang Perizinan dan Nonperizinan kepada Kepala Dinas Penanaman Modal dan Pelayanan Terpadu Satu Pintu Kabupaten Kuningan(DPMPTSP). Dinas Penanaman Modal dan Pelayanan Terpadu Satu Pintu(DPMPTSP) mengeluarkan berbagai macam izin baik izin mendirikan bangunan maupun izin nonbangunan.salah satu izin adalah izin mendirikan bangunan(IMB) yang di keluarkan oleh Dinas Penanaman Modal dan Pelayanan Terpadu Satu Pintu pada pihak pemohon. Untuk mendapatkan izin pemohon harus meliputi persyaratan administratif dan persyaratan teknis, persyaratan administratif meliputi data pemohon dan persyaratan teknis meliputi data tanah, Setelah semua syarat terpenuhi maka pihak dari Dinas Penanaman Modal dan Pelayanan Terpadu Satu Pintu(DPMPTSP) dapat menyerahkan SK kepada pemohon.[1]

Di Kabupaten Kuningan pengecekan pada ijin bangunan yang sudah terdaftar pada dinas penanaman modal dan terpadu satu pintu(DPMPTSP) masih menggunakan manual atau belum menggunakan teknologi, untuk memudahkan pengecekan atau pengontrolan dan meminimalisir rawannya pemalsuan izin yang sudah diberikan oleh dinas penanaman modal dan terpadu satu pintu (DPMPTSP) agar tidak disalahgunakan untuk kepentingan-kepentingan oknum-oknum yang tidak bertanggungjawab untuk kepentingan sendiri dan tentu saja merugikan berbagai pihak terutama kedinasan dan juga masyarakat.Untuk menghilangkan kekhawatiran akanizin mendirikan bangunan maka harus adanya sistem atau teknologi informasi yang dapat membantu untuk pengecekan izin mendirikan bangunan salah satunya dengan menggunakan teknologi *QR Code*.

QR Code adalah perkembangan dari barcode atau kode batang yang hanya mampu menyimpan informasi secara horizontal sedangkan *QR Code* mampu menyimpan informasi lebih banyak, baik secara horizontal maupun verticalmisalnya dalam bentuk URL, teks, angka, dll [2]. Kode tersebut bisa berupa kode ujian, ataupun kode-kode yang lainnya yang perlu untuk diamankan, untukitu diperlukan sebuah metode khusus dalam pengamanannya agar dapat meningkatkan kerahasiaan informasi. Ada beberapa upaya dalam meningkatkam kerahasiaan informasi salah satunya adalah dengan pengimplementasian algoritma Kriptografi *RSA*.[3]

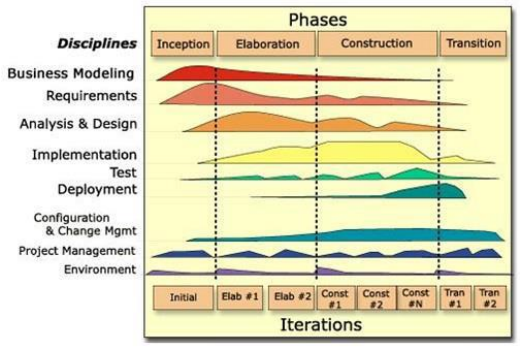
2. METODE PENELITIAN

2.1 Metodologi Pengembangan Perangkat Lunak

Metode pengembangan sistem yang digunakan dalam perancangan aplikasi perangkat lunak ini menggunakan metode RUP (Rational Unified Process). RUP adalah pendekatan pengembangan perangkat lunak yang dilakukan berulang-ulang (iterative), focus pada arsitektur (architecture-centric), lebih diarahkan berdasarkan

p-ISSN : 1858-3911, e-ISSN : 2614-5405
https://journal.uniku.ac.id/index.php/ilkom

penggunaan kasus (use case driven)[4]. Tahapan metode RUP dapat dilihat pada gambar 1.



Gambar 1. Tahapan Metode RUP

1. Inception

Tahap ini merupakan tahap untuk menentukan ruang lingkup proyek, memodelkan proses bisnis yang akan digunakan dan mendefinisikan kebutuhan sistem yang akan dibuat. Pada tahap ini penulismelakukan observasi ke Dinas Penanaman Modal dan Pelayanan Terpadu Satu Pintu serta melakukan wawancara kebagian perizinan untuk mengetahui lebih dalam tentang izin bangunan. Data dan informasi tersebut kemudian menjadi acuan untuk perancangan aplikasi yang akan dibuat.

2. Elaboration

Pada tahap ini penulis dapat melakukan identifikasi masalah pada sistem yang dibuat. Di dalam elaboration terdapat dua tahapan itu :

a. Analisis

Terdapat tiga fase, dalam tahapan sistem pada jalur pengembangan sistem RUP yaitu : analisis permasalahan, analisis persyaratan dan analisis keputusan.

b. Perancangan

Pada tahap perancangan terdiri dari : perancangan aplikasi menggunakan diagram UML meliputi use case diagram, diagram activity, class diagram, scenario, sequence.

3. Construction

Pada fase konstruksi mulai dilakukan sederetan iterasi yang melibatkan beberapa proses seperti analisa desain, implementasi kode program terhadap perangkat lunak dan testing (pengujian). Fase ini merupakan fase utama dimana aplikasi dibangun mulai dari perancangan sampai aplikasi di uji.Iterasi dimaksudkan untuk memperbaiki unit dari aplikasi apabila terjadi kesalahan dan memerlukan perbaikan.

4. Transition

Fase terakhir dari metode RUP adalah fase peralihan dimana pada fase ini semua proses yang telah dimodelkan akan menjadi suatu produk serta melakukan beberapa fase tambahan seperti melakukan pengujian terhadap aplikasi beta dan membuat dokumentasi tambahan seperti pengujian langsung oleh calon pengguna aplikasi untuk mendapatkan informasi apabila perbaikan sewaktu-waktu diperlukan.Tahap ini lebih pada deployment atau instalasi sistem agar dapat dimengerti oleh pengguna.

2.2 Algoritma *Kriptografi RSA*

Algoritma yang digunakan untuk mengenkripsi dan mendekripsi data adalah algoritma kriptografi RSA. Algoritma RSA itu sendiri merupakan algoritma asimetris, sehingga memiliki kunci *public* dan kunci *privat*.

RSA memiliki dasar proses enkripsi dan dekripsinya pada konsep bilangan prima dan aritmatika modulo. Kunci dekripsi dan enkripsi keduanya merupakan bilangan bulat. Kunci enkripsi tidak dirahasiakan dan diketahui oleh umum sehingga kunci enkripsi biasa disebut juga dengan kunci

p-ISSN : 1858-3911, e-ISSN : 2614-5405
https://journal.uniku.ac.id/index.php/ilkom

publik, namun kunci untuk dekripsi bersifat rahasia. Kunci deskripsi dibangkitkan dari beberapa buah bilangan prima bersama-sama dengan kunci enkripsi. Semakin besar bilangan non primanya maka semakin sulit pemfaktorannya. Semakin sulit pemfaktorannya, maka semakin kuat algoritma RSA-nya[5].

Algoritma pembangkitan kunci dalam algoritma RSA dapat dijelaskan sebagai berikut[5] :

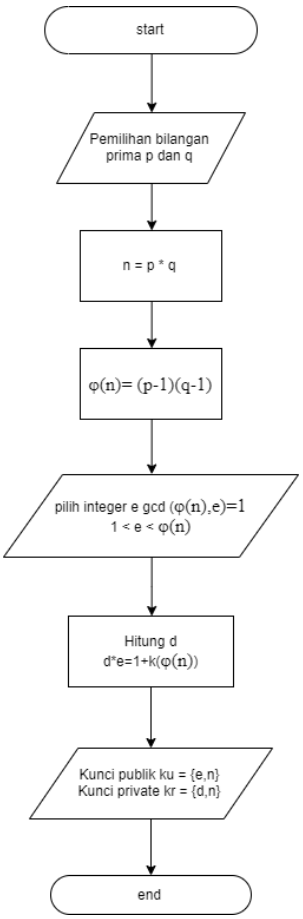
1. Dipilih dua bilangan prima $p \neq q$ secara acak dan terpisah untuk tiap-tiap p dan q.
2. Hitung N dengan persamaan: N = p q.
3. Hitung φ dengan persamaan: φ = (p-1)(q-1).
4. Dipilih bilangan bulat (*integer*) antara satu dan φ ($1 < e < \varphi$) yang juga merupakan *coprime* dari φ.
5. Hitung d dengan persamaan : $de \equiv 1 \pmod{\varphi}$.

Hasil dari algoritma ini:

Kunci *public* : pasangan (N,e)

Kunci *privat* : pasangan (N,d)

Flowchart pembangkitan kunci algoritma kriptografi RSA dapat dilihat pada gambar 2. berikut :



Gambar 2. Flowchart Pembangkitan Kunci Algoritma RSA

Contoh Perhitungan :

1. Dipilih bilangan prima p = 47 dan q = 71
2. Hitung nilai N dengan rumus: N = p . q = 3337
3. Hitung nilai φ (N) dengan persamaan: φ (N)= (p – 1)(q – 1) = 3220.
4. Dipilih e = 79,
5. Maka d = 1019

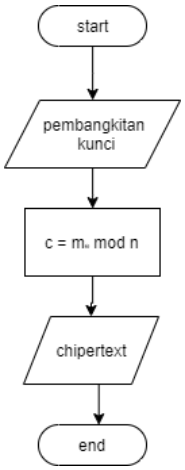
Algoritma enkripsi yang digunakan dalam algoritma RSA dapat dijelaskan sebagai berikut :

1. Disusun *plaintext* menjadi blok-blok m1, m2, …, mi
2. Hitung *ciphertext* ci dengan rumus : Ci = Mie mod N

Flowchart proses enkripsi algoritma kriptografi RSA dapat dilihat pada

p-ISSN : 1858-3911, e-ISSN : 2614-5405
https://journal.uniku.ac.id/index.php/ilkom

Gambar 3 :

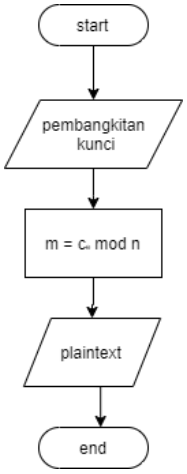


Gambar 3. Flowchart Enkripsi Algoritma RSA

Algoritma dekripsi yang digunakan dalam algoritma RSA dapat dijelaskan sebagai berikut :

1. Gunakan kunci *privat* untuk menghitung Mi = Ci *d* mod N
2. Carilah nilai m dengan rumus : Mi = Ci *d* mod N

Flowchart proses dekripsi algoritma kriptografi RSA dapat dilihat pada gambar 4.



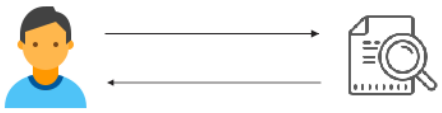
Gambar 4. Flowchart Dekripsi Algoritma RSA

3. HASIL DAN PEMBAHASAN

3.1. Analisis Sistem

Aplikasi yang akan ini di rancang bertujuan untuk memberikan kemudahan dalam pengecekan IMB berdasarkan data yang mana di dalam program yang di buat akan dapat memberi kemudahan untuk pengecekan IMB.

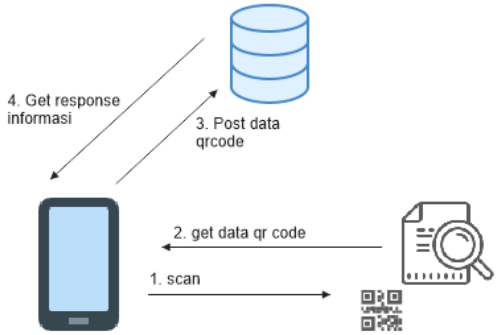
Tahap ini mempelajari dan mengevaluasi sistem yang sedang berjalan di institusi tersebut. adapun hal hal yang dilakukan dalam menganalisa sistem yang sedang berjalan tersebut dengan meneliti hal hal yang berhubungan dengan proses pengelolahan data. Berikut gambar 5. yang menunjukan hasil Analisis sistem yang sedang berjalan :



Gambar 5. Rich picture sistem yang sedang berjalan

Dari rich picture sistem yang sedang berjalan diatas menunjukan bahwa surat izin dicek secara manual dengan mengecek nomor surat izin pada surat izin yang ditunjukan di arsip DPMPTSP, kelemahan dari sistem yang sedang berjalan yaitu surat izin mudah dipalsukan seperti halnya membuat duplikasi surat yang semirip dengan surat izin yang resmi.

3.2. Analisis Sistem Yang Di Usulkan



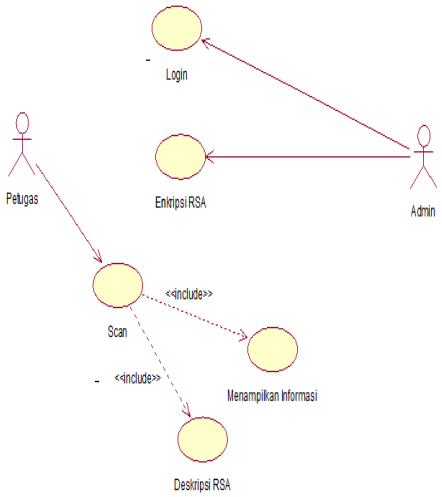
Gambar 6. Rich picture analisis sistem yang diusulkan

p-ISSN : 1858-3911, e-ISSN : 2614-5405
https://journal.uniku.ac.id/index.php/ilkom

Dari gambat rich picture yang di usulkan dapat dilihat bahwa surat izin akan memiliki barcode resmi yang dapat dicek melalui aplikasi android yang telah terhubung dengan data surat yang ada database sehingga dapat menghindari duplikasi surat / pemalsuan surat.

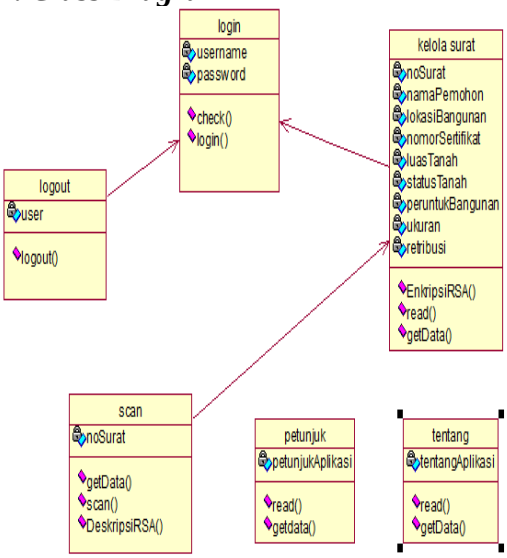
3.3. Perancangan Sistem

1. Use Case Diagram



Gambar 7. Use Case Diagram Aplikasi Pengecekan IMB

2. Class Diagram



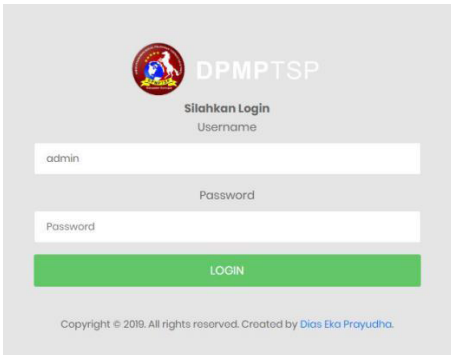
Gambar 8. Class Diagram

3.4. Implementasi Perangkat Lunak

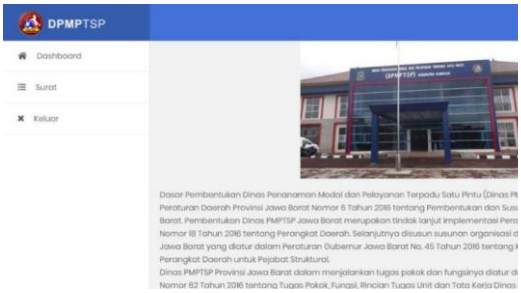
Perangkat lunak merupakan penghubung antara pengguna sistem dengan perangkat keras, perangkat lunak yang digunakan penulis adalah sebagai berikut :

1. Sistem Operasi Windows 10 64bit
2. Android Studio 3.2.1
3. JDK Versi 1.8.0
4. SDK dan Emulator MEMU

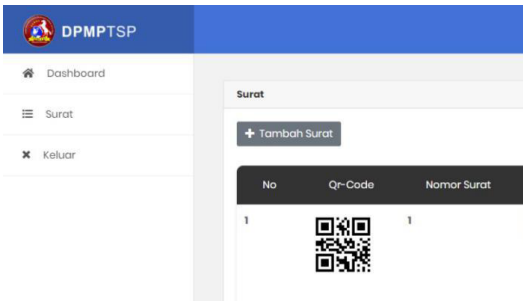
a. Interface Web Administrator



Gambar 9. Login Web Administrator



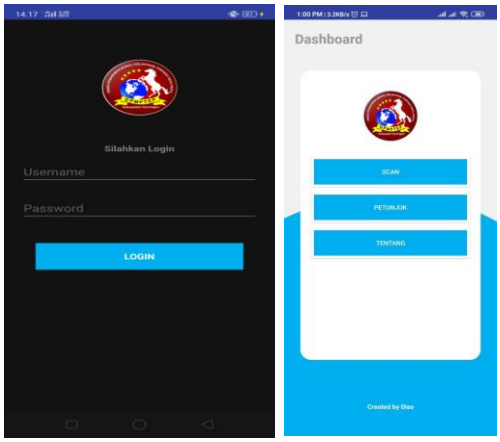
Gambar 10. Dashboard Web Administrator



Gambar 11. Kelola Surat Web Administrator

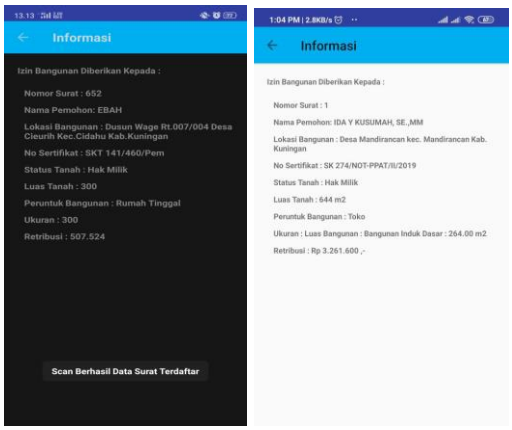
b. Interface Aplikasi Android

p-ISSN : 1858-3911, e-ISSN : 2614-5405
https://journal.uniku.ac.id/index.php/ilkom



Gambar 12. Tampilan Aplikasi Android User

Gambar 13. Tampilan Menu Scan Surat



Gambar 14. Hasil Scan Informasi

4. KESIMPULAN

1. Sistem dapat membantu pengguna untuk memberi keamanan pada surat izin.
2. Sistem ini dapat memindai / scan Qrcode pada surat izin DPMPTSP.
3. Sistem ini dapat mengenkripsi dan deskripsi nomor surat pada qrcode dengan menggunakan Algoritma RSA.
4. Kelebihan sistem yang dibuat dengan sistem lainnya adalah sistem ini dapat memindai qrcode yang telah dienkripsi dengan Algoritma RSA, sehingga Qrcode yang dibuat tidak mudah dipalsukan atau dibaca dengan aplikasi sejenisnya.

5. SARAN

Adapun saran-saran yang ingin disampaikan untuk pengembangan lebih lanjut adalah sebagai berikut.

1. Penulis mengharapkan adanya pengembangan aplikasi oleh mahasiswa lainnya agar tercipta aplikasi yang lebih baik lagi di kemudian hari.
2. Penulis mengharapkan pengembang kedepannya dapat menambahkan menambahkan fitur seperti cetak surat izin di web administrator sehingga lebih memudahkan user.
3. Penulis mengharapkan aplikasi ini dapat dibangun dengan sistem operasi ios sehingga tidak hanya dapat berjalan diaplikasi android saja.

DAFTAR PUSTAKA

[1] G. S. Rahman, H. Bekti, and M. . E. Munajat, “Kualitas Pelayanan Izin Mendirikan Bangunan (IMB) Di Dinas Penanaman Modal Pelayanan Terpadu Satu Pintu (DPMPTSP) Kabupaten Ciamis,” *J. Manaj. Pelayanan Publik*, 2019, doi: 10.24198/jmpp.v2i2.21405.

[2] H. A. Gunawan, Z. Arifin, and I. F. Astuti, “Keamanan Login Web Menggunakan Metode 3Des Berbasis Teknologi Quick Response Code,” *Inform. Mulawarman J. Ilm. Ilmu Komput.*, 2014.

p-ISSN : 1858-3911, e-ISSN : 2614-5405
https://journal.uniku.ac.id/index.php/ilkom

[3] R. Munir, "Algoritma Enkripsi Citra Digital Dengan Kombinasi Dua Chaos," *Chaos*, 2012.
[4] M. A.S Rosa dan Shalahuddin, "UML, Use Case Diagram, Activity Diagram, Class Diagram," in *Rekayasa Perangkat Lunak Terstruktur*, 2013.
[5] J. Teknik, I. Fakultas, and S. Dan, "IMPLEMENTASI ALGORITMA RC4 PADA APLIKASI SMART CARD LAYANAN TRANSAKSI PEMINJAMAN," 2014.