JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 4, Nomor 4, Oktober 2020, Page 898-903
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI 10.30865/mib.v4i4.2256

Implementasi Enkripsi-Dekripsi dengan Algoritma RC2 Menggunakan Java

Muhammad Iqbal Assegaf*, Rahma Destias, Nidhea Sitaresmi, Yudi Wiharto

Fakultas Teknologi Informasi, Universitas Budi Luhur Jakarta, Indonesia,
Email: [1,*]1711500890@student.budiluhur.ac.id, [2]1711500254@student.budiluhur.ac.id,
[3]1711503019@student.budiluhur.ac.id, [4]yudi.wiharto@budiluhur.ac.id
Email Penulis Korespondensi: 1711500890@student.budiluhur.ac.id

Abstrak−Kriptografi merupakan salah satu cara yang digunakan untuk mengamankan data. Untuk itu perlunya sebuah keamanan data dengan cara enkripsi dan dekripsi suatu data menggunakan kriptografi algoritma *Rivest Code 2* (RC 2). Dalam kriptografi algoritma *Rivest Code 2* (RC 2), dirancang dalam pemrograman java netbeans yang diantaranya adalah kemampuan untuk beroperasi langsung untuk diimplementasikan dengan mode algoritma RC 2. Spesifikasi arsitektur dan bahasa yang menjadi tempat inplementasi algoritma yang ditentukan belum mendukung pengoperasian 64 bit yang mudah.sebab karna itu dari pada menggunakan 2 register 64 bit seperti pada RC2, RC2 menggunakan 4 register 32 bit. Karena menggunakan 4 register maka akan terdapat 2 operasi rotasi pada setiap *half-round* yang ada, dan juga akan lebih banyak bit-bit yang digunakan untuk mempengaruhi banyaknya bit yang dirotasi. Operasi perkalian ini sangat efektif dalam menghasilkan efek *diffusion* atau penyebaran yang tentu saja mengakibatkan RC2 lebih aman. Aplikasi yang dihasilkan menggunakan Bahasa pemograman java yang cukup mudah untuk digunakan.

Kata Kunci: Kriptografi, Rivest Code 2(RC 2), Keamanan Data, Enkrip, Dekrip, Algoritma.

Abstract−Cryptography is a security tool used to hide a message. For that we need a security by means of encryption and decryption of data using cryptographic algorithms Rivest Code 2 (RC2). In the cryptographic algorithms Rivest Code 2 (RC2), designed in java programming netbeans which include the ability to operate directly for RC2 algorithm implemented by mode. Specifications architectures and languages into a specified algorithm implementation does not yet support 64-bit operating efficiently. Therefor, instead of using two 64-bit registers as in RC2, RC2 uses four 32-bit registers. Because it uses four registers there will be two rotation operation on each half-round there, and it will also be a lot of bits that will be used to affect the number of bits that are rotated. This multiplication operation is very effective in producing the effect of diffusion or which of course resulted in the deployment of more secure RC2. Android-based application that is generated by utilizing the latest technology.

Keywords: Cryptography, Rivest Code 2 (RC2), Data Security, Encryption, Decryption, Algorithm

1. PENDAHULUAN

Dunia teknologi informasi semakin berkembang dengan cepat dan pesat sehingga banyak informasi yang bermuculan baik informasi yang bisa dipusblikasikan dan dirahasiakan . dalam banyak kasus permasalahan data dan informasi yang sangat rahasia dapat diambil dan dimanfaatkan oleh pihak yang bertanggung jawab , oleh sebab itu penting bagi kita mempelajari tentang pengamanan data. Keamanan menjadi aspek yang sangat penting saat ini dimana pertukaran data dan informasi menjadi tuntutan baik pekerjaan dan lainya.Berbagi cara dilakukan untuk mengamankan data atau informasi. Berdasarkan masalah diatas dapat kita simpulkan dengan menggunakan sebuah Teknik yang berguna untuk mengamankan data atau informasi. Pengamanan tersebut bernama Kriptografi, Kriptografi adalah ilmu yang mempelajari Teknik matetmatis yang berhubungan dengan aspek keamanan informasi seperti tingkat keyakinan,Integritas data,autentikasi keaslian data[1].

Kriptografi merupakan bagian ilmu yang mempelajari tentang cara menjaga agar data atau pesan aman.berbagai macam teknik digunakan untuk upaya mengamankan data informasi yang sangat penting[2].Teknik yang digunakan dalam kriptografi adalah mengubah algoritma matematika dengan tujuan kerahasiaan , integritas data, autentikasi dan *non*-repudiasi[3]. Banyak sekali metode kriptografi yang bisa digunakan seperti RSA, RC2, RC4, RC5, RC6, DES, AES dan lain sebaginnya.

Dari sekian banyak algoritma pengkodeaan salah satunnya yaitu algoritma RC2,algoritma ini merupakan salah satu generasi awal seblum algoritma RC4 maupun RC6 algoritma ini bersifat simetris artinya kunci untuk mengenkripsi sama dengan kunci untuk mendeskripsi algoritam RC2 ini muncul karna pasaat itu algoritma DES yang merupakan algoritma standar baku sudah mulai banyak ditebus para *Hacker*[4]. Metode enkripsi RC2 sangat cepat kurang lebih 10 kali lebih cepat dari DES,Menurut hasil pengetesan kecepatan algoritma RC2 adalah 5380,035 Kbytes/detik pada Pentium 1333 memori 16 MB pada windows 95[5]. Kriptografi dapat diimplementasikan menggunakan java yang disebut JCA atau *Java Cryptography architecture* merupakan sejumlah API yang dipakai untuk mengimplementasikan konsep-konsep kriptografi modern seperti sidik digital, *message* digest, sertifikat, enkripsi, pembangkitan dan manajemen kunci, pembangkitan bilangan acak yang aman dan seterusnya[6].

Tujuan dari penelitiaan ini berguna untuk menganalisis bagaimana cara kerja kriptografi RC2 berbasis java dalam layanan keamanan data, memberi pemahaman bagaimana algoritma enkripsi RC2 melakukan proses enkripsi dan dekripsi serta membangun sutu program yang dapat menjaga keamanan data menggunakan algoritma kriptografi RC2 berbasis java.

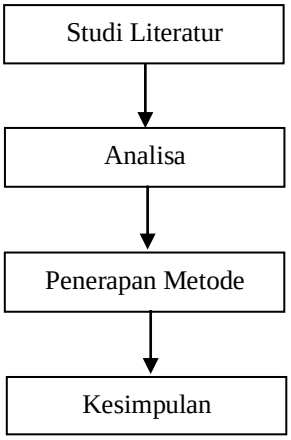
Submitted: **04/06/2020**; Accepted: **16/08/2020**; Published: **20/10/2020**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 4, Nomor 4, Oktober 2020, Page 898-903
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI 10.30865/mib.v4i4.2256

2. METODOLOGI PENELITIAN

2.1 Tahapan Penelitian

Metode ini digunakan untuk pedoman, dalam pelaksanaan penelitiaan agar hasil yang dicapi tidak menyimpang dari tujuan yang dilakukan sebelumnya. Tahapan yang akan dilakukan dalam metode penilitiaan dapan dilihat pada gambar 1.

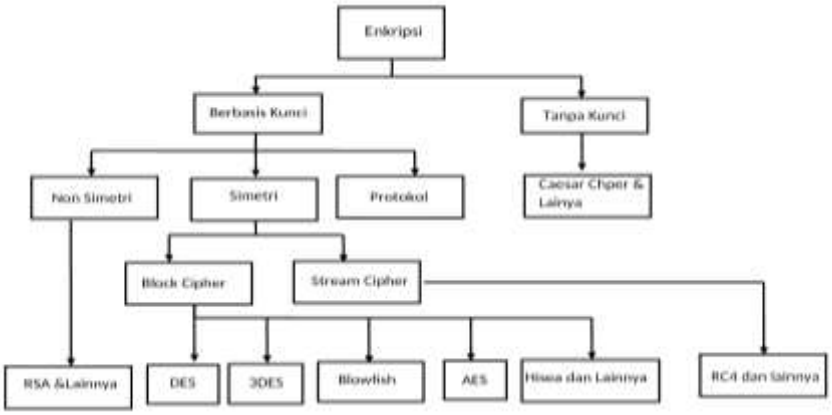


Gambar 1. Diagram tahapan penelitian

2.2 Kriptografi

Kriptografi Merupakan sebuah seni dan ilmu yang menciptakan sebuah system kripto yang mampu menyediakan keamanan informasi, dan berkaitan erat dengan pengamanaan data digital. Ilmu ini terdiri dari mekanisme perancangan yang didasarkan pada algoritma matematik yang menawarkan sejumlah keamanan informasi fundamental. Kebalikan dari kriptografi adalah kriptanalis, yang merupakan seni dan ilmu dalam membongkar teks *chipper*.Kriptanalis sering kali dipakai untuk mempelajari kekuatan keamanan dari rancangan atas sebuah teknik kriptografi yang baru [7]

Metode kriptografi terdiri dari dua yaitu berbasisi kunci dan tanpa kunci, kemudiaan dari pembagiaan ini diturunkan menjadi banyak metode yang di temukan oleh beberapa perusahaan dan peneliti keamanan[8]



Gambar 2. Algoritma Kriptografi Enkripsi Populer (Faheem et.al.,2017)

Menurut Maltius Celcius Sinaga yang di tuliskan pada bukunya yang berjudul Kriptogarfi python mengatakan bahwa Kriptografi merupakan cabang teknik, namun tidak biasa hal ini berkaitan dengan tentangan yang aktif, pintar dan jahat. Teknik jenis lain (seperti Teknik kima dan sipil) hanya mentuhkan gaya natural netral.Terdapat juga riset berkebang yang memebriksa hubungan antara masalah kriptografi dan fisika kuantum[9].

2.3 Algoritma RC2

RC 2 adalah blok chipper didesain oleh Ron Rivest pada tahun 1987. Pengembang RC2 disponsori oleh Lotus yang sedang mencari suati *chipper* setelah evaluasi oleh NSA untuk diekspor sebagai bagian dari softwarrLotus Notes. Setelah negosiai lanjut, cippher ini disetujui dan diekspor pada tahun 1989,sperti diketahui pembatasan kunci untuk ekspor kriptografi oleh pemerintah AS hanya sebesar 40 bit. Semua ini termuat dalam *export regulations for cryptograph*(10). RC 2 adalah *chipper* blok yang menggunkan 64 bit sebagai ukuran per bloknya

Submitted: **04/06/2020**; Accepted: **16/08/2020**; Published: **20/10/2020**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 4, Nomor 4, Oktober 2020, Page 898-903
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI 10.30865/mib.v4i4.2256

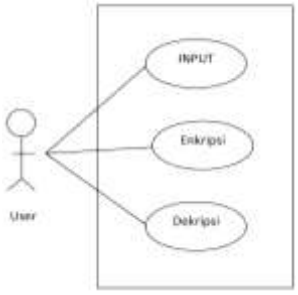
dengan kunci yang ukuranya bervariasi (0-124 bit). Dengan mengubah ukuran kunci ini, performasi RC 2 dapat menjadi 2 atau 3 kali baik dibandi DES (*Data Encryption Standart),*algoritma yang dikembangkan oleh NSA (*National Security Agent* dan telah ditetapkan sebagi algoritma enkripsi standart oleh pemerintah AS pada tahun 1976-1997 (yang kemudiaan digantikan oleh AES, *Advanced Encryption Standard*) [11]. Ada dua tahapan untuk pembangkitan aliran kunci algorithma RC 2 yaitu Key Scheduling Algorithm (KSA) dan Pseudo Random Generator Algorithm (PRGA). Key Scheduling Algorithm (KSA) merpakan tahapan pemberian nilai awal berdasarkan kunci enkripsi. State dari nilai awal tersebut berupa array dengan representasi permutasi 256 byte (dengan indeks 0 sampai dengan 255) dinamakan array S menggunakan rentang tersebut karena RC2 mengenkripsi pada mode byte (255 = 2^8 dan 8 bit = 1 byte). Artinya maksimal panjang kunci yang dapat tersimpan pada array U adala 256 karakter.

3. HASIL DAN PEMBAHASAN

3.1 Perancangan Sistem

a. ***Usecase***

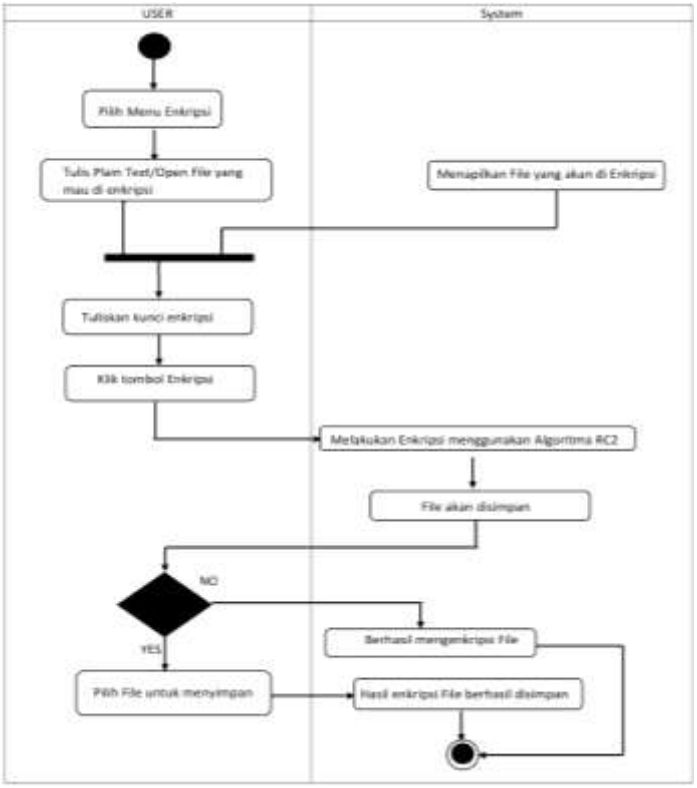
Sesuai dengan namanya diagram ini dapat digunakan untuk menggambarkan penggunan dari system atau product[12].dapat kita lihat pada gambar 2 yaitu bagaimana cara penggunaan dari aplikasi enkrip dan dekrip.



Gambar 3. Use case sistem enkripsi dan dekripsi.

b. ***Diagram Activity***

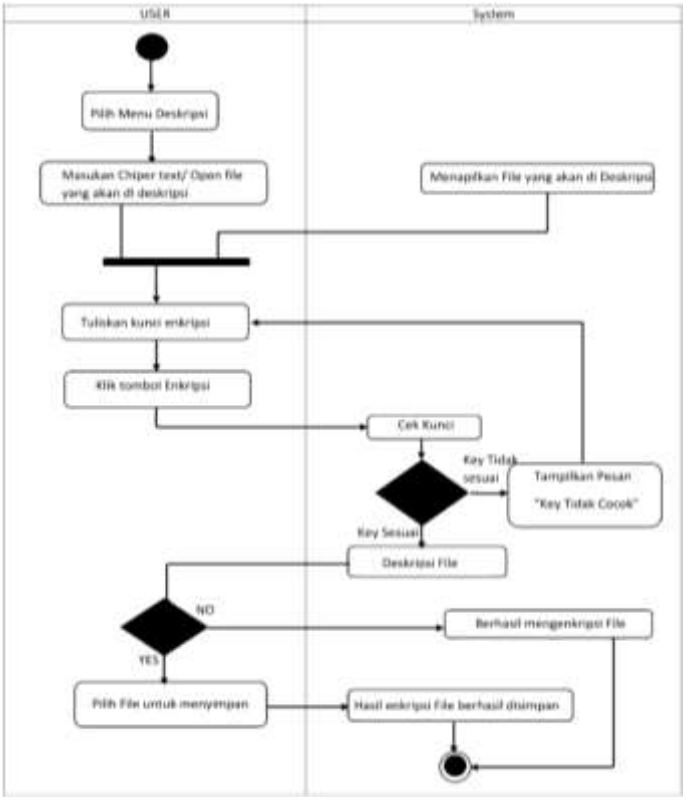
Diagram Activity menggambarkan *work flow* atau aktivitas dari sebuah system atau proses bisnis[13]. Pada gambar 3 menjelaskan tentang *diagram activity* untuk enkrip sedangkan dan gambar 4 untuk dekrip.



Gambar 4. *Activity* Enkripsi.

Submitted: **04/06/2020**; Accepted: **16/08/2020**; Published: **20/10/2020**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 4, Nomor 4, Oktober 2020, Page 898-903
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI 10.30865/mib.v4i4.2256



Gambar 5. *Activity* Dekripsi

3.2 Penerapan Algoritma RC2

Pada bagiaan ini trdapat tahapan untuk mengenkripsi dan mendekripsi mengunakan algoritma RC 2, adapun tahapanya seperti berikut:

a. Proses Enkripsi
   1. Membuka data yang akan di enkripsi
   2. Memasukan kunci untuk data yang akan dienkripsi.
   3. Menginisialisasikan K=key, P=Plaintext, I= Isitext
   4. Setelah itu aka nada pengulangan dari proses yang telah diketahui hasilnya dimana i=0; i<panjang_P; i++

b. Proses Dekripsi
   1. Buka data yang akan di dekripsi
   2. Index = Isi text
   3. s = (char)(index-1)
   4. dimana i=1; i<=jumlahkey; i++
   5. jikakunci = text
   6. maka i= jumlah key +1; i<isitext; 1++

3.3 Tahap Pengujian

Pada tahapan pengujiaan ini terdapat 2 halaman muka yaitu halaman muka enkripsi dan halaman muka pada dekripsi

Gambar 6. Form enkripsi

Submitted: **04/06/2020**; Accepted: **16/08/2020**; Published: **20/10/2020**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 4, Nomor 4, Oktober 2020, Page 898-903
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI 10.30865/mib.v4i4.2256

Pada gambar 5, terdapat gambar halaman muka enkripsi di halaman muka tersebut terdapat 2 kolom yang dapat digunakan pertama terdapat kolom untuk membuka file baru dengan mengklik *open file* , *open file* sendiri akan membuka file dan hanya file berformat .txt saja yang bisa di enkrip, setelah itu kolom kedua ada kunci , kunci ini berguna untuk mengenkrip data supaya hasil data tidak bisa di buka oleh pihak lain.

Gambar 7. Form Dekripsi

Selanjutnya pada gambar 6 sudah ada halaman muka untuk dekripsi , dimana halaman dekripsi ini sama dengan halaman muka enkrip, terdapat 2 kolom yang dapat digunakan untuk mengisi nama file dan kunci yang sudah di buat supaya dekripsi bisa berhasil.

Berikut ada beberapa perbandingan file yang belum dienkripsi dan yang telah dienkripsi :

(A) File sebelum di enkripsi (B) File yang telah dienkripsi

Gambar 8. File yang belum dan sudah di enkripsi

(A) File masih terenkrispi (B) File sudah didekripsi

Gambar 9. File yang masih terenkripsi dan terdekripsi

Pengujian selanjutnya adalah menguji isi dokumen text untuk di enkripsi dan di dekripsi. Dokumen text tersebut berformat .txt. hasil pengujian enkripsi dapat dilihat pada table 1 dan untuk melihat hasil pengujiaan dekripsi ada pada table 2.

Tabel 1. Hasil Enkripsi

No	Nama file	Kunci	Nama file setelah di enkripsi	Ukuran file
1	Kriptografi	123	Kritografi_enkripsi.txt	Tetap
2	Asimetris.txt	abc	Asimetris_enkripsi.txt	Tetap
3	Sikancil.txt	!A1b	Sikanci_enkripsi.txt	Tetap

Tabel 2. Hasil Dekripsi

No	Nama file	Kunci	Nama file setelah di enkripsi	Ukuran file
1	Kritografi_enkripsi.txt	123	Kriptografi	Tetap
2	Asimetris_enkripsi.txt	abc	Asimetris.txt	Tetap

Submitted: **04/06/2020**; Accepted: **16/08/2020**; Published: **20/10/2020**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 4, Nomor 4, Oktober 2020, Page 898-903
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI 10.30865/mib.v4i4.2256

No	Nama file	Kunci	Nama file setelah di enkripsi	Ukuran file
3	Sikanci_enkripsi.txt	!A1b	Sikancil.txt	Tetap

Dari hasil uji coba ini dapat disimpulkan bahwa, kita bisa membuat *key* dengan kombinasi huruf dan angka serta kita dapat mengenkripsi sebuah dokumen .txt yang berisi angka maupun text ,dan semua text dapat di enkripsi dan bisa di dekripsi jika *key* yang di gunakan sama.

4. KESIMPULAN

Hasil dari penelitian dan pembahsan yang telah dilakukan, dapat diambil beberapa kesimpulan sebagaai berikut :

1. Aplikasi menggunakan algoritma kriptografi RC 2 dapat berjalan dengan baik.
2. Dengan mengunakan perngkat lunak ini, tujuan dari penelitian tercapai, keamanan pada pesan, data, maupun informasi.
3. Pesan kesalah akan ditampilkan apabila terjadi suatu kesalahan pada saat enkrip dan dekrip. Saat enkrip memasukan bit bernilai kosong dan saat dekrip salah memasukan kunci/*key*.

REFERENCES

[1] H. Mukhtar, *Kriptografi untuk Keamanan Data*. Yogyakarta: Deepublish, 2018.
[2] I. A. Apreja A , Syarif Z, " Analisis Tingkat Keamanan Enkripsi Data Menggunakan Algoritma Base 64 Encode," *Annu. Res. Semin.*, vol. Vol.3, No., 2017.
[3] M. Fikry, " Aplikasi Java Kriptografi Menggunakan Algoritma Vigenere," *Techsi*, vol. 8, no. 1, pp. 1– 9, 2016.
[4] S. Maslakah and G. S. Widya, " ENKRIPSI DAN DESKRIPSI DENGAN METODE DATA RC2 DENGAN MENGGUNAKAN BAHASA PEMROGRAMAN JAVA," no. 1412120087, pp. 1– 10, 2017.
[5] N. Jumrotul, M. Rifa' i Abdul, and I. Prasetyo Budi, " JURNAL KEAMANAN KOMPUTER APLIKASI ENKRIPSI-DESKRIPSI DENGAN ALGORITMA RC2 MENGGUNAKAN JAVA NETBEANS," pp. 1– 9, 2017.
[6] V. Siahaan and R. H. Sianipar, *DATABASE DAN KRIPTOGRAFI MENGGUNAKAN JAVA/MYSQL*. Sparta Publishing, 2019.
[7] V. Siahaan, *BUKU PINTAR JAVA/SQLITE: Membuat Aplikasi Dekstop Kriptografi*. Balige Publishing, 2020.
[8] I. Gunawan, *Keamana Data : Teori dan Implementasi*, Volume 1 d. Google Publisher, 2020.
[9] M. C. Sinaga, *Kriptografi Python*. 2017.
[10] Mardiana, " Pengembang Algoritma Block Chiper RC6 Pada Citra Digital," Universitas Sumatera Utara, 2013.
[11] M. Naufal, " IMPLEMENTASI STEGANOGRAFI DAN KRIPTOGRAFI UNTUK KEAMANAN DATA DENGAN METODE RC2 DAN LSB PADA CITRA BITMAP," Sekolah Tinggi Manajemen Informatika dan Komputer TRIGUNA DHARMA MEDAN, 2013.
[12] E. Sutanto, *Pemogram Andoroid Dengan Menggunakan Eclips dan StarUML*. AIRLANGGA UNIVERSITY PRESS, 2018.
[13] A. Hendini, " Pemodelan Uml Sistem Informasi Monitoring Penjualan Dan Stok Barang," *J. Chem. Inf. Model.*, 2013, doi: 10.1017/CBO9781107415324.004.

Submitted: **04/06/2020**; Accepted: **16/08/2020**; Published: **20/10/2020**