[TEKNOLOGINUSANTARA][Volume 6 No. 2][2024][Hal. 67 - 76]
http://ojs.uninus.ac.id/index.php/teknologinusantara
E-ISSN : 2964-4577

TEKNOLOGI NUSANTARA
Jurnal Penelitian Fakultas Teknik UNINUS
http://ojs.uninus.ac.id/index.php/teknologinusantara
E-ISSN : 2964-4577

IMPLEMENTASI ALGORITMA RSA DALAM BAHASA C++ UNTUK ENKRIPSI DAN DEKRIPSI PESAN

Jihan Dzakiyyah Azhari
Fakultas Teknik, Universitas Islam Nusantara
jihanazhari439@gmail.com

Nurul Karimah
Fakultas Teknik, Universitas Islam Nusantara
nkarimah915@gmail.com

Ririn Riskianti
Fakultas Teknik, Universitas Islam Nusantara
ririnriskianti02@gmail.com

Muhamad Ramdhan Mardiansyah
Fakultas Teknik, Universitas Islam Nusantara
ram.ardiansyah18@gmail.com

Muhammad Luthfi Ramadhan
Fakultas Teknik, Universitas Islam Nusantara
luthfiramadhan155@gmail.com

ABSTRACT

In the era of digital communication, message security has become increasingly critical, especially for messages containing confidential information. One effective method to secure such messages is through cryptography, specifically using the RSA algorithm. The RSA algorithm transforms readable messages, known as plaintext, into unreadable messages, known as ciphertext, which contain secret codes. Encryption is the process of converting plaintext into ciphertext, while decryption is the process of converting ciphertext back into plaintext.. Among various cryptographic algorithms, RSA stands out for its robustness and reliability. This study develops an RSA algorithm using the C++ programming language, aiming to secure information within messages transmitted to others, thereby maintaining their confidentiality. The implementation of the RSA algorithm in C++ demonstrates its practical application in enhancing message security, ensuring that confidential information remains protected during transmission..

Keywords: *Cryptography, Encryption, Decription, RSA, Ciphertext and Plaintext.*

[TEKNOLOGINUSANTARA][Volume 6 No. 2][2024][Hal. 67 - 76]
http://ojs.uninus.ac.id/index.php/teknologinusantara
E-ISSN : 2964-4577

ABSTRAK

Di era komunikasi digital, keamanan pesan menjadi semakin penting, terutama untuk pesan yang berisi informasi rahasia. Salah satu metode efektif untuk mengamankan pesan tersebut adalah melalui kriptografi, khususnya menggunakan algoritma RSA. Algoritma RSA mengubah pesan yang dapat dibaca, yang dikenal sebagai teks biasa, menjadi pesan yang tidak dapat dibaca, yang dikenal sebagai teks sandi, yang berisi kode rahasia. Proses mengubah plaintext menjadi ciphertext disebut enkripsi, sedangkan proses mengubah ciphertext kembali menjadi plaintext disebut dekripsi. Di antara berbagai algoritma kriptografi, RSA menonjol karena ketahanan dan keandalannya. Penelitian ini mengembangkan algoritma RSA dengan menggunakan bahasa pemrograman C++, yang bertujuan untuk mengamankan informasi dalam pesan yang dikirimkan kepada orang lain, sehingga menjaga kerahasiaannya. Penerapan algoritma RSA di C++ menunjukkan penerapan praktisnya dalam meningkatkan keamanan pesan, memastikan bahwa informasi rahasia tetap terlindungi selama transmisi.

Keywords: Kriptografi, Enkripsi, Dekripsi, RSA,Ciphertext dan Plaintext.

PENDAHULUAN

Di era digital yang berkembang pesat, keamanan informasi sudah menjadi aspek yang sangat diperlukan. Peningkatan signifikan dalam penggunaan teknologi informasi di berbagai sektor seperti bisnis, pendidikan dan komunikasi telah meningkatkan kebutuhan akan perlindungan data terhadap akses tidak sah dan penyalahgunaan. Salah satu metode efektif untuk menjamin keamanan data adalah melalui kriptografi, khususnya algoritma RSA.

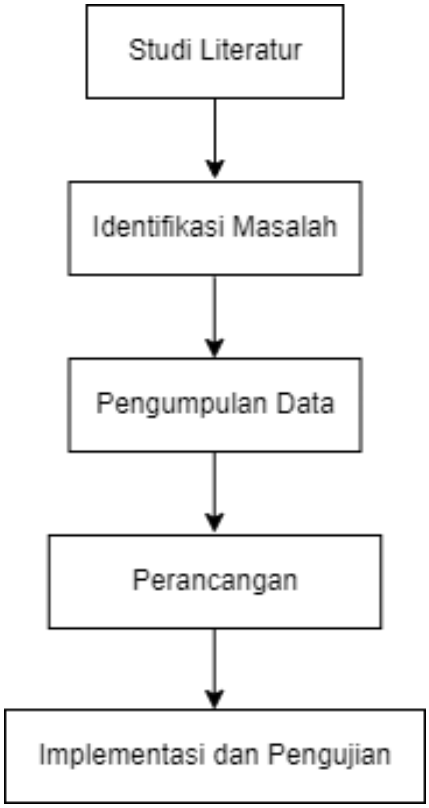
Penerapan algoritma RSA dalam enkripsi dan dekripsi pesan menawarkan banyak manfaat. RSA memainkan peran penting dalam enkripsi kunci publik dan pertukaran kunci. Hal ini didasarkan pada tantangan matematis dalam memfaktorkan bilangan besar, di mana memecah suatu bilangan menjadi faktor primanya sulit dilakukan secara komputasi. Meskipun memiliki keamanan yang tinggi, penerapan RSA memerlukan pemahaman mendalam tentang prinsip matematika yang mendasari algoritma serta penerapan praktisnya.

Penelitian ini mendalami implementasi kriptografi menggunakan algoritma RSA untuk enkripsi dan dekripsi pesan, memberikan panduan praktis dan pemahaman teoritis bagi pengguna dan pengembang teknologi informasi. Penelitian tersebut bertujuan untuk menghasilkan solusi efektif untuk meningkatkan keamanan komunikasi digital dan berkontribusi positif terhadap perkembangan teknologi informasi yang lebih aman.

[TEKNOLOGINUSANTARA][Volume 6 No. 2][2024][Hal. 67 - 76]
http://ojs.uninus.ac.id/index.php/teknologinusantara
E-ISSN : 2964-4577

METODOLOGI PENELITIAN

Berikut merupakan alur dari penelitian :



1. Studi Literatur

   Langkah awal dalam melakukan penelitian ini meliputi tinjauan pustaka dan kajian menyeluruh terhadap konsep-konsep terkait keamanan pesan, khususnya berfokus pada Kriptografi, Algoritma RSA, dan Bahasa Pemrograman C++.

   a. Kriptografi

      Kriptografi berasal dari bahasa Yunani, yaitu crypto yang berarti rahasia dan graphia yang berarti tulisan. Dalam terminologi, kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan selama pengirimannya dari satu tempat ke tempat lainnya.

      Kriptografi erat kaitannya dengan enkripsi yang mengacak data dengan menjaga kerahasiaan menggunakan kode rahasia. Keamanan dalam kriptografi dapat menyembunyikan data dengan melalui sistem kunci, enkripsi dan dekripsi.

   b. Algoritma RSA

      Algoritma RSA melakukan enkripsi dan dekripsi berdasarkan konsep bilangan prima dan aritmatika modular. Kunci enkripsi dan dekripsi keduanya berupa bilangan bulat. Kunci enkripsi bersifat publik dan dapat diakses oleh siapa saja, sedangkan kunci dekripsi dirahasiakan

dan dikenal sebagai kunci privat. Kunci privat ini diperoleh dari penggabungan beberapa bilangan prima dengan kunci enkripsi.

Untuk menemukan kunci dekripsi, seseorang harus memecah bilangan komposit menjadi faktor-faktor primanya, yang merupakan tugas sulit tanpa algoritma efisien yang diketahui. Semakin besar bilangan komposit, semakin sulit untuk memfaktorkannya, sehingga memperkuat keamanan algoritma RSA.Langkah-langkah dalam menggunakan algoritma RSA sebagai berikut:

1) Pembuatan Kunci
   - Pilih dua bilangan prima, misalnya a dan b dan rahasiakan .
   - Hitunglah nilai berikut (n = a * b). Untuk nilai n tidak perlu dirahasiakan.
   - Kemudian hitunglah (m = (a - 1) * (b - 1)). Nilai a dan b dihapus setelah nilai m sudah dihitung, hal ini supaya terjaga kerahasiaannya.
2) Enkripsi
   - Ubah pesan yang akan dienkripsi menjadi bentuk numerik, misalnya dengan skema pengkodean ASCII atau UTF-8.
   - Mengubah pesan yang dienkripsi menjadi bentuk numerik, dengan menggunakan karakter ASCII yang berfungsi untuk memanipulasi teks.
   - Hitunglah pesan yang sudah dirahasiakan (chipertext) pada nilai c dari pesan yang dikirim (plaintext) m dengan rumus (c = m^e mod n), untuk nilai e = eksponen publik dan nilai n = modulus.
3) Dekripsi
   - Hitung pesan yang dikirim (plaintext) m dari pesan yang sudah dirahasiakan (ciphertext) c dengan rumus (m = c^d mod n), untuk nilai d = eksponen privat dan nilai n = modulus.
   - Mengubah kembali nilai numerik m menjadi berbentuk pesan asli.

c. Bahasa Pemrograman C++

Bahasa C++ merupakan bahasa pemrograman yang populer di dunia, bahasa ini dikenal dengan eksekusinya yang cepat dan lebih efisien. Hal ini sangat penting dalam kriptografi, karena digunakan untuk memproses bilangan besar dengan cepat. Implementasi RSA dengan menggunakan bahasa C++ ini sangat memungkinkan dengan adanya memanfaatkan sistem dan penggunakan kriptografi yang kuat dan aman.

2. Identifikasi Masalah

Dalam konteks penelitian ini, masalah utama yang ingin diatasi adalah kebutuhan akan transmisi pesan yang aman di dunia yang semakin digital. Pesatnya perkembangan teknologi informasi bisa menyebabkan peningkatan yang signifikan dalam volume pertukaran data. Hal ini dapat meningkatkan resiko akses tidak sah dan penyalahgunaan informasi yang sensitif. Pada permasalahan tersebut, solusi yang dapat diambil untuk menjaga keamanan data pesan yaitu dengan membuat sebuah program

pengamanan data menggunakan metode RSA, yang memiliki fungsi untuk menjaga kerahasiaan.

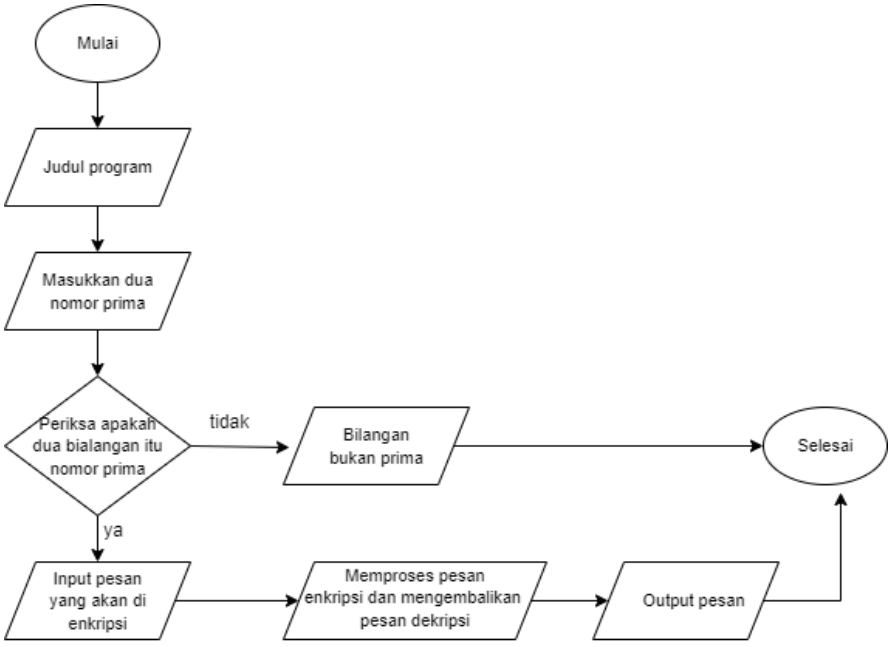
3. Pengumpulan Data

   Pengumpulan data dilakukan dengan membaca, mencatat dan mempelajari dari beberapa referensi seperti jurnal nasional, jurnal internasional dan situs web lainnya yang berkaitan dengan topik yang dibahas yaitu berkaitan dengan Algoritma RSA.

4. Perancangan

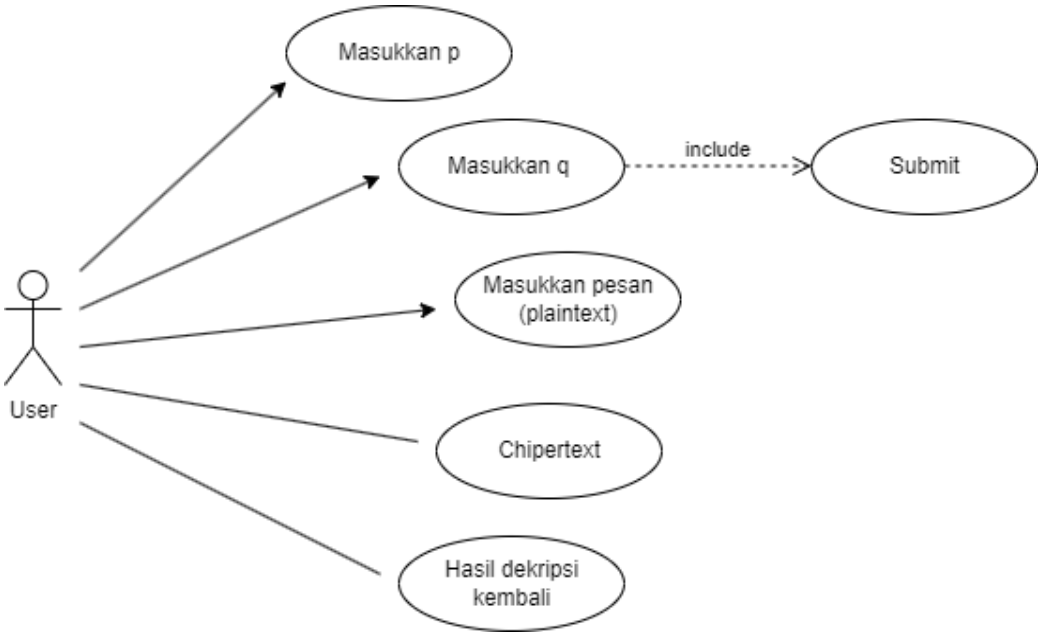
   Perancangan dilakukan dengan mengambil suatu tindakan yang jelas, pada metode ini meliputi pembuatan beberapa diagram seperti flowchart, use case diagram, activity diagram, sequence diagram. Berikut merupakan perancangan yang dibutuhkan.

- Flowchart

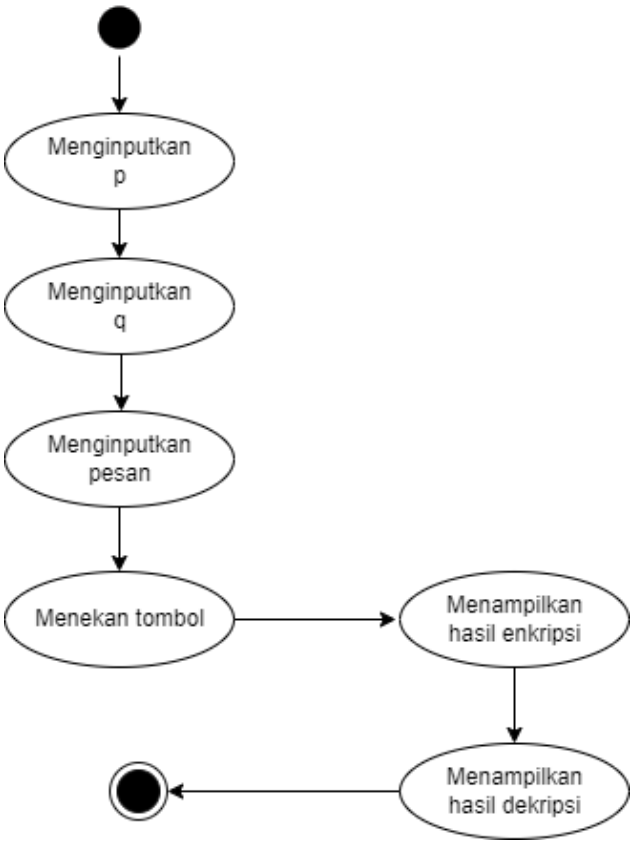


[TEKNOLOGINUSANTARA][Volume 6 No. 2][2024][Hal. 67 - 76]
http://ojs.uninus.ac.id/index.php/teknologinusantara
E-ISSN : 2964-4577

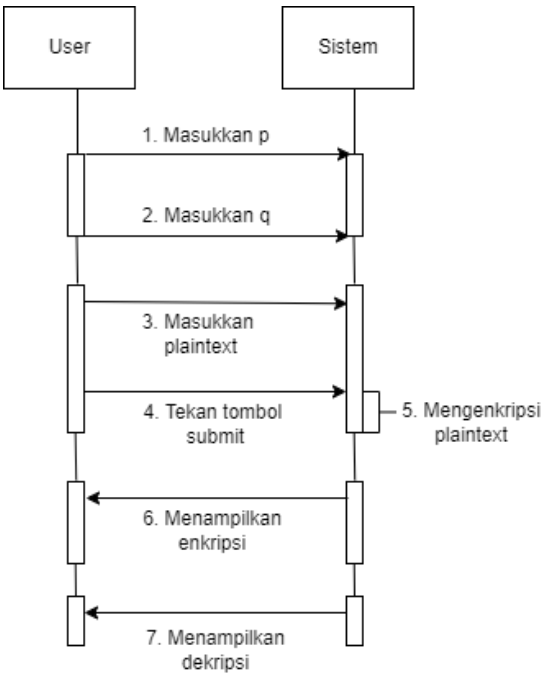
- Use Case Diagram



- Activity Diagram



- Sequence Diagram



5. Implementasi dan Pengujian

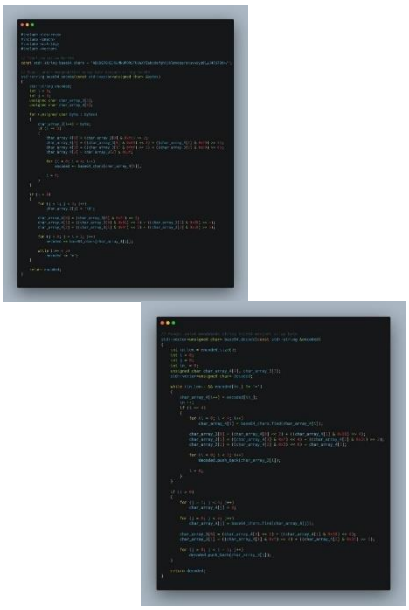
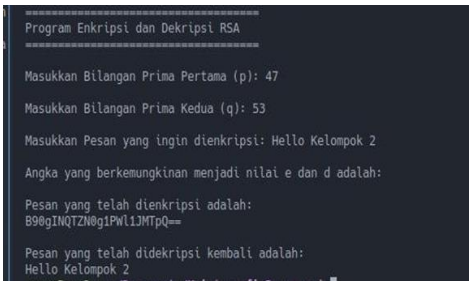
Implementasi merupakan pengembangan dari perancangan sistem. Setelah perancangan sistem dibentuklah program yang merupakan perwujudan dari rancangan tersebut, pengujian dilakukan dengan melakukaknnya sebuah percobaan.

HASIL DAN PEMBAHASAN

Beberapa hasil kebutuhan sistem untuk pengamanan data menggunakan algoritma RSA antara lain :

a. Program ini memberikan hasil rancangan yang dapat menjaga kerahasiaan data pesan.
b. Program ini menghasilkan sebuah proses enkripsi pada pesan, yaitu mengacak isi teks pesan menjadi sebuah teks pesan yang sulit dibaca.
c. Program ini dapat mengembalikan pesan teks yang tadinya sudah di enkripsi, kemudian di dekripsikan kembali menjadi pesan teks yang bisa dibaca.

Berikut merupakan tabel dari hasil percobaan implementasi dari bahasa pemrograman C++.

No	Hasil	Uji Coba	Keterangan
1		Berhasil	Source code untuk Algoritma RSA
2		Berhasil	Output dari source code

Pada source code diatas user diminta untuk memasukkan dua bilangan prima, kemudian memasukkan pesan yang ingin dienkripsikan. Pesan yang telah dienkripsikan tersebut akan berubah menjadi ciphertext atau bahasa yang tidak bisa dipahami (rahasia).

KESIMPULAN

Berikut merupakan beberapa kesimpulan yang diambil berdasarkan hasil dari penelitian :

1. Program ini bermanfaat untuk masyarakat mengenai pentingnya metode enkripsi dan kriptografi dalam menjaga keamanan pribadi, sehingga diperlukan edukasi yang menyeluruh dan berkelanjutan.
2. Mengatasi kendala akibat kurangnya tingkat keahlian teknis dalam implementasi enkripsi dan kriptografi memerlukan pendekatan yang terintegrasi, termasuk pengembangan alat dan perangkat lunak yang lebih user-friendly, serta peningkatan akses terhadap sumber daya.
3. Untuk menggunakan enkripsi dan kriptografi secara efektif dalam meningkatkan keamanan data, diperlukan penerapan standar keamanan yang ketat dan praktik terbaik yang diakui secara luas. Selain itu, penting untuk selalu melakukan pembaruan terhadap sistem enkripsi guna menghadapi ancaman dan kerentanan terbaru.

SARAN

Untuk mengembangkan program yang telah dibuat, peneliti menyarankan :

1. Dapat mempertimbangkan pengembangan lebih lanjut untuk mendukung algoritma lain dengan teknik enkripsi yang modern untuk meningkatkan keamanan dari kinerja.
2. Perlu dilakukan optimasi kode C++ untuk meningkatkan efisiensi proses enkripsi dan dekripsi, terutama untuk pesan yang lebih besar.
3. Dapat menambahkan penjelasan materi yang terkait dengan lebih jelas dan lengkap.
4. Mengembangkan program ini menjadi program yang lebih user-friendly.

UCAPAN TERIMAKASIH

Terima kasih disampaikan untuk dosen mata kuliah Metodologi Penelitian dan rekan-rekan yang telah ikut berkontribusi dalam penelitian ini.

DAFTAR PUSTAKA

Herawati, A. N. (2022). Enkripsi dan Dekripsi Pesan Menggunakan Vigenere-Multiplicative Cipher dan Linear Block Cipher (LBC). Jurnal Informatika dan Teknologi Komputer, 1(1).

Dewaweb. (2022, April 13). Mengenal Kriptografi, Pengertian, Jenis dan Algoritmanya. Dewaweb. Retrieved May 18, 2024, from

https://www.dewaweb.com/blog/apa-itu-kriptografi/

Fatonah, & Mulyana, D. I. (2022). Implementasi Metode Rivest Shamir Adleman untuk Enkripsi dan Dekripsi Text. Jurnal Informatika dan Teknologi Komputer, 3(1), 32-39.

Alasi, & Satria, T. (2019). Implementasi Kriptografi dengan Algoritma Caesar Cipher untuk Keamanan Data Microsoft Office Word dan Excel. Jurnal Informasi Komputer Logika, 1-4.

Hana Dwi Putra, S. (2018). Implementasi Enkripsi dalam Pengamanan File Data Karyawan dengan Metode Algoritma DES (Data Encryption Standard) pada CV. Sinergi Informasi Global. Jurnal Ilmu Administrasi, Ilmu Sosial dan Ilmu Politik, 13(2).

Simargolang, M. Y. (2017, July). Implementasi Kriptografi RSA dengan PHP. Jurnal Teknologi Informasi, 1(1).

Puspasari, E. K. (2022, September 13). Bahasa C++ adalah: Pengertian dan Manfaat. Alterra Academy. Retrieved May 18, 2024, from https://academy.alterra.id/blog/bahasa-c-adalah-pengertian-dan-manfaat%EF%BF%BC

Anshori, Y., Dodu, A. Y. E., & Wedananta, D. M. P. (2019). Implementasi Algoritma Kriptografi Rivest Shamir Adleman (RSA) pada Tanda Tangan Digital. Jurnal Informatika dan Teknologi Komputer, 18(2), 110-121.

Alasi, T. S., & AAS, A. T. (2020). Algoritma Vigenere Cipher untuk Penyandian Record Informasi pada Database. Jurnal Informasi Komputer Logika, 1(4), 1-7. Available Online at [http://ojs.logika.ac.id/index.php/jikl] (http://ojs.logika.ac.id/index.php/jikl).