e-ISSN 2828-0490
JURNAL MEDIA COMPUTER SCIENCE

The Implementation Of Modern Cryptography On Document Data Security

Penerapan Kriptografi Modern Pada Pengamanan Data Dokumen

Triza Randes Syafutra[1)]; Khairil[2)]; Eko Suryana [3)]
[1,2,3)]*Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Dehasen Bengkulu*
Email : [1)] trizarandes05@gmail.com

How to Cite :
Syafutra, T. R., Khairil., Suryana, E. (2022). The Implementation Of Modern Cryptography On Document Data Security. Jurnal Media Computer Science, 1(2). DOI:

ARTICLE HISTORY
Received [3 Juni 2022]
Revised [28 juni 2022]
Accepted [18 Juli 2022]

KEYWORDS
Cryptography, Documents, Data Security.

ABSTRAK

Aspek keamanan data telah menjadi aspek yang sangat penting dari suatu sistem informasi. Banyak orang mulai mencari cara untuk mengamankan data atau informasi, karena perkomputeran secara global telah menjadi tidak aman dan seringkali luput dari perhatian pemakai komputer dan mulai menjadi isu yang sangat serius. Sehingga, diperlukan suatu cara untuk mengamankan data yang rahasia dan penting. Salah satu metode kriptografi yang bisa dimanfaatkan adalah metode RSA. Algoritma RSA merupakan salah satu algoritma public key yang populer dipakai dan bahkan masih dipakai hingga saat ini. Kekuatan algoritma ini terletak pada proses eksponensial, dan pemfaktoran bilangan menjadi 2 bilangan prima yang hingga kini perlu waktu yang lama untuk melakukan pemfaktorannya Implementasi sistem menggunakan bahasa pemrograman Visual Basic 2010 dan metode yang digunakan dalam penelitian ini adalah metode terapan (applied research). Dimana hasil pengujian yang telah dilakukan diperoleh hasil dimana Algoritma RSA dapat memberikan keamanan tambahan terhadap dokumen, hal ini dikarenakan data teks yang dimiliki oleh pengguna akan di eknripsi dan digantikan dengan deretan angka yang tidak mewakilkan isi dari data yang asli.

ABSTRACT

The aspect of data security has become a very important aspect of an information system. Many people start looking for ways to secure data or information, because global computing has become insecure and often escapes the attention of computer users and is starting to become a very serious issue. So, we need a way to secure confidential and important data. One of the cryptography methods that can be used is the RSA method. The RSA algorithm is one of the most popular public key algorithms used and is still used today. The strength of this algorithm lies in the exponential process, and factoring a number into 2 prime numbers which until now has taken a long time to factorize. The implementation of the system used the Visual Basic 2010 programming language and the method used in this research is an applied research method. Where the results of the tests that have been carried out are obtained where the RSA Algorithm can provide additional security to the document, this is because the text data owned by the user will be encrypted and replaced with a row of numbers that does not represent the contents of the original data.

PENDAHULUAN

Aspek keamanan data telah menjadi aspek yang sangat penting dari suatu sistem informasi. Banyak orang mulai mencari cara untuk mengamankan data atau informasi, karena perkomputeran secara global telah menjadi tidak aman dan seringkali luput dari perhatian pemakai komputer dan mulai menjadi isu yang sangat serius. Sehingga, diperlukan suatu cara untuk mengamankan data yang rahasia dan penting. Salah satu cara menjaga keamanan dan kerahasiaan data tersebut yaitu dengan digunakannya algoritma kriptografi untuk melakukan penyandian data

Dokumen merupakan hal yang paling penting. Dokumen merupakan surat penting atau berharga yang sifatnya tertulis atau tercetak yang berfungsi sebagai bukti ataupun keterangan. Pada saat ini, orang-orang lebih banyak menggunakan dokumen elektronik karena dokumen elektronik disimpan dengan menggunakan komputer atau perangkat elektronik lain untuk menampilkan atau memprosesnya.

Seiring perkembangan teknologi, dokumen yang seharusnya bersifat rahasia bisa diakses oleh orang yang tidak berhak. Maka diperlukan pengamanan untuk melakukan pencegahan atas sampainya informasi ke tangan yang tidak berhak. Banyak sekali metode pengamanan yang dilakukan untuk menjaga agar dokumen tersebut aman, seperti dengan pemberian sandi isi pesan dan metode lainnya untuk memperkuat keamanan

Kriptografi salah satu dari sekian banyak cara yang bisa diterapkan pada data untu memberikan keamanan tambahan akan sangat membantu dalam mengamankan data-data pada kantor notaris. Salah satu metode kriptografi yang bisa dimanfaatkan adalah metode RSA. Algoritma RSA merupakan salah satu algoritma public key yang populer dipakai dan bahkan masih dipakai hingga saat ini. Kekuatan algoritma ini terletak pada proses eksponensial, dan pemfaktoran bilangan menjadi 2 bilangan prima yang hingga kini perlu waktu yang lama untuk melakukan pemfaktorannya.

Algoritma ini dinamakan sesuai dengan nama penemunya, Ron Rivest, Adi Shamir dan Adleman (Rivest-Shamir-Adleman) yang dipublikasikan pada tahun 1977 di MIT, menjawab tantangan yang diberikan algoritma pertukaran kunci Diffie Hellman.

Skema RSA sendiri mengadopsi dari skema block cipher, dimana sebelum dilakukan enkripsi, plainteks yang ada dibagi – bagi menjadi blok – blok dengan panjang yang sama, dimana plainteks dan cipherteksnya berupa integer(bilangan bulat) antara 1 hingga n, dimana n berukuran biasanya sebesar 1024 bit, dan panjang bloknya sendiri berukuran lebih kecil atau sama dengan log(n) +1 dengan basis 2.

LANDASAN TEORI

Pengertian Kriptografi

Kata-kata “cryptography”, “cryptology” dan “cryptanalysis” umunya berubah-ubah dan masing-masing dari kata tersebut memiliki makna yang berbeda. Cryptography yang awal katanya menggunakan kata “crypt”, dalam bahasa Yunani kruptos yang artinya sembunyi. Kata terakhir “graphy” mengacu pada arti tulisan. Kriptografi memiliki arti sebagai tulisan yang tersembunyi. (Batten, 2013). Secara umum, kriptografi mengacu pada bagian enkripsi untuk membangun sebuah sistem transmisi rahasia. Sistem transmisi rahasia tersebut merupakan proses enkripsi dalam kriptografi, dimana mengubah plainteks (informasi awal) menjadi cipherteks.

Enkripsi

Enkripsi (encryption) adalah seni dari meng-enchiper suatu data, yang menterjemahkan data tersebut menjadi suatu data yang tidak dapat dibaca oleh siapapun, tapi hanya dapat dibaca oleh penerima data yang dimaksud.(Dony Ariyus, 2010).

Maksud meng-enchiper yaitu proses perubahan teks asli (plaintext)/data ke dalam bentuk kode. Kode dalam konteks ini adalah sistem untuk menampilkan data dengan set karakter, angka,

e-ISSN 2828-0490
JURNAL
MEDIA COMPUTER SCIENCE

simbol, kata dan atau sinyal yang telah ditentukan sebelumnya. Secara singkat proses enkripsi yaitu algoritma yang mengubah plaintext ke dalam bentuk ciphertext dengan menggunakan sebuah kunci.

Dekripsi

Dekripsi adalah proses pembuatan kembali data dari pesan yang dienkripsi. Pada prinsipnya data yang dienkripsi tidak bisa dibaca, tanpa menggunakan kunci yang bekerja sebagai panduan referensi untuk seluruh penggantian yang dilakukan ketika data dienkripsi.
Secara singkat proses dekripsi yaitu algoritma yang mengubah ciphertext ke dalam plaintext dengan menggunakan sebuah kunci. Dan kunci itu sendiri bisa berbentuk apapun, mungkin sebuah tabel yang menampilkan penggantian karakter untuk sebuah karakter atau kata untuk kata atau set penggantian lebih canggih.

Kunci

Kunci merupakan nilai yang sangat spesifik dan erat kaitannya dengan algoritma kriptografi untuk menghasilkan teks terenkripsi (Ciphertext) dan text biasa (plaintext) yang spesisfik pula. Kunci benar-benar merupakan bagian terkecil yang paling mendasar. Ukuran kunci diwujudkan dalam bentuk bit. Dengan kunci itulah, kita nanti akan bisa melakukan proses enkripsi dan dekripsi.

Algoritma RSA

RSA merupakan algoritma kriptografi yang menggunakan dua kunci berbeda pada proses enkripsi dan dekripsi-nya (Singh, 2017). RSA menganut sistem algoritma kunci publik yang saat ini telah digunakan secara luas. RSA pertama kali dipublikasikan pada tahun 1977. RSA merupakan metode kriptografi asimetris yang beroperasi pada mode blok. RSA membutuhkan dua kunci yang berbeda pada proses enkripsi dan dekripsi nya sehingga proses enkripsi dan dekripsi hanya dapat dilakukan oleh pihak yang memiliki kunci yang sesuai. Walaupun kunci enkripsi diketahui oleh pihak yang tidak berhak, pesan tidak dapat di dekripsi menggunakan kunci tersebut.

METODE PENELITIAN

Dalam melakukan penelitian ini, penulis menggunakan metode terapan (applied research). Penelitian terapan dilakukan berkenaan dengan kenyataan-kenyataan praktis, penerapan, dan pengembangan ilmu pengetahuan yang dihasilkan oleh penelitian dasar dalam kehidupan nyata. Penelitian terapan berfungsi untuk mencari solusi tentang masalah-masalah tertentu. Tujuan utama penelitian terapan adalah pemecahan masalah sehingga hasil penelitian dapat dimanfaatkan untuk kepentingan manusia baik secara individu atau kelompok.

HASIL DAN PEMBAHASAN

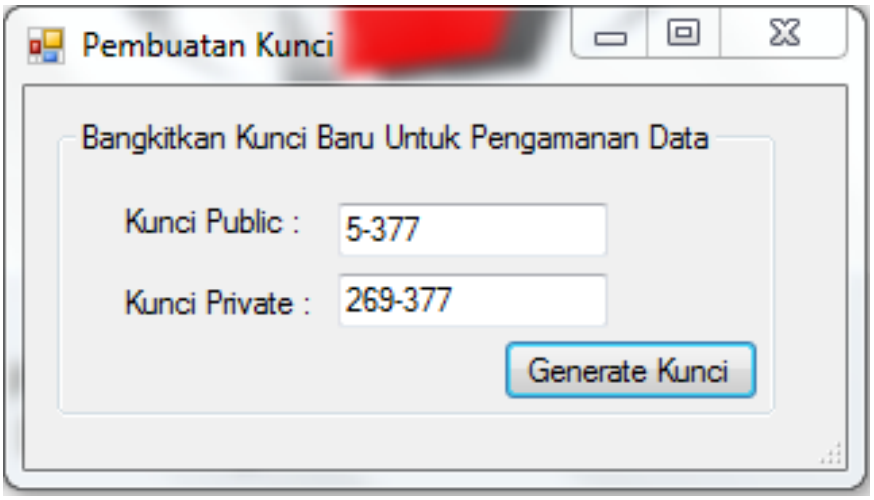
Pengujian Sistem Kriptografi RSA

Langkah selanjutnya dalam implementasi adalah pengujian jalannya sistem. Pengujian ini dilakukan untuk dapat memastikan kemampun sistem dalam melakukan enkripsi, dekripsi, dan pembangkitan kunci yang sesuai dengan tujuan awal dan juga memastikan tidak adanya kesalahan didalam sistem yang dibuat oleh penulis.

Gambar 1 Halaman Utama

Pada halaman ini, pengguna akan memilih proses mana yang akan dilakukan sesuai dengan kebutuhan dari masing-masing pengguna.untuk mempermudah pengujian maka penulis menentukan langkah selanjutnya adalah melakukan proses generate kunci. Proses ini dapat dilihat pada gambar berikut:

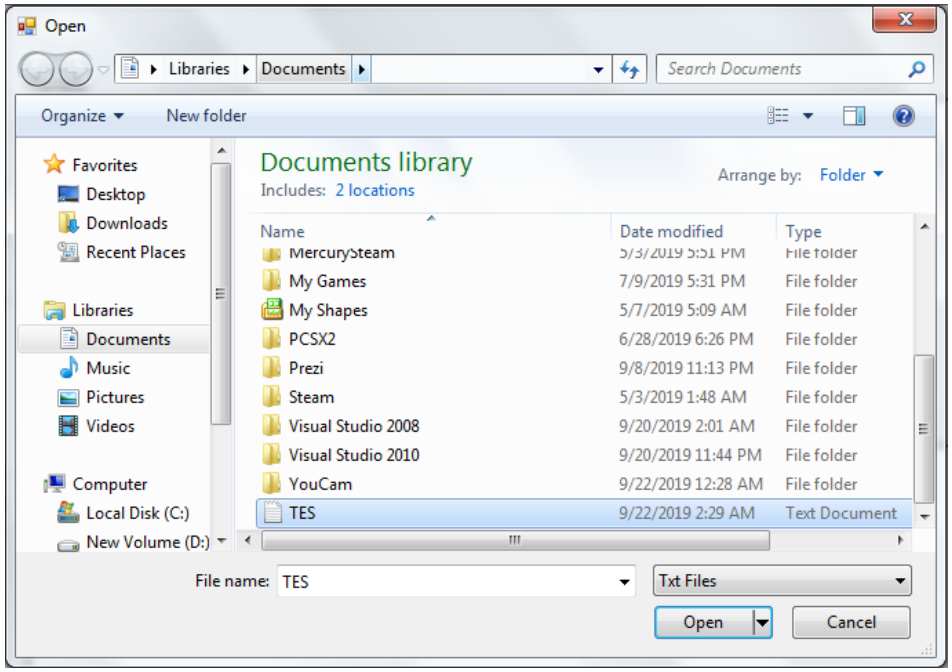
Gambar 2 Proses Pembangkitan Kunci



Pada gambar diatas dapat dilihat bahwasanya kunci yang diangkitkan ada dua yaitu kunci publik dan kunci private. Kunci publik yang akan digunakan untuk proses enkripsi adalah 5-377 sedangkan kunci private yang akan digunakan untuk proses dekripsi adalah 269-377. Kunci publik akan didistribusikan pada semua pengguna yang akan melakukan proses enkripsi namun kuncil private hanya akan dipegang oleh satu orang saja yaitu penerima data. Langkah selanjutnya setelah proses pembangkitan kunci adalah masuk kedalam proses enkripsi, untuk lebih jelasnya dapat dilihat pada gambar berikut:

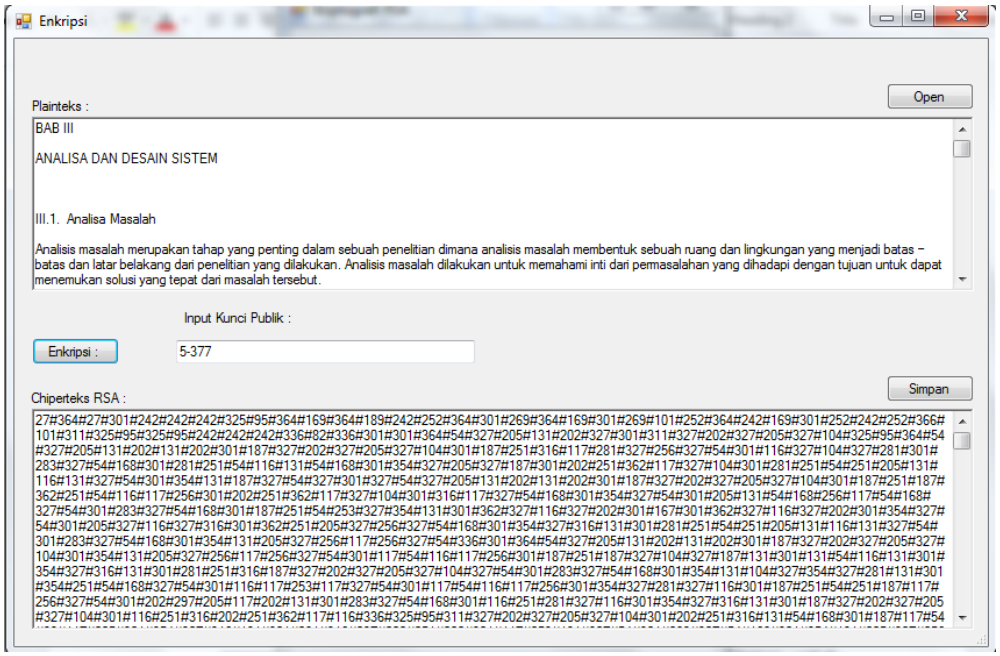
e-ISSN 2828-0490
JURNAL
MEDIA COMPUTER SCIENCE

Gambar 3Halaman Load Data Teks



Pada pengujian ini untuk menghindari kesalahan dalam pengolahan data, digunakan data dengan ekstensi pure teks yang paling baik yaitu notepad. Pada pengujian ini digunakan data dengan nama "TES". Selanjutnya data akan dipili dan di-load kedalam sistem untuk selanjutnya akan di enkripsi. Untuk proses enkripsi sendiri dapat dilihat pada gambar berikut ini:

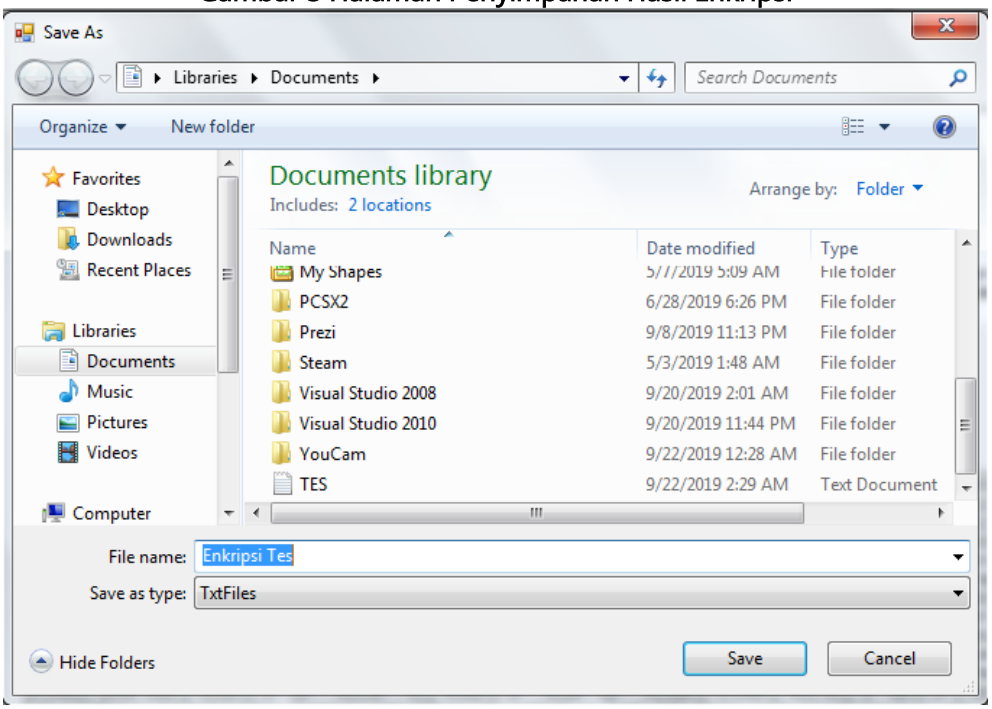
Gambar 4. Proses Enkripsi Berhasil



Pada gambar diatas dapat dilihat kunci yang digunakan adalah kunci publik yaitu "5-377". Gambar diatas jug menunjukkan proses enkripsi yang berhasil dimana sistem mampu mengubah

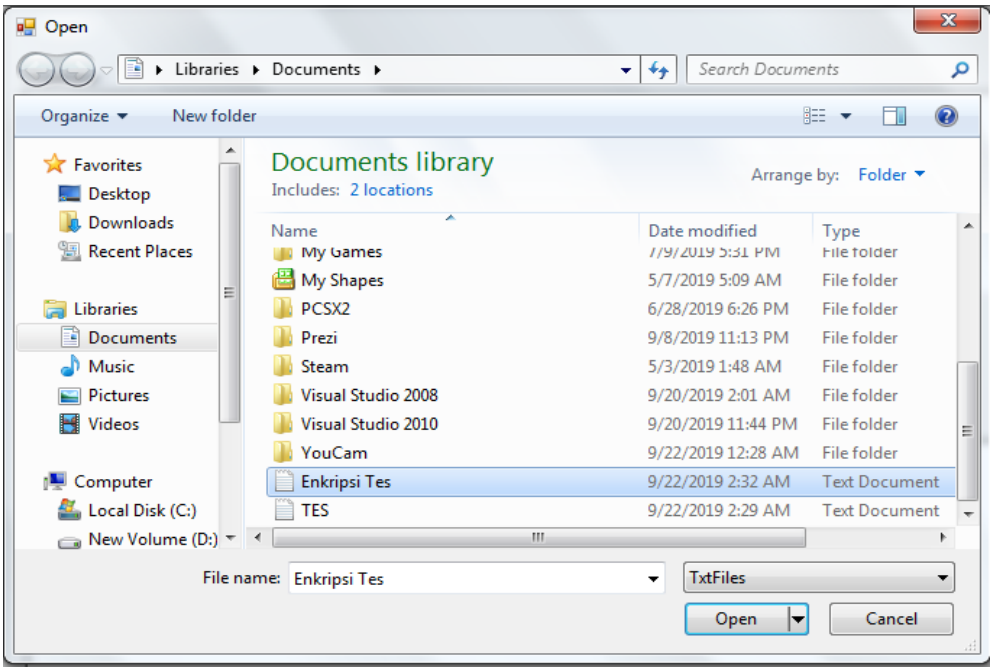
data dan tidak meninggalkan jejak-jejak yang bisa merepresentasikan isi dari data asli. Kemudian data hasil enkripsi atau chipperteks akan disimpan untuk keperluan pengujian proses dekripsi. Untuk lebih jelasnya proses penyimpanan dapat dilihat pada gambar 5. berikut:

Gambar 5 Halaman Penyimpanan Hasil Enkripsi



Setelah data sukses disimpan langkah selanjutnya adalah menguji proses dekripsi. Kunci yang digunakan adalah "269-377" kunci ini adalah kunci private yang biasanya hanya dimiliki oleh penerima data. Selanjutnya proses pengujian akan dilaksanakan dengan cara memilih data hasil enkripsi. Seperti yang ditampilkan pada gambar 6.

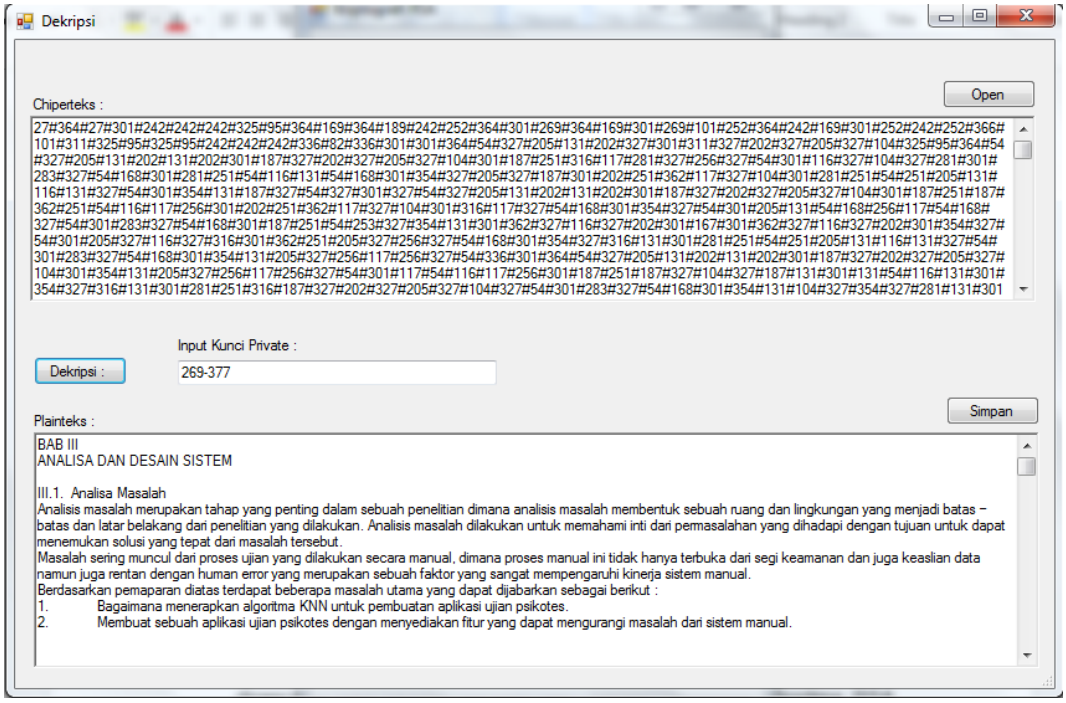
Gambar 6 Halaman Pemilihan Data Chiperteks



e-ISSN 2828-0490
JURNAL
MEDIA COMPUTER SCIENCE

Setelah data chiperteks berhasil diload, langkah selanjutnya adalah melakukan proses dekripsi. Kunciyang digunakan adalah kunci private yaitu "269-377". Untuk lebih jelasnya dapat dilihat pada gambar berikut:

Gambar 7. Proses Dekripsi Berhasil



Seperti yang tampak pada gambar diatas data yang sebelumnya tidak bisa dibaca dapat dikembalikan kedalam bentuk yang bisa dibaca atau plainteks kembali. Sehingga dapat disimpulkan sistem yang dirancang oleh penulis berhasil dan mampu menerima algoritma RSA dengan baik dan sesuai dengan tujuan awal pembuatan sistem.

KESIMPULAN DAN SARAN

Kesimpulan

1. Pengimplementasian algoritma RSA didalam sistem yang dirancang oleh penulis berjalan dengan baik.
2. Algoritma RSA dapat memberikan keamanan tambahan terhadap berkas / dokumen digital, hal ini dikarenakan data teks yang dimiliki oleh pengguna akan di eknripsi dan digantikan dengan deretan angka yang tidak mewakilkan isi dari data yang asli.
3. Aplikasi pengamanan data yang dirancang oleh penulis dapat mengikuti seluruh prosedur pengamanan data yang diatur didalam algoritma RSA

Saran

1. Memberikan keamanan tambahan seperti steganografi atau kompresi data didalam sistem untuk memberikan keamanan yang lebih baik bagi perusahaan atau pengguna sistem.
2. Pengimplementasian algoritma RSA dapat lebih diperluas dengan menerapkan algoritma tersebut pada tipe-tipe data lainnya

DAFTAR PUSTAKA

Abu, N. A., & Ghafar, A. H. (2016). A Secure Cryptographic Algorithm against Side Channel Attacks. International Journal of Cryptology Research 5(2): 45-55 (2015). ISSN 1985-5753

Alfina, O., & Harahap, F. (2019). PEMODELAN UML SISTEM PENDUKUNG KEPUTUSAN DALAM PENENTUAN KELAS SISWA SISWA TUNAGRAHITA. METHOMIKA: Jurnal Manajemen Informatika & Komputerisasi Akuntansi, 143-150.

Ariyus, D. (2010). Kriptografi. Yogyakarta: Penerbit Andi

Haviluddin. (2016). Memahami Penggunaan UML (Unified Modelling Language). Jurnal Informatika Mulawarman, 18-29.

Nuraini, R. (2015). DESAIN ALGORITHMA OPERASI PERKALIAN MATRIKS MENGGUNAKAN METODE FLOWCHART. JURNAL TEKNIK KOMPUTER, 144 -151.

Pratama, E. C., & Nasution, S. M. (2015). Perancangan Dan Implementasi Secure Cloud Dengan Menggunakan Diffie-Hellman Key Exchange Dan Serpent Cryptography Algorithm. e-Proceeding of Engineering : Vol.2, No.3. ISSN : 2355-9365

R.H Sianipar. (2017). Visual Basic.Net Untuk Programmer. Yogyakarta: Andi Offset.

Singh, T. C. (2017). Lucas Numbers and Cryptography. Department of Mathematics National Institute of Technology Rourkela

Suendri. (2018). Implementasi Diagram UML (Unified Modelling Language) Pada Perancangan Sistem Informasi Remunerasi Dosen Dengan Database Oracle (Studi Kasus: UIN Sumatera Utara Medan). ALGORITMA: Jurnal Ilmu Komputer dan Informatika, 1-9.

.