Pengamanan File dengan Algoritma Kriptografi Rivest Shamir Adleman (RSA) Studi Kasus SMP Muhammadiyah 4

Windarto [1)], Fitria Chairul Qomariah [2)], Lusi Fajarita [3)]

[1,2,3)] Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
Jl. Ciledug Raya, Petukangan Utara, Jakarta Selatan, 12260
Email: windarto@budiluhur.ac.id [1)], 1611500164@student.budiluhur.ac.id [2)], lusi.fajarita@budiluhur.ac.id [3)]

Abstrak — Kriptografi adalah ilmu yang mempelajari bagaimana melakukan enkripsi dan dekripsi, dengan memanfaatkan model matematika tertentu. Enkripsi adalah teknik penyajian yang mengubah sebuah pesan yang dapat dibaca (plaintext) menjadi sebuah pesan yang acak dan sulit diartikan (ciphertext). Untuk dapat membaca pesan yang terenkripsi diperlukan proses terbalik dari enkripsi yang disebut dekripsi. Kriptografi banyak jenisnya karena tiap-tiap algoritme dalam kriptografi memiliki perbedaan dalam tingkat kerumitan dan proses perhitungannya. Berdasarkan sifat kuncinya, algoritme kriptografi dibagi menjadi dua yaitu kriptografi simetris yang hanya memakai satu kunci rahasia dan kriptografi asimetris yang memakai sepasang kunci publik dan kunci rahasia. Pada penelitian ini algoritme kriptografi yang digunakan adalah algoritme kriptografi asimetris RSA yang ditemukan oleh Ron Rivest, Adi Shamir, dan Leonard Adleman pada tahun 1978 dan RSA merupakan singkatan inisial dari nama mereka bertiga. RSA digunakan karena merupakan algoritme kriptografi asimetris yang paling sering digunakan pada saat ini. Data yang digunakan data yang diambil di SMP Muhammadiyah 4 yang ingin file datanya diamankan agar terhindar dari pencurian data. Dari hasil analisis tersebut maka diberikan solusi berupa sebuah aplikasi keamanan file yang dibuat dengan bahasa pemrograman berbasis desktop dengan menerapkan algoritma kriptografi RSA. Hasil pengujian terhadap implementasi algoritme RSA, menghasilkan nilai akurasi sebesar 100%.

Kata kunci: kriptografi, rivest shamir adleman (RSA), asimetris, enkripsi, dekripsi.

Abstract — Cryptography is the study of how to encrypt and decrypt, by utilizing certain mathematical models. Encryption is a presentation technique that converts a message that can be read (plaintext) into a message that is random and difficult to interpret (ciphertext). To be able to read an encrypted message requires the reverse process of encryption called decryption. There are many types of cryptography because each algorithm in cryptography has a different level of complexity and calculation process. Based on the nature of the key, cryptographic algorithms are divided into two, namely symmetric cryptography which uses only one secret key and asymmetric cryptography which uses a pair of public and secret keys. In this study, the cryptographic algorithm used is the RSA asymmetric cryptography algorithm which was invented by Ron Rivest, Adi Shamir, and Leonard Adleman in 1978 and RSA is an abbreviation of the initials of the three of them. RSA is used because it is the most widely used asymmetric cryptographic algorithm today. The data used are data taken at SMP Muhammadiyah 4 who want their data files to be secured to avoid data theft. From the results of the analysis, a solution is given in the form of a file security application created with a desktop-based programming language by applying the RSA cryptographic algorithm. The test results on the implementation of the RSA algorithm, resulted in an accuracy value of 100%.

Keywords: cryptography, rivest shamir adleman (RSA), asymmetric, encryption, decryption.

I. PENDAHULUAN

I.1. Latar Belakang

Salah satu dampak negatif dalam perkembangan serta kemajuan teknologi informasi pada saat ini ialah pencurian data. Dari kurangnya kesadaran dan kewaspadaan akan keamanan data dapat menimbulkan celah-celah pencurian data melalui media elektronik sehingga sangat rentan sekali untuk disalahgunakan oleh pihak yang tidak bertanggung jawab. Dengan adanya pencurian data tersebut, maka aspek keamanan data dalam melakukan aktifitas pertukaran dan penyimpanan data informasi amatlah penting agar keaslian pada data tersebut akan tetap terjaga.

Pada umumnya, masyarakat melakukan komputerisasi dengan menggunakan aplikasi Microsoft Office, pada pengolahan kata akan disimpan menggunakan aplikasi Microsoft Word maupun Microsoft Power Point, dan pada pengolahan angka akan disimpan menggunakan aplikasi Microsoft Excel. Ada juga beberapa contoh file dokumen yang perlu diamankan antara lain *.doc, *.xls, *.txt. Resiko yang ditimbulkan dari data yang disimpan dalam bentuk digital mudah untuk dicuri oleh pihak yang tidak bertanggung jawab.

Dari pihak sekolah SMP Muhammadiyah 4 ingin mengamankan dokumen bentuk *.doc, dokumen seperti nilai siswa/i pada setiap semesternya. Berkas yang dimaksud antara lain berupa nilai siswa, data siswa maupun kurikulum yang sedang digunakan oleh sekolah, sehingga tidak boleh disebarluaskan kepada pihak luar yang tidak bertanggung jawab dan dapat mengakibatkan resiko yang cukup fatal bagi sekolah maupun siswa.

Berdasarkan latar belakang tersebut, dapat dirumuskan permasalahan yaitu bagaimana cara mengamankan dokumen penting di SMP Muhammdiyah 4 dari pengungkapan data pada saat terjadi pencurian informasi?

Adapun penelitian ini dibatasi pada ruang lingkup yaitu: algoritme kriptografi yang digunakan adalah algoritme kriptografi RSA dan dokumen digital yang akan diamankan adalah dokumen IPS semester genap serta penilaian kinerja guru dalam format file microsoft word dan microsoft excel.

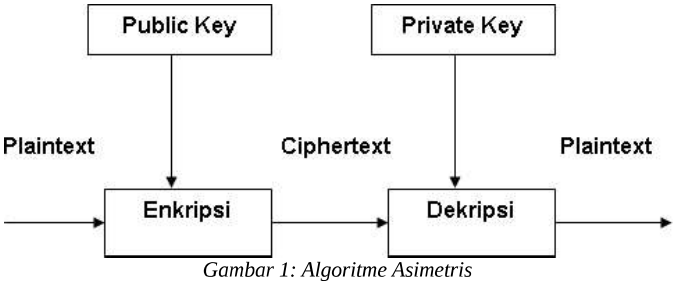
Diharapkan dengan adanya penelitian ini, maka dapat dihasilkan sebuah aplikasi keamanan data dengan mengimplementasikan metode kriptografi algoritme RSA yang dapat mengamankan sebuah isi data digital agar terhindar dari pencurian dan penyalahgunaan data dari pihak yang tidak memiliki akses pada data tersebut.

II. TINJAUAN STUDI

Kriptografi merupakan teknik pengamanan informasi yang dilakukan dengan cara mengolah informasi awal (plaintext) dengan suatu kunci tertentu menggunakan suatu metode enkripsi tertentu sehingga menghasilkan suatu informasi baru (ciphertext) yang tidak dapat dibaca secara langsung. Ciphertext tersebut dapat dikembalikan menjadi informasi awal (plaintext) melalui proses dekripsi. Kriptografi merupakan bidang ilmu yang bisa menjadi solusi dari masalah keamanan data. [1]

Keamanan dari suatu kriptografi terletak pada kerahasiaan kunci sedangkan algoritme kriptografi diasumsikan diketahui oleh umum. Sistem kriptografi yang kuat memiliki kemungkinan jangkauan kunci yang sangat besar sehingga sistem tidak dapat dipecahkan dengan mencoba semua kemungkinan kunci secara brute force (kasar), sistem kriptografi yang kuat juga menciptakan ciphertext yang acak untuk semua standar statistik. [2]

Algoritme kriptografi asimetris adalah algoritme kriptografi kunci public memiliki dua buah kunci yang berbeda pada proses enkripsi dan dekripsinya. Dimana kunci yang digunakan untuk proses enkripsi disebut public key dan dekripsi disebut private key. Entitas pengirim akan mengenkripsi dengan menggunakan kunci publik, sedangkan entitas penerima mendekripsi menggunakan kunci privat. Skema dari kriptografi asimetris dapat dilihat pada gambar dibawah ini:



Gambar 1: Algoritme Asimetris

Dalam kriptografi, RSA adalah algoritme untuk enkripsi kunci public (public-key encryption). Algoritme ini adalah algoritme pertama yang diketahui paling cocok untuk menandai dan untuk enkripsi dan salah satu penemuan besar pertama dalam kriptografi kunci publik. RSA masih digunakan secara luas dalam protokol-protokol perdagangan elektronik, dan dipercayai sangat aman karena diberikan kunci-kunci yang cukup panjang dan penerapannya yang sangat mutakhir. Algoritme RSA ditemukan oleh Ron Rivest, Len Adleman, dan Adi Shamir pada tahun 1977 di Massachusetts Institute of Technology (MIT) dan dipublikasikan pada tahun 1978. RSA menggunakan dua buah bilangan bulat prima untuk mendapatkan public key dan private key yang akan digunakan dalam proses enkripsi dan dekripsi pesan. RSA digunakan pada aplikasi ini untuk mengenkripsi pesan rahasia yang berupa file agar keamanan dari pesan rahasia tadi semakin kuat proses dari enkripsi dilakukan sebelum file rahasia disembunyikan pada arsip ZIP.

II.1. Algoritme Pembangkitan Pasangan Kunci

Untuk pembangkitan pasangan kunci RSA, digunakan algoritme sebagai berikut [3]:

- Dipilih dua buah bilangan prima sembarang yang besar **p** dan **q**.
- Nilai **p** dan **q** harus dirahasiakan.
- Dihitung **n = p x q**. Besaran **n** tidak perlu dirahasiakan.
- Dihitung **m = (p-1)(q-1)**
- Dipilih **e** (kunci publik) yang relatif prima terhadap **m**.

- Relatif prima terhadap **m** artinya faktor pembagi terbesar keduanya adalah 1, secara matematis disebut **gcd (e, m) = 1**. Untuk mencarinya dapat digunakan algoritme Euclid.
- Dihitung **d** (kunci pribadi), untuk mencari nilai **d** secara matematis **(d x e) mod n = 1**.
  Dapat juga digunakan algoritme Extended Euclid.
- Hasil dari algoritme tersebut diperoleh:
  - Kunci publik adalah pasagan **(e, n)**.
  - Kunci pribadi adalah pasangan **(d, n)**.

II.2. Enkripsi Pesan

Menggunakan kunci publik **(e, n)**

Plaintext m dinyatakan menjadi blok-blok $\mathbf{m_1, m_2, m_3, \ldots}$

Setiap blok $\mathbf{m_1}$, di enkripsikan menjadi blok ci, dengan rumus $\mathbf{c_i = mie \bmod n}$.

II.3. Dekripsi Pesan

Menggunakan kunci privat **(d, n)**.

Pilih ciphertext **c**

Setiap blok $\mathbf{c_i}$ didekripsikan menjadi blok $\mathbf{m_i}$, dengan rumus $\mathbf{m_i = c_i d \bmod n}$.

II.4. Implementasi Algoritme RSA

Misalkan p=13 dan q= 31 (keduanya prima), kemudian hitung modulus n (public key)

n = p.q = 13.31 = 403;

m = (p - 1)(q - 1) = (13 – 1)(31 -1) = 360

e = bilangan relatif prima dengan 360 adalah 7.

Kemudian tentukan nilai d dengan rumus

(e.d) mod m = 1

(7.d) mod 360 = 1

Ditentukan dengan cara menguji setiap nilai integer 1,2,3,…. Sampai ditentukan nilai **d** bilangan bulat.

Cek nilai **d**

(7.d) mod 360n= 1

Ditemukan nilai **103, karena (7.103) mod 360 => 721 mod 360 = 1** (bilangan bulat)

Kemudian sudah terkumpul

n = 403 **e = 7**

m = 360 **d = 103**

Plaintext B E L A J A R

Tabel 1: Enkripsi

Enkripsi			
B	66^7 mod 403	326 dec	ņ
E	69^7 mod 403	121 dec	y
L	76^7 mod 403	236 dec	ì
A	65^7 mod 403	234 dec	ê
J	74^7 mod 403	334 dec	Ŏ
A	65^7 mod 403	234 dec	ê
R	82^7 mod 403	173 dec	¬

Tabel 2: Dekripsi

Dekripsi			
ņ	326^{103} mod 403	66	B
y	121^{103} mod 403	69	E
ì	236^{103} mod 403	76	L
ê	234^{103} mod 403	65	A
Ŏ	334^{103} mod 403	74	J
ê	234^{103} mod 403	65	A
¬	173^{103} mod 403	82	R

II.5. Penelitian Terkait

Pada penelitian berjudul “Plug-In pada Microsoft Office Word untuk Enkripsi Dokumen dengan Menggunakan Algoritme Kunci Publik RSA” yang dilakukan oleh Zamah Sari, Ali Sofyan Kholimi dan Miftah Faisal Hamdani dan telah diterbitkan pada jurnal REPOSITOR vol.2 tahun 2020 (ISSN 2714-7975) mendapati hasil bahwa kemudahan penggunaan aplikasi Ms. Office Word menyebabkan data yang telah dibuat rentan terhadap suatu perubahan.

Hal ini memberikan suatu kesempatan kepada pihak lain untuk melakukan duplikasi ataupun modifikasi tanpa izin dari pemilik asli untuk berbagai kepentingan. Untuk mengatasi hal tersebut, diperlukan suatu sistem keamanan yang dapat mengamankan informasi dari pihak–pihak yang tidak berkepentingan. Adapun dari pihak Microsoft sendiri telah memberikan suatu sistem pengaman dalam bentuk password untuk membuka ataupun modifikasi data yang ada dalam Ms. Office Word.

Namun, sistem tersebut masih bisa diretas oleh aplikasi pihak ketiga yang bisa diunduh secara bebas di internet. Maka dalam penelitian tersebut dibuat suatu aplikasi plug-in berupa kriptografi untuk melindungi data pengguna dengan lebih baik lagi. Kriptografi ialah suatu cara untuk memastikan bahwa confidentiality (kerahasiaan), authentication (autentikasi), integrity (integritas), availability (ketersediaan) dan identification (identifikasi) pengguna data dapat

dipertahankan serta keamanan dan privasi data dapat disediakan untuk pengguna. [4]

Pada penelitian berjudul "Analisis dan Perancangan Aplikasi Kriptografi Keamanan File Berbasis Teks dengan menggunakan Metode RSA" yang dilakukan oleh Leo Benny dan telah diterbitkan pada jurnal Riset dan E-jurnal manajemen Informatika Komputer vol.1 tahun 2017 (ISSN: 2541-1330) mendapati bahwa keabsahan pengiriman maupun penerimaan file dokumen seperti pada kasus pengiriman file, pengiriman file via internet, email maupun via offline antar sesama perusahaan sangatlah diperlukan. Hal ini dikarenakan bahwa pengiriman file bisa dilakukan dengan mudah, maka aspek-aspek keamanan dalam proses pengirimannya perlu diperhatikan.

Untuk itu diperlukan suatu cara untuk mengamankan pesan rahasia tadi agar tidak diketahui oleh orang yang tidak berkepentingan. Penyembunyian pesan rahasia yang berupa file dalam arsip ZIP dapat menjadi salah satu solusi untuk keamanan data yang bersifat rahasia jika data tersebut ingin dikirimkan. Arsip ZIP merupakan kumpulan dari beberapa file yang terkompresi dimana ukuran dari file-file tersebut beragam. Biasanya orang tidak memperhatikan ukuran file dari arsip ZIP karena ukuran dari file-file di dalam arsip ZIP tersebut terkompresi. Dari hasil uji coba yang dilakukan, file yang berisi pesan rahasia berhasil disembunyikan pada arsip ZIP serta tidak akan terbaca pada aplikasi pembaca arsip ZIP. [5]

Pada penelitian berjudul "Implementasi Kriptografi RSA untuk Peningkatan Keamanan Database E-Commerce" yang dilakukan oleh Suci Rahmadhiyanti Nama dan telah diterbitkan di Jurnal Pelita Informatika vol.18 tahun 2019 (ISSN: 2301-9425) mendapati bahwa pada setiap sistem database, kemungkinan terjadinya kerusakan terhadap sistem dan hardware selalu ada. Namun hal tersebut juga memiliki dampak buruk karena rawan terjadi pencurian data.

Hal ini tentu akan merugikan banyak pihak, terutama bagi perusahaan, pengusaha, pemerintah, bank, dan pihak lain yang memiliki dokumen rahasia. Oleh karena itu, keamanan informasi merupakan faktor penting yang harus dipenuhi. Sebelum terjadi kerusakan yang mempengaruhi sistem maka keamanan database harus terjaga dengan mengimplementasikan kriptografi RSA untuk peningkatan keamanan database.

Tujuannya adalah untuk menjaga keamanan dan meningkatkan keamanan database sehingga menjamin proses operasional harian yang kritis bisa tetap berjalan, meskipun sistem sedang mengalami kerusakan. [6]

III. METODOLOGI

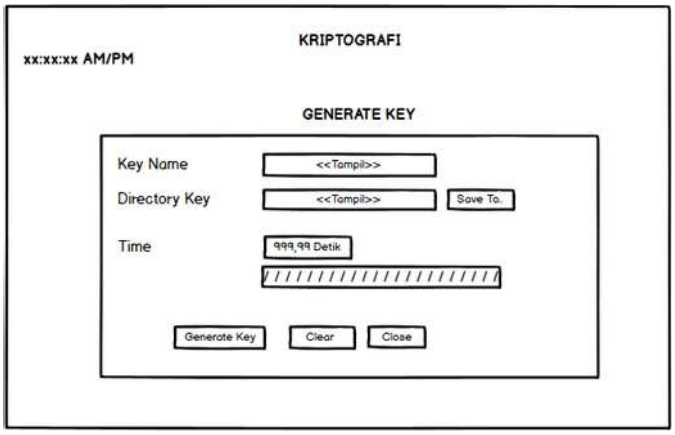
III.1. Data Penelitian dan Rencana Pengujian

Metode penelitian digunakan sebagai pedoman dalam pelaksanaan penelitian agar hasil yang dicapai tidak menyimpang dari tujuan yang telah dilakukan sebelumnya. Data yang akan digunakan dalam penelitian ini adalah data dari sekolah SMP Muhammadiyah 4 yang berupa dokumen RPP IPS semester genap dan penilaian kinerja guru *.doc, *.xls.

Penerapan metode yang akan digunakan dalam penelitian ini adalah dengan dengan menerapkan algoritma RSA (Rivest Shamir Adleman) pada aplikasi enkripsi dan dekripsi yang dibuat agar dapat menyandikan dokumen yang telah disebutkan. Pengujian aplikasi akan dilakukan dengan menguji semuan kemungkinan penyandian file yang dilakukan dari aplikasi dengan melihat keberhasilan penyandian file yang diujicobakan.

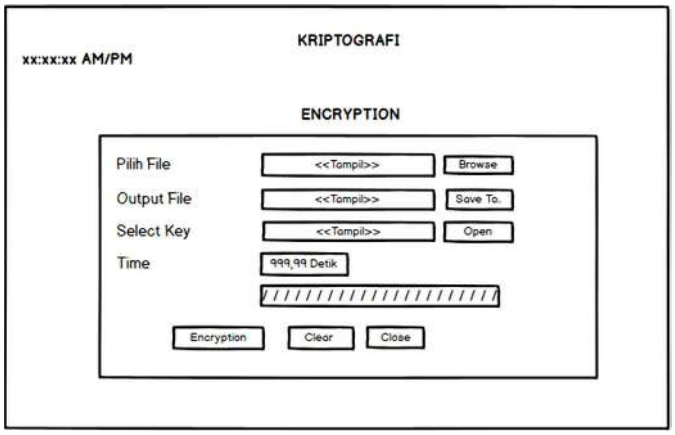
III.2. Rancangan Layar

Pada Form Generate Key, berfungsi untuk membuat sepasang Public key dan Private Key. Sepasang kunci ini nantinya akan digunakan saat akan melakukan encryription dan decryption sebuah file. Pengguna juga harus memasukan Key Name dan memilih tempat dimana akan disimpannya Key yang sudah dibuat. Berikut adalah tampilannya:



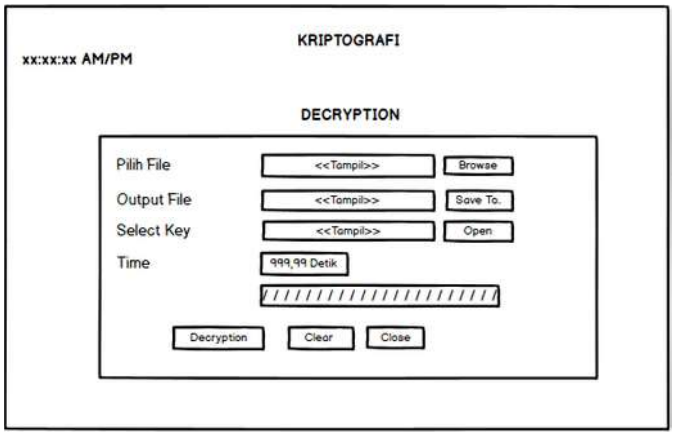
Gambar 2: Rancangan Layar Halaman Generate Key

Form Encryption, berfungsi untuk melakukan Encryption file. Pengguna harus memilih file yang akan dienkripsi, lalu memasukan lokasi dimana file akan disimpan, dan memasukan Public Key yang sudah dibuat sebelumnya. Berikut adalah tampilannya:



Gambar 3: Rancangan Layar Halaman Enkripsi

Pada Form Decryption, berfungsi untuk melakukan Decryption file. Penguna harus memilih file yang akan di decryption, lalu memasukan lokasi dimana file akan disimpan, dan memasukan Public Key yang sudah dibuat tadi. Berikut adalah tampilannya:



Gambar 4: Rancangan Layar Halaman Dekripsi

IV. HASIL DAN PEMBAHASAN

Pada bagian ini dibahas mengenai implementasi serta evaluasi dari sistem aplikasi pengamanan data (kriptografi). Ujicoba dilakukan dengan menggunakan file dokumen yang telah disebutkan pada bagian sebelumnya yang didapatkan dari SMP Muhammdiyah 4. File yang diujicobakan berkestensi *.doc, *.xls, dan *.txt.

Pada pengujian ini, akan membahas tentang perbandingan-perbandingan antara proses enkripsi dan proses dekripsi. File yang digunakan untuk pengujian yaitu *.doc, *.xls, dan *.txt.

IV.1. Proses Enkripsi

Pengujian proses enkripsi dapat dilihat di tabel dibawah ini:

Tabel 3: Pengujian Proses Enkripsi

Nama *File* Asli	Ukuran *File*Asli	Ukuran *File* Hasil Enkripsi	Waktu Enkripsi (detik)
RPP ips semester Genap	39 KB	98 KB	0.858
1 Lembar.doc			
New 1.txt	1 KB	3 KB	0.281
01 Penilaian Kinerja Guru 2017.xls	210 KB	637 KB	0.156

IV.2. Proses Dekripsi

Pengujian proses dekripsi dapat dilihat pada tabel dibawah ini:

Tabel 4: Pengujian Proses Dekripsi

Nama *File* Enkripsi	Ukuran *File* Enkripsi	Ukuran *File* Hasil Dekripsi	Waktu Dekripsi (detik)
en. RPP ips semester Genap 1 Lembar.doc	98 KB	39 KB	4.852
en.New 1.txt	3 KB	1 KB	3.963
en. 01 Penilaian Kinerja Guru 2017.xls	637 KB	210 KB	0.983

IV.3. Evaluasi Program

Dari serangkaian pengujian program yang telah dilakukan pada beberapa dokumen yang berjenis file *.doc, *.xls, dan *.txt. Terdapat kelebihan dan kekurangan dari hasil pengujian program tersebut antara lain :

- Kelebihan Program
  - File yang terenkripsi dapat dikembalikan secara utuh
  - Tidak menyebabkan kerusakan pada isi file
  - Apabila file enkripsi dibuka dengan menggunakan aplikasi yang lain, maka isi file tentu tidak akan sama seperti isi file yang asli. Sehingga keamanannya tetap terjamin.
- Kekurangan Program
  - File yang dienkripsi hanya dapat dilakukan pada jenis file *.doc, *.xls, dan *.txt.
  - Semakin besar ukuran file yang di-input, maka prosesnya pun akan berjalan semakin lama.

V. KESIMPULAN DAN SARAN

V.1. Kesimpulan

Berdasarkan perancangan, pembuatan, serangkaian uji coba dan analisis program aplikasi kriptografi ini, maka dapat diambil kesimpulan diantara lain:

- Dengan adanya aplikasi kriptografi, proses penyimpanan data-data sekolah yang penting menjadi lebih aman dan nyaman dari orang orang yang tidak berkepentingan.
- Proses dekripsi dengan kunci yang sesuai akan mengembalikan file menjadi file semula tanpa mengalami perubahan sedikit pun.
- Pada aplikasi yang dikembangkan ini, satu file asli dapat menghasilkan ciphertext yang berbeda-beda, karena proses pembangkitkan kunci RSA didasarkan oleh nilai P dan Q yang acak.
- Kriptografi RSA berhasil di implementasikan diaplikasi ini.

V.2. Saran

Adapun saran yang mungkin diperlukan untuk membuat aplikasi ini dapat berjalan dengan lebih baik lagi antara lain :

- Aplikasi ini diharapkan dapat ditingkatkan kinerjanya sehingga tidak hanya dapat mengenkripsi file dokumen *.doc, *.txt dan *.xls saja, namun bisa juga untuk file docx, video, audio maupun file gambar.
- Waktu proses enkripsi dan dekripsi file yang rata-rata berukuran besar diharapkan dapat berjalan lebih cepat pada hardware yang lebih baik.
- Disandingkan dengan algoritme kompresi dengan file yang lebih kecil.

VI. DAFTAR PUSTAKA

[1] D. Ariyus, “Pengantar Ilmu Kriptografi,” Penerbit Andi, 2008, doi: 10.1017/CBO9781107415324.004.

[2] I. Halik and Y. Prayudi, “Studi dan Analisis Algoritma Rivest Code 6 (RC6) dalam Enkripsi/Dekripsi Data,” Snati, vol. 6, no. D, 2005, [Online]. Available: http://journal.uii.ac.id/index.php/Snati/article/view/1402.

[3] A. Ginting, R. R. Isnanto, and I. P. Windasari, “Implementasi Algoritma Kriptografi RSA untuk Enkripsi dan Dekripsi Email,” J. Teknol. dan Sist. Komput., vol. 3, no. 2, p. 253, 2015, doi: 10.14710/jtsiskom.3.2.2015.253-258.

[4] M. F. Hamdani, Z. Sari, and A. S. Kholimi, “Plug-in Pada Microsoft Office Word Untuk Enkripsi Dokumen Dengan Menggunakan Algoritma Kunci Publik Rsa,” J. Repos., vol. 2, no. 6, p. 781, 2020, doi: 10.22219/repositor.v2i6.303.

[5] L. Benny, “Analisis Dan Perancangan Aplikasi Kriptografi Keamanan File Berbasis Teks Dengan Menggunakan Metode Rsa,” vol. 1, no. April P-ISSN: 2541-1322, pp. 15–23, 2017.

[6] S. Rahmadhiyanti, “Implementasi Kriptografi Rsa Untuk Peningkatan Keamanan Database E-Commerce,” Pelita Inform., vol. 8, p. 4, 2019.