Jurnal Ilmu Komputer dan Informatika (JIKI)
Vol. 2, No. 1, Juni 2022, Hal. 57-66
https://jiki.jurnal-id.com
DOI: https://doi.org/10.54082/jiki.19
P-ISSN: 2807-6664
E-ISSN: 2807-6591

Implementasi Algoritma Kriptografi Rivest Shamir Adlemen untuk Mengamankan Data Ijazah pada SMK Swasta Prama Artha Kab. Simalungun

Wahyudi[*1], Dedy Hartama[2], Ika Okta Kirana[3], Sumarno[4], Indra Gunawan[5]

[1,2,3,4,5]Teknik Informatika, STIKOM Tunas Bangsa Pematangsiantar, Indonesia
Email: [1]yudi19821@gmail.com, [2]dedyhartama@amiktunasbangsa.ac.id,
[3]ikaokta@amiktunasbangsa.ac.id, [4]sumarno@amiktunasbangsa.ac.id, [5]indra@amiktunasbangsa.ac.id

Abstrak

Data ijazah merupakan suatu data yang tergolong sangat penting pada sebuah instansi sekolah. Keamanan data tersebut sangat diperlukan untuk menjaga kerahasiaan data dimana pada data ijazah terdapat nomor ijazah yang merupakan satu-satunya bukti surat tamat belajar di sekolah, guna menghindari terjadinya pencurian maupun manipulasi data tersebut maka dibutuhkan sebuah sistem keamanan data. Salah satu teknik dalam mengamankan data yaitu dengan menggunakan Kriptografi yaitu sebuah ilmu matematika yang berhubungan dengan aspek keamanan data. Salah satu ilmu kriptografi yang penulis terapkan dalam mengamankan data ijazah dengan mengimplementasikan algoritma RSA (Rivest Shamir Adlemen). Hasil akhir yang dicapai pada penelitian ini yaitu dapat mengenkripsi data ijazah menjadi *chipertext* agar tidak dapat dibaca atau di manipulasi oleh orang lain, dan *Decrypt* file tersebut menjadi *plaintext* agar dapat dibaca kembali.

Kata kunci: Enkripsi, Data Ijazah, *Decrypt*, Rivest Shamir Adlemen

Abstract

Ijazah data is data that is classified as very important in a school institution. Data security is very necessary to maintain the confidentiality of data where in the certificate data there is a certificate number which is the only proof of graduation from school, in order to avoid theft or manipulation of the data, a data security system is needed. One of the techniques in securing data is by using cryptography, which is a mathematical science that deals with aspects of data security. One of the cryptographic sciences that the author applies in securing diploma data is by implementing the RSA algorithm (Rivest Shamir Adlemen). The final result to be achieved in this research is that it can encrypt the certificate data into cypertext so that it cannot be read or manipulated by others, and describe the file into plaintext so that it can be read again.

Keywords: *Data Ijazah, Rivest Shamir Adlemen, Encryption, Description*

1. PENDAHULUAN

Pada zaman teknologi informasi, data atau informasi merupakan suatu aset yang sangat berharga dan harus dilindungi. Yang terjadi selanjutnya adalah kemajuan teknologi komputer. Kemajuan teknologi komputer bermanfaat bagi segala aspek kehidupan manusia. Dari hal-hal kecil yang sederhana hingga hal-hal yang sangat kompleks, komputer dapat melakukannya. Keunggulan dari aplikasi komputer ini selain memberi kemudahan terhadap berbagai kegiatan pengolahan data dan informasi di berbagai bidang kehidupan misalnya sekolah-sekolah.

Dengan kemajuan teknologi informasi, komunikasi dan komputer, muncul masalah baru yaitu keamanan data dan informasi dan dalam hal ini membuka kemungkinan bagi para penyerang yang secara tidak bertanggung jawab menggunakannya sebagai kejahatan dan tentunya akan merugikan beberapa pihak.

Saat ini semakin banyak sekolah yang menyadari pentingnya mengamankan suatu data salah satunya adalah data ijazah. Untuk menjaga kerahasiaan data ijazah yang sangat peting di dalam dunia pendidikan diperlukan cara atau teknik enkripsi dan *Decrypt* yang berfungsi agar data tidak akan mudah di curi atau diketahui oleh orang lain serta data tidak akan mudah di ubah.

DOI: https://doi.org/10.54082/jiki.19
P-ISSN: 2807-6664
E-ISSN: 2807-6591

SMK Swasta Prama Artha saat ini belum menerapkan sistem keamanan sebuah data sehingga data sering sekali tersebar baik di media penyimpanan maupun di media komunikasi khususnya pada data ijazah yang sangat penting didalam sekolah. Jika data tersebut sampai jatuh ketangan yang salah dapat dijadikan untuk mencari keuntungan dan tindak kejahatan oleh sesorang. Apalagi data yang ada setiap tahun akan terus bertambah mengingat ijazah merupakan satu satunya yang diberikan oleh pemerintah sebagai bukti lulus siswa dan keamanan yang sangat rentan dalam mengaksesnya, sehingga sangat rawan diambil dan digunakan oleh pihak yang tidak berhak.

Algoritma kriptografi RSA dianggap dapat memenuhi tingkat sekuriti yang tinggi. Dengan kombinasi hasil kali 2 (dua) bilangan prima. Keamanan algoritma RSA terletak pada sulitnya untuk memfaktorkan bilangan prima yang relatif lebih besar. Pemfaktoran dilakukan untuk memperoleh kunci privat. Selama bilangan pemfaktoran prima yang besar belum ditemukan algoritma yang berhasil memecahkan, maka selama itu pula algoritma RSA akan tetap terjamin keamanannya [1]. Penggunaan algoritma RSA selanjutnya yaitu pada penelitian yang dilakukan oleh Noviana Astuti tentang kemanan implementasi dokumen *office* emnggunakan algoritma RSA yang sangat baik tingkat kemanannya [2].

Dari uraian di atas, penerapan algoritma kriptografi RSA menjadi solusi yang baik untuk keamanan data ijazah yang akan dibangun pada SMK Swasta Prama Artha Kecamatan Bandar Huluan untuk menjamin keamanan dan kerahasiaan data ijazah yang disimpan didalam komputer ataupun data yang dikirimkan dengan penggunaan algoritma RSA pada pesan teks yang pengamanannya berupa file document dan penjumlahan angka sehingga isi datanya tidak dapat dimengerti oleh pihak lain.

2. TINJAUAN PUSTAKA

2.1. Keamanan Data

Masalah keamanan data merupakan masalah yang sangat serius dalam kegiatan bisnis di era digital. kegiatan bisnis di era digital merupakan kegiatan bisnis yang sebagian besar menggunakan teknologi aplikasi komputer serta menjadikan komputer server sebagai tempat menyimpan data-data dalam kegiatan bisnis sehingga dapat disimpulkan media komputer menjadi faktor utama di dalam kegiatan bisnis yang dilakukan. Masalah utama adalah keamanan data yang disimpan di komputer serta data yang dikirimkan melalui jaringan komputer dan aplikasi komputer [3].

2.2. Kriptografi

Kata kriptografi berasal dari bahasa Yunani. Dalam bahasa Yunani kriptografi terdiri dari dua buah kata yaitu cryptos dan graphia. Kata sandi berarti rahasia (secret), dan graphia berarti tulisan. Jadi berarti dalam kata sandi adalah yang ditulis secara rahasia. Menurut terminologinya, kriptografi adalah ilmu yang mempelajari bagaimana menjaga kerahasiaan pesan sehingga isi pesan yang dikirimkan aman bagi penerima pesan [4].

Dalam kriptografi, pesan atau informasi yang dapat di baca disebut sebagai *plaintext* atau *clear text*. Proses pengubahan teks asli (plain text) menjadi teks sandi (ciphertext) disebut enkripsi. Pesan yang belum dibaca disebut ciphertext. Proses kebalikan dari enkripsi disebut dekripsi. Dekripsi Mengembalikan teks sandi (teks sandi) sebagai teks asli (teks biasa). Proses enkripsi dan dekripsi membutuhkan untuk menggunakan total informasi rahasia, biasanya disebut kunci [5].

2.3. Algoritma RSA (Rivest Shamir Adlemen)

Algoritma RSA dibuat oleh 3 orang peneliti dari MIT (Massachussets Institute of Technology) pada tahun 1976, yaitu: Ron (R)ivest, Adi (S)hamir, dan Leonard (A)dleman. Kekuatan algoritma RSA terletak pada sulitnya memfaktorkan bilangan besar menjadi faktor-faktor bilangan primanya, sehingga semakin besar bilangan prima yang digunakan semakin baik atau aman. Dalam kriptografi menggunakan algoritma RSA terdapat tiga proses yaitu proses pembangkitan kunci publik dan kunci privat, proses enkripsi, dan proses dekripsi [6].

Pada tahun 1977, Ronald L. Rivest, Adi Shamir, dan Leonard M. Adleman merumuskan algoritma praktis yang mengimplementasikan sistem kriptografi kunci publik yang disebut dengan sistem

DOI: https://doi.org/10.54082/jiki.19
P-ISSN: 2807-6664
E-ISSN: 2807-6591

kriptografi RSA. Sepasang kunci yang dipakai pada kedua proses ini adalah kunci publik (*e*,*n*) sebagai kunci enkripsi dan kunci privat *d* sebagai sebagai kunci dekripsi dimana *e*, *d* dan *n* adalah bilangan bulat positif. Algoritma RSA adalah sebuah *block cipher algorithm* (algoritma yang bekerja per blok data) yang mengelompokkan plaintext menjadi blok-blok terlebih dahulu sebelum dilakukan enkripsi hingga menjadi ciphertext [7].

Pada algoritma RSA terdapat 3 langkah utama yaitu *keygeneration* (pembangkit kunci), enkripsi dan dekripsi. Kunci pada RSA mencakup dua buah kunci, yaitu *public key* dan *private key*. *Public key* digunakan untuk melakukan enkripsi, dan dapat diketahui oleh orang lain. Sedangkan *private key* tetap dirahasiakan dan digunakan untuk melakukan dekripsi [8]**.**

Algoritma RSA memiliki besaran-besaran sebagai berikut:

1. p dan q bilangan prima (rahasia)
2. n = p x q (tidak rahasia)
3. $\phi(n) = (p-1)(q-1)$ (rahasia)
4. e (kunci enkripsi) (tidak rahasia)
5. d (kunci dekripsi) (rahasia)
6. m (plainteks) (rahasia)
7. c (cipherteks) (tidak rahasia)

RSA adalah suatu blok sandi rahasia tempat teks asli dan teks rahasia merupakan bilangan bulat antara 0 dan n-1 untuk beberapa n. Enkripsi dan dekripsi berasal dari beberapa bentuk berikut ini, untuk beberapa blok teks asli M dan blok teks rahasia C.

$$C = M' \bmod n$$

$$M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \text{ od } n$$

Blok pengirim maupun penerima harus mengetahui nilai n dan e, dan hanya penerima saja yang mengetahui nilai d. ini merupakan algoritma enkripsi kunci umum dengan kunci umum sebesar KU = {e,n} dan kunci khusus sebesar KR = {d,n}. Agar algoritma ini bisa memenuhi syarat sebagai enkripsi kunci umum yang baik, maka harus memenuhi ketentuan-ketentuan seperti berikut:

1. Kemungkinan menemukan nilai e,d,n sedemikian rupa sehingga $M^{ed}=M \bmod n$ untuk semua M<n
2. Relative mudah menghitung M^e dan C^d untuk semua nilai M < n
3. Tidak mudah menghitung menentukan d, yang diberi e dan n.

Dua ketentuan pertama bisa terpenuhi dengan mudah. Sedangkan ketentuan ketiga baru bisa terpenuhi untuk nilai e dan n yang besar. Pembangkitan Kunci

1. Memilih dua bilangan prima p, q. Bilangan ini harus cukup besar (minimal 100 digit).
2. Menghitung n = p . q. Bilangan n disebut *parameter security* (sebaiknya $p \neq q$, sebab jika p = q maka $n = p^2$ sehingga p dapat diperoleh dengan menarik akar pangkat dua dari n).
3. Menghitung $\varphi(n) = (p-1)(q-1)$.
4. Memilih bilangan bulat e dengan algoritma Euclid yaitu gcd $(\varphi(n),e)=1$; dimana $1< e < \varphi(n)$.
5. Menghitung d dengan rumus d = e-1mod $\varphi(n)$ Atau $e \cdot d \equiv 1 \pmod{\varphi(n)}$. Perhatikan bahwa $e \cdot d \equiv 1 \pmod{\varphi(n)}$ ekivalen dengan $e \cdot d = 1 + k\,\varphi(n)$, sehingga secara sederhana d dapat dihitung dengan : $d = (1 + k \cdot \varphi(n)) / e$
6. Kunci umum (kunci public) adalah KU = {e,n}
7. Kunci pribadi (kunci privat) adalah KR = {d,n}

2.4. Ijazah

Ijazah merupakan bukti seseorang yang telah menyelesaikan masa pendidikannya. Ijazah diberikan oleh lembaga pendidikan kepada peserta didiknya yang telah dinyatakan "Lulus". Ijazah yang sah atau asli adalah ijazah yang dikeluarkan oleh satuan pendidikan yang telah diakreditasi oleh pemerintah. Jenis ijazah yang dimiliki oleh seseorang dikelompokkan berdasarkan jenjang pendidikannya, yaitu SD, SMP, SMA, Pendidikan Tinggi [9].

Ijazah merupakan bukti seseorang telah menyelesaikan masa pendidikkannya. Ijazah diberikan oleh lembaga pendidikan kepada peserta didiknya yang telah dinyatakan “lulus”. Ijazah yang sah atau asli adalah ijazah yang dikeluarkan oleh satuan pendidikan yang telah diakreditasi oleh pemerintah. Saat ini

DOI: https://doi.org/10.54082/jiki.19
P-ISSN: 2807-6664
E-ISSN: 2807-6591

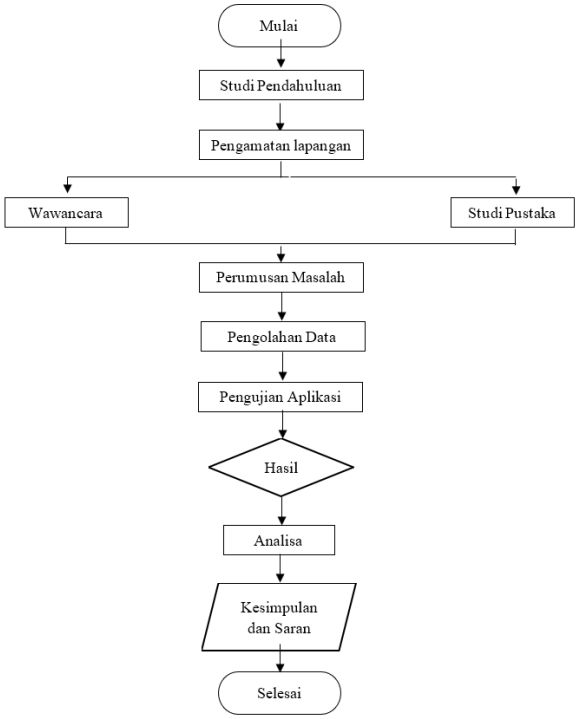
ijazah merupakan dokumen yang penting yang digunakan sebagai syarat seseorang untuk melamar pekerjaan [10].

3. METODE PENELITIAN

Metode penelitian merupakan prosedur dan langkah-langkah yang dilakukan peneliti untuk mengumpulkan data. Adapun prosedur dan langkah-langkah yang harus ditempuh adalah waktu penelitian, sumber data, dan data yang diperoleh selanjutnya diolah dan dianalisis.

3.1. Rancangan Penelitian

Dalam aplikasi kriptografi algoritma RSA yang menggunakan Kunci Public dan Kunci private tahapan ini dimaksudkan agar perancangan mudah dipahami berdasarkan urutan langkah dari awal hingga akhir proses. Berikut adalah rancangan penelitian bisa dilihat pada Gambar 1 berikur ini.



Gambar 1. Rancangan Penelitian

Penjelasan Alur penelitian yang dibuat penulis seperti pada gambar 1 sebagai berikut:

1. Studi Pendahuluan
   Studi pendahuluan dilaksanakan untuk memperoleh masukan mengenai data yang akan diteliti. Melalui studi ini, diharapkan dapat memperoleh informasi mengenai permasalahan yang diangkat dalam penelitian dan variable-variabel yang terkait dengan masalah tersebut.
2. Pengamatan di Lapangan
   Pada tahap ini penulis melakukan *Interview* di SMK Swasta Prama Artha yang beralamat di Serbelawan Kecamatan Bandar Huluan, Kabupaten Simalungun tentang Keamanan data-data yang akan diamankan. Berbagai referensi yang mengacu dari berbagai sumber, baik dari buku maupun dari jurnal yang dijadikan referensi untuk memperoleh data dan teori yang dibutuhkaan untuk mendukung penulis dalam melakukan penelitian.
3. Perumusan Masalah
   Permasalahan yang penulis rumuskan untuk menyelesaikan masalah tersebut yaitu bagaimana cara membuat suatu system untuk mengamankan data ijazah pada SMK Swasta Prama Artha yang

DOI: https://doi.org/10.54082/jiki.19
P-ISSN: 2807-6664
E-ISSN: 2807-6591

beralamat di Serbelawan Kecamatan Bandar Huluan, Kabupaten Simalungun menggunakan algoritma RSA.

4. Pengolahan Data
   Pada langkah ini data-data yang sudah didapat dari studi pendahuluan dan pengamatan di lapangan yang kemudian diolah untuk menyelesaikan permasalahan data yang ditemukan.
5. Pembuatan Aplikasi
   Setelah data yang sudah diolah atau ditentukan langkah selanjutnya adalah merancang aplikasi yang dapat menyelesaikan permasalah yang dialami.
6. Pengujian Aplikasi
   Setelah pembuatan aplikasi yang sudah jadi, kemudian langkah pengujian aplikasi yang sudah dirancang untuk memperoleh hasil akhir, apakah aplikasi yang dirancang sesuai yang diharapkan untuk menyelesaikan masalah yang sudah didapat.

3.2. Prosedur Pengumpulan Data

Studi pustaka merupakan metode pengumpulan data yang diperoleh dari buku-buku atau jurnal dalam pencarian referensi terkait pengumpulan data maupun perancangan aplikasi yang akan dibangun, yaitu referensi mengenai dokumen, kriptografi, algoritma RSA.

Analisis yang dilakukan adalah analisis terhadap pola dan karakteristik dari algoritma kriptografi terkait dan analisis terhadap test-case untuk validasi algoritma kriptografi yang dapat diterapkan.

3.3. Analisa Data

Analisis data merupakan tahapan dimana dilakukannya analisis terhadap data-data apa saja yang diolah dalam system atau prosedur sebuah rancangan, dalam hal ini data yang akan dienkripsi pada aplikasi kriptografi ini adalah *file* dengan ekstensi *pdf*. Bahan yang digunakan dalam penelitian ini adalah data ijazah pada SMK Swasta Prama Artha yang beralamat di Serbelawan Kecamatan Bandar Huluan, Kabupaten Simalungun. Bahan tersebut akan digunakan sebagai sampel untuk ujicoba enkripsi menggunakan algoritma RSA. Bahasa pemogram pada penelitan ini PHP dan Database MYSQL. Editor yang digunakan dalam membangun aplikasi ini yaitu *Sublime Text 3*.

3.4. Instrument Penelitian

Instrumen penelitian yang dipergunakan dalam penelitian ini berupa wawancara terhadap SMK Swasta Prama Artha yang beralamat di Serbelawan Kecamatan Bandar Huluan, Kabupaten Simalungun tentang data apa yang akan di amankan.

Instrumen penelitian adalah suatu alat pengumpul data yang digunakan untuk mengukur fenomena alam maupun sosial yang diamati. Dengan demikian, penggunaan instrumen penelitian yaitu untuk mencari informasi yang lengkap mengenai suatu masalah, fenomena alam maupun sosial.

Setelah melakukan wawancara terhadap SMK Swasta Prama Artha yang beralamat di Serbelawan Kecamatan Bandar Huluan, Kabupaten Simalungun. maka di tentukan data yang diamankan adalah data-data ijazah. Maka diperlukan cara atau teknik enkripsi dan dekripsi yang berfungsi agar data tidak akan mudah dicuri dan disalahgunakan. Adapun alur penelitian yang digunakan dalam menyelesaikan kasus ini ditunjukkan pada Gambar 2.

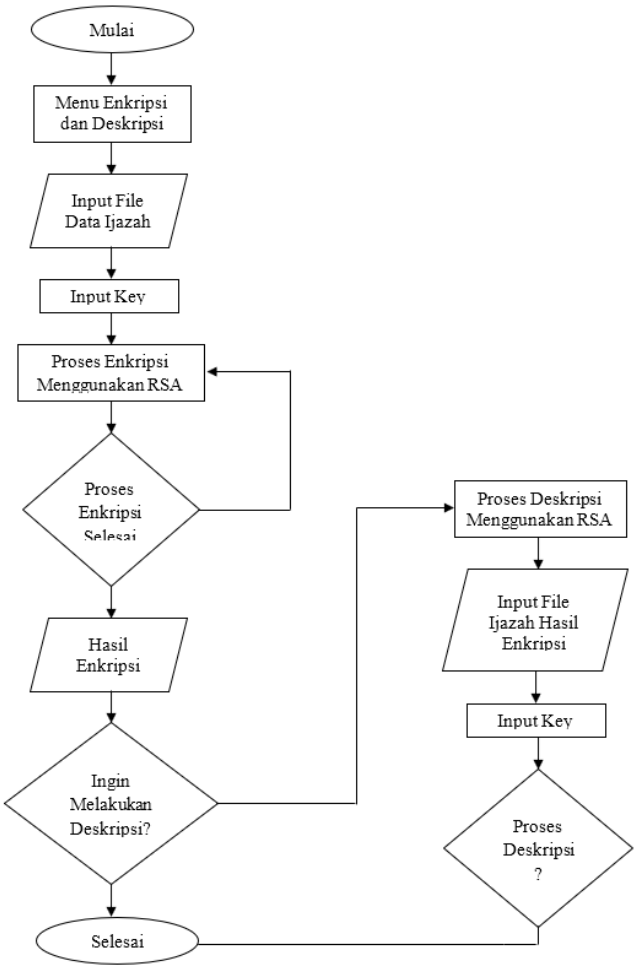
Berdasarkan Gambar di atas dapat dijelaskan bahwa:

1. Mulai adalah kondisi dimana program baru saja dijalankan pada aplikasi metode *RSA*.
2. Input *file* data ijazah adalah kondisi dimana aplikasi diberikan inputan *file* data ijazah yang akan diproses. Kemudian user diminta memasukkan *key* yang sudah ditentukan.
3. Proses enkripsi adalah kondisi dimana pengguna memilih proses enkripsi data *file* data ijazah yang sudah diinputkan, setelah itu akan terjadi dua kondisi yaitu apakah sudah selesai diproses atau masih belum, Jika proses sudah selesai maka muncul hasil enkripsi, sebaliknya jika belum maka akan terus dilakukan proses enkripsi sampai seluruh inputan benar selesai dienkripsi.
4. Setelah muncul hasil enkripsi maka akan ada kondisi apakah akan langsung didekripsi atau tidak oleh pengguna, jika tidak maka hasil enkripsi menjadi hasil final akan tetapi jika pengguna

DOI: https://doi.org/10.54082/jiki.19
P-ISSN: 2807-6664
E-ISSN: 2807-6591

melakukan dekripsi maka akan dilakukan proses dekripsi dengan memasukan key yang sudah ditentukan.

5. Selesai adalah kondisi dimana hasil yang diinginkan oleh pengguna sudah keluar, maka aplikasi sudah selesai berjalan.



Gambar 2. Instrument Penelitian

3.5. Pemodelan Metode

Dalam melakukan enkripsi data menggunakan RSA ada beberapa tahapan yang harus dilakukan yaitu menentukan 2 buah bilangan prima acak sampai kepada pembangkitan kunci. Keamanan dari algoritma RSA masih tergolong cukup aman selagi masih belum ditemukannya faktorisasi prima dari kunci pribadi maka selama itu keamanan menggunakan algoritma RSA masih terjaga. Berikut ini akan dijelaskan bagaimana proses pembangkitan kunci RSA:

1. Pilih 2 buah bilangan prima yang acak, dalam kasus ini penulis memilih p=17 dan q=11.
2. Tahap Hitung nilai n dimana n = p*q = 187.
3. Tahap Hitung nilai totient(n) = (p-1)*(q-1)=16*10=160.
4. Tahap Pilih nilai e sedemikian sehingga relatif prima terhadap totient(n) =160 dan kurang dari totient(n); maka harus didapatkan nilai e*d mod 160 =1.
5. Karena hasil totient(n) berakhiran 4 maka kita mengambil angka 5 karena hasil dari 5 mod 4 =1, maka kita harus mencari 161 karena nilai 161 mod 160=1, maka didapatkan e*d mod 160 = 1 dimana nilai e = 7 dan nilai d = 23.

Berdasarkan uraian diatas maka didapatkan kunci private (d) = 23 dan kunci publik (e) = 7 dengan n = 187.

DOI: https://doi.org/10.54082/jiki.19
P-ISSN: 2807-6664
E-ISSN: 2807-6591

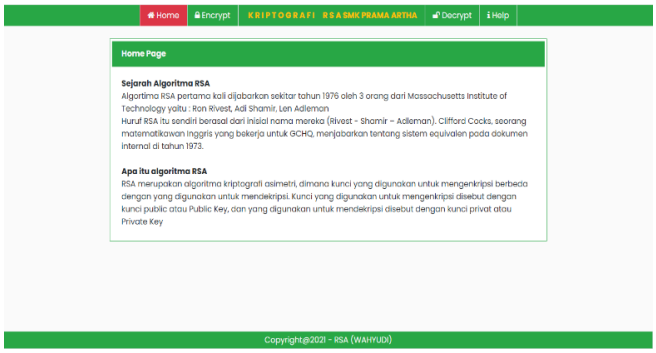
4. HASIL DAN PEMBAHASAN

Dalam implementasi sistem akan dibahas mengenai tampilan akhir antarmuka sistem yang disesuaikan dengan perancangan sistem yang telah dibuat pada pembahasan sebelumnya.

4.1. Hasil

1. Tampilan Menu Utama

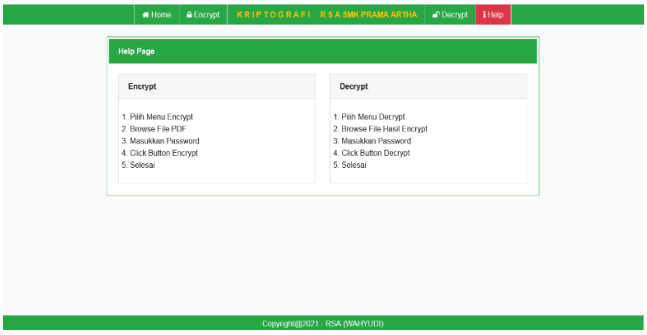
Form ini menampilkan menu-menu yang ada pada *form* utama admin. Tampilan form ini dapat dilihat seperti Gambar 3 di bawah ini.



Gambar 3. Tampilan Menu Utama

2. Tampilan Menu *Help*

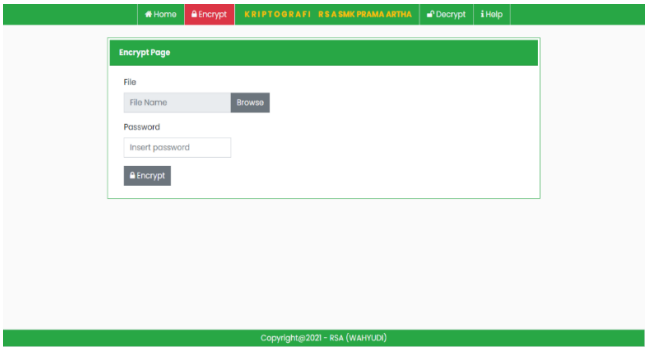
Jika *User* mengalami kesulitan dalam menggunakan aplikasi tersebut maka *user* dapat melihat cara kerjanya dengan mengklik menu *help*, seperti pada Gambar 4 di bawah ini.



Gambar 4. Tampilan Menu *Help*

3. Tampilan Menu Enkripsi

Dimana pada tampilan ini akan mengupload *file pdf* yang akan dienkripsi. Tampilan enkripsi ini dapat dilihat seperti pada Gambar 5 di bawah ini.

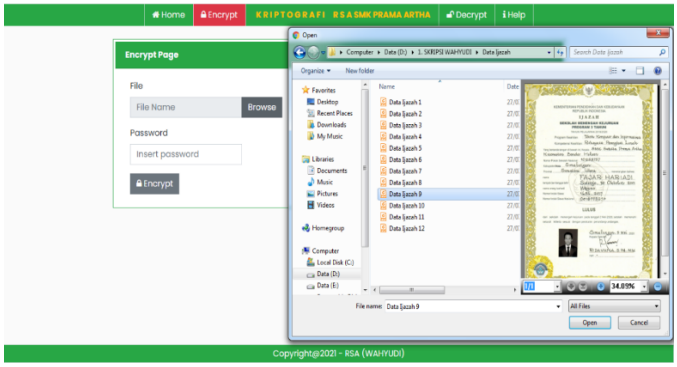


Gambar 5. Tampilan Menu Enkripsi

DOI: https://doi.org/10.54082/jiki.19
P-ISSN: 2807-6664
E-ISSN: 2807-6591

4. Tampilan Pencarian *File* Enkripsi

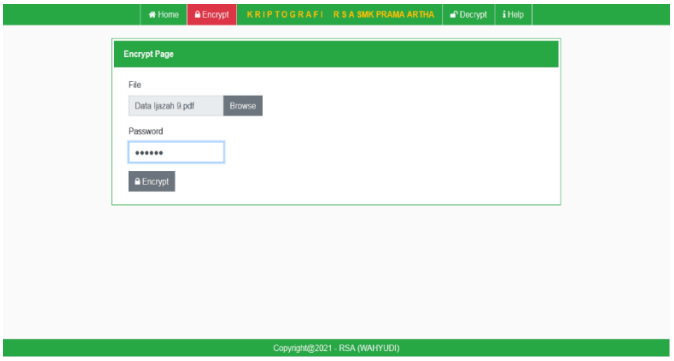
Setelah muncul *menu* enkripsi dilakukan *upload file pdf* dengan mencari data ijazah yang akan dienkripsi. Setelah itu pilih *open*, menu pencarian *file* yang akan di enkripsi dapat dilihat seperti pada Gambar 6 di bawah ini.



Gambar 6. Tampilan Menu Pencarian File Enkripsi

5. Tampilan *Menu* Pengisian *Password/* Kunci Enkripsi

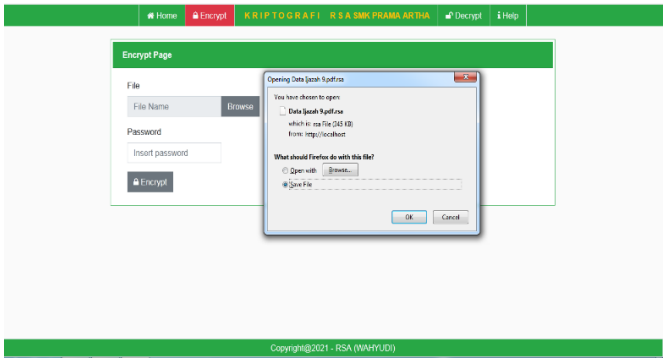
Sebelum mengenkripsi file maka user terlebih dahulu memasukkan password, password yang dimasukkan sesuai keinganan *user*. lalu klik *encrypt* untuk melakukan proses *enkripsi file*, tampilan pengisian *password* dapat dilihat pada Gambar 7 di bawah ini.



Gambar 7. Tampilan Menu pengisian *Password*

6. Tampilan Proses Enkripsi Berhasil

Proses enkripsi berhasil selanjutnya pilih *save file* lalu klik ok, data ijazah akan tersimpan dan dapat dilihat hasil enkripisinya. Proses enkripsi berhasil dapat dilihat pada Gambar 8 di bawah ini.

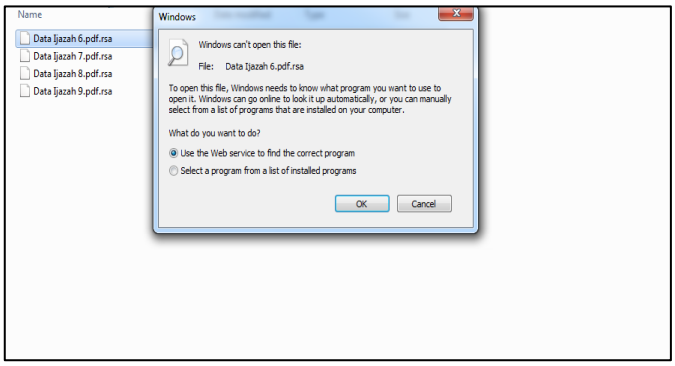


Gambar 8. Proses Enkripsi Berhasil

DOI: https://doi.org/10.54082/jiki.19
P-ISSN: 2807-6664
E-ISSN: 2807-6591

7. Tampilan *File* Hasil Enkripsi

Hasil enkripsi telah tampil dimana isi dari *file pdf* tidak bisa dibuka dan dilihat. Tampilan hasil enkripsi dapat dilihat pada Gambar 9 di bawah ini.



Gambar 9. Tampilan Hasil Enkripsi

Proses *Decrypt* file yang telah berhasil di enkripsi yaitu sama dengan proses enkripsi *file* tersebut, mulai dari *upload file* hingga sampai *download file* hasil *Decrypt*

4.2. Pembahasan Prosedur Kerja Sistem

1. Dalam tampilan menu utama terdapat menu aplikasi yaitu menu *Home* Enkripsi *file*, *Help* dan *Decrypt file*.
2. Pada menu utama pilih enkripsi *file*, jika sudah selesai maka selanjutnya muncul tampilan pencarian *file* yang akan dienkripsi. Jika sudah selesai pilih *file* yang akan dienkripsi.
3. Kemudian pengisian *password* untuk melakukan enkripsi setelah memilih file yang akan dienkripsi.
4. Jika telah selesai file akan tersimpan di komputer dan *user* dapat mellihat *file* hasil enkripsi.
5. Untuk melakukan *Decrypt* pilih menu decrypt kemudian *user* diminta untuk memasukkan *file* yang sebelumnya dienkripsi.
6. Pengisian *password* sebagai langkah selanjutnya dengan memasukkan *password* sesuai keinginan *user* dalam bentuk angka tetapi harus sama dengan *password* yang digunakan untuk mengenkripsi *file* sebelumnya.
7. Jika *password* yang diinputkan berbeda pada saat enkripsi *file* sebelumnya maka proses *Decrypt* tidak berjalan atau proses *error*.
8. Jika semua benar *password* yang diinputkan sama dengan *password* enkripsi maka selanjutnya akan muncul perintah untuk mendownload *file* tersebut.

5. KESIMPULAN

Pengamanan data pada SMK Swasta Prama Artha Bandar Huluan memiliki beberapa kesimpulan yaitu penggunaan Aplikasi yang dibangun dapat membantu dalam mengamankan data *file* ijazah pada SMK Swasta Prama Artha Bandar Huluan menggunakan metode Algoritma Kriptografi *RSA* (*Rivest Shamir Adleman*), Data Ijazah yang dienkripsi dan di*Decrypt* hanya dapat dibuka dan dilihat oleh orang yang memiliki dan mengetahui *password* enkripsi. Penggunaan Sistem yang dibangun mampu memberikan keamanan yang baik sehingga data ijazah tidak dapat dibuka dan dilihat oleh orang yang tidak berkepentingan atau yang tidak berhak.

DAFTAR PUSTAKA

[1] I. Gunawan, “Kombinasi Algoritma Caesar Cipher dan Algoritma RSA untuk pengamanan File Dokumen dan Pesan Teks,” InfoTekJar (Jurnal Nas. Inform. dan Teknol. Jaringan), vol. 2, no. 2, pp. 124–129, 2018, doi: 10.30743/infotekjar.v2i2.266.

DOI: https://doi.org/10.54082/jiki.19
P-ISSN: 2807-6664
E-ISSN: 2807-6591

[2] N. ASTUTI, "Implementasi Keamanan Dokumen Office Dengan Algoritma Rhivest Shamir Adleman (RSA)," Universitas Pembangunan Panca Budi, 2021.

[3] S. Susanto and A. A. Trisusilo, "Penerapan Algoritma Asimetris Rsa Untuk Keamanan Data Pada Aplikasi Penjualan Cv. Sinergi Computer Lubuklinggau Berbasis Web," Simetris J. Tek. Mesin, Elektro dan Ilmu Komput., vol. 9, no. 2, pp. 1043–1052, 2018, doi: 10.24176/simet.v9i2.2537.

[4] A. Arief and R. Saputra, "Implementasi Kriptografi Kunci Publik dengan Algoritma RSA-CRT pada Aplikasi Instant Messaging," Sci. J. Informatics, vol. 3, no. 1, pp. 46–54, 2016, doi: 10.15294/sji.v3i1.6115.

[5] 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.

[6] A. Syahputra, I. Algoritma, and F. Untuk, "Implementasi Algoritma Freivlds Untuk Pembangkitan Kunci Algoritma RSA Pada Pengamanan Data Video," vol. 10, pp. 70–77, 2021.

[7] P. Pahrizal and D. Pratama, "Implementasi Algoritma Rsa Untuk Pengamanan Data Berbentuk Teks," Pseudocode, vol. 3, no. 1, pp. 44–49, 2016, doi: 10.33369/pseudocode.3.1.44-49.

[8] S. Sumarno, "Analisis Kinerja Kombinasi Algoritma Message-Digest Algortihm 5 (MD5), Rivest Shamir Adleman (RSA) dan Rivest Cipher 4 (RC4) Pada Keamanan E-Dokumen," J. Sist. Inf. dan Ilmu Komput. Prima (JUSIKOM PRIMA), vol. 2, no. 1, pp. 41–48, 2018, [Online]. Available: http://jurnal.unprimdn.ac.id/index.php/JUSIKOM/article/view/140.

[9] L. Ambarwati, B. Web, and D. Menggunakan, "Perancangan Sistem Pengecekan Ijazah berbasis Web _ Lia Ambarwati - Academia."

[10] W. W. Sari, "Implementasi Metode MD2 Untuk Otentikasi Hasil Scan Citra Ijazah," Resolusi Rekayasa Tek. Inform. dan Inf., vol. 1, no. 5, pp. 302–311, 2021.