Jurnal Mahajana Informasi. Vol. 6, No. 2, Desember 2021
e-ISSN : 2527-8290

Rancang Bangun Sistem Keamanan Data Digital Dengan Metode RSA Berbasis Dekstop

Riki Rezki[1*], R. Fanry Siahaan[2]

[1]Program Studi Teknik Informatika, STMIK Pelita Nusantara, Jl. Iskandar Muda No.1 Medan, Sumatera Utara, Indonesia
[2] Program Studi Teknik Informatika, , Jl. Medan Lubuk Pakam Simp. Timbangan, Deli Serdang, Sumatera Utara, Indonesia

E-mail[1]: rikirezki19@gmail.com , rfanry@gmail.com

Abstrak

Ada banyak data digital dan salah satunya adalah file PDF (Portable Document Format) memiliki kelebihannya yaitu sifatnya yang sangat fleksibel dan kekurangan file (Portable Document Format) ialah apabila tidak dapat di edit dengan mudah. File PDF (Portable Document Format) ini dapat dibuka di komputer manapun atau bahkan smartphone tanpa adanya perubahan pada data atau isinya. Namun saat ini telah banyak teknik agar dapat mengubah isi dari PDF tersebut. Dampak yang terjadi jika dokumen yang menyimpan berbagai informasi atau data rahasia tidak memiliki keamanan terhadap ancaman dari dalam maupun luar akan menimbulkan beberapa dampak, misalnya terganggunya kegiatan operasional, rusaknya reputasi, kerugian finansial, karya cipta, dan kehilangan kepercayaan dari pihak lainnya. Ada banyak teknik dalam mengamankan data agar data tersebut tidak mudah di curi atau dipersalah-gunakan, Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentifikasi data. Algoritma RSA (Rivest Shamir Adleman) merupakan algoritma kriptografi kunci-publik yang paling popular untuk mengamankan data digital atau dokumen dengan menerapkan algoritma RSA harus dapat merubah isi yang nantinya akan sulit dimengerti pihak lain agar data tersebut aman.

Kata Kunci : Kriptografi, PDF, RSA.

Abstract

There is a lot of digital data and one of them is a PDF file (Portable Document Format) which has the advantage that it is very flexible and the disadvantage of the file (Portable Document Format) is that it cannot be edited easily. This PDF (Portable Document Format) file can be opened on any computer or even a smartphone without any changes to the data or contents. But now there are many techniques to be able to change the contents of the PDF. The impact that occurs if documents that store various confidential information or data do not have security against threats from inside or outside will cause several impacts, such as disruption of operational activities, damage to reputation, financial losses, copyrighted works, and loss of trust from other parties. There are many techniques in securing data so that the data is not easily stolen or misused, Cryptography is the study of mathematical techniques related to information security aspects, such as data confidentiality, data validity, data integrity, and data authentication. The RSA algorithm (Rivest Shamir Adleman) is the most popular public-key cryptography algorithm for securing digital data or documents by applying the RSA algorithm to be able to change the content which will be difficult for other parties to understand so that the data is safe.

Keywords: *Cryptography, PDF, RSA.*

Pendahuluan

Perkembangan teknologi saat ini telah mempengaruhi berbagai aktivitas kehidupan manusia dan salah satunya adalah pencurian data, melalui perkembangan teknologi saat ini pencurian data sangat mungkin dilakukan karena kurangnya tingkat keamanan pada sebuah sistem sehingga sangat perlu ditingkatkan kembali keamanan pada suatu sistem tersebut khususnya pada sebuah dokumen [1]. Pada setiap

perusahaan pasti memiliki dokumen penting yang harus dijaga kerahasiaannya, karena pada saat ini dokumen adalah sumber media yang sangat berpengaruh dalam menyimpan berbagai hal berharga atau hal-hal lain terutama yang bersifat rahasia [2]. Maka dibutuhkan sebuah metode atau cara keamanan yang mampu mengamankan dokumen.

Ada banyak data digital dan salah satunya adalah file PDF (Portable Document Format) merupakan sebuah format berkas yang dibuat oleh Adobe System pada tahun 1993 untuk keperluan pertukaran dokumen digital. Format PDF (Portable Document Format) digunakan untuk mrepresentasikan dokumen dua dimensi meliputi teks, huruf, citra dan grafik [3]. File PDF (Portable Document Format) memiliki kelebihannya yaitu sifatnya yang sangat fleksibel dan kekurangan file (Portable Document Format) ialah apabila tidak dapat di edit dengan mudah. File PDF (Portable Document Format) ini dapat dibuka di komputer manapun atau bahkan smartphone tanpa adanya perubahan pada data atau isinya. Namun saat ini telah banyak teknik agar dapat mengubah isi dari PDF tersebut. Dampak yang terjadi jika dokumen yang menyimpan berbagai informasi atau data rahasia tidak memiliki keamanan terhadap ancaman dari dalam maupun luar akan menimbulkan beberapa dampak, misalnya terganggunya kegiatan operasional, rusaknya reputasi, kerugian finansial, karya cipta, dan kehilangan kepercayaan dari pihak lainnya. Ada banyak teknik dalam mengamankan data agar data tersebut tidak mudah di curi atau dipersalah-gunakan, salah satunya adalah dengan kriptografi.

Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentifikasi data [4]. Berdasarkan jenis kunci yang digunakan, kriptografi terbagi atas dua metode, yaitu kriptografi kunci simetris dan kriptografi kunci asimetris. Perbedaan dari kedua kriptografi ini terletak pada penggunaan kunci. Symmetric cryptosystem atau kriptografi simetris atau disebut juga algoritma kriptografi konvensional adalah algoritma yang menggunakan kunci untuk proses enkripsi sama dengan kunci untuk proses dekripsi.

Algoritma RSA (Rivest Shamir Adleman) merupakan algoritma kriptografi kunci-publik yang paling popular. Menurut [3] Penerapan algoritma kriptografi RSA menjadi solusi yang baik pada sistem penjualan yang akan dibangun CV. Sinergi Computer Lubuk linggau untuk menjamin kerahasiaan data-data penjualan yang disimpan didalam database, dengan penggunaan algoritma RSA ke dalam sistem penjualan tersebut maka data yang disimpan di dalam database berupa penjumlahan angka sehingga isi datanya tidak dapat dimengerti oleh pihak lain. Sedangkan Pada kriptografi modern, algoritma yang digunakan tidak dirahasiakan sebab setiap kali algoritma diketahui lawan, maka kriptografer (cryptographer) harus membuat algoritma baru, dengan demikian cukup kuncinya yang harus dirahasiakan dan benar-benar dijaga keamanannya [5]. Maka dapat disimpulkan bahwa untuk mengamankan data digital atau dokumen dengan menerapkan algoritma RSA harus dapat merubah isi yang nantinya akan sulit dimengerti pihak lain agar data tersebut aman.

Metode

1. Keamanan Data

Keamanan data merupakan apek penting untuk menjaga sebuah data maupun informasi supaya aman dan tidak mudah dibaca. Maka dari itu, data tersebut perlu untuk dijaga kerahasiaannya [6]. Data yang telah dibajak menimbulkan resiko bila informasi yang sensitif dan berharga dibaca oleh orang yang tidak bertanggungjawab. Dalam bidang teknologi informasi dan komunikasi terutama pada pertukaran suatu data atau informasi yang dikirim kepada penerima terkadang menjadi pertanyaan apakah informasi yang dikirim benar dari pengirim yang sebenarnya atau tidak, kemudian apakah data yang diterima sesuai dengan isi informasi dari pengirim yang sebenarnya dan tidak ada perubahan informasi yang terkandung didalamnya.

2. *Kriptografi*

Kriptografi berasal dari bahasa Yunani, menurut bahasa dibagi menjadi dua kripto dan graphia, kripto berarti secret (rahasia) dan

graphia berarti writing (tulisan). Menurut teminologinya kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ketempat yang lain [7].

Sedangkan [8] Kriptografi adalah bidang pengetahuan yang menggunakan persamaan matematis untuk melakukan proses enkripsi dan dekripsi. Teknik ini untuk mengkonversi data ke bentuk kode-kode tertentu agar informasi tidak dapat terbaca oleh siapapun kecuali pihak yang berhak.

Dalam kriptografi terdapat beberapa istilah atau terminologi penting sebagai berikut [9]:

a. Plainteks dan Cipherteks.

Plainteks (pesan) merupakan data/informasi yang dipahami maknanya. Pesan dapat dikirim atau disimpan dalam media penyimpanan. Agar pesan tidak dapat dipahami oleh pihak yang tidak berkepentingan, pesan perlu disandikan kedalam bentuk yang tidak dapat dipahami yang disebut ciphertext.

b. Peserta Komunikasi.

Komunikasi data melibatkan pertukaran pesan diantara paling kurang dua entitas. Entitas pertama adalah pengirim yang mengirim pesan kepada entitas lainnya. Entitas kedua adalah penerima yang menerima pesan tersebut. Entitas-entitas ini dapat berupa orang, mesin (komputer), kartu kredit, dan lain sebagainya.

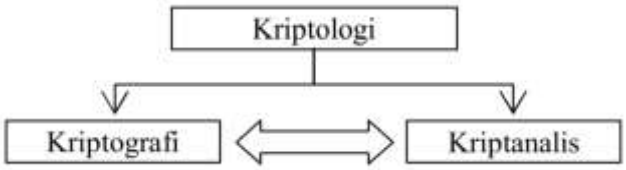
c. Enkripsi dan Dekripsi.

Penyandian pesan dari plaintext ke ciphertext dinamakan enkripsi, sedangkan mengembalikan pesan dari ciphertext ke plaintext dinamakan dekripsi. Enkripsi dan dekripsi dapat diterapkan pada pesan yang dikirim dan yang disimpan. Encryption of data in motion mengacu pada enkripsi pesan yang ditransmisikan melalui saluran komunikasi, sedangkan encryption of data at-rest mengacu pada enkripsi pesan yang tersimpan didalam storage.

d. Kriptanalis dan Kriptologi.

Kriptografi selalu berkembang karena memiliki ilmu yang berlawanan, yaitu kriptanalisis. Kriptografi adalah ilmu dan seni memecahkan cipherteks menjadi plainteks tanpa memerlukan kunci dan pelakunya disebut kriptanalis. Kriptografer mentransformasikan plainteks ke cipherteks dengan kunci, sebaliknya kriptanalis memecahkan cipherteks untuk menemukan plainteks tanpa kunci. Jadi, kriptologi adalah studi mengenai kriptografi dan kriptanalis.

Hubungan antara kriptologi, kriptografi, dan kriptanalis sebagai berikut [6] :



Gambar 1 Hubungan Kriptologi, Kriptografi, dan Kriptanalisis

3. Algoritma RSA

RSA merupakan salah satu dari Public Key Cryptosystem yang sangat sering digunakan untuk memberikan kerahasiaan terhadap keaslian suatu data digital [3]. Keamanan enkripsi dan dekripsi data model ini terletak pada kesulitan untuk memfaktorkan modulus n yang sangat besar. Dari sekian banyak algoritma kriptografi dengan kuncipublik yang pernah dibuat, algoritma yang paling populer adalah algoritma rsa [1]. Algoritma RSA yang dibuat oleh Ron Rivest, Adi Shamir dan Leonard Adleman pada tahun 1976. 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 besar belum ditemukan algoritma yang berhasil memecahkan, maka selama itu pula algoritma rsa akan tetap terjamin keamananannya. Algoritma RSA merupakan algoritma kriptografi kunci-publik yang paling popular. Algoritma RSA ini ditemukan oleh Ron Rivest, Adi Shamir, dan Leonard Adleman pada tahun1978 dan RSA merupakan singkatan inisial dari nama mereka bertiga. RSA digunakan karena merupakan algoritma kriptografi asimetris yang paling sering digunakan pada saat ini dikarenakan kehandalannya.

Keamanan algoritma RSA ini terletak pada sulitnya memfaktorkan bilangan besar menjadi faktor-faktor prima [5]. Pemfaktoran dilakukan

untuk memperoleh kunci privat. Selama pemfaktoran bilangan besar menjadi faktor-faktor prima belum ditemukan algoritma yang mangkus, maka selama itu pula keamanan algoritma RSA tetap terjamin. Besaran-besaran yang digunakan pada algoritma RSA [10].

Hasil dan Pembahasan

RSA termasuk dalam jenis algoritma kriptografi yang sifatnya simetri, Tingkat keamanan algoritma untuk penyandian RSA sangat bergantung dengan ukuran kunci sandi tersebut (dalam bit), karena jika makin besar ukuran kunci, maka makin besar juga kemungkinan kombinasi kunci yang bisa dibobol dengan metode RSA akan mengecek suatu kombinasi satu persatu kunci atau lebih dikenal dengan istilah brute force attack. Jika dibuat suatu sandi RSA dengan panjang 256 bit, maka metode brute force attack yang akan menjadi tidak ekonomis dan sia-sia dimana para hacker tidak akan sanggup untuk membobol sandi tersebut.

1. **Proses Pembuatan Kunci**

Tahapan Ekspansi Kunci :

Memilih dua buah bilangan prima berukuran besar p dan q. Kedua bilangan ini tidak dapat sama. Untuk memperoleh tingkat keamanan yang tinggi p dan q harus berukuran hingga 1024 bit.

a. Hitung n = p x q
b. Hitung m = (p-1) x (q-1)
c. Memilih e yang relatif prima terhadap m. Untuk menghasilkan e perlu mencari gcd(e,m)=1, artinya faktor pembagi terbesar e dan m adalah 1, mencarinya dengan algoritma euclidean :
d. r0=q1r1+r2,dimana,0<r2<r1r0=q1r1+r2,dimana,0<r2<r1
e. r1=q2r2+r3,dimana,0<r3<r2r1=q2r2+r3,dimana,0<r3<r2
f. rn=⋯.rn=⋯.

Perhitungan ini dilakukan dengan cara memilih nilai e secara acak sebagain nilai percobaan. Perhitungan akan berhenti jika nilai r berahir pada angka 0. Jika nilai sebelum r terahir adalah 1 maka angka yang menjadi percobaan benar sebagai e. Tetapi jika nilai sebelum r terahir tidak 1, maka angka tersebut bukanlan e yang diharapkan, maka coba angka lain.

Mencari d dengan rumus : e x d mod m = 1, dengan mencari nilai d yang jika dikalikan dengan e dan Ketika di mod-kan dengan m maka hasilnya adalah 1.

Kemudian didapatlah sepasang kunci : kunci public = (e,n) dan kunci private = (d,n).

2. **Proses Enkripsi**

Enkripsi, mengubah pesan asli menjadi tersandi adalah inti dari kriptografi. Oleh karena itu, tujuan dari ekspansi kunci adalah untuk dapat mengenkripsi pesan dengan kunci public yang telah didapat. Berikut adalah rumus dan proses enkripsi :

Misal pesan yang ingin dienkripsi sebagai contoh adalah 14, jika pesan berupa huruf maka conversikan ke dalam bentuk angka dengan ASCII code (American Standard Code for Information Interchange). Kemudian enkripsi dengan rumus :

C=M e (mod n)

Keterangan : C = Cipherteks, M = Message (Pesan), maka :

C=147(mod 33),C=20

3. **Proses Dekripsi**

Untuk mengembalikan pesan asli, kita ambil pesan tersandi yang tadi sudah didapat yaitu 20, maka dekripsikan dengan rumus berikut :

M=C d (mod n)

Keterangan : C = Cipherteks, M = Message (Pesan), maka :

M=203(mod 33),C=14

4. **Perhitungan RSA**

Langkah-langkah dalam mengenkripsi atau mengdekripsi RSA adalah sebagai berikut :

a. Pilih 2 buah bilangan prima p dan q.
b. Hitung nilai n = p * q
c. Hitung nilai m = (p-1) * (q-1).
d. Cari nilai e , dimana e merupakan relatif prima dari m.
e. Cari nilai d , yang memenuhi persamaan ed ≡ 1 mod m atau d = e-1 mod m.
f. Kunci public (e , n) dan kunci private (d , n).
g. Fungsi enkripsi → E (ta)=tae mod n ; dimana ta merupakan karakter ke-a dari message (pesan) yang akan dienkripsi.

h. Fungsi dekripsi → D (ca)=cad mod n ; dimana ca merupakan karakter ke-a dari ciphertext yang akan didekripsikan.

Contoh kasus, misalnya terdapat dua orang, Andi yang ingin mengirimkan pesan kepada Budi, maka komputer Andi akan memberitahukan kepada komputer Budi untuk membuat kunci publik dan kunci private (kunci dibuat oleh orang yang akan menerima pesan, sehingga kunci private tidak akan pernah meninggalkan komputer penerima, sedangkan kunci publik akan dikirimkan kepada komputer pengirim pesan, dimana kunci publik hanya bisa digunakan untuk meng- enkripsi pesan).

Komputer Budi akan melakukan langkah-langkah berikut :

a. Men- generate bilangan prima p = 59 dan q = 67.
b. Menghitung nilai n = 59 * 67 = 3953.
c. Menghitung nilai m = (59-1) * (67-1) = 3828.
d. Mencari nilai e yang relatif prima terhadap m.
e. Pada langkah berikutnya, akan dicari nilai d dimana ed ≡ 1 (mod m) atau d=e-1 mod m
f. Langkah selanjutnya adalah menentukan kunci publik dan kunci private sebagai berikut :
   Kunci publik = 277, 3953
   Kunci private = 2833, 3953
g. Kunci private tetap berada dikomputer Budi, namun kunci publik dikirimkan ke komputer Andi, dimana komputer Andi akan menggunakan kunci publik untuk meng-enkripsi pesan yang akan dikirimkan ke komputer Budi.
h. Langkah selanjutnya komputer Andi akan mengenkripsi pesan yaitu : "GO" maka komputer Andi perlu mengetahui kode ASCII karakter "G" dan "O" yaitu : 71 dan 79 , kemudian melakukan enkripsi dengan fungsi enkripsi → E(ta)=tae mod n :
   E(71)=71277 mod 3953 = 1798
   E(79)=79277 mod 3953 = 2444

Jadi komputer Andi akan mengirimkan pesan dengan angka c1=1798 dan c2=2444 kepada komputer Budi.

Dalam perhitungan diatas, untuk mencari sisa bagi pangkat yang besar dapat menggunakan algoritma modular exponent

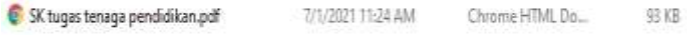
i. Langkah terakhir komputer Budi akan mendekripsi ciphertext c1=1798 dan c2=2444 dengan fungsi dekripsi → D(ca)=cad mod n
   D(1798)=17982833 mod 3953 = 71 → "G"
   D(2444)=24442833 mod 3953 = 79 → "O"

Dapat terlihat bahwa ciphertext yang dikirimkan oleh Andi dikembalikan menjadi pesan "GO"

5. Hasil dan Penjelasan

Pada tahapan ini akan menjelaskan hasil pada metode RSA yang dimana teknik enkripsi dalam menyandikan dan teknik dekripsi dalam mengembalikan file kebentuk semula, adapun tabel perubahan pada enkripsi dan dekripsi tersebut adalah sebagai berikut:

File yang akan di enkripsi adalah dokumen, uji coba data dengan mengambil salah satu sample yaitu data Surat masuk (SK tugas tenaga pendidikan) dengan data yang dapat di enkripsi berupa no berkas = 8000194302015



Gambar 2 Dokumen Yang Akan Di Enkripsi

Pada dokumen PDF tentu memiliki kode berkas atau Certificate thumbeline yang mempengaruhi dokumen tersebut jika nomor berkas tersebut berubah, maka dalam penelitian ini dalam algoritma Rijndael akan melihat nomor dokumen dan merubahnya dengan teknik enkripsi. Berikut adalah nomor berkas pada dokumen pada gambar 4.7 yang dilihat secara manual melalui sistem default pada windows.

Gambar 3 Certificate thumbeline Dokumen

Setelah mendapatkan nomor dokumen, langkah selanjutnya adalah mengubah nilai dokumen tersebut menjadi nilai baru. Berikut adalah kunci publik dan kunci privat yang di gunakan adalah:

a. Kunci Publik : PENUSA
b. Kunci Privat : MEDAN

Langkah selanjutnya adalah dengan melakukan ekspansi kunci dengan cara Memilih dua buah bilangan prima berukuran besar p dan q. Kedua bilangan ini tidak boleh sama. Untuk memperoleh tingkat keamanan yang tinggi pilih p dan q yang berukuran hingga misalnya 1024 bit.

Kunci Publik = PENUSA = 80 69 78 85 83 65
Kunci Privat = MEDAN = 77 69 68 65 78

Kemudian menjumlahkan tiap karakter dengan menambahkan bilangan decimal asscii. Sehingga didapatlah untuk nilai PENUSA = 80 69 78 85 83 65 = 460, dan nilai MEDAN = 77 69 68 65 78 = 357.

Selanjutnya mencari nilai bilangan prima dengan ketentuan yang sudah di tetapkan dari system. Bilangan harus dibuat dalam bentuk bilangan prima, maka peneliti mengambil nilai p = 59 dan q = 67 sesuai dengan contoh kasus yang digunakan sehingga hasilnya.

Menghitung nilai n (mod) = 59 * 67 = 3953.

Langkah selanjutnya adalah menentukan kunci publik dan kunci private sebagai berikut :

Kunci publik = 460, 3953
Kunci private = 357, 3953

Saat melakukan enkripsi, gunakan 1 kunci untuk enkripsi dan 1 kunci untuk dekripsi. Disini kunci publik akan digunakan untuk mengunci file pdf yang sebelumnya sudah disediakan dengan nomor berkas adalah = 8000194302015 dan akan dirubah sehingga bentuk dari file pdf tidak lagi dapat diketahui bahkan isinya. Berikut adalah penjelasan perubahan nilai tersebut yang dituliskan dengan tabel sebagai langkah enkripsi adalah sebagai berikut:

Tabel 1 Enkripsi

No. Berkas	Kode ASCII	Publik Key	Mod
8	56	460	3953
0	48	460	3953
0	48	460	3953
0	48	460	3953
1	49	460	3953
9	57	460	3953
4	52	460	3953
3	51	460	3953
0	48	460	3953
2	50	460	3953
0	48	460	3953
1	49	460	3953
5	53	460	3953

Penjelasan di atas adalah dengan mengubah nomor berkas menjadi nilai dengan kode ASCII dengan nilai decimal yaitu “8” memiliki karakter “56” sehingga nilai dari nomor berkas “8000194302015” adalah “56 48 48 48 49 57 52 51 48 50 48 49 53” kemudian melakukan enkripsi dengan fungsi enkripsi → E(ta)=tae mod n kemudian hitung tiap nilai dari nomor berkas. Berikut penjelasan dari perhitungannya :

$E(56)=56^{460} \bmod 3953 = 1644$
$E(48)=48^{460} \bmod 3953 = 518$
….
$E(53)=53^{460} \bmod 3953 = 442$

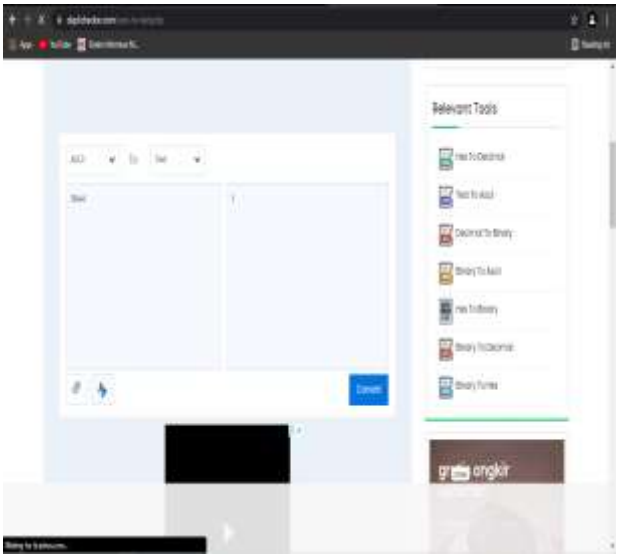
Sehingga didapat hasilnya adalah C1 = 1644, C2 = 518, C3 = 518, C4 = 518, C5 = 3892, C6 = 1405, C7 = 3163, C8 = 3389, C9 = 1644, C10 = 418, C11 = 1644, C12 = 3892, C13 = 442. Maka dapat dituangkan kedalam bentuk table hasil dari perubahan nilai berkas yaitu sebagai berikut :

Tabel 2 Enkripsi (2)

Nomor Berkas	Hasil ASCII	Nomor Berkas Baru
8	1644	l
0	518	
0	518	
0	518	
1	3892	4
9	1405	}
4	3163	[
3	3389	=
0	1644	l
2	418	□
0	1644	l
1	3892	4
5	442	□

Dalam proses mengubah bentuk nilai ASCII kedalam karakter symbol dibantu dengan

aplikasi coverter online dengan situs "https://www.duplichecker.com/ascii-to-text.php" yaitu media yang memberikan fasilitas dalam merubah nilai ASCII kedalam bentuk karakter sismbol. Berikut tangkapan layarnya :



Gambar 4 *Converter ASCII Online*

Selanjutnya untuk mengembalikan file kebentuk semula adalah dengan mengubah nomor berkas yang sudah terenkripsi menjadi semula dengan cara mendekripsi file tersebut dengan kunci public, karena sebelumnya sudah digunakan 1 kunci yaitu kunci publik untuk mengunci, maka membuka file selanjutnya adalah dengan menggunakan kunci privat. Berikut adalah penjelasan dari perhitungan yang dituangkan dalam bentuk tabel.

Tabel 3 Dekripsi

No. Berkas	Kode ASCII	Private Key	Mod
l	1644	357	3953
	518	357	3953
	518	357	3953
	518	357	3953
4	3892	357	3953
}	1405	357	3953
[	3163	357	3953
=	3389	357	3953
l	1644	357	3953
□	418	357	3953
l	1644	357	3953
4	3892	357	3953
□	442	357	3953

Langkah terakhir yaitu melakukan dekripsi ciphertext C1 = 1644, C2 = 518, C3 = 518, C4 = 518, C5 = 3892, C6 = 1405, C7 = 3163, C8 = 3389, C9 = 1644, C10 = 418, C11 = 1644, C12 = 3892, C13 = 442 dengan fungsi dekripsi → D(ca)=cad mod n. Berikut penjelasan dari perhitungannya :

D(1644)= 1644^{357} mod 3953 = 56 → "8"

D(518)= 518^{357} mod 3953 = 48 → "0"

…..

D(442)= 442^{357} mod 3953 = 53 → "5"

Sehingga didapat hasilnya adalah P1 = 56, C2 = 48, C3 = 48, C4 = 48, C5 = 49, C6 = 57, C7 = 52, C8 = 51, C9 = 48, C10 = 50, C11 = 48, C12 = 49, C13 = 53. Maka dapat dituangkan kedalam bentuk table hasil dari perubahan nilai berkas yaitu sebagai berikut :

Tabel 4 Dekripsi (2)

Nomor Berkas	Hasil ASCII	Nomor Berkas Kembali
l	56	8
	48	0
	48	0
	48	0
4	49	1
}	57	9
[	52	4
=	51	3
l	48	0
□	50	2
l	48	0
4	49	1
□	53	5

Pada penelitian ini, data yang akan di amankan adalah dokumen, langkah dalam melakukan pengamanan dokumen adalah dengan mengubah dokumen tersebut sehingga sulit untuk dibuka ataupun di ketahui orang lain. Adapun tahapan yang akan di lakukan adalah:

a. Mencari nilai pada dokumen untuk dijadikan sebagai plainteks.
b. Nilai pada dokumen akan dikonversi kedalam bentuk desimal sesuai kode ASCII.
c. Dengan menggunakan kunci untuk mengenkripsi, nilai desimal yang dihasilkan oleh dokumen akan dirubah sesuai hasil yang didapat.
d. Nilai dokumen yang telah berubah akan diterapkan kembali kedokumen.
e. Dokumen yang sudah mendapatkan nilai baru, isi pada format dokumen akan berubah dan isi tidak akan sama.

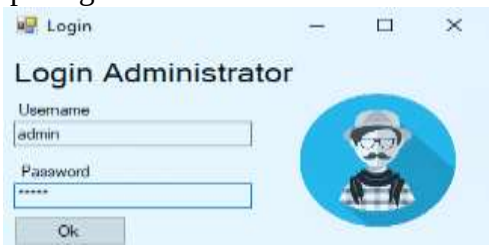
f. Untuk mengetahui bahwa dokumen sudah amankan, ekstensi dokumen akan diubah kedalam format *.Enk.

Pembahasan

Berdasarkan hasil yang didapat diatas maka dapat dilakukan pembahasan mengenai hasil akhir dalam penelitian ini. Pada tahapan Implementasi sistem yang akan dibahas tentang tahapan-tahapan saat menjalankan sistem yang dibangun.

1. Tampilan *Form Login*

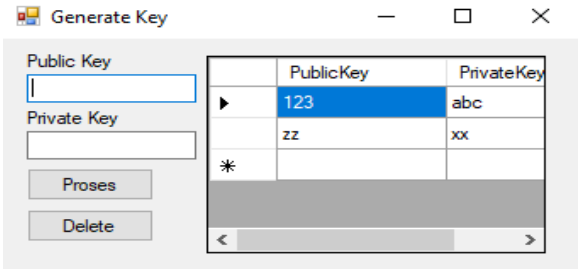
Login merupakan suatu tahapan utama untuk masuk kesebuah sistem, dan pada tampilan menu awal dari program yang dimana admin akan mengisi *username* dan *password* agar bisa masuk ke menu utama. Tampilan *form login* pada gambar di bawah ini:



Gambar 5 Tampilan *Login*

2. Tampilan *Form Generate Key*

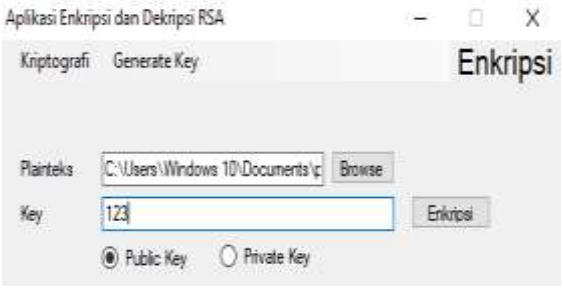
Pada tampilan ini akan dibangun sebuah kunci yang nantinya akan dipakai untuk mengamankan data. Berikut tampilan *form generate key* pada gambar di bawah ini:



Gambar 6 Tampilan Generate Key

3. Tampilan *Form Enripsi*

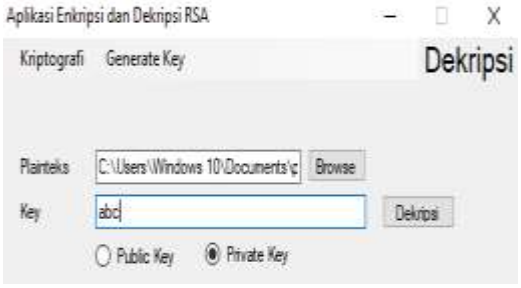
Pada menu ini adalah untuk mengamankan dokumen dengan pilihan kunci publik atau kunci privat. Berikut tampilan *form Enkripsi* pada gambar di bawah ini:



Gambar 7 Tampilan *Enkripsi*

4. Tampilan *Form Dekripsi*

Pada tampilan ini berfungsi untuk mengembalikan data kesemula. Tampilan *form dekripsi* dapat dilihat pada gambar di bawah ini:



Gambar 8 Tampilan *Dekripsi*

Kesimpulan

Adapun kesimpulan pada peneitian ini yaitu sebagai berikut :

Dalam merancang sebuah sistem dalam mengamankan data digital (dokumen) dibuat dengan menggunakan aplikasi Visual Studio 2019 dengan database yang digunakan adalah microsoft access dengan format (*.accdb) sebagai media penyimpanan user login dan kunci. Dengan menggunakan UML sebagai perancangan sistem juga design untuk perancangan antarmuka.

Pengamanan data digital dengan menerapkan algoritma RSA (Rivest Shamir Adleman) adalah sebagai suatu cara dalam mengamankan data, dikarena metode RSA yang memakai 2 (dua) buah kunci yaitu public key dan private key akan lebih dapat mengamankan data tersebut.

Kata pengantar

Dalam kesempatan ini penulis juga ingin menyampaikan terimakasih kepada Kedua Orang Tua saya atas kasih sayang yang diberikan kepada penulis serta doa, semangat, dukungan dan dorongan moril dan material sehingga skripsi ini dapat terselesaikan dengan

baik. Dengan terselesaikan penyusunan skripsi ini dengan baik juga berkat dukungan dari banyak pihak, penulis mengucapkan terimakasih kepada berbagai pihak yang turut membantu dalam menyelesaikan skripsi ini baik secara langsung maupun secara tidak langsung.

Referensi

[1] E. H. Rachmawanto, C. A. Sari, and K. Kunci, "Keamanan File Menggunakan Teknik Kriptografi Shift Cipher," *Jl. Nakula Semarang*, vol. 14, no. 50131024, pp. 329–335, 2015.

[2] Y. Prasetio and B. Triandi, "Perancangan Aplikasi Pengamanan File Teks dengan Skema Hybrid Menggunakan Algoritma Enigma dan Algoritma RSA Designing Application for Safeguarding Text Files with Hybrid Schemes Using Enigma Algorithms and RSA Algorithms," *46. IT J.*, vol. 6, no. 1, pp. 2252–746, 2018.

[3] R. Siringoringo, "Analisis dan Implementasi Algoritma Rijndael (AES) dan Kriptografi RSA pada Pengamanan File," *KAKIFIKOM Kumpul. Artik. Karya Ilm. Fak. ...*, vol. 02, no. 01, pp. 31–42, 2020, [Online]. Available: https://core.ac.uk/download/pdf/327176749.pdf.

[4] T. H. Saputro, N. H. Hidayati, and E. I. H. Ujianto, "Survei Tentang Algoritma Kriptografi Asimetris," *J. Inform. Polinema*, vol. 6, no. 2, pp. 67–72, 2020, doi: 10.33795/jip.v6i2.345.

[5] K. D. R. Sianipar, S. W. Siahaan, M. Siregar, and I. Gunawan, "Pengamanan File Suara Menggunakan Kriptografi Algoritma Rijndael Dengan Proses Enkripsi Dan Dekripsi," *TECHSI - J. Tek. Inform.*, vol. 11, no. 3, p. 431, 2019, doi: 10.29103/techsi.v11i3.1967.

[6] M. D. Irawan, "Implementasi Kriptografi Vigenere Cipher Dengan Php," *J. Teknol. Inf.*, vol. 1, no. 1, p. 11, 2017, doi: 10.36294/jurti.v1i1.21.

[7] A. Utama and R. F. Siahaan, "Penerapan Kriptografi untuk Pengamanan Data Transaksi Deposito pada Easy Tronik dengan Metode RC-5," *J. Ilmu Komput. dan Sist. ...*, vol. 3, no. 3, pp. 29–39, 2021, [Online]. Available: http://ejournal.sisfokomtek.org/index.php/jikom/article/view/86.

[8] A. Prayitno and N. Nurdin, "Analisa Dan Implementasi Kriptografi Pada Pesan Rahasia," *J. Elektron. Sist. Inf. dan Komput.*, vol. 3, no. 1, pp. 1–11, 2017, [Online]. Available: nnurdin69@gmail.com.

[9] S. Bandung, "SISTEM KEAMANAN SHORT MESSAGE SERVICE (SMS) MENGGUNAKAN," vol. 6, no. 2, pp. 5–10, 2017.

[10] I. Gunawan, "Pengamanan Acakan Biss Menggunakan Algoritma RSA," *Jurasik (Jurnal Ris. Sist. Inf. dan Tek. Inform.*, vol. 2, no. 1, p. 58, 2017, doi: 10.30645/jurasik.v2i1.19.