Jurnal CyberTech

Vol.4. No.3, Februari 2021
P-ISSN : 9800-3456
E-ISSN : 2675-9802

Implementasi Algoritma *Rivest Shamir Adleman* (RSA) Untuk Keamanan Data Nilai Siswa Pada SMK Multi Karya Medan

Machsudirwan Alrido[1], Nurcahyo Budi Nugroho[2], Moch. Iswan Perangin-Angin[3]

[1,2] Program Studi Sistem Informasi, STMIK Triguna Dharma
[3] Program Studi Manajemen Informatika, STMIK Triguna Dharma

Article Info

Article history:
Received Jun 12th, 201x
Revised Aug 20th, 201x
Accepted Aug 26th, 201x

Keyword:
Keamanan Data
Kriptografi
Algoritma RSA

ABSTRACT

Zaman semakin maju dan canggih, maka semakin besar pula pengaruh perkembangan teknologi dan komunikasi terhadap keamanan data. Dimana banyaknya kasus pencurian data yang sangat beragam seperti pencurian data yang bersifat privasi seperti data identitas, data perusahaan, laporan keuangan, bahkan data nilai siswa. Bagaikan peran jantung terhadap tubuh makhluk hidup, peran keamanan data merupakan hal yang sangat penting dalam suatu instansi, perusahaan ataupun organisasi demi menjaga beberapa aspek keamanan seperti kerahasiaan, integritas, otentikasi, dan lain sebagainya. Saat ini untuk memudahkan dalam beraktivitas termasuk Sekolah Menengah Kejuruan Multikarya yang merupakan instansi pendidikan yang memiliki beberapa data penting dan masih menggunakan sistem offline atau cetak berkas, salah satunya adalah data nilai siswa dimana di zaman teknologi yang serba canggih ini sangat rentan untuk dicuri dan dimanipulasi. Berdasarkan masalah diatas maka diperlukan suatu aplikasi mengenai pengamanan untuk mengamankan data nilai siswa dengan menggunakan teknik pengamanan kriptografi algoritma Rivest Shamir Adleman (RSA) dimana aplikasi ini berbasis desktop. Dengan aplikasi ini para guru atau wali kelas pada SMK Multi Karya dapat dengan mudah mengamankan data nilai siswa.

Corresponding Author: [1]Machsudirwan Alrido
Nama :
Program Studi
STMIK Triguna Dharma
Email:

1. PENDAHULUAN

Teknologi Informasi dan Komunikasi saat ini berkembang pesat, sehingga untuk mendapatkan informasi lebih cepat dan mudah. Begitu juga pada SMK Multi Karya Medan yang sudah menerapkan Sistem Informasi dalam penyebaran informasi di lingkup sekolah, dimulai dari sistem pendaftaran yang berbasis online dan penyebaran informasi melalui web Sekolah Multi Karya. Sejak tahun 1990 SMK Multi Karya Medan merupakan lembaga pendidikan dibawah naungan Yayasan Multi Gemilang Prestasi yang menyelenggarakan kegiatan belajar mengajar. Perkembangan teknologi memiliki dampak positif dan sangat bermanfaat bagi masyarakat era digital saat ini, namun juga memiliki dampak negatif salah satunya potensi

kejahatan manipulasi data nilai siswa yang disebabkan oleh pihak-pihak yang tidak berhak dan tidak bertanggung jawab.

Kriptografi merupakan salah satu teknik pengamanan data yang diterapkan untuk menyandikan teks atau karakter. Terdapat beberapa algoritma dalam ilmu Kriptografi yang dapat digunakan dalam penyandian. Pada penelitian ini menggunakan algoritma RSA (*Rivest Shamir Adleman*). Dari tingkat keamanannya Algoritma RSA dapat dinyatakan sangat aman dan diterapkan secara luas pada sejumlah aplikasi. Metode ini merupakan algoritma asimetris yang menggunakan sepasang kunci, yaitu kunci *public* dan kunci *private*. Kunci *public* dapat diketahui oleh siapa saja, sedangkan kunci *private* hanya pihak tertentu saja yang dapat mengetahuinya. Tingkat keamanan algoritma RSA ini terletak pada sulitnya pemfaktoran bilangan besar menjadi faktor-faktor prima.

Demi menjaga kerahasiaan dan manipulasi data maka dilakukan penerapan kriptografi untuk mengamankan data nilai siswa pada SMK Multi Karya Medan, maka diangkat sebuah penelitian berjudul "Implementasi Algoritma *Rivest Shamir Adleman* (RSA) Untuk Keamanan Data Nilai Siswa Pada SMK Multi Karya Medan".

2. METODE PENELITIAN

2.1 Kriptografi

Perkembangan teknologi informasi di era digital, kriptografi memiliki peranan penting dalam menjaga kerahasiaan dan keamanan data. Hal ini disebabkan karena banyaknya data yang bersifat rahasia yang disimpan dalam beberapa media komputer. Maka ilmu kriptografi akan selalu dikembangkan oleh orang demi menjaga dan mengamankan data dari ancaman kejahatan seperti pencurian dan manipulasi data.

2.2 Definisi Kriptografi

Kriptografi berasal dari Bahasa Yunani, yaitu *Crypto* yang berarti *secret* (rahasia) dan *Graphia* yang berarti (*writing*). Dalam arti lain kriptografi adalah tulisan rahasia. Dapat disimpulkan bahwa kriptografi adalah ilmu atau seni yang mempelajari tentang bagaimana menjaga kerahasiaan suatu pesan yang disampaikan ke penerima pesan dengan aman. (Ariyus, 2008).

Menurut *Request of Comments* (RFC), kriptografi adalah ilmu matematika yang berhubungan dengan transformasi data agar arti data tersebut menjadi sulit untuk dipahami (untuk menyembunyikan maknanya), mencegahnya dari perubahan tanpa izin, atau mencegahnya dari penggunaannya yang tidak sah. Jika transformasinya dapat dikembalikan, kriptografi juga dapat diartikan sebagai proses mengubah kembali data yang terenkripsi menjadi bentuk yang mudah dipahami. Sehingga, kriptografi juga dapat diartikan sebagai proses untuk melindungi data dalam arti luas. (Zelvina dkk, 2012:Vol.I).

2.3 Tujuan Kriptografi

Tentunya kriptografi merupakan teknik atau seni yang bertujuan untuk mengamankan data dari berbagai ancaman kejahatan dari pihak-pihak yang tidak berhak dan tidak bertanggung jawab. Adapun beberapa aspek-aspek keamanan sebagai berikut :

1. Kerahasiaan (*confidentiality*)
   Adalah layanan yang ditujukan untuk menjaga agar pesan tidak dapat dibaca oleh pihak-pihak yang tidak berhak.

2. Integritas data (*data integrity*)
   Adalah layanan yang menjamin bahwa pesan masih asli atau belum pernah dimanipulasi selama pengiriman.

3. Otentikasi (*authentication*)
   Adalah layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak-pihak yang berkomunikasi (*user autehentication*).

4. *Non-repudiation*
   Adalah layanan untuk menjaga entitas yang berkomunikasi melakukan penyangkalan. (Pabokory dkk, 2015:Vol.X).

Ada beberapa ancaman yang mungkin terjadi menurut W. Stallings, yaitu :

1. *Interruption*, perangkat sistem rusak atau menjadi tidak tersedia, merupakan ancaman terhadap aspek *availability* (ketersediaan).
2. *Interception*, akses informasi yang dilakukan oleh pihak yang tidak berwenang.
3. *Modification*, pihak yang tidak memiliki wewenang tidak hanya mengakses informasi tetapi juga melakukan perubahan terhadap informasi.
4. *Fabrication*, penyisipan objek palsu ke dalam sistem oleh pihak yang tidak berwenang. (Chazar, 2015:Vol.VII).

2.4 Macam-Macam Algoritma Kriptografi

Berdasarkan kunci yang digunakan algoritma kriptografi dibagi menjadi tiga bagian, yaitu :

1. Algoritma simetris
2. Algoritma asimetris
3. Fungsi *Hash*

2.4.1 Algoritma Simetris

Algoritma ini menggunakan satu kunci yang sama dalam proses enkripsi dan dekripsi sehingga algoritma ini bisa disebut juga sebagai *single-key*. Dalam pengiriman pesan menggunakan algoritma ini, penerima pesan harus diberitahu terlebih dahulu kunci yang digunakan agar bisa mendekripsi pesan. Tingkat keamanan algoritma ini bergantung pada kunci. Apabila kunci tersebut dapat diketahui oleh pihak lain, maka dia dapat melakukan enkripsi dan dekripsi pesan. Beberapa algoritma yang menggunakan kunci simetris diantaranya : *Rivest's Cipher* (RC2) , RC4, RC5, RC6, *International Data Encryption Algorithm* (IDEA), *Data Encryption Standard* (DES), *Advanced Encryption Standard* (AES), *One Time Pad* (OTP), dan lainnya. (Ariyus, 2008).

Didalam algoritma simetris (*Symmetric Algorithms*), pada proses enkripsi dan dekripsi kunci yang digunakan pada prinsipnya identik dengan $K_1 = K_2 = K$, tetapi hanya satu buah kunci dapat pula diturunkan dari kunci yang lainnya, maka sistem ini biasa disebut juga dengan *secret-key ciphersystem*. (Santi, 2010:Vol.XV).

2.4.2 Algoritma Asimetris

Berbeda dengan algoritma simetris, dalam proses enkripsi dan dekripsi algoritma ini menggunakan dua buah kunci yang berbeda, sehingga algoritma ini disebut juga sebagai public-key atau kunci publik. Kunci yang digunakan untuk proses enkripsi bersifat tidak rahasia (dapat diketahui oleh publik), sedangkan kunci yang digunakan untuk proses dekripsi bersifat rahasia (kunci privat). Walaupun kunci publik diketahui orang lain dalam pengiriman pesan, namun orang tersebut tidak dapat melakukan proses deskripsi karena kunci privat yang dapat membuka isi pesan tersebut. Adapun algoritma yang menggunakan kunci asimetris yaitu : *Digital Signature Algorithm* (DSA), *Diffie Helman* (DH), *Rivest Shamir Adleman* (RSA), *Elliptic Curve Cryptography* (ECC) dan lain sebagainya. (Ariyus, 2008).

Kunci yang digunakan berbeda untuk proses enkripsi dan dekripsinya dalam algoritma asimetris. Biasa disebut juga dengan sistem kriptografi kunci publik (*public-key*) karena untuk enkripsi kunci yang dibuat dapat diketahui oleh siapa saja, sedangkan untuk proses dekripsinya hanya dapat dilakukan oleh yang berhak

dan berwenang yang memiliki kunci rahasia untuk mendekripsinya, disebut *private-key*. (Ginting, 2015:Vol.III).

2.4.3 Fungsi *Hash*

Fungsi *Hash* atau biasa disebut dengan *one-way function* (fungsi satu arah), merupakan fungsi matematika yang mengambil input panjang variabel dan mengubahnya ke digit biner dengan panjang yang tetap. Biasa digunakan dalam membuat sidik jari dari suatu pesan, yang merupakan suatu tanda bahwa pesan tersebut berasal dari orang yang diinginkan. (Ariyus, 2008).

"Fungsi *Hash* satu arah merupakan fungsi *hash* yang bekerja dalam satu arah, dimana sebuah pesan yang telah diubah menjadi *message digest* tidak dapat dikembalikan lagi menjadi pesan awal, jadi dua pesan yang berbeda akan selalu menghasilkan nilai hash yang berbeda." (Santoso, 2013).

2.5 Terminologi Kriptografi

Dalam ilmu kriptografi ada beberapa terminologi atau istilah-istilah yang penting dalam kriptografi, yaitu :

1. Pesan (*Plaintext* dan *Ciphertext*) : Pesan (message) adalah data atau informasi yang dapat dibaca dan dimengerti maknanya. Pesan asli disebut *plaintext*. Sedangkan pesan yang sudah disandikan disebut *ciphertext*.
2. Pengirim dan Penerima : Komunikasi data melibatkan pertukaran pesan antara dua entitas. Pengirim (*sender*) adalah entitas yang mengirim pesan kepada entitas lainnya. Penerima (*receiver*) adalah entitas yang menerima pesan.
3. Penyadap (*eavesdropper*) adalah orang yang mencoba menangkap pesan selama ditransmisikan.
4. Kriptanalisis dan Kriptologi : Kriptanalisis (*cryptanalysis*) adalah ilmu dan seni untuk memecahkan chiperteks menjadi *plaintext* tanpa mengetahui kunci yang digunakan. Pelakunya disebut kriptanalis. Kriptologi (*cryptology*) adalah studi mengenai kriptografi dan kriptanalisis.
5. Enkripsi dan Dekripsi : Proses menyandikan *plaintext* menjadi *ciphertext* disebut enkripsi (*encryption*) atau *enciphering*. Sedangkan proses mengembalikan *ciphertext* menjadi *plaintext* semula dinamakan dekripsi (*decryption*) atau *deciphering*.
6. Cipher dan Kunci : Algoritma kriptografi disebut juga cipher yaitu aturan untuk *enchipering* dan *dechipering*, atau fungsi matematika yang digunakan untuk enkripsi dan dekripsi. Kunci (key) adalah parameter yang digunakan untuk transformasi *enciphering* dan *dechipering*. Kunci biasanya berupa string atau deretan bilangan. (Sitinjak dkk, 2010:2).

2.6 Algoritma RSA

Dalam kriptografi, RSA adalah algoritma untuk enkripsi kunci publik (public-key encryption). Algoritma ini adalah algoritma pertama yang diketahui paling cocok untuk menandai (signing) dan untuk enkripsi (encryption) 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 penerapan-penerapannya yang sangat up-to-date (mutakhir). (Arifin, 2009:Vol.IV no.9).

Algoritma RSA didesain sesuai fungsinya sehingga kunci yang digunakan untuk enkripsi berbeda dari kunci yang digunakan untuk dekripsi. Algoritma disebut juga dengan kunci publik karena kunci enkripsi dapat dibuat publik yang berarti semua orang boleh mengetahuinya, namun hanya orang tertentu yang dapat melakukan dekripsi terhadap pesan tersebut. (Lubis dkk, 2013:2).

Berdasarkan kutipan diatas dapat disimpulkan bahwa algoritma RSA adalah salah satu teknik kriptografi modern yang memiliki dua kunci yang berbeda dalam proses penyandian pesan, dimana kunci enkripsi dapat diketahui semua orang dan proses dekripsi hanya dapat dilakukan orang tertentu.

Algoritma RSA memiliki besaran-besaran yang penting untuk diketahui, diantaranya sebagai berikut.

1. p dan q bilangan prima (rahasia)
2. n = p . q (tidak rahasia)
3. Φ(n) = (p-1)(q-1) (rahasia)
4. e (kunci enkripsi) (tidak rahasia)
5. d (kunci dekripsi) (rahasia)
6. m (*plaintext*) (rahasia)
7. c (*ciphertext*) (tidak rahasia)

2.7 Sejarah RSA

Algoritma RSA ditemukan pada tahun 1977 oleh Ron Rivest, Adi Shamir, dan Leonard Adleman, kemudian dipatenkan di MIT (*Massachusetts Institute Technology)* pada tahun 1983. Setelah paten tersebut berakhir pada tahun 2000, algoritma RSA dapat digunakan dengan bebas oleh semua orang hingga saat ini. RSA sendiri merupakan penggabungan inisial dari ketiga nama mereka (Rivest-Shamir-Adleman). Dikenal sangat aman dikarenakan algoritma ini terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima. (Listiyono, 2009).

2.8 Tahap Tahap Algoritma RSA

Pada prinsipnya keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima. Pemfaktoran dilakukan unutk memperoleh kunci privat. Selama pemfaktoran bilangan besar menjadi factor-faktor prima belum ditemukan algoritma yang mangkus, maka selama itu pula keamanan algoritma RSA tetap terjamin. Berikut tahap-tahap algoritma RSA.

1. Proses Pembangkitan Kunci
   a. Pilih secara acak dua buah bilangan prima, dimana p dan q tidak sama.
   b. Hitung n = p.q
   c. Hitung Φ(n) = (p-1)(q-1)
   d. Pilih kunci public, e , yang relative prima terhadap Φ(n)
   e. Bangkitkan kunci privat dengan mengunakan persamaan e . d ≡ 1 (mod Φ(n)). Perhatikan bahwa e . d ≡ 1 (mod Φ(n) (ekivalen dengan e . d = 1 + k Φ(n), sehingga secara sederhana d dapat dihitung dengan d = (1 + k Φ(n)) / e.
2. Proses Enkripsi

   Proses enkripsi pada algoritma RSA dengan rumus :

   $E_e(m) = c \equiv m^e \bmod n$
3. Proses Dekripsi

   Proses dekripsi pada algoritma RSA dengan rumus :

   $D_d(m) = m \equiv c^d \bmod n$

2.9 UML (*Unified Modeling Language*)

Menurut Rosa dan Shalahuddin (2016 : 133) “UML adalah salah satu standar bahasa yang banyak digunakan di dunia industri untuk mengidentifikasikan *requeriment* (tata syarat), membuat analisis dan desain, serta menggambarkan arsitektur dalam program berorientasi objek”. *Unified Modeling Language* (UML) merupakan sebuah standarisasi bahasa pemodelan dalam pemograman berorientasi objek untuk membangun perangkat lunak. Dalam membangun sistem perangkat lunak dibutuhkan pemodelan visual untuk penggambaran agar mudah dalam dokumentasi diri secara detail dan spesifikasi. membangun dan dokumentasi diri sistem perangkat lunak. UML merupakan visual unutk pemodelan dan komunikasi mengenai sebuah sistem dengan menggunakan diagram dan teks-teks pendukung (Rosa dan Shalahuddin, 2016 : 141).

2.10 Perhitungan Algoritma Kriptografi RSA Pada Keamanan Data Nilai

Dalam proses enkripsi dan dekripsi, algoritma ini memiliki dua buah kunci yang berbeda, kunci privat atau kunci rahasia yang digunakan untuk mendekripsi sebuah pesan dimana kunci ini dirahasiakan, dan kunci publik yang digunakan untuk mengenkripsi pesan dimana kunci ini tidak bersifat rahasia. Contoh data yang akan digunakan dalam proses enkripsi dan dekripsi adalah sebagai berikut :

NOMOR			NAMA SISWA	NO UJIAN	Pengetahuan (KI-3)		Ketrampilan (KI-4)	
Urut	PE	NIS			Angka 10-100	Predikat	Angka 10-100	Predikat
1	433	108.18	ADIMAS RIDO SIAHAAN	106	75	C	75	C
2	177	109.18	ALHADI KHALIQ	107	75	C	75	C
3	341	110.18	CHRISPO ANDREAS SIPANGKAR	108	68	C	68	C
4	206	111.18	DAVIN RADITYA	109	74	C	74	C
5	248	112.18	ERLANGGA AROSA	110	78	C	78	C
6	128	113.18	FAARIS NAZRUDDINSYAH	111	75	C	75	C
7	139	114.18	FADHILA RUSMIAJI PANGESTU	112	73	C	73	C
8	213	115.18	FAHRUL RISKI	113	76	C	76	C
9	142	116.18	FARHAN	114	74	C	74	C
10	200	117.18	FERDYMAS ARFA	115	74	C	74	C
11	021	118.18	HERI PRATAMA PUTRA PURBA	116	65	D	65	D
12	246	119.18	RAMADANU	117	74	C	74	C

Gambar 1. Contoh Data Nilai Siswa

Agar lebih jelasnya berikut proses perhitungan algoritma RSA :

1. Pilih dua buah bilangan prima secara acak (p dan q), yaitu bilangan asli yang lebih besar daripada angka satu yang faktor pembaginya adalah satu dan bilangan itu sendiri. Maka bilangan prima dimulai dari angka 2, 3, 5, 11, 13, 17, 19, 23, 27, 29 dan seterusnya. Angka p dan q yang dipilih adalah p = 17 dan q = 19
2. Tentukan nilai n.
   n = p . q
   n = 17. 19
   n = 323
3. Tentukan nilai Φ(n).
   Φ(n) = (p-1) (q-1) = (17-1) (19-1)
   Φ(n) = 288
4. Pilih kunci publik yang relatif prima dengan Φ(n), maka e = 71.
5. Hitung nilai d = (1 + k x 288) / 7. Maka dapat ditentukan nilai d berupa bilangan bulat adalah d = 215

Setelah perhitungan diatas, maka dapat ditentukan :

Kunci publik : (e = 71, n = 323)

Kunci *private* : (d = 215, n = 323)

Berdasarkan perhitungan diatas, maka dapat dilakukan proses enkripsi untuk menghasilkan cipherteks dengan rumus $c = m^e \bmod n$ yaitu :

Plainteks	ASCII *code*	$C = m^e \bmod n$
R	82	$82^{71} \bmod 323 = 244$
A	65	$65^{71} \bmod 323 = 278$
M	77	$77^{71} \bmod 323 = 172$
A	65	$65^{71} \bmod 323 = 278$
D	68	$68^{71} \bmod 323 = 102$
A	65	$65^{71} \bmod 323 = 278$
N	78	$78^{71} \bmod 323 = 124$
U	85	$85^{71} \bmod 323 = 17$
7	55	$55^{71} \bmod 323 = 47$
4	52	$52^{71} \bmod 323 = 205$
C	67	$67^{71} \bmod 323 = 135$

Gambar 2. Proses Perhitungan Enkripsi

Berdasarkan Gambar 2. diatas, maka cipherteks yang dihasilkan adalah c = 244 278 172 278 102 278 124 17 47 205 135.

Kemudian melakukan proses dekripsi untuk mengembalikan cipherteks ke plainteks agar data dapat dibaca. Dekripsi dilakukan dengan persamaan $m = c^{d} \bmod n$ yaitu :

Cipherteks	$m = c^{d} \bmod n$	Karakter
244	$244^{215} \bmod 323 = 82$	R
278	$278^{215} \bmod 323 = 65$	A
172	$172^{215} \bmod 323 = 77$	M
278	$278^{215} \bmod 323 = 65$	A
102	$102^{215} \bmod 323 = 68$	D
278	$278^{215} \bmod 323 = 65$	A
124	$124^{215} \bmod 323 = 78$	N
17	$17^{215} \bmod 323 = 85$	U
47	$47^{215} \bmod 323 = 55$	7
205	$205^{215} \bmod 323 = 52$	4
135	$135^{215} \bmod 323 = 67$	C

Gambar 3. Proses Perhitungan Dekripsi

3. ANALISIS DAN HASIL

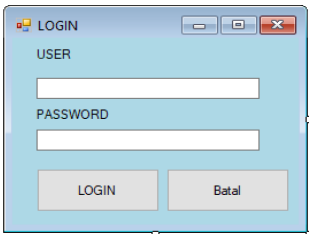
3.1 Analisis

Tahap analisis data merupakan di mana data yang dikumpulkan dengan menggunakan berbagai teknik pengumpulandata (misalnya observasi, interview, angket, maupun teknik pengumpulan data yang lain), diolah, dan disajikan untuk membantu peneliti menjawab permasalahan yang ditelitinya. Analisis data adalah proses menyusun, mengkategorikan data, mencari pola atau tema dengan maksud untuk memahami maknanya. Tujuan analisis pada pokoknya ialah menemukan suatu teori yang didasarkan atas data langsung dari lapangan. Itu sebabanya maka pengumpulan data harus berpedoman pada usaha mengembangkan suatu teori.

Analisa yang akan dilakukan adalah untuk memecahkan pemasalahan dalam melakukan pengamanan data nilai siswa pada SMK Multi Karya Medan. Adapun *output* atau hasil yang didapatkan yaitu dapat mengamankan data nilai siswa dengan teknik kriptografi atau dengan cara penyandian. Hal-hal yang dianalisis pada tahap analisis sistem adalah analisis masalah, analisis fungsional, analisis prosedur sistem yang sedang berjalan, analisis aliran informasi, analisis pengkodean, analisis basis data, dan analisis kebutuhan non-fungsional.

1. Tampilan halaman *login*

Berikut ini merupakan tampilan dari *form login* yang berfungsi untuk melakukan proses validasi *username* dan *password user.*



Gambar 1. Halaman Login

2. Tampilan Form Utama

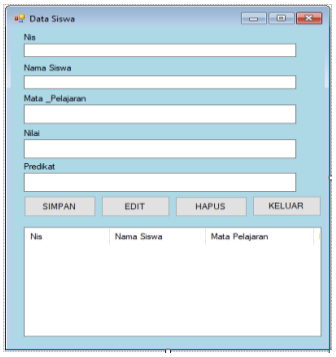
Form Utama digunakan sebagai penghubung untuk *Form* Data Siswa dan ada beberapa Form lainnya salah satunya ada *Form* Proses Enkripsi dan Dekripsi bertujuan untuk mengakhiri program secara keseluruhan.

a. File memasukan *form* data Siswa , Enkripsi dan Dekripsi
b. Keluar untuk menutupi atau mengakhiri programMerupakan tampilan yang muncul setelah *form login* telah dijalankan oleh *user*,di halaman ini *user* dapat melihat profil pengguna dan pada halaman ini *user* dapat memilih menu diantaranya yaitu: kirim pesan, enkripsi, logout.

Gambar 2. Halaman Form Utama

3. Tampilan Form Data Nilai Siswa

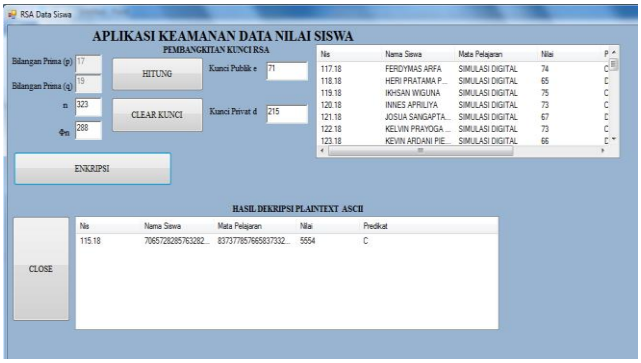
Form Data Nilai Siswa adalah *Form* yang berfungsi untuk mengolah data tentang kriteria yang sesuai dengan penilaian yang dimiliki.



Gambar 3. Tampilan Form Data Nilai Siswa

4. Tampilan Form Enkripsi

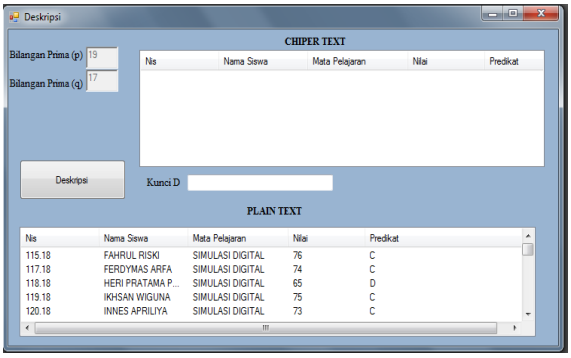
Form Enkripsi adalah Form yang berfungsi untuk mengolah data siswa yang diubah menjadi kode untuk mengamankan data.



Gambar 4. Tampilan Form Enkripsi

5. Tampilan Form Dekripsi

Form Data Dekripsi adalah Form yang berfungsi untuk mengolah data yang di enkripsikan menjadi data siswa kembali seperti semula.



Gambar 5. Tampilan Form Dekripsi

4. KESIMPULAN

Berdasarkan penelitian yang dilakukan mengenai pengamanan Data Nilai Siswa pada SMK Multi Karya Medan menggunakan Algoritma RSA, maka dapat disimpulkan beberapa hal sebagai berikut.:

1. Algoritma RSA dianggap sebagai algoritma kriptografi yang paling aman saat ini dikarenakan belum ditemukannya algoritma yang efisien untuk memecahkan sistem keamanan RSA.
2. Semakin panjang suatu kunci maka tingkat keamanan semakin terjamin.
3. Algoritma ini hanya mampu mengamankan tipe data berbasis teks.
4. Keluaran yang dihasilkan memiliki panjang karakter yang berbeda dengan karakter yang dimasukkan (*plaintext*), ini disebabkan karena semakin besar bilangan prima yang digunakan maka semakin besar pula hasil dari proses enkripsi sehingga hasil proses enkripsi melebihi dari 256 karakter pada tabel ASCII.

UCAPAN TERIMA KASIH

Syukur Alhamdulillah saya ucapkan kehadirat Allah Subhanahu Wa Ta'ala atas rahmat dan hidayah-Nya serta memberi saya kesempatan dalam menyelesaikan jurnal ilmiah ini dengan baik. Ucapan terima kasih yang besar ditujukan untuk kedua orang tua, yang telah mengasuh, membesarkan dan selalu memberikan doa, motivasi serta pengorbanan baik bersifat moril maupun materil yang tidak terhingga selama menjalani pendidikan. Ucapan terima kasih yang sebesar-besarnya juga ditujukan terutama kepada Bapak Rudi Gunawan, SE., M.Si., selaku Ketua Sekolah Tinggi Manajemen Informatika Dan Komputer (STMIK) Triguna Dharma Medan. Bapak Zulfian Azmi, ST., M.Kom., selaku Wakil Ketua I Bidang Akademik STMIK Triguna Dharma Medan. Bapak Marsono, S.Kom., M.Kom.,selaku Ketua Program Studi Sistem Informasi STMIK Triguna Dharma Medan. Bapak Nurcahyo Budi Nugroho, S.Kom., M.Kom., selaku Dosen Pembimbing I yang telah meluangkan waktu untuk membimbing dan memberikan arahan kepada saya sehingg penelitian ini dapat terselesaikan dengan baik dan tepat waktu. Bapak Moch. Iswan Perangin-angin S.Kom., M.Kom., selaku Dosen Pembimbing II yang telah memberikan bimbingan tata cara penulisan, saran sehingga penelitian ini dapat terselesaikan dengan baik dan tepat waktu. Seluruh Staff Karyawan di STMIK Triguna Dharma yang menuntun saya selama mengikuti perkuliahan sampai dengan selesai.

REFERENSI

[1] Ariffin, Z. (2009). Studi Kasus Penggunaan Algoritma RSA Sebagai Algoritma Kriptografi yang Aman. *Jurnal Informatika*
Mulawarman, *4*(3), 8-9.

[2] Ariyus, D. (2008). *Pengantar Ilmu Kriptografi*. Yogyakarta : C.V ANDI OFFSET.

[3] Chazar, C. (2015). Standar Manajemen Keamanan Sistem Informasi Berbasis ISO/IEC 27001:2005. *Jurnal Informasi*, *7*(2),

49-50.
[4] Ginting, A., Isnanto, R.R., & Windasari, I.P. (2015). Implementasi Algoritma Kriptografi RSA untuk Enkripsi dan Dekripsi Email. *Jurnal Teknologi dan Sistem Komputer, 3*(2), 254.
[5] Harahap, M.K. (2016). Analisis Perbandingan Algoritma Kriptografi Klasik Vigenere Cipher dan One Time Pad. *Jurnal Nasional Informatika dan Teknologi Jaringan, 1*(1), 62.
[6] Listiyono, H. (2009). Implementasi Algoritma Kunci Public Pada Algoritma RSA. *Dinamika Informatika, 1*(2), 96. Lubis, M.S., Budiman, M.A., & Manik, K.L. (2013). Penggunaan Algoritma RSA Dengan Metode The Sieve of Eratosthenes dalam Enkripsi dan Dekripsi Pengiriman Email. *Seminar Nasional Aplikasi Teknologi Informasi 2013*.
[7] Nathasia, N.D., & Wicaksono, A.E. (2011). Penerapan Teknik Kriptografi Stream-Cipher Untuk Pengaman Basis Data. *Jurnal Basis Data ICT Research Center UNAS, 6*(1), 4.
[8] Pabokory, F.N., Astuti, I.F., & Kridalaksana, A.H. (2015). Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, dan File Dokumen Menggunakan Algoritma *Advanced Encryption Standard*. *Jurnal Informatika Mulawarman, 10*(1), 22.
[9] Rosa A.S., & Shalahuddin, M. (2014). *Rekayasa Perangkat Lunak Struktur dan Berorientasi Objek*. Bandung : Informatika.
[10] Santi, R.C.N. (2010). Implementasi Algoritma Enkripsi Playfair pada File Teks. *Jurnal Teknologi Informasi DINAMIK, 15*(1), 28.
[11] Santoso, K.I. (2013). Dua Faktor Pengamanan *Login Web* Menggunakan Otentikasi *One Time Password* dengan *Hash SHA. Seminar Nasional Teknologi & Komunikasi Terapan 2013*.
[12] Santoso, & Nurmalina, R. (2017). Perencanaan dan Pengembangan Aplikasi Absensi Mahasiswa Menggunakan Smart Card Guna Pengembangan Kampus Cerdas. *Jurnal Integrasi, 9*(1), 86-87.
[13] Sitinjak, S., Fauziah, Y., & Juwariyah. (2010). Aplikasi Kriptografi File Menggunakan Algoritma Blowfish. *Semina Nasional Informatika 2010*.
[14] Syahputra, H., & Herdiyatmoko, H.F. (2012). Aplikasi Enkripsi Data Pada File Teks dengan Algoritma RSA (*Rivest ShamirAdleman*). *Seminar Nasional Teknologi dan Komunikasi Terapan 2012.*
[15] Zelvina, A., Efendi, S., & Arisandi, D. (2012). Aplikasi Pembelajaran Kriptografi Kunci Publik ElGamal Untuk Mahasiswa. *Jurnal Dunia Teknologi Informasi, 1*(1), 57.

BIBLIOGRAFI PENULIS

Nama	:	Machsudirwan Alrido
NIM	:	2015020298
Program Studi	:	Sistem Informasi STMIK Triguna Dharma
Deskripsi	:	Merupakan seorang mahasiswa STMIK Triguna Dharma Stambuk 2015 pada Program Studi Sistem Informasi yang sedang dalam proses menyelesaikan skripsi dan memiliki minat dan fokus dalam bidang keilmuan Teknik Komputer dan Jaringan, juga mempunyai hobi fotografi dan memasak. Aktif pada Organisasi Kemahasiswaan Islam eksternal seperti HMI, BKLDK dan Organisasi Kampus lainnya.

	Nama : Nurcahyo Budi Nugroho, S.Kom., M.Kom. NIDN : 0130038201 Program Studi : Sistem Informasi Deskripsi : Dosen Tetap STMIK Triguna Dharma yang aktif mengajar dan fokus pada bidang keilmuan Pemrograman dan Keamanan Komputer.
	Nama : Moch. Iswan Perangin-Angin, S.Kom., M.Kom. NIDN : 0120118902 Program Studi : Manajemen Informatika Deskripsi : Dosen Tetap STMIK Triguna Dharma yang aktif mengajar dan fokus pada bidang kecerdasan buatan. Prestasi : Telah menulis 1 buku dibidang Ilmu Komputer.