J-SISKO TECH
Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD
P:ISSN : 2621-8976 E-ISSN : 2615-5133 ■ 88
Vol.4, No.1, Januari 2021, pp.88-91

Penerapan Algoritma RSA (Rivest Shamir Adelman) Untuk Mengamankan Nilai Siswa SMP HKBP P. Bulan

Badrul Anwar*, Rini Kustini*, Iskandar Zulkarnain*
* Program Studi Sistem Informasi, STMIK Triguna Dharma

Abstrak

Keamanan data merupakan hal sangat penting didalam era digital saat ini, berbagai permasalah keamanan data seperti pencurian data, perusakan data, penyadapan informasi telah sering terjadi. Oleh karena itu dibutuhkan suatu mekanisme pengamanan data untuk memastikan suatu data tetap aman terhadap pihak-pihak yang tidak berwenang. Mekanisme pengamanan data yang dapat diandalkan dalam era dital saat ini adalah kriptografi. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasian, integritas data, autentikasi entitas, dan autentikasi sumber data.

Kata kunci : Algoritma RSA Kriptografi

Abstract

Data security is very important in today's digital era, various data security issues such as data theft, data destruction, information tapping have often occurred. Therefore we need a data security mechanism to ensure that data remains safe with unauthorized parties. Data security mechanism that can be relied upon in the era of the current era is cryptography. Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data source authentication.

Keywords: Algoritma RSA Kriptografi

1. PENDAHULUAN

Di era perkembangan teknologi yang semakin pesat, kebutuhan akan informasi memberikan dampak yang sangat besar bagi perkembangan dunia digital saat ini. Informasi yang dulunya berbentuk fisik atau dapat disentuh, sekarang telah menjadi informasi yang dapat diolah oleh komputer.

Saat ini instansi-instansi pemerintahan maupun swasta menggunakan komputer sebagai proses pengolahan data yang berjalan pada instansi tersebut. Salah satu instansi swasta yang menerapkannya adalah lembaga pendidikan SMP HKBP P. BULAN. SMP HKBP P. BULAN melakukan proses pengolahan nilai siswa dengan menggunakan komputer. Setiap data-data nilai siswa yang telah diolah dengan program aplikasi Microsoft excel natinya akan disimpan di dalam memori penyimpanan komputer yaitu hardisk atau media penyimpanan lainnya. Penyimpanan data nilai siswa pada hardisk ini tentunya menimbulkan permasalahan seperti perubahan data nilai siswa oleh pihak-pihak yang tidak memiliki hak atas pengubahan data tersebut. Selama ini SMP HKBP P. Bulan belum memiliki fasilitas pengamanan data nilai siswa yang menjamin data nilai setiap siswa tetap aman dari pihak-pihak yang ingin memanipulasi data tersebut.

Dari permasalahan diatas beberapa literature tentang pengamanan data, diantaranya menggunakan kriptografi untuk menjaga kerahasiaan informasi [1]. Kriptografi adalah ilmu yang mempelajari teknik matematis yang berhubungan dengan aspek keamanan informasi seperti tingkat keyakinan, integritas data, autentikasi entitas dan autentikasi keaslian data [2]. Salah satu algoritma kriptografi asimetri atau algoritma yang memiliki kunci yang berbeda untuk proses enkripsi dan dekripsi ialah RSA. Algoritma RSA mendasarkan proses enkripsi dan dekripsinya pada konsep bilangan prima dan aritmetika modulo,

baik kunci enkripsi maupun dekripsi keduanya merupakan bilangan bulat. Melalui penelitian ini diharapkan algoritma RSA dapat diterapkan untuk mengenkripsi file yang berekstensi .xlsx.

2. METODE PENELITIAN

Algoritma RSA mendasarkan proses enkripsi dan dekripsinya pada konsep bilangan prima dan aritmetika modulo, baik kunci enkripsi maupun dekripsi keduanya merupakan bilangan bulat [3]. Kunci untuk enkripsi sifatnya tidak dirahasiakan atau bersifat umum, sedangakan kunci untuk dekripsi bersifat rahasia. RSA memiliki tingkat keamanan yang cukup baik, keamanan algoritma tersebut terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima, pemfaktoran ini bertujuan untuk menemukan kunci privat. Sampai saat ini belum ditemukan sebuah algoritma yang mangkus untuk memfaktorkan bilangan bulat yang besar menjadi faktor-faktor primanya.

Pada algoritma *RSA* proses enkripsi dan dekripsi dapat dilakukan dengan terlebih dahulu membangkitkan kunci publik dan kunci privat. Algoritma pembangkitan kunci *RSA* dapat dijelaskan sebagai berikut ini:

1. Pilih dua buah bilangan prima $p \neq q$ secara acak
2. Hitung nilai n dengan persamaan sebagai berikut:
   $n = p \times q$
3. Hitung fungsi *totient euler* φ dengan persamaan sebagai berikut:
   $\varphi(n) = (p - 1) \times (q - 1)$
4. Pilih nilai e sebagai kunci publik, yang relatif prima dengan hasil nilai $\varphi(n)$ (fungsi *totient euler*)
5. Hitung d untuk menghasilkan kunci privat, dengan persamaan sebagai berikut: $e \times d \equiv 1 \pmod{\varphi(n)}$

Hasil dari algoritma pembangkitan kunci tersebut adalah sebagai berikut:

1. Pasangan dari kunci publik yang digunakan untuk mengenkripsi data adalah pasangan nilai (n , e).
2. Pasangan dari kunci privat yang digunakan untuk mendekripsi data kembali adalah pasangan nilai (n ,d).

Setelah proses membangkitkan kunci selesai, maka untuk proses enkripsi dan dekripsi dapat diformulasikan secara *matematis* sebagai berikut:

$C = m^e \ mod \ n$ (proses enkripsi dengan m sebagai plainteks)

$M = C^d \ mod \ n$ (proses dekripsi dengan c sebagai cipherteks)

Untuk dapat mengetahui dengan lebih jelas prinsip kerja algoritma RSA ini, kita terapkan langkah-langkah tersebut di dalam contoh berikut. Langkah pertama yang harus dilakukan adalah melakukan pembangkitan kunci publik dan kunci privat sebagai berikut:

1. Ambil bilangan prima p dan q
   P = 47 dan q = 71
2. Hitung n = (p).(q) = 3337
3. Hitung $\varphi(n) = (p - 1) \times (q - 1) = 3220$
4. Pilih nilai e yang relatif prima terhadap $\varphi(n)$ dalam hal ini e = 79
5. Pilih d dengan persamaan $e \times d \equiv 1 \pmod{\varphi(n)}$, atau dengan persamaan sebagai berikut $d = \frac{1+(k\,(3220))}{79}$, dengan mencoba beberapa nilai k diperoleh d = 1019 dimana d bernilai bulat.
6. Proses pembakitan kunci menghasilkan kunci publik dan kunci privat sebagai berikut:
   kunci publik = (e = 79 , n = 3337)
   kunci privat = (d = 1019 , n = 3337)

Berikut merupakan contoh penerapan algoritma RSA untuk mengenkripsi karakter B dan r yang dalam karakter *ASCII* yaitu 66 dan 114.

c1(B) = $66^{79} \pmod{3337}$

= $[(66^{32} \pmod{3337}) (66^{32} \pmod{3337}) (66^{14} \pmod{3337})(66 \pmod{3337})] \pmod{3337}$

= 795

c2(r) = $114^{79} \pmod{3337}$

= $[(114^{32} \pmod{3337}) (114^{32} \pmod{3337}) (114^{14} \pmod{3337})$
$(114 \pmod{3337})] \pmod{3337}$ = 2560

Berikut merupakan contoh penerapan algoritma RSA untuk mendekripsi kembali bilangan 795 dan 2560:

p1(795) = 795^{1019} mod 3337
= [(795^{50} mod 3337) (795^{50} mod 3337) (795^{18} mod 3337)(795 mod 3337)] mod 3337
= 66(B)

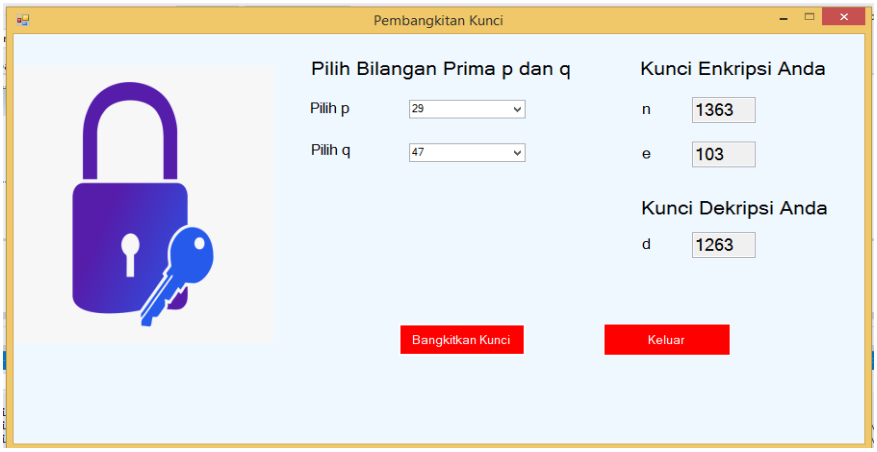
p2(2560) = 2560^{1019} mod 3337
= [(2560^{50} mod 3337) (2560^{50} mod 3337) (2560^{18} mod 3337)
(2560 mod 3337)] mod 3337 = 114(r)

3. ANALISA DAN HASIL

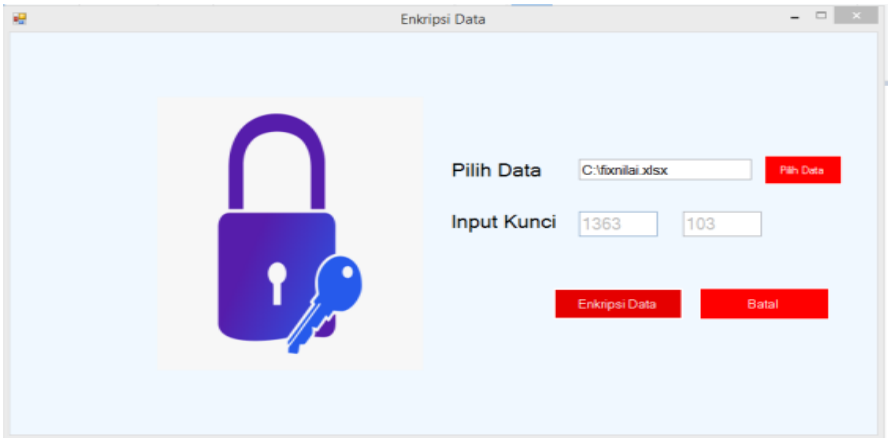
Pada bagian ini, penelitian akan menjelaskan bagaiman menerapkan algoritma RSA untuk mengamankan data nilai siswa SMP HKBP P. Bulan. Penerapan ini dilakukan dengan memanfaatkan aplikasi bahasa pemerograman visual basic.

3.1 Aplikasi

Bahasa pemerograman adalah kumpulan instruksi standar yang berfungsi untuk memerintah komputer agar menghasilkan output. Bahasa pemerograman terdiri dari sintaks-sintaks khusus yang digunakan untuk melakukan proses komputasi dan algoritma. Beberapa contoh bahasa pemerograman yang banyak digunakan pada saat ini adalah: c++, c, pascal dan visual basic. Dalam penelitian ini bahasa pemerograman yang digunakan adalah visual basic untuk melakukan enkripsi dan dekripsi data dan pembangkitan kunci.



Gambar 1. Proses Pembangkitan Kunci Algoritma RSA



Gambar 2. Proses Enkripsi File Nilai

	Kelas :			IX	Semester : 1			
Nama	Pendidikan Agama dan Budi Pekerti				Pendidikan Pancasila dan Kewarganegara			
	Pengetahuan		Ketrampilan		Pengetahuan		Ketrampilan	
	Angka	Huruf	Angka	Huruf	Angka	Huruf	Angka	Huruf
BRILIAN DEMAK B. PANJAIT/	1670+874+	337+	1670+1378	337+	1670+1378	337+	1670+1670	337+
ANGREY TIA SIHOMBING	1290+1572	526+	1290+794+	526+	1670+146+	337+	1290+233+	337+
ARIEF SUNYATA SIHOTANG	1670+874+	337+	1670+1378	337+	1670+1290	337+	1290+233+	337+
ARJUN TULUS PANDIANGAN	1670+874+	337+	1670+1378	337+	1670+1290	337+	1670+146+	337+
CANTIKA PUTRI AYU SIMANI	1290+874+	526+	1290+372+	526+	1290+1378	526+	1290+1378	526+
CINDY ANGRAENI SEBAYAN(	1290+1378	526+	1290+1670	526+	146+1572+	1727+	146+233+	526+
DANIEL PARSAORAN HUTAG	1670+794+	337+	1670+1378	337+	1670+1290	337+	1670+146+	337+
FEBRIANI RUT MAYA	1290+372+	526+	1290+1290	526+	1290+372+	526+	1290+372+	526+

Gambar 3. Hasil Enkripsi Nilai Siswa

	Kelas :			IX	Semester : 1			
Nama	Pendidikan Agama dan Budi Pekerti				Pendidikan Pancasila dan Kewarganegara			
	Pengetahuan		Ketrampilan		Pengetahuan		Ketrampilan	
	Angka	Huruf	Angka	Huruf	Angka	Huruf	Angka	Huruf
BRILIAN DEMAK B. PANJAIT/	73	C	75	C	75	C	77	C
ANGREY TIA SIHOMBING	82	B	84	B	79	C	80	C
ARIEF SUNYATA SIHOTANG	73	C	75	C	78	C	80	C
ARJUN TULUS PANDIANGAN	73	C	75	C	78	C	79	C
CANTIKA PUTRI AYU SIMANI	83	B	86	B	85	B	85	B
CINDY ANGRAENI SEBAYAN(	85	B	87	B	92	A	90	B
DANIEL PARSAORAN HUTAG	74	C	75	C	78	C	79	C
FEBRIANI RUT MAYA	86	B	88	B	86	B	86	B
FERDI RIONALDO PASARIBU	82	B	85	B	80	C	81	C

Gambar 4. Hasil Dekripsi Nilai Siswa

4 Kesimpulan

1. Dengan adanya aplikasi enkripsi dan dekripsi data ini dapat mengamankan nilai siswa.
2. Algoritma RSA memiliki tingakat keakuratan yang cukup baik.

UCAPAN TERIMA KASIH

Puji Syukur kepada Tuhan Yang Maha Esa atas karunia-Nya, dengan kasih sayang dan kekuatan-Nya dalam menyelesaikan karya tulis ini sebagai skripsi dengan judul : "Penerapan Algoritma RSA Untuk Mengamankan Nilai Siswa Smp HKBP P.Bulan". dapat diselesaikan dengan tepat pada waktu yang telah ditentukan. Terima kasih tak terhingga kepada kedua orang tua tercinta yang telah memberikan doa dan dukungan baik secara moral maupun materil sehingga mampu menyelesaikan pendidikan dari tingakat sekolah dasar sampai bangku perkulihaan dengan baik

REFERENSI

[1] D. Sinaga and C. Umam, "Implementasi kriptografi *vigenere cipher* pada media teks dengan kombinasi transposisi kolom 1,2," *Pros. SENDI_U 2018 ISBN 978-979-3649-99-3*, no. 1, pp. 978–979, 2018.

[2] M. Y. Simargolang, "Implementasi Kriptografi Rsa Dengan Php," *J. Teknol. Inf.*, vol. 1, no. 1, p. 1, 2017.

[3] Arif Prayitno Nurdin, "Analisa Dan Implementasi Kriptografi Pada Pesan Rahasia Menggunakan Algoritma *Cipher Transposition*," *Jesik*, vol. 3, no. 1, pp. 1–3, 2017.