Jurnal CyberTech
Vol.1. No.2, Mei 2018, pp. 417~425
P-ISSN : 9800-3456
E-ISSN : 2675-9802

Implementasi Kriptografi Metode RSA (Rivest Shamir Adleman) Pada Debitur

Muhammad Yusuf *, Azanuddin, Jufri Halim ****
*Program Studi Sistem Informasi, STMIK Triguna Dharma
** Program Studi Sistem Informasi, STMIK Triguna Dharma

Article Info

Article history:
Received Mei 12th, 2018
Revised Mei 20th, 2018
Accepted Mei 26th, 2018

Keyword:
Kriptografi RSA,Debitur

ABSTRACT

PT. Multimestika Dayasemesta pertama kali dibuka pada tahun 1995 dan pertama kali menjual sepatu dan campas rem untuk mobil.perusahaan tersebut telah berkembang hingga memiliki ribuan mitra dan telah menjual suku cadang untuk mobil maupun motor. Saat ini perusahaan tersebut hany6a menggunakan oengaman yang disediakan oleh software untuk mengamankan data mitranya yang meliput nama tok, lokasi, no.hp dan aset. Pada permasalahan yang dibahas, dapat menerapkan Perancangan Aplikasi Keamanan Data salah satunya ialah menggunakan algoritma Rivest Shamir Adleman(RSA) dalam mengamankan data debitur. Dengan mengamankan data debitur bertujuan untuk membantu sales ounter dalam mengamankan data debitur. Hasil penelitian merupakan terciptanya sebuah aplikasi Pengamanan Data dengan Algoritma Rivest Shamir Adleman(RSA) yang dapat membantu owner dalam mengamankan data debitur di PT. Multimestika Dayasemesta.

First Author
Nama : Muhammad Yusuf
Kampus : STMIK Triguna Dharma
Program Studi : Sistem Informasi
E-Mail : bangucup1997@gmail.com

1. PENDAHULUAN

PT. Multimestika Dayasemesta pertama kali dibuka pada tahun 1995 dan pertama kali menjual sepatu dan campas rem untuk mobil. Perusahaan tersebut telah mengalami pasang surut, puncaknya terjadi pada krisis moneter yang melanda indonesia. Perusahaan tersebut berhasil bertahan dan sejak saat itu perusahan tersebut terus berkembang hingga telah memiliki banyak cabang di seluruh indonesia dan memiliki ribuan mitra dan telah menjual berbagai suku cadang baik untuk motor dan mobil.

Saat ini perusahaan tersebut hanya menggunakan pengamanan biasa kepada data yang mereka miliki yaitu dengan cara menggunakan pengaman yang disediakan oleh perangkat *software* yang mana ketika login semua orang yang di bagian penjualan bisa mengakses nya, ditambah lagi masih kurangnya pengamanan dalam mengamankan data para debitur yang meliputi data nama toko, lokasi, nope, dan aset dari toko tersebut. Maka dari itu saya mengambil kesempatan ini untuk membantu perusahaan tersebut dalam mengamankan data-data debitur yang mereka miliki dengan tujuan untuk meminimalisir terjadinya kebocoran data.

Debitur merupakan pihak yang berutang kepada pihak lain, biasanya dengan menerima sesuatu dari kreditur yang dijanjikan debitur untuk dibayar kembali pada masa yang akan datang. Pemberian pinjaman kadang memerlukan juga jaminan atau agunan dari pihak debitur. Jika seorang debitur gagal membayar pada waktu yang dijanjikan, suatu proses koleksi formal dapat dilakukan yang kadang mengizinkan penyitaan harta milik debitur untuk memaksa pembayaran.[1]

Data adalah fakta mengenai objek, orang dan lain-lain menjelaskan bahwa basis data adalah bentuk dan penggabungan dari sekumpulan data yang saling terkait untuk memudahkan aktivitas dalam memperoleh informasi. Pembuatan basis data bertujuan untuk mengatasi masalah.[2]

RSA adalah algoritma Kriptografi asimetris. Pertama kali dipekenalkan tahun 1977 oleh ron Rivers, Adi Shamir, dan Leonard Adleman. Penaman RSA berdasarkan inisial nama depan ketiga penemunya. Algoritma tersebut kemudian dipatenkan oleh Massachusetts Institute of Technology pada tahun 1983 di Amerika Serikat dan belaku hingga 21 september 2000. Pada tahun 2005, dibilang faktorisasi terbesar yang digunakan secara umum ialah sepanjang 633 bit, menggunakan metode terdistribusi mutakhir. Kunci RSA pada umumnya sepanjang 1024-2048 bit. [3]

Berdasarkan masalah yang dihadapi, maka penulis mengangkat judul sebagai inti pembahasan dalam penelitian yaitu **"Implementasi Kriptografi Algoritma RSA (Rivest Shamir Adleman) Pada Debitur Di PT. Multimestika Dayasemesta"**

2. KAJIAN PUSTAKA

2.1 Kriptografi

Kriptografi merupakan ilmu dan seni untuk nenjaga kerahasiaan dari suatu pesan dengan cara mengubah pesan tersebut kedalam bentuk yang tidak lagi dimengerti maknanya.[4]

2.2 Algoritma *Rivest Shamir adleman* (RSA)

Rivert Shamir adleman merupakan algoritma kriptografi yang diperkenalkan pada tahun 1977. Sebagai algortima kunci public, RSA mempunyai dua kunci yaitu kunci *public* dan kunci *privat*. Kunci *public* diketahui oleh siapa saja. Sedangkan kunci *privat* hanya pihak tertentu yang boleh mengetahui, dan digunakan untuk proses dekripsi.[10]

Adapun algoritma penyelesaian metode RSA sebagai berikut:

1. Langkah Pertama : Menginput Plaintext.
   Menginputkan Kunci Publik dimana kunci tersebut nantinya akan diproses dan hasilnya akan menjadi cipherteks.

2. Langkah Kedua : Merubah cipherteks kembali menjadi Plaintext awal.
   Algoritma Pembangkit Kunci RSA:

Proses pembangkitan kunci Rivest Shamir Aldeman

Pilih dua bilangan prima $p \neq q$ secara acak dan terpisah untuk tiap tiap p dan q.

Hitung N dengan pesamaan $N = p\ q$.

Hitung φ dengan persamaan$\varphi = (p-1)(q-1)$.

Dipilih bilangan bulat (i*nteger*) antara satu dan $\varphi(1 < e < \varphi)$ yang juga merupakan coprime dari φ.

Hitung d dengan persamaan de = $1 = (mod\varphi)$.

Hasil dari algoritma ini:

Kunci *public* : pasangan (N,e)

Kunci *privat* : pasangan (N,d)

Proses enkripsi

Susun *plaintext* menjadi blok blok m1, m2,…,mm

Hitung *plaintext* C dengan rumus $C_i = m^e \ mod \ n$

Proses dekripsi

Gunakan kunci *privat* untuk menghitung $C_i = m^e \ mod \ n$

Carilah nilai m dengan rumus $C_i = m^d \ mod \ n$

3. METODOLOGI PENELITIAN

3.1 Metodologi Penelitian

Metodologi penelitian merupakan cara yang digunakan untuk memperoleh data menjadi informasi yang lebih akurat sesuai permasalahan yang akan diteliti. Penelitian yang baik harus berdasarkan dengan metodologi penelitian yang baik pula.

Adapun metode dalam penelitian ini mencakup :

1. Observasi

   Sebelum melakukan penelitian lebih lanjut, peneliti melakukan pra riset guna mengetahui masalah yang terjadi dengan data debitur yang tejadi di PT.Multimestika Dayasemesta. Dalam hal ini akan dirumuskan dalam pebelitian ini sehingga menemukan rumus apa saja yang perlu dipersiapkan untuk bagaimana menyelesaikan masalah tersebut.

2. Wawancara

   Untuk mendapatkan data yang yang baik, dalam hal ini peneliti melakukan wawancara kepada pihak manajer PT. Multimestika Dayasemesta dan pihak lain yang terlibat dalam mendukung penelitian ini. Dalam hal ini peneliti melakukan wawancara kepada manajer PT. Multimestika Dayasemesta

3.2 Algoritma Sistem

Di dalam penelitian ini, dijadikan sebuah metode peracangan sistem yaitu *waterfall algoritm.*
Berikut ini adalah fase yang dilakukan dalam penelitian yaitu:
Analisis masalah dan kebutuhan
Desain sistem
Pembangunan sistem
Implementasi sistem

3.2.1 Penyelesaian

Berikut ini adalah data debitur yang di dapat dari PT. MULTIMESTIKA DAYASEMESTA Medan, yang akan diamankan. Dalam pengujiannya, sebagai contoh data yang digunakan sebagai sampel dalam penelitian ini yaitu sebagai berikut:

Tabel 3.1 Data Debitur

Nama	STAR DIESEL
Alamat	Jl. Laksana No 85, Kotamatsum Kec Medan Area
No.Hp	081300000000
Aset	Rumah Pribadi, Toko Sendiri, Pegawai 4 Orang

3.3.3 Penyelesaian Masalah Dengan Menggunakan Algortima RSA

Sesuai dengan referensi yang telah dipaparkan pada bab sebelumnya, berikut ini adalah langkah-langkah penyelesaiannya yaitu:

3.3.3.1 Proses Enkripsi algoritma RSA

Proses enkripsi algoritma Rivest Shamir Adleman (RSA), yaitu sebagai berikut:

1. Pilihlah bilangan prima dengan sembarang, dalam pemilihan ini, di pilih nilai prima (p) = 47 dan nilai (q) = 71.
2. Untuk mencari nilai dari kedua bilangan tersebut, maka dilakukan perkalian $n = p * q$
   $n = 47 * 71 = 3337$
3. Hitung (*phi*) $n = (p-1)$ (q-1) = *3220*
4. Pilih nilai *e* dengan syarat $e > 1$ dan *greatest comman divisior* (*e,3220*) = 1
   Nilai *e* yang di ambil adalah 79.
   Bukti:
   (79, 3220)
   3220 mod 79 = 60
   79 mod 60 = 19
   60 mod 19 = 3
   3 mod 1 = 0
5. Sehingga $de = 1$ (mod 3220) dan $d < 3220$
   $d * 79 = 1 \bmod 3220$
   $d * 79 \bmod 3220 = 1$
   $d = 3337$
   Bukti:
   1019 * 79 mod 3220 = 1
   Sehingga pasangan kunci yang di dapat adalah :
   Kunci enkripsi (*public key*) (*e,n*) = (79, 3337)
   Kunci dekripsi (*private key*) (*d,n*) = (1019, 3337)

   Berdasarkan data yang ada maka dibuat perhitungannya, berikut salah satu data yang dipakai
   Plaintext = STAR DIESEL
   ASCII = 83 84 65 82 32 68 73 69 83 69 76
   Tabel 3.2 karakter pi dan kode ASCII

Pi	Keterangan	Kode ASCII
P1	S	83
P2	T	84
P3	A	65
P4	R	82
P5	Spasi	32
P6	D	68
P7	I	73
P8	E	69
P9	S	83
P10	E	69
P11	L	76

Algoritma Enkripsi yang digunakan dalam algoritma RSA dapat dijelaskan sebagai berikut

1. Disusun *plaintext* menjadi blok-blok m1,m2…,mi
2. Hitung *ciphertext* ci dengan rumus $Ci = M_i^e \ mod \ N$

$$c1 = 83^{79} \ mod \ 3337 = 2251$$

$$c2 = 84^{79}\ mod\ 3337 = 1995$$
$$c3 = 65^{79}\ mod\ 3337 = 541$$
$$c4 = 82^{79}\ mod\ 3337 = 724$$
$$c5 = 32^{79}\ mod\ 3337 = 1379$$
$$c6 = 68^{79}\ mod\ 3337 = 2753$$
$$c7 = 73^{79}\ mod\ 3337 = 725$$
$$c8 = 69^{79}\ mod\ 3337 = 1684$$
$$c9 = 83^{79}\ mod\ 3337 = 2251$$
$$c10 = 69^{79}\ mod\ 3337 = 1689$$
$$c11 = 76^{79}\ mod\ 3337 = 1903$$

Hasil enkripsi
2251.1995.541.724.1379.2753.725.1684.2251.1689.1903

3.3.3.2 Proses Dekripsi algoritma RSA

Algoritma dekripsi yang digunakan dalam algoritma RSA dapat dijelaskan sebagai berikut

1. Gunakan kunci *privat* untuk menghitung $Mi = C_i^d mod\ N$
2. Carilah nilai M dengan rumus $Mi = C_i^d\ mod\ N$
3. Dekripsi dilakukan menggunakan kunci *Privat* d = 1019, 3337
4. Blok blok *ciphertext* didekripsikan sebagai berikut

$$2251^{1019}\ mod\ 3337 = 83$$
$$1995^{1019}\ mod\ 3337 = 84$$
$$541^{1019}\ mod\ 3337 = 65$$
$$274^{1019}\ mod\ 3337 = 82$$
$$1379^{1019}\ mod\ 3337 = 32$$
$$2753^{1019}\ mod\ 3337 = 68$$
$$725^{1019}\ mod\ 3337 = 73$$
$$1689^{1019}\ mod\ 3337 = 69$$
$$2251^{1019}\ mod\ 3337 = 83$$
$$1689^{1019}\ mod\ 3337 = 69$$
$$1903^{1019}\ mod\ 3337 = 76$$

Hasil dekripsi

83 = S	68 = D
84 = T	73 = I
65 = A	69 = E
82 = R	83 = S
32 = spasi	69 = E
	76 = L

Akhirnya diperoleh kembali p*laintext* semula
ASCII = 83 84 65 82 32 68 73 69 83 69 76
Dalm karakter asli = STAR DIESESL

IMPLEMENTASI DAN PENGUJIAN

1. Form login

Form login merupakan tampilan ketika pengguna menjalankan program. Tampilan ini berisikan *username* dan *password* yang harus di isi terlebih dahulu

Gambar 4.12 *form* login

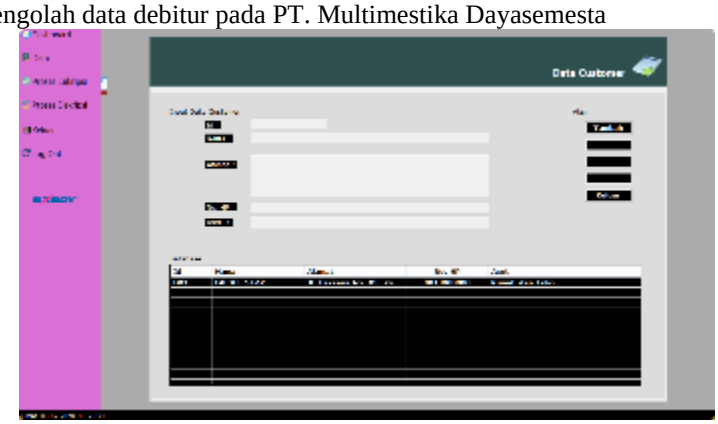
2. Form menu utama

Merupakan tampilan awal pada saat aplikasi dijalankan

Gambar 4.13 form menu utama

3. Form debitur

Form ini berfungsi untuk mengolah data debitur pada PT. Multimestika Dayasemesta



Gambar 4.14 *form* input data debitur

4. Form enkripsi

Form ini berfungsi untuk enkripsi data debitur

Gambar 4.15 *form* enkripsi

5. Form dekripsi

Form ini berfungsi untuk dekripsi data

Gambar 4.16 *form* dekripsi

5.1 KESIMPULAN

Berdasarkan penelitian yang telah dilalui dalam tahap perancangan dan evaluasi kriptografi dalam mengamankan data debitur di PT. Multimestika Dayasemesta menggunakan metode Rivest Shamir Adleman maka dapat disimpulkan bahwa:

1. Algoritma Rivest Shamir Adleman(RSA) digunakan sebagai sistem dalam pengamanan data yang merupakan algoritma yang cukup rumit dalam perhitungannya untuk mengamankan data yang cukup banyak sehingga dapat mengurangi resiko dalam penyalahgunaan dan dapat mengoptimalkan dalam pengamanan data untuk mengamankan data debitur.
2. Dengan cara merancang sistem aplikasi yang dapat digunakan dalam mengamankan data debitur dan mengenkripsi data menjadi karakter sehingga dapat mengamankan data dengan maksimal dan baik.
3. Dengan sistem yang telah dibangun menggunakan aplikasi *Visual Studio* pada kriptografi dalam pengamanan data menggunakan algoritma Rivest Shamir Adleman(RSA), Sehingga sistem ini mampu membantu *sales counter*dalam mengamankan data debitur .

Saran

Adapun saran-saran yang dapat disampaikan kepada pembaca dan kepada seluruh pihak yang berkaitan dengan perancangan sistem ini, yaitu:

1. Diharapkan dalam penelitian yang selanjutnya dapat dikembangkan dengan menggabungkan algoritma yang lain sehingga dapat meningkatkan kinerja sistem.
2. Kepada *sales counter* yang akan menggunakan sistem ini harus diberikan pelatihan untuk pengoperasiannya. Hal ini disampaikan agar penggunaan sistem ini dapat lebih maksimal dan menghindari kesalahan yang tidak diinginkan.
3. Sistem ini masih dibuat hanya kepada PT. Multimestika Dayasemesta, disarankan agar sistem ini juga dapat di gunakan untuk perusahaan lainnya.

4. Diharapkan dalam penelitian selanjutnya dapat membangun Sistem Pengamanan Data dengan menggunakan algoritma dan aplikasi yang lain.

UCAPAN TERIMA KASIH

Pada kesempatan ini saya ucapkan terimakasih kepada Bapak, Ibu dan keluarga saya atas segala doa, semangat dan motivasinya. Selain itu, terimakasih sebesar-besarnya kepada semua pihak yang telah membantu untuk menyelesaikan penulisan skripsi ini, yaitu :

1. Bapak Rudi Gunawan, SE, M.Si, Selaku Ketua STMIK Triguna Dharma Medan.
2. Bapak Zulfian Azmi, ST, M.Kom, Selaku Wakil Ketua I Bidang Akademik STMIK Triguna Dharma Medan.
3. Bapak Marsono. S.Kom, M.Kom, Selaku Ketua Program Studi Sistem Informasi STMIK Triguna Dharma Medan.
4. Bapak Azanuddin, S.Kom, M.Kom , selaku Dosen Pembimbing I yang membimbing mahasiswa dalam isi dan tata bahasa selama menyelesaikan skripsi.
5. Bapak Jufri Halim, SE., MM, selaku Dosen Pembimbing II yang membimbing mahasiswa dalam teknik penulisan skripsi.
6. Seluruh Dosen, Staff dan Pegawai STMIK Triguna Dharma.
7. Terimakasi juga disampaikan kepada PT. Multimestika Dayasemesta yang telah mengizinkan melakukan penelitian dan memberikan data yang benar sehingga skripsi ini dapat terselesaikan dengan baik.

Akhir kata saya ucapkan rasa terima kasih kepada semua pihak yang terlibat dalam penyelesaian skripsi ini Skripsi ini masih sangat jauh dari sempurna. Oleh karena itu, diharapkan saran dan kritik yang sifatnya membangun dari para pembaca demi kesempurnaan skripsi ini.

Daftar Pustaka

[1] Y. Yusmita, R. P. Ariyanti, E. D. P. Njoto, and R. Yudistira, "Perlindungan Hukum Terhadap Debitur Dan Kreditur Dalam Melakukan Perjanjian Baku," *DiH J. Ilmu Huk.*, vol. 15, no. 1, pp. 59–67, 2019, doi: 10.30996/dih.v15i1.2265.

[2] M. N. Fauzy and Dkk, "Keamanan basis data pada validasi data sistem informasi kepakaran," *J. Inf. Politek. Indonusa*, vol. 4, no. 3, 2018.

[3] R. S. A. Rivest and S. Adleman, "Enkripsi File Audio Mp3 Dan Wav Menggunakan Metode Kriptografi," pp. 1–8, 2020.

[4] H. S. Sulun, "Penerapan Algoritma Kriptografi RSA dalam Pengiriman Data Melalui Socket Berbasis TCP / IP," *Sekol. Tek. Elektro dan Inform. Inst. Teknol. Bandung*, 2018.

[5] I. Pendahuluan and B. W. C. O. Jones, "IMPLEMENTASI KRIPTOGRAFI RSA UNTUK PENINGKATAN KEAMANAN DATABASE E-COMMERCE," vol. 18, pp. 627–630, 2019.

[6] Z. Arifin, K. kunci, A. Rsa, K. Privat, and K. Publik, "Studi Kasus Penggunaan Algoritma RSA Sebagai Algoritma Kriptografi yang Aman," *J. Inform. Mulawarman Progr. Stud. Ilmu Komput. Univ. Mulawarman*, vol. 4, no. 3, pp. 7–14, 2009.

[7] R. West, J. Brown, and M. Jarvis, "Epidemic of youth nicotine addiction? What does the National Youth Tobacco Survey reveal about high school e-cigarette use in the USA? (Preprint)," *Qeios*, 2019, doi: 10.32388/745076.3.

[8] A. Widiasari, "Implementasi Algoritma Kriptografi Rsa Pada Aplikasi Smart Card Skripsi," 2014.

[9] A. P. Wahyadyatmika, R. R. Isnanto, and M. Somantri, "Implementasi Algoritma Kriptografi RSA pada Surat Elektronik (E-Mail)," *Transient*, vol. 3, no. 4, pp. 1–9, 2014.

[10] Y. Anshori, A. Y. Erwin Dodu, and D. M. P. Wedananta, "Implementasi Algoritma Kriptografi Rivest Shamir Adleman (RSA) pada Tanda Tangan Digital," *Techno.Com*, vol. 18, no. 2, pp. 110–121, 2019, doi: 10.33633/tc.v18i2.2166.

[11] 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.

[12] S. M. Ayu *et al.*, "REKAYASA PERANGKAT LUNAK PENGOLAHAN DATA PRODUK MASUK DAN KELUAR MENGGUNAKAN PHP DAN MySQL (Studi Kasus : Suzuya Rocky Plaza Padang)," vol. 5, no. 1, pp. 23–29, 2017, doi: 10.21063/JTIF.2017.V5.1.23-29.

[13] Firdaus and A. Saputra, "Sistem Informasi Manajemen Pendistribusian Barang Bekas Pada UD. Yuli Mutiara Dengan Bahasa Pemograman PHP Dan Database MySQL," *Maj. Ilm.*, vol. 25, no. 2, pp. 138–148, 2018.

BIOGRAFI PENULIS

<table>
<tr>
<td>  </td>
<td>Data Diri
Nama : Muhammad Yusuf
Tempat/Tanggal Lahir : Medan, 14Maret 1997
Jenis Kelamin : Laki Laki
Agama : Islam
Status : Belum Menikah
Pendidikan Terakhir : Sekolah Menengah Atas
Kewarganegaraan : Indonesia
E-mail : bangucup1997@gmail.com

Pendidikan Formal
1. Tahun 2004 - 2010 : SD 105299
2. Tahun 2010 -2013 : SMP Swasta Yayasan Pendidikan Islam Delitua
3. Tahun 2013 -2016 : SMA N1 Delitua</td>
</tr>
<tr>
<td>  </td>
<td>Azanuddin, S.Kom., M.Kom

Dosen pengajar tetap STMIK TRIGUNA DHARMA</td>
</tr>
<tr>
<td>  </td>
<td>Jufri Halim, SE., MM

Dosen pengajar tetap STMIK TRIGUNA DHARMA</td>
</tr>
</table>