Jurnal CyberTech
Vol.x. No.x, Maret 2019, pp. xx~xx
P-ISSN : xxxx-xxxx
E-ISSN : xxxx-xxxx

Implementasi Metode RSA Untuk Mengamankan Data Pembayaran Uang SPP Di SMK Harapan Bangsa Tanjung Morawa

Rudianto. [#1], **Nurcahyo budi nugroho, S.Kom., M.Kom** [#2], **Firahmi Rizky, S.Kom., M.Kom**[#3]
[#1] Program Studi Sistem Informasi, STMIK Triguna Dharma
[#2,3] Program Studi Sistem Informasi, STMIK Triguna Dharma

Article Info

Article history:
Received xxxx xx[th], 2020
Revised xxxx xx[th], 2020
Accepted xxxx xx[th], 2020

Keyword:
Kriptografi
RSA
Data Siswa

ABSTRAK

SPP adalah salah satu upaya pengendalian mutu sekolah. Data siswa merupakan hal yang sangat dijaga kerahasiaanya agar terhindar dari pihak yang tidak bertanggung jawab. Oleh karen itu dibutuhakan pegaman data sistem atas pencurian database dengan menggunakan kriptografi.

Kriptografi adalah ilmu untuk mengurangi resiko ancaman keamanan dengan melakukan proses enkripsi dan dekripsi pada data dan informasi. Penerapan satu teknik kriptografi memiliki tingkat resiko kebocoran data yang lebih tinggi dari keamanan yang menerapkan lebih dari satu teknik kriptografi. Oleh karena itu, diperlukan penerapan dua teknik kriptografi yang mampu mengamankan pesan email sebelum proses pengiriman. Kriptografi RSA yang populer dengan penggunaan kunci publiknya digunakan untuk mengamankan salah satu komponen dari Blowfish yaitu kunci simetris.

Penelitian ini bertujuan membuat sistem yang dapat mengamankan pesan email dan kunci simetris sebelum dilakukan proses pengiriman dengan mengkombinasikan kriptografi Blowfish dan RSA diharapkan dapat meningkatkan keamanan secara lebih. Tahap uji serangan brute force yang dilakukan sebanyak tiga kali menghasilkan plaintext yang tidak utuh dan tahap uji ukuran data setelah dienkripsi membengkak sebesar 0,09KB dari hal tersebut maka kombinasi teknik kriptografi yang digunakan aman dan efisien.

***Kata Kunci**: Data Siswa, Kriptografi, RSA*

Aplikasi pendataan siswa, nilai, maupun pembayaran uang

Nama : Rudianto
Kator : STMIK Triguna Dharma
Program Studi : Sistem Informasi
Email : reizaandiraalisriya@gmail.com

%1. PENDAHULUAN

Keamanan data merupakan hal yang sangat penting dalam menjaga kerahasiaan informasi terutama yang berisi informasi sensitif yang hanya boleh diketahui isinya oleh pihak yang berhak saja, apalagi jika pengirimannya

dilakukan melalui jaringan publik, apabila data tersebut tidak diamankan terlebih dahulu, akan sangat mudah disadap dan diketahui isi informasinya oleh pihak-pihak yang tidak memiliki wewenang.. Aplikasi pendataan nilai mata pelajaran adalah salah satu upaya pengendalian mutu penilaian, karena merupakan suatu penyelesaian yang dapat membantu pendidik dalam mengolah data nilai pengetahuan ,sikap spritual, keterampilan, dan Menyusun hasil penilaian. Data nilai merupakan hal yang sangat dijaga kerahasiaanya agar terhindar dari pihak yang tidak bertanggung jawab. Oleh karen itu dibutuhakan pegaman data sistem atas pencurian *database* dengan menggunakan kriptografi.

Kriptografi adalah ilmu untuk mengurangi resiko ancaman keamanan dengan melakukan proses enkripsi dan dekripsi pada data dan informasi. Penerapan satu teknik kriptografi memiliki tingkat resiko kebocoran data yang lebih tinggi dari keamanan yang menerapkan lebih dari satu teknik kriptografi. Oleh karena itu, diperlukan penerapan dua teknik kriptografi yang mampu mengamankan pesan email sebelum proses pengiriman. Kriptografi RSA yang populer dengan penggunaan kunci publiknya digunakan untuk mengamankan salah satu komponen dari Blowfish yaitu kunci simetris. Penelitian ini bertujuan membuat sistem yang dapat mengamankan pesan email dan kunci simetris sebelum dilakukan proses pengiriman dengan mengkombinasikan kriptografi Blowfish dan RSA diharapkan dapat meningkatkan keamanan secara lebih. Tahap uji serangan brute force yang dilakukan sebanyak tiga kali menghasilkan plaintext yang tidak utuh dan tahap uji ukuran data setelah dienkripsi membengkak sebesar 0,09KB dari hal tersebut maka kombinasi teknik kriptografi yang digunakan aman dan efisien.

%1. Kajian Pustaka

%1.%2. Kriptografi

Kriptografi adalah studi yang bertujuan untuk mengamankan dan merahasiakan dengan melakukan proses enkripsi dan dekripsi pada data yang akan diamankan . Enkripsi merupakan proses pengubahan data menjadi bentuk sandi yang tidak dipahami dan dibaca, sedangkan dekripsi merupakan proses pengembalian data dalam bentuk sandi ke dalam bentuk semula yang dapat dipahami dan memiliki makna. Dalam kriptografi terdapat beberapa teknik penyandian data yaitu simetris dan asimetris. Kriptografi simetris menggunakan kunci yang sama (kunci simetris) untuk melakukan proses enkripsi dan dekripsi. Kriptografi asimetris menggunakan kunci yang berbeda untuk proses enkripsi (menggunakan kunci publik) dan dekripsi (menggunakan kunci privat). Kedua teknik tersebut memiliki keunggulan dan kekurangan masing-masing yang diukur berdasarkan durasi enkripsi, durasi dekripsi, tingkat perubahan yang dihasilkan, entropi, dan jumlah bit yang dibutuhkan untuk pengkodean secara optimal

Salah satu metode kriptografi simetris yaitu Blowfish. Blowfish termasuk metode yang menerapkan cipherblock pada proses enkripsi data dalam 8 byte (64 bit) blok dengan ukuran kunci 32 bit sampai dengan 448 bit dan cocok digunakan untuk menyandikan file berukuran besar, tetapi terbilang kurang aman karena kunci yang digunakan hanya satu . Dan salah satu metode kriptografi asimetris yaitu RSA. RSA adalah Kriptosistem kunci publik pertama dan digunakan secara luas untuk mengamankan transmisi data dan cocok digunakan untuk mengenkripsi data berukuran kecil, karena proses enkripsi dan dekripsi RSA terbilang lama . Blowfish dengan waktu enkripsi dan dekripsi terbilang cepat yaitu dengan input sebesar 69 KB lama proses enkripsi sebesar 85 ms dan proses dekripsi sebesar 51 ms dan Kriptografi Hill Cipher dan RSA dengan hasil proses enkripsi RSA lebih cepat dikarenakan data yang dienkripsi berukuran 9 byte dari matriks yang telah ditentukan .

%1.%2. RSA (Rivest Shamir Adleman)

Kriptografi *Hill Cipher* dan RSA dengan hasil proses enkripsi RSA lebih cepat dikarenakan data yang dienkripsi berukuran 9 byte dari matriks yang telah ditentukan. Kriptografi Hill Cipher dan RSA dengan hasil proses enkripsi RSA lebih cepat dikarenakan data yang dienkripsi berukuran 9 byte dari matriks yang telah ditentukan

Penerapan algoritma kriptografi RSA menjadi solusi yang baik pada sistem untuk menjamin kerahasiaan data-data penjualan yang disimpan didalam database, dengan penggunaan algoritma RSA ke dalam sistem data tersebut maka data yang disimpan di dalam database berupa penjumlahan angka sehingga isi datanya tidak dapat dimengerti oleh pihak lain. Proses signing dilakukan dengan mengubah sebuah isi dokumen menjadi message digest dan mengenkripsinya menggunakan algoritma kriptografi RSA. Sementara, proses verifikasi dilakukan dengan membandingkan hasil dekripsi isi dokumen yang diterima (ciphertext) dengan message digest dari isi dokumen sebenarnya.

%1. **Metodologi Penelitian**

%1.%2. **Algoritma Sistem**

Algoritma sistem merupakan penjelasan langkah-langkah penyelesaian masalah dalam perancangan sistem penerapan metode RSA dalam mengamankan data SPPpada SMK Harapan Bangsa Tanjung Morawa.

3.3.1 Digital Signature Menggunakan Algoritma RSA

Langkah pertama dalam Algoritma RSA adalah melakukan inisialisasi terhadap nilai bilang prima p = 29 dan q = 43 yang diambil secara acak. Berikut ini adalah salah satu data tabel 3.1 yang dimana setiap plainteks akan di ubah ke bentuk kode ASCII yaitu sebagai berikut:

Tabel 3.1 ASCII

No	*Plainteks*	*Kode ASCII*
1	***1***	*49*
2	***5***	*53*
3	***1***	*49*
4	***1***	*49*
5	***0***	*48*
6	***1***	*49*

Berikut metode RSA:

%1. Pembangkit Kunci Metode RSA

%2. Pilihlah bilangan prima yang sudah di dapat diatas adalah (p)= 29 dan nilai (q)=43.

%2. Untuk mencari nilai dari kedua bilangan tersebut, maka dilakukan perkalian n = p * q n = 29 * 43 = 1247

%2. Hitung (phi)n=(p-1)(q-1) n=28 * 42 =1176

%2. Pilih nilai edengan syarat e> 1 = 1

Nilai eyang di ambil adalah 53. Bukti:

(53, 1176)

1176 mod 53 = 10

53 mod 10 = 3

10 mod 3 = 1

3 mod 1 = 0

Sehingga d*e=1(mod 1176) dan d<1176 d*53=1mod1176

d*53 mod1176 = 1 d = 821

Bukti:

821 * 53 mod 1176 = 1

Sehingga pasangan kunci yang di dapat adalah :

Publickey(e,n) = (53, 1247) dan Privatekey(d,n) = (821, 1247)

%1. Enkripsi Data

C1 = 4953 mod 1247 = 36

C2 = 5353 mod 1247 = 1176

C3 = 4953 mod 1247 = 36

C4 = 4953 mod 1247 = 36

C5 = 48 mod 1247 = 292

C6 = 4953 mod 1247 = 36

Tabel 3.2 Hasil Enkripsi

Plaintext	*Hasil Enkripsi*	*Heksa*
49	*36*	*24*
53	*1176*	*498*
49	*36*	*24*
49	*36*	*24*
48	*292*	*124*
49	*36*	*24*

%1. Dekripsi Data

Langkah selanjutnya adalah melakukan dekripsi data dengan rumus

$P = C^d \bmod n$.

P1 = 36821 mod 1247 = 49
P2 = 1176821 mod 1247 = 53
P3 = 36821 mod 1247 = 49
P4 = 36821 mod 1247 = 49
P5 = 292821 mod 1247 = 48
P6 = 36821 mod 1247 = 49

Tabel 3.3 Hasil Dekripsi Data

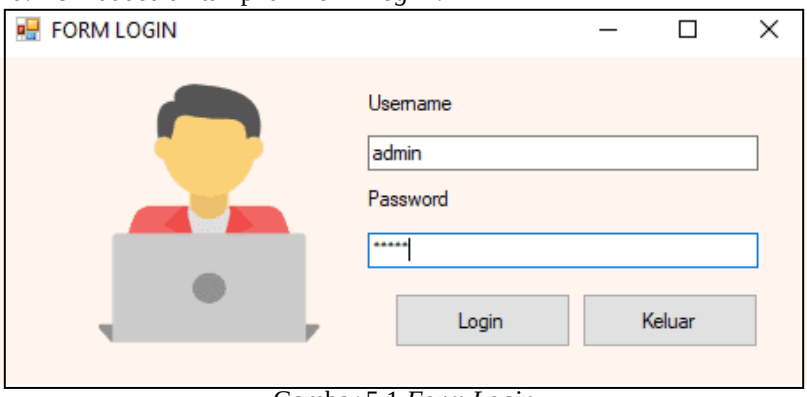
Chipertext	***Hasil DekripsiData***	***Plaintext***
36	*49*	***1***
1176	*53*	***5***
36	*49*	***1***
36	*49*	***1***
292	*48*	***0***
292	*49*	***1***

%1. **Pengujian dan implementasi**

Implementasi sistem adalah tahapan dimana sistem atau aplikasi siap untuk dioprasikan pada keadaan yang sebenarnya sesuai dari hasil analisis dan perancangan yang dilakukan, sehingga akan diketahui apakah sistem atau aplikasi yang dibangunn dapat menghasilkan suatu tujuan yang dicapa, dan aplikasi Kriptografi ini dilengkapi dengan tampilan yang bertujuan untuk memudahkan penggunanya. Fungsi dari *interface* (antarmuka) ini adalah untuk memberikan *input* dan menampilkan *output* dari aplikasi. Pada aplikasi ini memiliki *interface* yang terdiri dari *Form login, Form* Data siswa, , *Form* RSA, *Form Menu Utama, Form* Data login.

%1. *Form Login*

Form Login digunakan untuk mengamankan sistem dari *user-user* yang tidak bertanggung jawab sebelum masuk ke *Form* Utama. Berikut adalah tampilan *Form Login :*

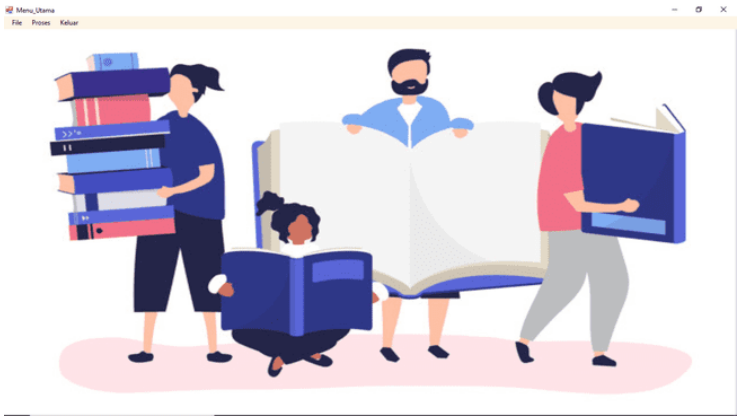


Gambar 5.1 *Form Login*

Keterangan : Tombol login digunakan untuk mem-validasikan *username* dan *password* yang telah kita isi pada kotak teks yang disediakan.

%1. *Form* Menu Utama

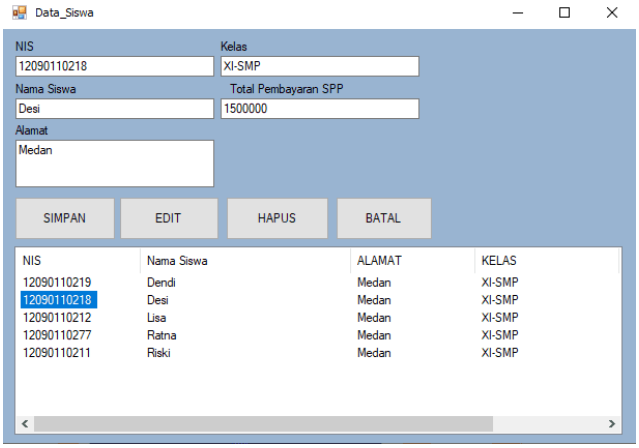
Form Menu Utama digunakan sebagai penghubung untuk *Form* Data Siswa, , *Menu RSA* dan ada beberapa *Form* lainnya.



Gambar 5.2 *Form Menu* Utama

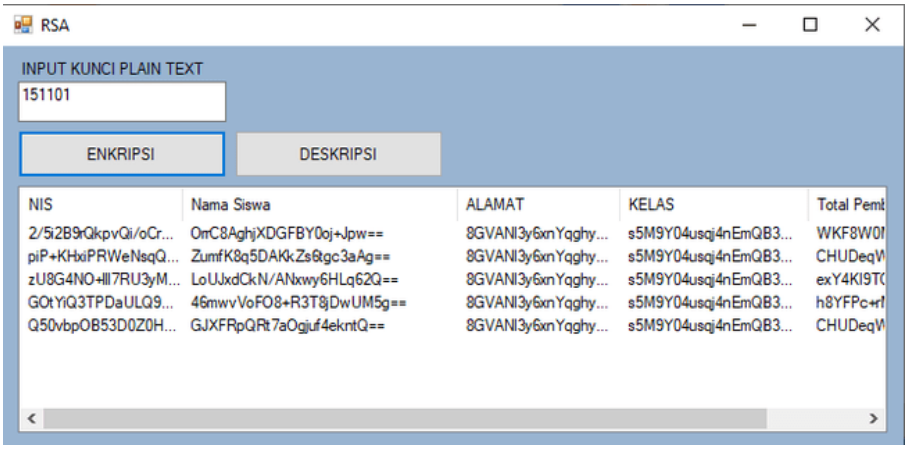
%1. *Form* Data Siswa

Form Data Siswa adalah *Form* pengolahan data siswa dalam penginputan data , ubah data dan penghapusan data siswa. Adapun *Form* siswa adalah sebagai berikut.



Gambar 5.3 *Form* Data Siswa

%1. *Form* Metode RSA



Gambar 5.4 *Form* Proses *RSA*

Dalam *Form* RSA dapat mengenkripsikan dan deskripsikan adalah sebagai berikut :

%1. Button Proses Enskrips berfungsi untuk memproses mengenkripsikan data siswa.

%1. Button Proses Deskripsi berfungsi untuk memproses mendenkripsikan data siswa.

%1. Button Keluar berfungsi untuk kembali ke *menu* utama.

%1. **Kesimpulan dan Saran**

Berdasarkan hasil analisa dari permasalahan yang terjadi dengan kasus yang di bahas Implementasi metode RSA untuk mengamankan data pembayaran SPP di SMK HARAPAN BANGSA Tanjung Morawa terhadap sistem yang dirancang dan dibangun maka dapat ditarik kesimpulan sebagai berikut :

%1. Untuk menganalisa masalah dalam mengamankan data pembayaran SPP di SMK HARAPAN BANGSA Tanjung Morawa dengan menggunakan metode RSA.
%1. Dapat membangun kriptografi mengamankan data pembayaran SPP di SMK HARAPAN BANGSA Tanjung Morawa dengan menggunakan metode RSA.
%1. Dapat mengimplemtasikan mengamankan data pembayaran SPP di SMK HARAPAN BANGSA Tanjung Morawa dengan menggunakan metode RSA.

Untuk meningkatkan kemampuan dan fungsi dari sistem ada beberapa saran yang sdapat diberikan untuk pengembangan yang bisa dilakukan yaitu :

%1. Sistem yang dirancang dan dibangun harus dikembangkan lagi dengan berbasis *Mobile* dan *Website*.
%1. Disarankan sistem tidak hanya menggunakan metode *RSA* akan tetapi bisa dipadukan dengan metode yang lain ataupun dengan kombinasi yang lain.

REFERENSI

[1] Luthfi Octafyan Prakoso, Hany Yusmaini, Maria Selvester Thadeus, Sugeng Wiyono i, " PERBEDAAN EFEK EKSTRAK BUAH NAGA MERAH (Hylocereus polyrhizus) DAN EKSTRAK BUAH NAGA PUTIH (Hylocereus undatus) TERHADAP KADAR KOLESTEROL TOTAL TIKUS PUTIH (Rattus norvegicus) " 2017.

[2] M. Puji Sari Ramadhan and M. Usti Fatimah S. Pane, Judul : Mengenal Metode Sistem Pakar, Cetakan Pertama ed., Fung Jurnal Perlindungan Tanaman Indonesia y, Ed., 2018.

[3] N. Budi Riyanto and O. Suria, "Sistem Pakar Diagnosa Penyakit Pencernaan Mengunakan Metode Teorema Bayes 7".

[4] M. J. Effendi, M. Triawan and S. Musirawas Lubuklinggau, "SISTEM PAKAR UNTUK MENDIAGNOSA PENYAKIT TANAMAN KOPI BERBASIS WEB," 2019.

[5] D. T. Yuwono, A. Fadlil and S. Sunardi, "Implementasi Metode Dempster Shafer Pada Sistem Pakar Diagnosa Gangguan Kepribadian," *JURNAL SISTEM INFORMASI BISNIS*, vol. 9, no. 1, p. 25, 7 5 2019.

[6] Evi Umayah U. dan Moch. Amrun H., " Uji Aktivitas Antioksidan Ekstrak Buah Naga (Hylocereus undatus (Haw.) Britt. & Rose) (Antioxidant Activity Assay of Dragon Fruit Extract (Hylocereus undatus (Haw.) Britt. & Rose), Jurnal ILMU DASAR, Vol. 8, no. 1,2007.

[7] Amanda Angelina Sinaga , Sri Luliana , Andhi Fahrurroji " Losio Antioksidan Buah Naga Merah (Hylocereus polyrhizus Britton and Rose) " *Orginal Articel*, 2015.

[8] Arif Wibowo, Ani Widiastuti, dan Wahyu Agustina " PENYAKIT-PENYAKIT PENTING BUAH NAGA DI TIGA SENTRA PERTANAMAN DI JAWA TENGAH ", Jurnal Perlindungan Tanaman Indonesia 2011.

[9] M. Zulfian Azmi, ST., M.Kom. dan Verdi Yasin, S.Kom ., Pengantar Sistem Pakar dan Metode (Introduction of Expert System and Methods), Jakarta: Mitra Wacana Media, 2019, pp. 11-17.

[10] ChairunNa s, "SISTEMPAKARDIAGNOSAPENYAKTTIROIDMENGGUNAKANMETOD E DEMPSTERSHAFE R," *JURNALTEKNOLOGIDANOPENSOURCE*, vol. VOL.2No.1, 2019.

[11] N. Sari Br Sembiring and M. Dayan Sinaga, "Penerapan Metode Dempster Shafer Untuk Mendiagnosa Penyakit Dari Akibat Bakteri Treponema Pallidum Application Of Dempster Shafer Method For Diagnosing Diseases Due To Treponema Pallidum Bacteria," *180. CSRID Journal*, vol. 9, no. 3, 2017.

UCAPAN TERIMA KASIH

Terima kasih diucapkan kepada pihak-pihak yang telah mendukung dalam proses pembuatan jurnal ini yang tidak dapat disebutkan satu persatu. Kiranya bisa memberi manfaat bagi pembaca dan dapat meningkatkan kualitas jurnal selanjutnya.

BIOGRAFI PENULIS

	**Rudianto**
	**Nurcahyo budi nugroho, S.Kom., M.Kom**
	Firahmi Rizky, S.Kom., M.Kom