Journal of Computer and Information Systems Ampera
Vol. 1, No. 1, January 2020 e-ISSN: 2775-2496
https://journal-computing.org/index.php/journal-cisa/index

Digital Signature Pada Citra Digital Menggunakan Algoritma Rc6 Studi Kasus: Dokumen Kartu Keluarga

Hasril Yusuf[1], Afriyudi[2], Hadi Syaputra*[3]

[1,2]Informatics Departement , Universitas Bina Darma, Palembang, Indonesia
[3]Information System Departement, Universitas Bina Darma y, Palembang, Indonesia
Email: hasriltugas95@gmail.com[1], afriyudi@binadarma.ac.id[2], hadisyaputra@binadarma.ac.id[3]

Abstract

The confidentiality of a document is an important requirement for the people of this age to protect their privacy from people who have no right to know it. To overcome this, an application that can encrypt document files in the form of digital images is needed so that it is not known by others. . The algorithm that has been developed in this study we use the RC6 algorithm as an algorithm method. The purpose of this system will be to help specifically in the administration section to enter or store documents, find and create reports that will be seen by government installations in an encrypted form, and if needed as information can easily be decrypted again. The development method uses the waterfall model. The analytical tool used is Use case, Activity, Diagram, and Class Diagram. The software used is Dreamweaver and Xampp. This system is built in order to provide convenience in processing document data.

Keywords: Document, Algorithm RC6, Dreamweaver, Xampp

1. PENDAHULUAN

Salah satu upaya untuk menjaga integritas informasi pada citra digital adalah dengan menyisipkan digital signature terlebih dahulu ke dalam citra digital yang akan dikirim. Digital signature atau yang juga disebut tanda tangan digital adalah suatu mekanisme untuk menggantikan tanda tangan secara manual pada dokumen kertas [1]. Digital signature memiliki fungsi sebagai penanda pada data yang memastikan bahwa data tersebut adalah data yang sebenarnya (utuh/integral). Penanda pada digital signature ini tidak semata hanya berupa tanda tangan digital, tetapi dapat berupa cap digital, text, bit, dan gambar. Aspek keamanan dan kerahasiaan bukan disediakan dengan sistem berupa tanda tangan digital, tetapi tanda tangan yang telah dienkripsi terlebih dahulu dengan algoritma tertentu.

DISDUKCAPIL (Dinas Kependudukan Dan Pencatatan Sipil) merupakan suatu dinas yang bergerak di bidang pendataan data penduduk, dalam suatu kegiatannya tak lepas dari pengelolaan dokumen kartu keluarga Dokumen kartu keluarga merupakan dokumen yang bersifat *confidentiality* atau rahasia dimana dokumen tersebut menyimpan informasi berupa data pendudukan dalam satu keluarga yang dilengkapi identitas no induk penduduk secara sah sesaui peraturan negara.

Tanda tangan digital (digital signature) adalah salah satu teknologi yang digunakan untuk meningkatkan keamanan jaringan [1]. Digital signature berfungsi sebagai penanda pada data untuk memastikan keaslian data. Digital signature dapat memenuhi setidaknya dua syarat keamanan jaringan, yaitu authenticity dan nonrepudiation. Digital signature dimasukkan ke dalam dokumen yang akan diamankan, dengan cara menyisipkan ke dalamnya. Penelitian yang dilakukan oleh Noertjahyana [3] membahas tentang penyisipan data ke dalam media lain. Noertjahyana memanfaatkan teknik ini untuk mengamankan pesan.

Menurut [5] melakukan pengujian analisa kefektifan enskripsi, dan evaluasi keamanan enskripsi citra digital dengan algoritma rc6. Hasil yang didapat menunjukan enskripsi pada citra digital dengan algoritma rc6 menunjukan hasil yang memuaskan dan cukup menjanjikan untuk menjaga keamanan file berupa citra digital. Algoritma RC6 dalam penerapan *Digital Signature* kedalam dokumen Cita *Digital* kartu penduduk adalah pada saat dokumen citra digital kartu penduduk dibuat maka pertama kali petugas akan memasukkan kunci dalam bentuk plainteks sebagai digital signature kedalam dokumen citra digital dilanjutkan dengan proses enkripsi pada algoritma RC6, setelah berhasil dikirimkan maka selanjutnya penerima harus memasukkan kunci dalam bentuk palinteks yaitu kunci *digital signature* sesuai dengan yang telah disisipkan di awal pada saat pembuatan citra *digital*.

Berdasarkan latar belakang diatas maka dilakaukan penelitian ini dengan judul "Digital Signature Pada Citra Digital Menggunakan Algoritma RC6 Study kasus Dokumen Kartu Keluarga".

2. METODOLOGI PENELITIAN

2.1 Metode Analisis

Didalam melakukan penelitian metodologi yang digunakan yaitu model *Waterfall*. Model *waterfall* menyediakan alur hidup perangkat

lunak secara sekuensial dan terurut dimulasi dari analisis, desai, pengodean, pengujian dan tahap pendukung [3]. Tahapan-tahapan metodologi *waterfall* [3] adalah sebagai berikut :

1) Analisis
   Proses pengumpulan analisis kebutuhan dilakukan secara intensif untuk mespefikasikan kebutuhan perangkat lunak agas dapat dipahami perangkat lunak seperti apa yang dibutuhkan oleh *user*. Spesifikasi kebutuhan perangkat lunak pada tahap ini perlu untuk didokumentasikan.
2) Desain
   Desain perangkat lunak adalah proses multi langkah yang fokus pada desain pembuatan program perangkat lunak termasuk struktur data, arsitektur perangkat lunak, representasi antarmuka, dan prosedur pengodean. Tahap ini mentranlasi kebutuhan desain agar dapat diimplementasikan menjadi program pada tahap selanjutnya.
3) Pembuatan Kode Program
   Desain harus ditranslasikan kedalam program perangkat lunak. Hasil dari tahap ini adalah program komputer sesuai dengan desain yang dibuat pada tahap desain.
4) Pengujian
   Pengujian fokus pada perangkat lunak secara dari segi logik dan fungsional dan memastikan bahwa semua bagian sudah diuji. Hal ini dilakukan untuk meminimalisir kesalahan (*error*) dan memastikan keluaran yang dihasilkan sesuai dengan yang diinginkan.
5) Pendukung Atau Pemeliharaan

   Tidak menutup kemungkinan sebuah perangkat lunak mengalami perubahan ketika sudah dikirim ke user. Perubahan bisa terjadi karena adanya kesalahan yang muncul dan tidak terdeteksi saat pengujian atau perangkat lunak harus beradaptasi dengan lingkungan baru.Metode Pengumpulan Data

2.2 Metode Pengumpulan Data

Adapun metode pengumpulan data yang diperoleh untuk penelitiian ini sebagai informasi untuk penelitian yang dilakukan yaitu :

1) Wawancara (*Interview*)
   Wawancara untuk mencari dan mengumpulkan data dengan cara langsung berbicara dengan para pengguna yang berkecimpung

didunia pengelolaan data dokumen apakah dengan sistem yang akan dibangun dapat memberikan pelayanan yang lebih baik.

2) Pengamatan (*Observasi*)
Pengamatan langsung terhadap instansi atau lembaga yang berhubungan dengan pengelolaan dokumen untuk memperoleh informasi yang nantinya akan digunakan dan diolah dalam menginpleentasikan metode RC6 pada pengelolaan dokumen penduduk.

3) Dokumentasi
Pengumpulan data yang dilakukan dengan mengamati proses pengelolaan dokumen penduduk berbasis web.

2.3 Algoritma RC6

Menurut [4], Metode Algoritma RC6 merupakan salah satu kandidat *Advanced Encryption* Standard (AES) yang diajukan oleh RSA *Security Laboratories* kepada NIST. Dirancang oleh *Ronald L Rivest, M.J.B. Robshaw, R. Sidney dan Y.L. Yin*, algoritma ini merupakan pengembangan dari algoritma sebelumnya yaitu RC5 dan telah memenuhi semua kriteria yang diajukan oleh NIST. RC6 adalah algoritma yang menggunakan ukuran blok hingga 128 bit, dengan ukuran kunci yang digunakan bervariasi antara 128, 192 dan 256 bit. Algoritma RC6 dilengkapi dengan beberapa parameter, sehingga dituliskan sebagai RC6-w/r/b. Parameter w merupakan ukuran kata dalam satuan bit, parameter r merupakan bilangan bukan negatif yang menunjukan banyaknya iterasi selama proses enkripsi dan parameter b menunjukan ukuran kunci enkripsi dalam byte. Setelah algoritma ini masuk dalam kandidat AES, maka ditetapkan bahwa nilai w = 32, r = 20 dan b bervariasi antara 16, 24 dan 32 byte. RC6-w/r/b memecah blok 128 bit menajdi 4 buah blok 32-bit, dan mengikuti aturan enam operasi dasar sebagai berikut:

1. a + b operasi penjumlahan bilangan integer
2. a - b operasi pengurangan bilangan integer
3. a $\oplus$ b operasi *exclusive-OR* (XOR)
4. a x b operasi perkalian bilangan integer
5. a<<<b a dirotasikan ke kiri sebanyak variabel kedua (b)
6. a>>>b a dirotasikan ke kanan sebanyak variabel kedua (b)

3. HASIL DAN PEMBAHASAN

3.1 Hasil Pengujian

Hasil pengujian ini terdiri daridua komponen yaitu pengujian black box dan pengujian perhitungan. Pengujian dilakukan dengan melakukan uji coba dengan 50 data sampel.

3.1.1 Hasil Pengujian *Black-Box*

Pengujian yang dilakukan terhadap sistem dengan menggunakan Metode *Black Box*. Menurut [2], Pengujian *Black-Box* berfokus pada persyaratan fungsional perangkat lunak. Dengan demikian, pengujian *black-box* memungkinkan perekayasaan perangkat lunak mendapatkan serangkaian kondisi input yang sepenuhnya menggunakan semua persyaratan fungsional untuk suatu program.
Pengujian *black-box* berusaha menemukan kesalahan dalam kriteria sebagai berikut:

a. fungsi-fungsi tidak benar atau hilang
b. kesalahan *interface*
c. kesalahan dalam struktur data atau akses database eksternal
d. kesalahan kinerja
e. inisialisasi dan kesalahan terminasi

Tabel 1. Hasil Pengujian Sistem

Modul yang diuji	Teknik Pengujian	Hasil	Kriteria
Halaman *Login user*	Mengakses halaman *login user*	Menampilkan halaman *login user*	a, b
Halaman *home user*	Mengakses halaman *home user*	Menampilkan halaman *home user*	a,b

Tabel 2. Hasil Pengujian Sistem (Lanjutan)

Modul yang diuji	Teknik Pengujian	Hasil	Kriteria
Halaman User	Memilih menu User	Menampilkan halaman User.	a,b

Vol. 1, No. 1, January 2020 e-ISSN: **2775-2496**

https://journal-computing.org/index.php/journal-cisa/index

Modul yang diuji	Teknik Pengujian	Hasil	Kriteria
Halaman User	Mengisi data dan memilih *button* simpan	Data tersimpan dan menampilkan halaman berhasil melakukan penyimpanan data pengguna.	a,b,c
Halaman Data Kabupaten	Memilih menu Data Kabupaten	Menampilkan halaman Data Kabupaten.	a,b
Halaman Tambah Data Kabupaten	Mengklik *button* Tambah	Data berhasil menampilkan halaman tambah data kabupaten.	a,b,c
Halaman Edit Data Kabupaten	Mengklik *button* Edit	Data berhasil menampilkan halaman edit data kabupaten.	a,b,c
Halaman Hapus Data Kabupaten	Memilih menu hapus	Data berhasil dihapus.	a,b
Halaman Data Kecamatan	Memilih menu Data Kecamatan	Menampilkan halaman Data Kecamatan.	a,b
Halaman Tambah Data Kecamatan	Mengklik *button* Tambah	Data berhasil menampilkan halaman tambah data kecamatan.	a,b,c
Halaman Edit Data Kecamatan	Mengklik *button* Edit	Data berhasil menampilkan halaman edit data kecamatan.	a,b,c
Halaman Hapus Data Kecamatan	Memilih menu hapus	Data berhasil dihapus.	a,b
Halaman Data RT	Memilih menu Data RT	Menampilkan halaman Data RT.	a,b
Halaman Tambah Data RT	Mengklik *button* Tambah	Data berhasil menampilkan halaman tambah data rt.	a,b,c
Halaman Edit Data RT	Mengklik *button* Edit	Data berhasil menampilkan halaman edit data rt.	a,b,c
Halaman Hapus Data RT	Memilih menu hapus	Data berhasil dihapus	a,b

Modul yang diuji	Teknik Pengujian	Hasil	Kriteria
Halaman Data RW	Memilih menu Data RW	Menampilkan halaman Data RW	a,b
Halaman Tambah Data RW	Mengklik *button* Tambah	Data berhasil menampilkan halaman tambah data rw.	a,b,c
Halaman Edit Data RW	Mengklik *button* Edit	Data berhasil menampilkan halaman edit data rw.	a,b,c
Halaman Hapus Data RW	Memilih menu hapus	Data berhasil dihapus.	a,b
Halaman Data Dokumen Penduduk	Memilih menu Data Dokumen Penduduk	Menampilkan halaman Data Dokumen Penduduk	a,b
Halaman Tambah Data Dokumen Penduduk	Mengklik *button* Tambah	Data berhasil menampilkan halaman tambah data dokumen penduduk.	a,b,c
Halaman Edit Data Dokumen Penduduk	Mengklik *button* Edit	Data berhasil menampilkan halaman edit data dokumen penduduk.	a,b,c
Halaman Hapus Data Dokumen Penduduk	Memilih menu hapus	Data berhasil dihapus	a,b
Halaman Download Dokumen Penduduk	Memilih menu Download	Data berhasil didownload	a,b

3.2. Pembahasan

Untuk Pembahasan dalam Digital Signature Dalam Pembuatan Dokumen Citra Digital Kartu Penduduk Mengunakan Metode Algoritma RC 6, penelitian ini mendapatkan beberapa hasil dari uji coba seperti berikut ini:

3.2.1 Enskripsi Dokumen

1) Penginputan dokumen penduduk, pengguna menambahkan file dokumen penduduk yang sudah di scan dengan cara diupload,

kemudian akan tampil halaman digital signatur yang dihalaman ini pengguna harus memasukkan kata kunci pengaman.
2) Pada saat proes upload file yang tadi di scan akan tersimpan kedalam database, pada saat ini proses RC6 sudah berjjalan untuk melakukan enkripsi dokumen dengan dilengkapi digital signature.
3) Hasil enkripsi dokumen setelah diinputkan dapat dilihat gambar di bawah ini.

3.2.2 Deskripsi Dokumen

1) Pada saat dokumen di download penguna maka akan tampil halaman untuk menginputan kaka kunci digital signature dari dokumen oenduduk yang akan di download.
2) Setelah selesai, sistem akan melakukan operasi dekripsi. Proses ini akan terus diulang sampai seluruh karakter terdekripsi.
3) Hasil dekripsi dokumen setelah diinputkan dapat dilihat gambar di bawah ini.

4. KESIMPULAN

Dari pembuatan pembuatan *digital signature* dokumen citra digital kartu penduduk mengunakan metode algoritma RC 6 yang dilakukan pada penelitian ini, maka dapat diambil kesimpulan sebagai berikut:

1) Algoritma *RC6* berfungsi dengan baik pada keamanan dokumen penduduk, besarnya file sangat mempengaruhi pada saat upload dan prosess *download*.
2) Memberikan solusi yang tepat untuk keamanan dokumen penduduk sehingga kerahasiaan dokumen lebih terjaga.
3) Penerapan metode RC6 dapat memberikan pelajaran bahwa metode RC6 dapat diterapkan untuk keamanan file dokumen pada saat di*upload*.

DAFTAR PUSTAKA

[1] Ahmaddul, H., Sediyono, E., 2012. Rancang Bangun Sistem Pengamanan Dokumen pada Sistem Informasi Akademik Menggunakan Digital signature dengan Algoritma Kurva Eliptik. Program Pascasarjana Universitas Diponegoro Semarang

Vol. 1, No. 1, January 2020 e-ISSN: **2775-2496**

https://journal-computing.org/index.php/journal-cisa/index

[2] Roger S. Pressman, 2012,Rekayasa Perangkat Lunak Pendekatan Praktisi (BukuSatu), ANDI Yogyakarta.

[3] Noertjahyana, A., Gunadi, K., Hartono, S. K. G., 2012. Aplikasi Metode Steganography pada Citra Digital dengan Menggunakan Metode LSB (*Least Significant Bit*). Universitas Kristen Petra

[4] Safaat 2013. *PemrogramanAplikasi Mobile Smartphone Dan Tablet PC Berbasis Android*. Informatika. Bandung.

[5] Ahmad h.e.h., Kalash, H.M, dan Allah, O.S.F.(2007). *Encryption Efficiency Analysis and Security Evaluation of RC6 Block Chipher for Digital Image*. *Internasional Journal of Coumputer, Information, and System Science, and Engineering* Vol. 1 No. 1.