IMPLEMENTASI ALGORITMA AES (ADVANCED ENCRYPTION STANDARD) DAN RSA (RIVEST SHAMIR ADLEMAN) UNTUK PENGAMANAN SURAT DI HUMANIKA

[1] *Binar Putri Pratiwi* (14 1065 1060)
[2] *Mudafiq Riyan Pratama, S. Kom., M. Kom.* [3] *Triawan Adi Cahyanto, M. Kom.*

Program Studi Teknik Informatika Fakultas Teknik
Universitas Muhammadiyah Jember

Email: binarpratiwi@gmail.com

ABSTRAK

Tandatangan tradisional dalam sistem persuratan di Humanika masih menjadi penentu keaslian dari sebuah surat, sehingga sering kali menjadi faktor penghambat implementasi dari sebuah sistem persuratan tersebut. Diperlukan sebuah sistem yang dapat menjadi pelengkap sekaligus dapat mempercepat secara signifikan pemrosesan dokumen digital yaitu dengan E-Signature atau biasa disebut juga Digital Signature. Digital signature bukanlah sebuah tandatangan fisik yang di scan lalu ditambahkan kedalam dokumen. Lebih dari itu sebuah tandatangan digital menggunakan teknik kriptografi yang dapat memastikan keaslian dan transparansi dari sebuah surat sehingga surat tersebut dapat dipertanggungjawabkan. Pengamanan tanda tangan digital surat ini menerapkan kombinasi algoritma *AES* dan *RSA*. Uji coba dilakukan berdasarkan skenario pengujian sistem terhadap pengaruh penggunaan algoritma AES dan RSA pada tanda tangan digital. Skenario pengujian ini menghasilkan sistem informasi manajemen persuratan tanpa AES dan RSA yang dapat menjamin dari pemalsuan surat karena pada proses validasi surat membutuhkan kode verifikasi, sedangkan tanpa AES dan RSA tidak membutuhkan kode verifikasi sehingga dapat memanipulasi keaslian surat tersebut.

Kata Kunci : *Digital Signature, Advanced Encryption Standar, Rivest Shamir Adleman.*

BAB I PENDAHULUAN

1.1. Latar Belakang

Surat merupakan salah satu media komunikasi yang sangat penting disuatu instansi, perusahaan maupun organisasi, baik untuk berkomunikasi dengan pihak diluar organisasi (eksternal) maupun didalam organisasi (internal). Tandatangan tradisional dalam surat masih menjadi penentu keaslian dari sebuah surat tersebut, sehingga sering kali menjadi faktor penghambat implementasi dari sebuah sistem persuratan. Diperlukan waktu panjang untuk proses tandatangan yang manual ini, seperti mendistribusikan surat kepada yang menandatangani, pemeriksaan kertas surat dan proses penandatanganan.

Dalam sebuah sistem persuratan, autentikasi atau keaslian sebuah dokumen sangat penting dan kritikal sehingga diperlukan sebuah sistem yang dapat menjadi pelengkap sekaligus dapat mempercepat secara signifikan pemrosesan dokumen digital yaitu E-Signature atau biasa disebut juga Digital Signature. Digital Signature pada dasarnya adalah sebuah proses untuk memastikan dokumen elektronik (email, spread sheet, dokumen) otentik. Otentik yang artinya dapat mengetahui siapa yang berhak mengesahkan dan tidak diubah setelah dokumen tersebut disahkan oleh yang berhak. Digital signature bukanlah sebuah tandatangan fisik yang di scan lalu ditambahkan kedalam dokumen. Lebih dari itu sebuah tandatangan digital menggunakan teknik kriptografi yang dapat memastikan keaslian dan transparansi dari sebuah dokumen sehingga dokumen tersebut dapat dipertanggungjawabkan (*Pratama Persadh, 2015*). Tanda tangan digital yang telah dirubah menggunakan teknik kriptografi tersebut disimpan dalam bentuk QRCode. Dengan QRCode informasi keaslian surat menjadi lebih sederhana atau simple dengan mengetikkan informasi kode validasi pada surat tersebut untuk keperluan komersil.

Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentifikasi (*Menezes, 1997)*. Sedangkan sistem kriptografi merupakan kumpulan yang terdiri dari plaintext berupa pesan asli yang akan dikirimkan, chipertext berupa pesan yang telah disandikan, kunci, enkripsi serta dekripsi. Sistem kriptografi dibagi menjadi dua, yaitu sistem kriptografi kunci simetri dan kriptografi asimetri atau yang lebih dikenal sebagai kriptografi kunci publik. Perbedaan pada kedua sistem kriptografi tersebut ada p ada kuncinya, jika pada sistem kriptografi kunci simetri hanya diperlukan kunci privat, sedangkan pada kriptografi kunci publik diperlukan kunci privat dan juga kunci publik. Kunci privat merupakan kunci yang tidak boleh diketahui oleh pihak lain kecuali dua pihak yang berkomunikasi, sedangkan kunci publik dapat diketahui oleh siapapun.

Penelitian ini menggunakan kombinasi algoritma kriptografi asimetris dan simetris, yaitu algoritma AES (Advanced Encryption Standard) dan RSA (Rivest Shamir Adleman). Algoritma AES merupakan algoritma simetris yang cukup aman untuk mengamankan data atau informasi yang bersifat rahasia. Pada tahun 2001, AES digunakan sebagai standar algoritma kriptografi terbaru yang dipublikasikan oleh Nasional Institute of Standard and Technology (NIST). AES menggunakan blok cipher simetris yang dimaksudkan untuk mengganti algoritma DES (*Stalling, 2011*). Algoritma RSA merupakan algoritma kriptografi asimetri, dimana kunci yang digunakan untuk mengenkripsi berbeda dengan yang digunakan untuk mendekripsi. Kunci yang digunakan untuk mengenkripsi disebut dengan kunci public, dan yang digunakan untuk mendekripsi disebut dengan kunci privat. Berdasarkan uraian latar belakang yang telah dikemukakan, maka dilakukanlah penelitian dengan judul "Implementasi Algoritma AES (Advanced Encryption Standard) Dan RSA (Rivest Shamir Adleman) Untuk Pengamanan Surat Di HUMANIKA".

1.2. Perumusan Masalah

Permasalahan yang dijadikan objek penelitian pada tugas akhir ini berdasarkan latar belakang yang telah dipaparkan adalah : Apakah *QRCode* dan algoritma *Advanced Encryption Standard* dan *Rivest Shamir Adleman* dapat menjamin keamanan tanda tangan surat pada sistem informasi manajemen persuratan di Humanika ?

1.3. Batasan Masalah

Untuk lebih memfokuskan pengerjaan penelitian ditetapkan pembahasan hanya dibatasi pada :

1. Data yang digunakan dalam penelitian ini adalah file yang berupa surat.

2. Penelitian hanya menggunakan metode *Advanced Encryption Standard* dan *Rivest Shamir Adleman*.
3. Studi kasus penelitian di Himpunan Mahasiswa Teknik Informatika Muhammadiyah Jember
4. Jenis surat yang digunakan adalah surat undangan dan surat keterangan aktif organisasi.
5. Bahasa pemrograman yang digunakan dalam penelitian ini adalah *php* (*Hypertext Prepocessor*).
6. Hasil enkripsi adalah *chippertext* yang berupa QRCode dan hasil dari dekripsi adalah *plaintext*.

1.4. Tujuan

Tujuan penelitian pada tugas akhir ini adalah menerapkan QRCode dan algoritma *Advanced Encryption Standard* serta *Rivest Shamir Adleman* untuk menjamin keamanan tanda tangan surat pada sistem informasi manajemen persuratan.

1.5. Manfaat

Adapun manfaat dari penelitian ini antara lain :

1. Bagi Peneliti, bisa menerapkan dan mengembangkan ilmu kriptografi yang diperoleh selama peneliti kuliah.
2. Bagi Kalangan akademik, diharapkan skripsi ini dapat dijadikan bahan pertimbangan untuk penelitian dan pengembangan lebih lanjut.

BAB II TINJAUAN PUSTAKA

2.1. Suara

Menurut I.G. Warsanto, dalam bukunya "Kearsipan I" mengatakan bahwa : "Surat adalah sejenis warkat yang dipergunakan sebagai sarana komunikasi tertulis antara pihak pertama dengan pihak lain dengan mempergunakan kertas berukuran tertentu".

2.2. Tandatangan Digital

Tanda tangan digital dibuat dengan menggunakan teknik kriptografi, suatu cabang dari matematika terapan yang menangani tentang pengubahan suatu informasi menjadi bentuk lain yang tidak dapat dimengerti dan dikembalikan seperti semula. Tanda tangan digital menggunakan "public key cryptography"(kriptografi kunci public), dimana algoritmanya menggunakan dua buah kunci, yang pertama adalah kunci membentuk tanda tangan digital atau mengubah data ke bentuk lain yang tidak dapat dimengerti, dan kunci kedua digunakan untuk verifikasi tanda tangan digital maupun mengembalikan pesan ke bentuk semula. Konsep ini juga dikenal sebagai "asymmetric cryptosystem" (sistem kriptografi non simetris).

Sistem kriptografi ini menggunakan kunci privat, yang hanya diketahui oleh penandatangan dan digunakan untuk membentuk tanda tangan digital, serta kunci public, yang digunakan untuk verifikasi tanda tangan digital. Jika beberapa orang ingin memverifikasi suatu tanda tangan digital yang dikeluarkan oleh seseorang, maka kunci public tersebut harus disebarkan ke orang-orang tersebut. Kunci privat dan kunci public ini sesungguhnya secata sistematis 'berhubungan' (memenuhi persamaan-persamaan dan kaidah-kaidah tertentu). Walaupun demikian, kunci privat tidak dapat ditemukan menggunakan informasi yang didapat dari kunci public.

Proses pembentukan dan verifikasi tanda tangan digital memenuhi unsur-unsur paling penting yang diharapkan dalam suatu tujuan legal, yaitu :

1. Otentikasi Penandatangan: Jika pasangan kunci public dan kunci privat berasosiasi dengan pemilik sah yang telah didefinisikan, maka tanda tangan digital akan dapat menghubungan/mengasosiasikan dokumen dengan penandatangan. Tanda tangan digital tidak dapat dipalsukan, kecuali penandatangan kehilangan kontrol dari kunci privat miliknya.
2. Otentikasi Dokumen: Tanda tangan digital juga mengidentikkan dokumen yang ditandatangani dengan tingkat kepastian dan ketepatan yang jauh lebih tinggi daripada tanda tangan di atas kertas.
3. Penegasaan: Membuat tanda tangan digital memerlukan penggunaan kunci privat dari penandatangan. Tindakan ini dapat menegaskan bahwa penandatangan setuju dan bertanggung jawab terhadap isi dokumen.
4. Efisiensi: Proses pembentukan dan verifikasi tanda tangan digital menyediakan tingkat kepastian yang tinggi bahwa tanda tangan yang ada merupakan tanda tangan sah dan asli dari pemilik kunci privat. Dengan tanda tangan digital, tidak perlu ada verifikasi dengan melihat secara teliti (membandingkan) antara tanda tangan yang terdapat di dokumen dengan contoh tanda tangan aslinya seperti yang biasa dilakukan dalam pengecekan tanda tangan secara manual.

2.4. Metode *Rivest Shamir Adleman*

Algoritma Rivest Shamir Adlmen didasarkan pada teorema Euler yang menyatakan bahwa

$$a\varphi(n) = 1 \pmod n \qquad (3.1)$$

dengan syarat (Munir, 2006) :

1. a harus relatif prima terhadap n
2. $\varphi(n) = n(1-1/p1)\ (1-1/p2)\ldots\ (1-1/pr)$, yang dalam hal ini p1, p2,…, pr adalah faktor prima dai n.

$\varphi(n)$ adalah fungsi yang menentukan berapa banyak dari bilangan-bilangan 1, 2, 3,…,n yang relative prima terhadap n.

berdasarkan sifat ak = bk(mod n) untuk k bilangan bulat > 1 maka persamaaan (3.1) dapat ditulis menjadi

$$a k\varphi(n) = 1k \pmod n \text{ atau}$$

$$a\ k\varphi(n) = 1 \pmod n \qquad (3.2)$$

bisa a diganti dengan m, maka persamaan (3.2) dapat ditulis menjadi

$$m\ k\varphi(n) = 1 \pmod n \qquad (3.3)$$

Berdasarkan sifat ac = bc (mod n), maka bila persamaan (3.3) dikali dengan m menjadi :

$$m\ k\varphi(n)+1 = m \pmod n \qquad (3.4)$$

yang dalam hal ini m relatif prima terhadap n.

Misalkan e dan d dipilih sedemikian sehingga $e.\ d = 1(\text{mod } \varphi(n))$ (3.5)

Atau

$$e.d = k\ \varphi(n)+1 \qquad (3.6)$$

Sulihkan (3.6) ke dalam persamaan (3.4) menjadi :

$$me.d = m \pmod n \qquad (3.7)$$

persamaan (2.7) dapat ditulis kembali menjadi :

$$(me)d = m \pmod n \qquad (3.8)$$

Yang artinya, perpangkatan m dengan e diikuti dengan perpangkatan dengan d menghasilkan kembali m semula. Berdasarkan persamaan (3.8), maka enkripsi dan dekripsi dirumuskan sebagai berikut :

$$Ee(m) = c = me \bmod n \qquad (3.9)$$

$$Dd(c) = m = cd \bmod n \qquad (3.10)$$

Karena e . d = d . e, maka enkripsi diikuti dengan dekripsi ekivalen dengan dekripsi diikuti enkripsi :

$$Dd(Ee(m)) = Ee(Dd(c)) = md \bmod n \qquad (3.11)$$

Oleh karena md mod n = (m +jn)d mod n untuk sembarang bilangan bulat j, maka tiap plainteks m, m + n, m + 2n, …., menghasilkan cipherteks yang sama. Dengan kata lain, transformasinya dari banyak ke satu. Agar transformasinya dari satu ke satu, maka m harus dibatasi dalam himpunan {0, 1, 2, …., n-1} sehingga enkripsi dan dekripsi tetap benar seperti pada persamaan (3.9) dan (3.10).

2.5. Metode Advance Encryption Standard

Rinjdael mendukung panjang kunci dari 128 sampai 256 bit dengan step 32 bit. Karena AES menetapkan panjang kunci adalah 128, 192, dan 256, maka dikenal sebagai AES-128, AES-192, dan AES-256, yang perbedaannya akan ditunjukan oleh table 2.2

Tabel 2.1. Tiga buah versi AES
(Sumber:Rinaldi Munir, 2006)

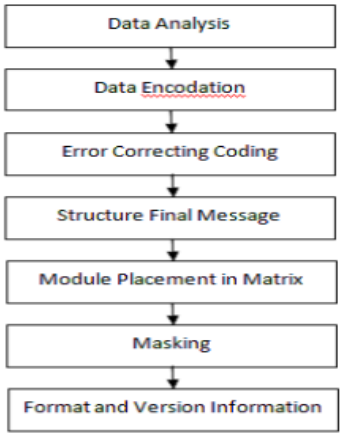
	Panjang Kunci (Nk words)	Ukuran Blok (Nb words)	Jumlah Putaran (Nr)
AES-128	4	4	10
AES-196	6	4	12
AES-256	8	4	14

2.6. QRCode

QRCode adalah image berupa matriks dua dimensi yang memiliki kemampuan untuk menyimpan data di dalamnya. QRCode merupakan evolusi dari kode batang (barcode). Barcode merupakan sebuah symbol penandaan objek nyata yang terbuat dari pola batang-batang berwarna hitam dan putih agar mudah untuk dikenali oleh komputer. Contoh sebuah QRCode dapat dilihat pada gambar 2.1.

Gambar 2.1. QRCode

Prosedur pembangkitan QRCode dari sebuah teks dapat dijelaskan dengan diagram alir pada gambar 2.1.



Gambar 2.2. Diagram alir proses pembangkitan QR Code

Langkah-langkah untuk membaca QR Code menjadi teks aslinya merupakan reserve atau kebalikan dari langkah-langkah pada pembangkitan QR Code. Secara umum prosedur pembacaan QR Code dapat dijelaskan dengan diagram alir pada gambar 2.2

2.7. Sniffing

Sniffing merupakan proses pengendusan paket data pada sistem jaringan komputer, yang diantaranya dapat memonitor dan menangkap semua lalu lintas jaringan yang lewat tanpa peduli kepada siapa paket itu di kirimkan. Contoh dampak negatif sniffing, seseorang dapat melihat paket data informasi seperti username dan password yang lewat pada jaringan komputer. Contoh dampak positif sniffing. Seorang admin dapat menganalisa paket-paket data yang lewat pada jaringan untuk keperluan optimasi jaringan, seperti dengan melakukan penganalisaan paket data, dapat diketahui dapat membahayakan performa jaringan atau tidak, dan dapat mengetahui adanya penyusup atau tidak. Bahaya yang mengancam dari proses sniffing yaitu hilangnya sifat privacy dan confidentiality seperti tercurinya informasi penting dan rahasia seperti username dan password. (Parmo, 2008).

Wireshark adalah tool yang ditujukan untuk penganalisaan paket data jaringan (Kurniawan, 2012). Wireshark disebut juga Network packet analyzer yang berfungsi menangkap paket-paket jaringan dan berusaha untuk menampilkan semua informasi dipaket tersebut sedetail mungkin. Sebenarnya network packet analyzer sebagai alat untuk memeriksa apa yang sebenarnya terjadi di dalam jaringan baik kabel maupun wireless. Dengan adanya wireshark ini semua sangat dimudahkan dalam hal memonitoring dan menganalisa paket yang lewat di jaringan. Ada beberapa contoh penggunaan Wireshark :

1. Admin sebuah jaringan menggunakan untuk troubleshooting masalah di jaringan.
2. Admin menggunakan Wireshark untuk mengamankan jaringannya.

Beberapa fitur kelebihan Wireshark, diantaranya :

1. Berjalan pada sistem operasi Linux dan Windows.
2. Menangkap paket (Capturing Packet) langsung dari network interface.
3. Mampu menampilkan hasil tangkapan dengan detail.
4. Dapat melakukan pemfilteran paket
5. Hasil tangkapan dapat di save, di import dan di export.

BAB III METODOLOGI PENELITIAN

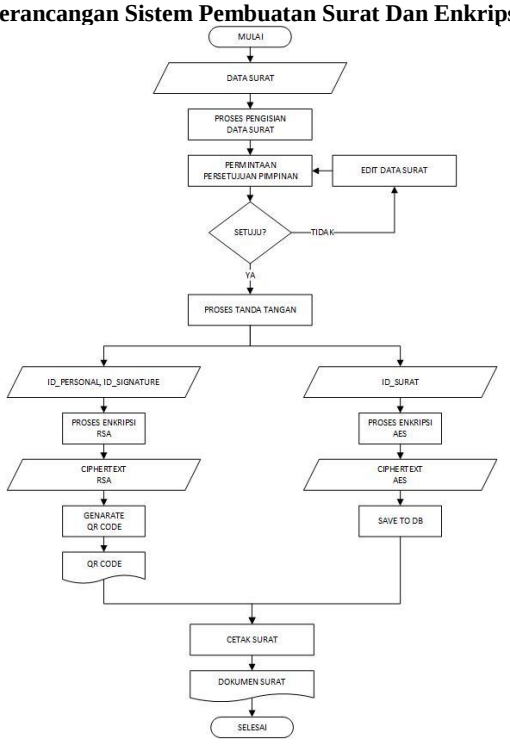
3.1. Studi Literatur

Tahap studi literatur mempelajari tentang semua informasi yang berhubungan dengan masalah yang akan dibahas dalam penelitian ini diambil dari berbagai sumber, seperti buku, jurnal, e-book, serta sumber-sumber lain yang dinilai dapat memberi tambahan wawasan untuk penelitian ini.

3.2. Pengambilan Data

Data yang digunakan untuk penelitian ini adalah yang bersumber dari data surat HUMANIKA(Himpunan Mahasiswa Teknik Informatika) di Universitas Muhammadiyah Jember.

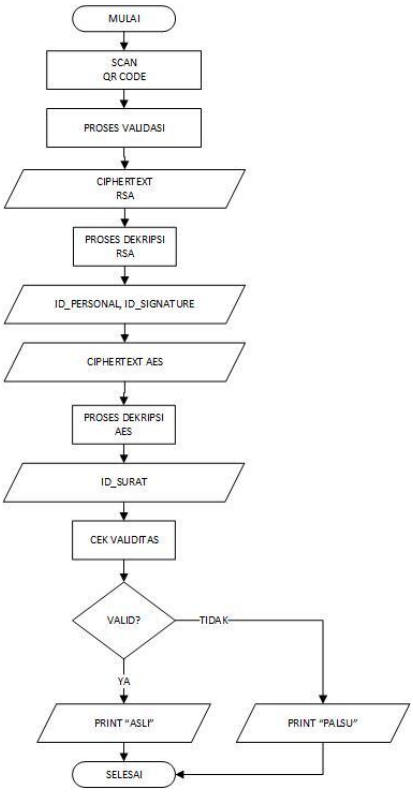
3.3. Perancangan Sistem Pembuatan Surat Dan Enkripsi



Gambar 3.1. Rancangan Sistem.

Gambar 3.1. menjelaskan tentang proses pembuatan surat dan proses enkripsi. Pembuatan surat dilakukan oleh seorang sekretaris. Setelah surat dibuat maka sekretaris meminta persetujuan Ketua Humanika. Jika Ketua Humanika menyetujui surat maka surat akan ditanda tangani, jika tidak maka surat harus di edit untuk mendapat persetujuan ketua Humanika. Proses enkripsi terjadi pada saat ketua menandatangani surat. Id Personal dan Id Signature digabung, sehingga menghasilkan chipertext RSA dan dicetak menjadi QRCODE, sedangkan Id Surat menjadi chipertext AES. RSA digunakan untuk mengamankan proses tanda tangan sedangkan AES digunakan untuk mengamankan database.

3.4. Perancangan Sistem Cek Validasi Dan Dekripsi



Gambar 3.2. menjelaskan tentang proses validitas dan proses dekripsi. Surat yang sudah disetujui ketua akan menghasilkan Qr Code. Untuk melihat keaslian surat tersebut, Qr Code di scan terlebih dahulu. Jika Qr Code valid maka surat tersebut asli, jika tidak maka palsu. Proses dekripsi terjadi pada saat chipertext RSA di scan dan di dekripsi menjadi id personal dan id signature. Dekripsi AES diambil dari chipertext AES yang di database dan diambil dari id personal, id signature.

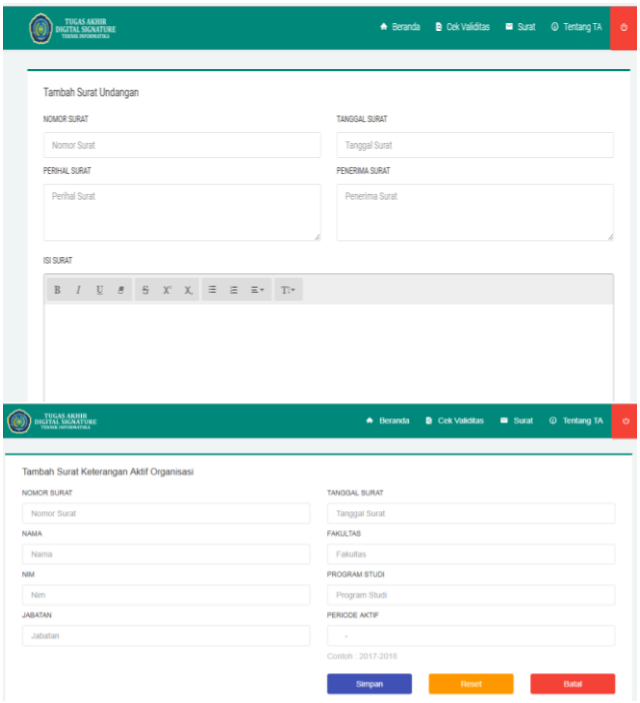
BAB IV IMPLEMENTASI DAN PENGUJIAN

4.1. Implementasi

Implementasi Antarmuka menggambarkan tampilan dari aplikasi yang dibangun berdasarkan rancangan antarmuka yang telah dibuat pada tahap sebelumnya. Antarmuka aplikasi untuk sistem informasi manajemen persuratan terdiri dari 4 bagian utama, yaitu:

1. Form Membuat Surat Undangan Dan Keterangan Aktif Organisasi

   Pada halaman surat undangan dan surat keterangan aktif organisasi, sekretaris harus mengisi kolom yang telah disediakan.



Gambar 4.1. Form Membuat Surat Undangan Dan Keterangan Aktif Organisasi

Gambar 4.1 contoh form keterangan aktif ogranisasi. Ada 8 data yang harus diisi yaitu, nomor surat, nama, nim, jabatan, tanggal surat, fakultas, program studi dan periode aktif.

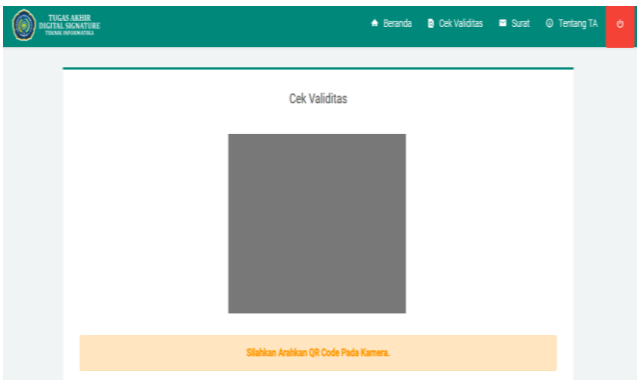
2. Form Permintaan Persetujuan Dan Proses Enkripsi

Setelah surat dibuat, sekretaris meminta persetujuan ke Ketua Humanika. Pada saat proses permintaan persetujuan, sekretaris tidak dapat mengedit surat tersebut.

Gambar 4.2. Form Data Training

3. Form Scan QRCode Dan Proses Dekripsi

Pada halaman ini, user dapat mengecek validitas surat tersebut dengan mengarahkan webcam atau kamera handphone ke QRCode yang ada di surat tersebut. Berikut form validitas, dapat dilihat di gambar 4.3



Gambar 4.3. Form Sumber Validitas

4.2. Pengujian

Pada tahap ini, pengujian pengamanan surat yang berupa tanda tangan digital sebagai instrumen sistem pengamanan surat. Adapun prinsip pengamanan tanda tangan ini adalah bagaimana sistem dapat mengamankan proses tanda tangan surat. Tanda tangan surat dalam bentuk teks dienkripsi dengan algoritma AES dan RSA, yang kemudian teks yang dienkripsi tersebut dijadikan QRCode sebagai penanda tangan digital sehingga tanda tangan surat tidak dapat dibaca oleh siapapun. Jika ingin dibaca oleh pemilik surat, maka surat tersebut harus dibuka dengan dekripsi menggunakan kunci public untuk memvalidasi tanda tangan digital tersebut.

Skenario uji coba pada Tugas Akhir ini dilakukan dengan menguji keaslian surat.

4.2.1. QRCode Tanpa Enkripsi AES dan RSA

a. Uji Coba Tanpa Enkripsi 1 : Membuat 2 surat keterangan aktif organisasi. Misalnya jika seseorang ingin memalsukan QRCode, QRCode dari surat pertama diletakkan di surat kedua.

TEKNIK INFORMATIKA
UNIVERSITAS MUHAMMADIYAH JEMBER
Jl. Karimata 49 Jember 68212
Email : humanika@unmuhjember.ac.id

SURAT KETERANGAN AKTIF ORGANISASI
Nomor : 1234

Yang bertandatangan di bawah ini :
Nama : **Arif Syaiful Rohman**
NIM. : 1510651002
Jabatan : KETUA UMUM HIMPUNAN MAHASISWA TEKNIK INFORMATIKA

Menyatakan bahwa :
NAMA : **IJAAH**
NIM. : 1410651089
Fakultas : Teknik
Program Studi : Teknik Informatika
Jabatan : sie keamanan

Menerangkan bahwa mahasiswa tersebut, aktif dalam organisasi **HIMPUNAN MAHASISWA TEKNIK INFORMATIKA** Universitas Muhammadiyah Jember periode 2017-2018.
Demikian surat keterangan ini dibuat dengan sebenar-benarnya dengan tanpa ada paksaan dari pihak manapun dan dapat digunakan sebagaimana mestinya.

VERIFIKASI SURAT	
Tanggal	: 05 Maret 2018
Nama	: Arif Syaiful Rohman
NIM	: 1510651002
Jabatan	: Ketua Umum HUMANIKA

Gambar 4.4. Surat Keterangan Aktif Organisasi ke 1

Gambar 4.4, keterangan aktif organisasi ini untuk Ijaah dengan jabatan sie keamanan.

HIMPUNAN MAHASISWA
TEKNIK INFORMATIKA
UNIVERSITAS MUHAMMADIYAH JEMBER
Jl. Karimata 49 Jember 68212
Email : humanika@unmuhjember.ac.id

SURAT KETERANGAN AKTIF ORGANISASI
Nomor : 4321

Yang bertandatangan di bawah ini :
Nama : **Arif Syaiful Rohman**
NIM. : 1510651002
Jabatan : KETUA UMUM HIMPUNAN MAHASISWA TEKNIK INFORMATIKA

Menyatakan bahwa :
NAMA : **inem**
NIM. : 1410651078
Fakultas : Teknik
Program Studi : Teknik Informatika
Jabatan : sie kebersihan

Menerangkan bahwa mahasiswa tersebut, aktif dalam organisasi **HIMPUNAN MAHASISWA TEKNIK INFORMATIKA** Universitas Muhammadiyah Jember periode 2017-2018.
Demikian surat keterangan ini dibuat dengan sebenar-benarnya dengan tanpa ada paksaan dari pihak manapun dan dapat digunakan sebagaimana mestinya.

VERIFIKASI SURAT	
Tanggal	: 05 Maret 2018
Nama	: Arif Syaiful Rohman
NIM	: 1510651002
Jabatan	: Ketua Umum HUMANIKA

Gambar 4.5. QRCode Surat Keterangan Aktif Organisasi ke 2

Gambar 4.5, keterangan aktif organisasi ini untuk inem dengan jabatan sie kebersihan.

Untuk melihat keaslian surat tanpa enkripsi AES dan RSA tidak ada kode verfikasinya. QRCode surat tanpa enkripsi ini dari id_surat surat tersebut. Cek validitas surat kedua yang QRCode suratnya dipalsukan dengan menempelkan QRCode surat pertama.

Gambar 4.6. Tampilan Hasil Scanning Surat Keterangan Aktif Organisasi

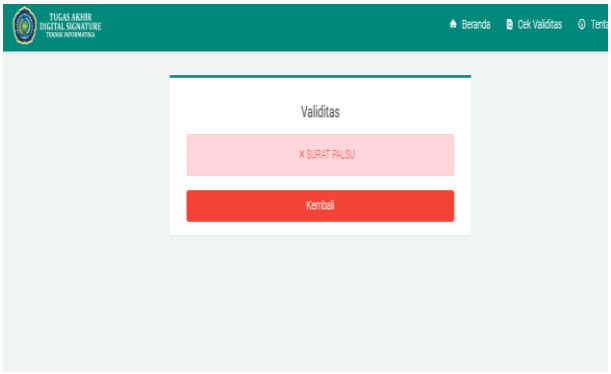
Gambar 4.6, menampilkan bahwa surat tersebut asli, tapi isi detail surat tersebut salah. Seharusnya surat keterangan aktif organisasi kedua penerimanya adalah inem dan nomor suratnya 4321.

b. Uji Coba Tanpa Enkripsi 2 : QRCode Palsu

Jika seseorang ingin membuat QRCode palsu, dia dapat mengambil QRCode dari mana saja untuk ditempelkan di surat tersebut. Uji coba di bawah ini akan menampilkan hasil scanning QRCode yang salah atau tidak valid.

Gambar 4.7. QRCode Palsu

Gambar 4.7, QRCode yang diuji berisikan QRCode yang tidak memiliki data id_surat di database.



Gambar 4.8. Tampilan Hasil Scanning QRCode Palsu

Gambar 4.8, jika surat palsu maka akan tampil seperti gambar diatas.

4.2.2. QRCode Dengan Enkripsi AES dan RSA

a. Uji Coba Enkripsi 1 : Surat Keterangan Aktif Organisasi Data Valid

Uji coba di bawah ini akan menampilkan hasil scanning QR Code surat keterangan aktif organisasi.

HIMPUNAN MAHASISWA
TEKNIK INFORMATIKA
UNIVERSITAS MUHAMMADIYAH JEMBER

SURAT KETERANGAN AKTIF ORGANISASI
Nomor : 014/D/IV/2015

Yang bertandatangan di bawah ini :
Nama : **Arif Syaiful Rohman**
NIM. : 1510651002
Jabatan : KETUA UMUM HIMPUNAN MAHASISWA TEKNIK INFORMATIKA

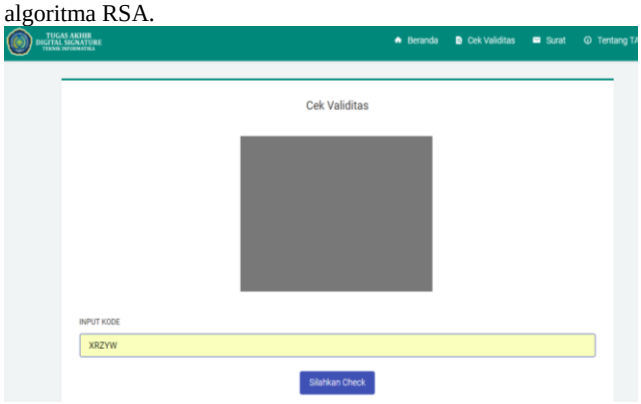
Menyatakan bahwa :
NAMA : **Anggar Wahyu Hidayatullah**
NIM. : 1510651079
Fakultas : Teknik
Program Studi : Teknik Informatika
Jabatan : Bidang Pendidikan

Menerangkan bahwa mahasiswa tersebut, aktif dalam organisasi **HIMPUNAN MAHASISWA TEKNIK INFORMATIKA** Universitas Muhammadiyah Jember periode 2017-2018.
Demikian surat keterangan ini dibuat dengan sebenar-benarnya dengan tanpa ada paksaan dari pihak manapun dan dapat digunakan sebagaimana mestinya.

VERIFIKASI SURAT	
Tanggal	: 29 November 2017
Nama	: Arif Syaiful Rohman
NIM	: 1510651002
Jabatan	: Ketua Umum HUMANIKA
Kode	: XRZYW

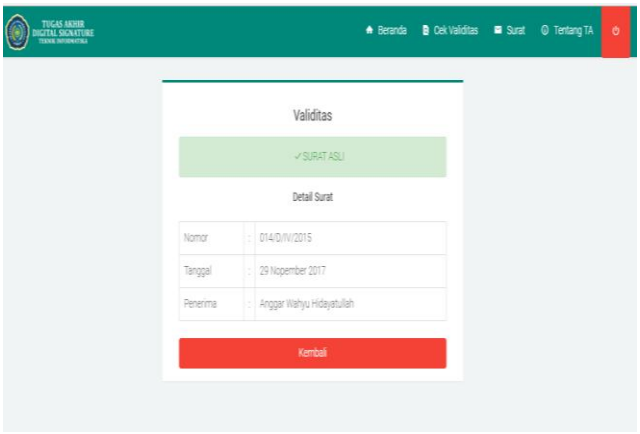
Gambar 4.9. QR Code Surat Keterangan Aktif Organisasi

Gambar 4.9, keterangan aktif organisasi ini untuk Anggar Wahyu Hidayatullah. QRCode surat dengan enkripsi ini adalah hasil penggabungan id_signature dan id_personal yang diproses algoritma RSA.



Gambar 4.10. Cek Validitas Surat Keterangan Aktif Organisasi

Gambar 4.10, Untuk melihat keaslian surat tersebut, diwajibkan memasukkan kode verifikasi.



Gambar 4.11. Tampilan Hasil Scanning Surat Keterangan Aktif Organisasi

Gambar 4.11, menampilkan bahwa surat tersebut asli, kode verifikasi benar dan QRCode tersebut memiliki data id_signature dan id_personal yang ada di database.

b. Uji Coba Enkripsi 2 : Surat Undangan Data Tidak Valid

Uji coba di bawah ini akan menampilkan hasil scanning QR Code Surat Undangan yang salah atau tidak valid. QRCode dengan kode verfikasi "CCA27" diinputkan dengan kode yang salah yaitu kode "CC567".

HIMPUNAN MAHASISWA
TEKNIK INFORMATIKA
UNIVERSITAS MUHAMMADIYAH JEMBER

Nomor : 026/HMJ/V/2017
Perihal : Undangan

Jember, 01 Januari 2018
Kepada YTH.
Deni Arifianto, M.Kom
di Tempat

Assalamu'alaikum Wr. Wb.

Salam silaturahmi kami sampaikan, seiring dengan Do'a semoga Rahmat, Taufik, dan Hidayah Allah SWT senantiasa menyertai derap akifitas kita sehari-hari.

Sehubungan dengan akan dilaksanakannya "**LKMM-TD 2017**" oleh Himpunan Mahasiswa Jurusan Teknik Informatika Fakultas Teknik Universitas Muhammadiyah Jember, yang Insya Allah akan dilaksanakan pada:

Hari/ Tanggal : Sabtu, 10 Juni 2017
Waktu : 14.00 - Selesai
Tempat : Gedung Cc

Untuk itu kami menyampaikan ***permohonan menjadi pemateri*** pada kegiatan yang kami maksud.

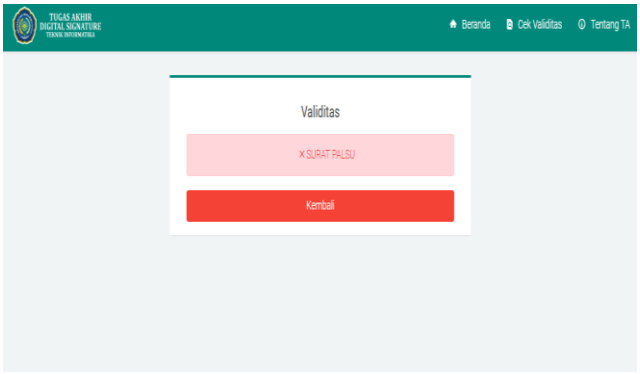
Demikian surat permohonan menjadi juri ini kami sampaikan, atas apresiasi dan kesediaannya kami sampaikan terima kasih.

Wassalamu'alaikum Wr. Wb

VERIFIKASI SURAT	
Tanggal	: Jember, 01 Januari 2018
Nama	: Arif Syaiful Rohman
NIM	: 1510651002
Jabatan	: Ketua Umum HUMANIKA
Kode	: CCA27

Gambar 4.12. QR Code Surat Undangan

Gambar 4.12, QRCode yang diuji berisikan surat undangan untuk Deni Arifianto, M.Kom dengan kode verifikasi yang tidak sesuai aslinya.



Gambar 4.13. Tampilan Hasil Scanning Surat Undangan

Gambar 4.13, jika kode verifikasi salah maka akan tampil seperti gambar diatas.
Dari uji keaslian surat tersebut, dapat dibuat tabel perbedaan tanda tangan digital dengan tidak di enkripsi dan dengan di enkripsi.

Tabel 4.1. Perbedaan Tidak Enkripsi dan Enkripsi

No	Tanpa Enkripsi AES dan RSA	Enkripsi AES dan RSA
1.	Tidak menggunakan kode cek validitas	Menggunakan kode cek validitas
2.	QRCode dihasilkan dari id surat	QRCode dihasilkan dari gabungan id_signature dan id personal yang dienkripsi RSA
3.	Ketika proses cek validitas, dapat membaca semua id surat yang di database.	Ketika proses cek validitas, hanya membaca id_signature dan id_personal yang sesuai dengan kode verifikasi.

BAB V KESIMPULAN DAN SARAN

5.1. Kesimpulan

Berdasarkan uraian permasalahan dan pembahasan pada bab sebelumnya, maka didapatkan beberapa kesimpulan tentang implementasi algoritma AES dan RSA untuk pengamanan tanda tangan surat di Humanika adalah :

1. Dari hasil uji keaslian surat, dapat dibuktikan bahwa penggunaan tanpa enkripsi AES dan RSA pada sistem informasi manajemen persuratan dapat dimanipulasi keaslian surat tersebut dengan membaca id_surat yang ada di database. Sedangkan penggunaan enkripsi AES dan RSA dibutuhkan kode verifikasi untuk memvalidasi bahwa surat yang diperiksa dapat terjamin keasliannya, kode verifikasi tersebut dari kunci public RSA dengan parameter yang di enkripsi id_signature dan id_personal.
2. Hasil pengujian keamanan jaringan penggunaan tanpa SSL dapat terbaca semua proses login, pembuatan surat dan id_surat yang disetujui, sedangkan jika menggunakan open SSL tidak ada data yang terbaca saat proses sistem informasi manajemen persuratan dijalankan.
3. QRCode pada sistem informasi manajemen persuratan sebagai tanda tangan digital dapat berfungsi sebagai autentikasi tanda tangan ketua Humanika dan memverifikasi surat yang sah.

5.2. Saran

Beberapa saran yang dapat dijadikan pertimbangan dalam mengembangkan penelitian ini adalah :

1. Pengembangan selanjutnya disarankan menggunakan versi mobile.
2. Dapat dikembangkan lagi antarmuka yang lebih menarik.

DAFTAR PUSTAKA

Albert, Rizal, Ike., Implementasi Algoritma Kriptografi RSA untuk Enkripsi dan Dekripsi Emai, Program Studi Sistem Komputer Fakultas Teknik Universitas Diponegoro, Jurnal Teknologi dan Sistem Komputer. Vol.3, No.2, 2015.

Kholifah, Riza, Nia., Membangun Sistem Informasi Pengelolaan Surat Menggunakan Metode Waterfall Studi Kasus Direktorat Perencanaan Dan Studi Kasus Direktorat Perencanaan Dan Pengembangan Pendanaan Pembangunan, Program Studi Sistem Informasi Universitas Telkom, Jurnal Tugas Akhir. Vol.2, No.1, 2015.

Menezes, A.J., Handbook of Applied Cyrptography, CRC Press, 1997.

Munir, Rinaldi., Kriptografi, Bandung, Informatika, 2006.

Raharjo, Budi., Pemrograman Web Dengan Php + Oracle, Bandung, Informatika Bandung, 2011.

Rahmad, Muhammad, Yudi dkk., Perancangan Aplikasi Kriptografi File Dengan Metode Algoritma Advanced Encryption Standard (AES), Tangerang: Jurnal Sisfotek Global. Vol. 6,No.2, 2016.

Rohman, Abdul., Mengenal Framework “Laravel”, 2014.

Rosnawan., Aplikasi Algoritma RSA Untuk Keamanan Data Pada Sistem Informasi Berbasis Web, Skripsi, Program Studi Matematika, Universitas Negeri Semarang, 2011.

Sipahutar, Tetti., Perancangan Aplikasi QR Code Generator Dan QR Code Reader Menggunakan Metode Stroke Histogram, 2014.

Stalling, William., Cryptography and Network Security Principles and Practices Third Edition, New Jersey, Prentice Hall, 2003.

Warsanto., Kearsiapn I, Kanisius (Anggota IKAPI), 1991.

Waskito., Sistem Navigasi Di Dalam Ruangan Berbasis QR Code Tag, Skripsi, Program Studi Teknik Informatika, Universitas Muhammadiyah Jember, 2017.

Wibowo, Budi, Junius., Penerapan Algoritma Kriptografi Asimetris RSA Untuk Keamanan Data Di Oracle: Jurnal Informatika, Vol 5, No.1, 2009.

Kurniawan, A. (2012). Network Forensic. Yogyakarta: Andi Offset.

Parmo, I. (2008, juni 6). Mengenal Dunia Hacking : Sniffing. Retrieved fromisparmo.web.id:http://isparmo.web.id/2008/06/06/mengenal-dunia-hacking-sniffing/

Supriyono., Pengujian Sistem Enkripsi-Dekripsi Dengan Metode RSA Untuk Pengamanan Dokumen: JFN, Vol 2 No 2, 2008.
Anonim, (2012). *Sinyal Audio (Gelombang Suara)*. Diakses 6 Januari 2016, Diambil kembali dari Elektronika Dasar : http://elektronika-dasar.web.id/sinyal-audio-gelombang-suara/