PENGEMBANGAN *QUICK RESPONSE CODE* PADA PELABELAN DOKUMEN SERTIFIKAT TANAH MENGGUNAKAN *ALGORITMA RSA* BERBASIS SERVIS

[1]Doni Prayugo Agung Pribadi (13 1065 1170), [2]Ari Eko Wardoyo, S.T., M.Kom.

[1]vheteblekem@gmail.com
[2]arieko@unmuhjember.ac.id

Teknik Informatika
Universitas Muhammadiyah Jember
Jln. Karimata No. 49, Telp (0331) 336728, Jember

ABSTRAK

Kehidupan bermasyarakat. Masalah yang kini mencuat adalah banyaknya ditemukan sertifikat ganda dan palsu, sehingga menimbulkan ketidakpastian hukum, karena jika tidak tangani dengan benar akan berpotensi merugikan berbagai pihak dan memunculkan sengketa hukum antara pihak terkait.

Dalam pembuatan dokumen, instansi negara pembuat dokumen tanah yang disebut BPN (Badan Pertanahan Nasional) saat ini masih memiliki kekurangan, diantaranya mengenai pengamanan isi dan kerahasian dokumen tersebut. SHM *(Sertifikat Hak Milik Tanah)* merupakan suatu bukti yang sah atas kepemilikan tanah tertentu, sehingga keaslian isi harus dijaga. Pelabelan dokumen SHM berupa *QR Code* yang telah terenkripsi adalah hal yang paling ampuh dalam mengatasi pemalsuan atau penggandaan dokumen. Sebuah ponsel yang memiliki sistem operasi dan dapat mengakses internet adalah salah satu ciri utama dari *Smartphone*. Metode yang digunakan nantinya adalah dengan memanfaatkan kode batang Qr Code dengan enkripsi algoritma RSA.

Jadi, data berupa identitas pemilik tanah nantinya akan dienkripsi otomatis oleh sistem dan generate ke dalam Qr Code. Hasil dari penelitian ini berupa dokumen SHM yang berlabel *QR Code* yang telah terenkripsi, sehingga jika ingin mengetahui keaslian dokumen langsung menggunakan android dengan menscan dokumen berlabel tersebut.

Kata Kunci : *Qr Code, algoritma RSA, kriptografi, SHM.*

I. PENDAHULUAN

Latar Belakang

Pada perkembangan teknologi yang semakin maju dan pesat saat ini tentu berpengaruh pada kemudahan yang diberikan dalam kehidupan sehari- hari terutama dalam bidang pemerintahan, perusahaan dan pendidikan. Pada bidang pemerintahan khususnya dalam pencacatan kepemilikan dan penguasaan tanah.

Pada akhir-akhir ini masalah pertanahan mencuat di permukaan dan banyak diungkap di surat kabar atau majalah. Sertifikat ganda menimbulkan ketidakpastian hukum, sebab apabila sertifikat itu digunakan untuk kepentingan tertentu, dapat menimbulkan ketidak-jelasan hak dan kewajiban bagi pemegangnya dan berpotensi merugikan berbagai pihak, serta berpotensi

memunculkan sengketa hukum di antara para pihak yang terkait.

Berawal pada tahun 1976 terdapat pemalsuan dokumen atas nama Yosef yang menyuruh karyawannya membelikan sebidang tanah, yaitu Ridwan untuk membeli sebidang tanah yang terletak di Kab. Gowa dengan luas sekitar 3.083 M2 (tiga ribu delapan puluh tiga meter persegi) dari seseorang yang bernama H. Gombong. Namun setelah SHM (*Sertifikat Hak Milik Tanah)* jadi, ridwan selaku karyawan melakukan pemalsuan dengan mengganti nama hak milik SHM, dengan modus kehilangan sertifikat asli dan membuat sertifikat palsu atas nama dirinya sendiri. (Riezyad, 2013).

Sertifikat hak milik tanah merupakan sebuah dokumen penting yang harus dijaga kerahasian dan keaslian bagi setiap pemilik tanah. Pada kasus ini pelabelan dokumen berperan penting dalam proses pembuatan sertifikat. Dengan memanfaatkan salah satu fitur dari *Smartphone* yang memiliki kemampuan untuk mengambil, menyimpan, serta menampilkan gambar dengan format JPEG karena sebagian besar *Smartphone* memiliki kamera. Ide yang muncul adalah untuk memanfaatkan *QR Code* dan *Smartphone* Android untuk menjadi sistem pelabelan dokumen. Dengan memanfaatkan *QR Code dan sandi Algoritma RSA*, data pemilik tanah serta area bidang tanah dapat disimpan dalam bentuk gambar *QR Code* yang kemudian disimpan di dalam ponsel ataupun di cetak.

Pada penelitian Tugas Akhir yang berjudul **"*Pengembangan Quick Response Code Pada Pelabelan Dokumen (Sertifikat Tanah) Menggunakan Kriptografi RSA Berbasis Service".*** peniliti ingin melakukan pengujian terhadap pembuatan dokumen sertifikat tanah yang masih memiliki kekurangan. Dengan adanya pelabelan dokumen pada sertifikat tanah menggunakan *QR Code*, peneliti berharap hal ini bermanfaat bagi pemilik sertifikat untuk menjamin keaslihan, ataupun bagi pihak BPN (Badan Pertanahan Nasional).

Rumusan Masalah

Berdasarkan latar belakang yang diuraikan sebelumnya, terdapat beberapa permasalahan yang akan diangkat dalam penelitian ini, antara lain :

1. Bagaimana mengatasi duplikasi sertifikat tanah?
2. Bagaimana cara mengantisipasi pemalsuan SHM?
3. Bagaimana cara mengamankan data *QR Code* dengan metode *kriptografi RSA* agar tidak mudah dimanipulasi oleh orang lain?

Batasan Masalah

Agar tidak menyimpang jauh dari permasalahan, maka penelitian ini mempunyai batasan masalah sebagai berikut :

1. Implementasi sistem ini hanya diterapkan untuk pelabelan dokumen SHM (sertifikat hak milik tanah) ditingkat kabupaten.
2. Penyimpanan *QR Code* data pemilik sertifikat hanya terletak pada dokumen yang sah dibuat oleh BPN.
3. Aplikasi berjalan minimal di android versi 2.3 (*GingerBread*).
4. Untuk mengamankan data agar tidak mudah dimanipulasi, data terlebih dulu di enkripsi menggunakan *Algoritma RSA.*
5. Menggunakan 160 karakter *ASCII*.

6. Data dan prosedur kepemilikan SHM diambil berdasarkan kantor pertanahan Lumajang.

Tujuan Penelitian

Berdasarkan rumusan masalah di atas maka tujuan dari penelitian ini adalah:

1. Menerapkan koordinat GPS berbasis android untuk mengantisipasi duplikasi dokumen SHM.
2. Mengatasi Adanya pemalsuan dokumen sertifikat tanah dengan penambahan label *QR Code* terenkripsi dengan metode algoritma RSA.

Manfaat Penelitian

Penelitian ini dilakukan dengan harapan dapat memberikan manfaat diantaranya sebagai berikut :

1. Mampu menjaga kerahasian dan keaslian isi dokumen tersebut.
2. Mengurangi kemungkinan akan adanya dokumen palsu.
3. Mengurangi kemungkinan akan adanya dokumen ganda.
4. Dapat memudahkan penomoran NIB melalui smartphone berbasis android.

II. LANDASAN TEORI

BPN (Badan Pertanahan Nasional)

Badan Pertanahan Nasional (disingkat BPN) adalah lembaga pemerintah non kementerian di Indonesia yang mempunyai tugas melaksanakan tugas pemerintahan di bidang Pertanahan sesuai dengan ketentuan peraturan perundang-undangan. BPN dahulu dikenal dengan sebutan *Kantor Agraria*. BPN diatur melalui Peraturan Presiden Nomor 20 Tahun 2015.

Pada masa pemerintahan Presiden Joko Widodo fungsi dan tugas dari organisasi Badan Pertanahan Nasional dan Direktorat Jenderal Tata Ruang Kementerian Pekerjaan Umum digabung dalam satu lembaga kementerian yang bernama Kementerian Agraria dan Tata Ruang. Atas perubahan ini sejak 27 Juli 2016 Jabatan Kepala BPN dijabat oleh Menteri Agraria dan Tata Ruangyaitu Sofyan Djalil (www.bpn.go.id).

Dokumen SHM *(Sertifikat Hak Milik Tanah)*

Sertifikat merupakan surat tanda bukti hak atas tanah, suatu pengakuan dan penegasan dari Negara terhadap penguasaan tanah secara perorangan atau bersama atau badan hukum yang namanya ditulis di dalamnya dan sekaligus menjelaskan lokasi, gambar, ukuran dan batas-batas bidang tanah tersebut.

Sertifikat sebagai tanda bukti yang kuat mengandung arti bahwa selama tidak dapat dibuktikan sebaliknya data fisik dan data yuridis yang tercantum di dalamnya harus diterima sebagai data yang benar, sebagaimana juga dapat dibuktikan dari data yang tercantum dalam buku tanah dan surat ukurnya.

2.2.1 Isi Sertifikat

Sertifikat tanah adalah hak berisikan dua bagian utama, yaitu Buku Tanah dan Surat ukur yang dijadikan satu buku dan disampul (sampul luar berwarna hijau, ukuran kwarto) menjadi sebuah dokumen dan diberi judul Sertipikat.2 Pasal 1 butir 19 PP No.24 Tahun 1997, menentukan bahwa : Buku tanah adalah dokumen dalam bentuk daftar yang memuat data yuridis dan data fisik suatu obyek pendaftaran tanah

yang sudah ada haknya. Buku tanah sebagaimana dimaksud dalam pasal di atas adalah dokumen dalam bentuk daftara yang memuat data yuridis dan data fisik suatu obyek pendaftaran tanah yang sudah ada haknya.

2.2.2 Kekuatan pembuktian sertifikat

Hak-hak subyek hukum atas suatu bidang tanah dengan alat bukti berupa suatu sertifikat harus dilindungi mengingat sertifikat ha katas tanah adalah bukti tertulis yang dibuat oleh pejabat berwenang. Dalam Pasal 32 ayat (2) PP No. 24 Tahun 1997 yang menentukan bahwa :

Dalam hal atas suatu bidang tanah yang sudah diterbitkan sertifikat secara sah atas nama orang atau badan hukum yang memperoleh tanah tersebut dengan itikad baik dan secara nyata menguasainya, maka pihak lain yang merasa mempunyai hak atas tanah tidak dapat menuntut pelaksanaan hak tersebut apabila dalam jangka waktu 5 (lima) tahun sejak diterbitkannya sertifikat tidak mengajukan keberatan secara tertulis kepada pemegang sertipikat dan Kepala Kantor Pertanahan yang bersangkutan ataupun tidak mengajukan gugatan ke Pengadilan mengenai Penguasaan tanah atau penerbitan sertipikat tersebut.

Pasal di atas menentukan secara tegas bahwa sertifikat merupakan surat tanda bukti yang berlaku sebagai alat pembuktian yang kuat dan merupakan alat bukti otentik yang memiliki kekuatan pembuktian yang sempurna. Otentik dalam hal ini meliputi unsur-unsur :

1. Bentuknya ditentukan oleh undang-undang.
2. Dibuat oleh atau dihadapan pejabat yang berwenang.
3. Akta itu dibuat oleh atau dihadapan pejabat umum yang berwenang untuk itu dan ditempat diman akta itu dibuat.

Android

Android adalah sistem operasi mobile berbasis *open source* yang di miliki raksasa internet saat ini, *Google*. Android dikembangkan dengan menggunakan kernel linux. Android memungkinkan untuk di modifikasi secara bebas dan di distibusikan oleh pembuat perangkat tersebut. Dengan sifat *open source* tersebut telah banyak mendorong komunitas pengembang aplikasi untuk menggunakan *source code* android sebagai dasar proyek pembuatan aplikasi.

Android dimulai sebagai sebuah start up rahasia pada tahun 2003, dan dibeli oleh Google pada tahun 2005 dan sebagai jalan google untuk memasuki pasar perangkat lunak bergerak. *Handphone* komersil pertama yang menggunakan OS Android adalah HTC Dream, yang diluncurkan pada 22 Oktober 2008. Dikutip dari okezone.com (2013), terungkap pula sebanyak 4,5 juta smartphone yang berhasil terjual di Indonesia selama Januari sampai Maret 2013, sebanyak 2,28 juta di antaranya menjalankan OS Android.

Sumber : *https://id.wikipedia.org/wiki/Daftar_versi_Android* dan *http://developer.android.com/index.html*

GPS (Global Positioning System)

GPS *(Global Positioning System)* adalah sistem navigasi yang berbasiskan

satelit yang saling berhubungan yang berada di orbitnya. Satelit-satelit itu milik Departemen Pertahanan *(Departemen of Defense)* Amerika Serikat yang pertama kali diperkenalkan mulai tahun 1978 dan pada tahun 1994 sudah memakai 24 satelit. Untuk dapat mengetahui posisi seseorang maka diperlukan alat yang diberi nama GPS *reciever* yang berfungsi untuk menerima sinyal yang dikirim dari satelit GPS. Posisi diubah menjadi titik yang dikenal dengan nama Way-point nantinya akan berupa titik-titik koordinat lintang dan bujur dari posisi seseorang atau suatu lokasi kemudian di layar pada peta elektronik. GPS adalah satu-satunya sistem satelit navigasi global untuk penentuan lokasi, kecepatan, arah, dan waktu yang telah beroprasi secara penuh didunia saat ini. GPS menggunakan konstelasi 27 buah satelit yang mengorbit bumi, dimana sebuah GPS receiver menerima informasi dari tiga atau lebih satelit tersebut seperti terlihat dalam Gambar 2.1 dibawah, untuk menentukan posisi. GPS *receiver* harus berada *dalam line-of sight* (LoS) terhadap ketiga satelit tersebut untuk menentukan posisi, sehingga GPS hanya ideal untuk diguakan dalam outdoor positioning, undergraduate thesis (Wildan Habibi, ITS, Surabaya Januari : 2011).

Quick Response Code

Quick Response Code sering di sebut *Qr Code* atau Kode *QR* adalah semacam simbol dua dimensi yang dikembangkan oleh Denso Wave yang merupakan anak perusahaan dari Toyota sebuah perusahaan Jepang pada tahun 1994. Tujuan dari *Qr Code* ini adalah untuk menyampaikan informasi secara cepat dan juga mendapat tanggapan secara cepat. Pada awalnya *Qr Code* digunakan untuk pelacakan bagian kendaraan untuk *manufacturing*. Namun sekarang, telah digunakan untuk komersil yang ditujukan pada pengguna telepon seluler. *Qr Code* adalah perkembangan dari *barcode* atau kode batang yang hanya mampu menyimpan informasi secara horizontal sedangkan *QR Code* mampu menyimpan informasi lebih banyak, baik secara horizontal maupun vertikal.

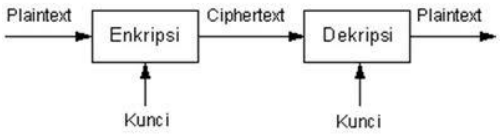
Gambar 2.1 Contoh *Qr Code"Dokumen Sertifikat Hak Milik Tanah Doni Prayugo Agung Pribadi"*

QR Code biasanya berbentuk persegi putih kecil dengan bentuk geometris hitam (dapat dilihat di gambar 2.1), meskipun sekarang banyak yang telah berwarna dan digunakan sebagai brand produk. Informasi yang dikodekan dalam *QR Code* dapat berupa URL, nomor telepon, pesan SMS, *V-Card,* atau teks apapun (Ashford,2010). *QR Code* telah mendapatkan standarisasi internasional ISO/IEC18004 dan Jepang JIS-X-0510 (Denso, 2011).

Kriptografi

Kriptografi berasal dari bahasa Yunani yaitu *cryptós* yang artinya *"secret"* (yang tersembunyi) dan *gráphein* yang artinya *"writting"* (tulisan). Jadi, kriptografi berarti "secret writting" (tulisan rahasia). Definisi yang dikemukakan oleh Bruce Schneier (1996), kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan *(Cryptography is the art and science of keeping messages secure)*. Kriptografi merupakan ilmu sekaligus seni untuk menjaga keamanan pesan (message). Algoritma kriptografi adalah :

1. Aturan untuk enkripsi *(enciphering)* dan dekripsi *(deciphering).*
2. Fungsi matematika yang digunakan untuk enkripsi dan dekripsi.



disebut sebagai *plaintext* ataupun dapat disebut juga sebagai *cleartext.* Proses yang dilakukan untuk mengubah plaintext ke dalam ciphertext disebut *encryption* atau *encipherment.* Sedangkan proses untuk mengubah ciphertext kembali ke plaintext disebut *decryption* atau *decipherment*.

Sandi *Algoritma RSA*

RSA di bidang kriptograf i adalah sebuah algoritma pada enkripsi *public key*. RSA merupakan algoritma pertama yang cocok untuk *digital signature* seperti halnya ekripsi, dan salah satu yang paling maju dalam bidang kriptografi *public key*. RSA masih digunakan secara luas dalam protokol *electronic commerce*, dan dipercaya dalam mengamankan dengan menggunakan kunci yang cukup panjang.

RSA sendiri dibuat pada tahun 1978. RSA adalah singkatan dari nama para penemunya, yaitu Ron Rivest, Adi Shamir, dan Leonard Adleman. RSA adalah salah satu algoritma penyandian yang paling banyak mengundang kontroversi, selain DES. Sejauh ini belum seorang pun yang berhasil menemukan lubang sekuriti pada DES dan RSA, tetapi tak seorang pun juga yang berhasil memberikan pembuktian ilmiah yang memuaskan dari keamanan kedua teknik sandi ini.

Untuk menyandi informasi dan untuk menerjemahkan pesan tersandi sebuah algoritma penyandian memerlukan sebuah data biner yang disebut kunci. Tanpa kunci yang cocok orang tidak bisa mendapatkan kembali pesan asli dari pesan tersandi. Pada DES digunakan kunci yang sama untuk menyandi (enkripsi) maupun untuk menterjemahan (dekripsi), sedangkan RSA menggunakan dua kunci yang berbeda. Isitilahnya, DES disebut sistem sandi simetris sementara RSA disebut sistem sandi asimetris. Kedua sistem ini memiliki keuntungan dan kerugiannya sendiri. Sistem sandi simetris cenderung jauh lebih cepat sehingga lebih disukai oleh sementara kalangan industri. Kejelekannya, pihak-pihak yang ingin berkomunikasi secara privat harus punya akses ke sebuah kunci DES bersama. Walaupun biasanya pihak-pihak yang terkait sudah saling percaya, skema ini memungkinkan satu pihak untuk memalsukan pernyataan dari pihak lainnya. RSA yang menggunakan algoritma asimetrik mempunyai dua kunci yang berbeda, disebut pasangan kunci (key pair) untuk proses enkripsi dan dekripsi. Kunci-kunci yang ada pada pasangan kunci mempunyai hubungan secara matematis, tetapi tidak dapat dilihat secara komputasi untuk mendeduksi kunci yang satu ke pasangannya. Algoritma ini disebut kunci publik, karena kunci enkripsi dapat disebarkan. Orang-orang dapat menggunakan kunci publik ini, tapi hanya orang yang mempunyai kunci privat sajalah yang bisa mendekripsi data tersebut.

2.7.1 Cara kerja sandi algoritma RSA

Tingkat keamanan algoritma penyandian RSA sangat bergantung pada ukuran kunci sandi tersebut (dalam bit), karena makin besar ukuran kunci, maka makin besar juga kemungkinan kombinasi kunci yang bisa dijebol dengan metode mengencek kombinasi satu persatu kunci atau lebih

dikenal dengan istilah brute force attack. Jika dibuat suatu sandi RSA dengan panjang 256 bit, maka metode brute force attack akan menjadi tidak ekonomis dan sia-sia dimana para hacker pun tidak mau/sanggup untuk menjebol sandi tersebut.

2.7.2 Proses Pembuatan Kunci

Dalam membuat suatu sandi, RSA mempunyai cara kerja dalam membuat kunci publik dan kunci privat adalah sebagai berikut:

1. Pilih dua bilangan prima p dan q secara acak , $p \neq q$. Bilangan ini harus cukup besar (minimal 100 digit).
2. Hitung $N = pq$. Bilangan N disebut *parameter sekuriti.*
3. Hitung $\varphi = (p\text{-}1)(q\text{-}1)$.
4. Pilih bilangan bulat (*integer*) antara satu dan φ ($1 < e < \varphi$) yang tidak mempunyai faktor pembagi dari φ.
5. Hitung d hingga $d\,e \equiv 1 \pmod{\varphi}$.

Keterangan :

a. Langkah 3 dan 4 dapat dihasilkan dengan cara algoritma Euclidean
b. Langkah 4 dapat dihasilkan dengan menemukan integer x sehingga $d = (x(p\text{-}1)(q\text{-}1) + 1)/e$ menghasilkan bilangan bulat, kemudian menggunakan nilai dari $d \pmod{(p\text{-}1)(q\text{-}1)}$.

Setelah melalu cara ini, maka kita akan mendapatkan kunci publik dan kunci privat. Kunci publik terdiri dari dua elemen, yaitu :

a. *N*, merupakan modulus yang digunakan
b. e, eksponen publik atau eksponen enkripsi.

dan kunci privat, yang terdiri dari:

a. *N*, merupakan modulus yang digunakan, sama seperti pada kunci publik.
b. *d*, eksponen pribadi atau eksponen deskripsi, yang harus dijaga kerahasiaanya.

Nilai p dan q sebaiknya dibuang atau dijaga kerahasiaannya, karena terdapat N dimana p dan q adalah faktor pembagi dari N. Walaupun bentuk ini memperbolehkan dekripsi secara cepat dan signing menggunakan *Chinese Remainder Theorem* (CRT), hal ini mejadi lebih tidak aman karena bentuk ini memperbolehkan *side channel attacks*. *Side channel attacks* adalah sebuah serangan yang berdasarkan informasi yang dikumpulkan dari implementasi fisik (atau kelemahan secara fisik) dari sebuah sistem kriptografi, dibanding dengan kelemahan teoritis dari algoritmanya sendiri. Sebagai contohnya, faktor-faktor kurun waktu dari informasi, konsumsi tenaga, bahkan suara yang ditimbulkan dapat membantu mempermudah informasi yang bisa diambil untuk menjebol sistem tersebut.

2.7.3 Proses Enkripsi Pesan

Misalkan pada suatu kasus si A ingin mengirim pesan m kepada si B. A mengubah m menjadi angka $n < N$, menggunakan protokol yang sebelumnya telah disepakati dan dikenal sebagai *padding scheme*. *Padding scheme* harus dibangun secara hati-hati sehingga tidak ada nilai dari m yang menyebabkan masalah keamanan. Contohnya, jika kita ambil contoh sederhana dari penampilan ASCII dari m dan menggabungkan bit-bit secara bersama-sama akan menghasilkan n,

kemudian pessan yang berisi ASCII tunggal karakter NUL (nilai numeris 0) akan menghasilkan $n = 0$, yang akan menghasilkan *ciphertext* 0 apapun itu nilai dari *e* dan *N* yang digunakan.

Maka A mempunyai nilai *n* dan mengetahui *N* dan *e*, yang telah diumumkan oleh B. A kemudian menghitung *ciphertext c* yang terkait pada *n*:

$c = n^e \mod N$

Perhitungan tersebut dapat diselesaikan dengan menggunakan metode *exponentation by squaring*, yaitu sebuah algoritma yang dipakai untuk komputasi terhadap sejumlah nilai integer yang besar dengan cepat. Kemudian A mengirimkan nilai *C* kepada B.

2.7.4 Proses Dekripsi Pesan

B sudah menerima *C* dari A, dan mengetahui kunci privat yang digunakan B. B kemudian mengembalikan nilai *n* dari *C* dengan langkah-langkah sebagai berikut:

$n = c^d \mod N$

Perhitungan diatas akan menghasilkan *n*, dengan begitu B dapat mengembalikan pesan semula *m*. Prosedur dekripsi bekerja karena.

$c^d \equiv (n^e)^d \equiv n^{ed} \pmod N$

Kemudian, karena $ed \equiv 1 \pmod{p-1}$ dan $ed \equiv 1 \pmod{q-1}$, hasil dari *Fermat's little theorem*.

$n^{ed} \equiv n \pmod p$

dan

$n^{ed} \equiv n \pmod q$

Karena *p* dan *q* merupakan bilangan prima yang berbeda, mengaplikasikan *Chinese remainder theorem* akan menghasilkan dua macam kongruen.

$n^{ed} \equiv n \pmod{pq}$

serta

$c^d \equiv n \pmod N$

2.7.5 Contoh Penghitungan RSA

Sekarang kita mencoba suatu contoh untuk mengenal lebih dalam sistem kerja enkripisi RSA. Misalnya kita mau mengenkripsi kata *"SECRET"* dengan RSA, lalu kita dekripsi kembali ke dalam *plain text*.

Karena *p* dan *q* berjumlah minimal 100 digit atau lebih, nilai *d* dan *e* bisa berjumlah sama dengan 100 digit dan nilai *N* akan berjumlah 200 digit. Untuk itu di contoh pemakaian berikut, kita akan memakai angka-angka yang kecil agar mudah dalam penghitungan. Cara pengerjaannya adalah:

1. Kita pilih $p = 3$ dan $q = 5$
2. Hitung $N = pq = 3*5 = 15$
3. Nilai *e* harus merupakan bilangan prima yang lebih besar dan relatif dekat dengan (p-1)(q-1) = (2)(4) = 8, sehingga kita pilih e = 11. Angka 11 adalah bilangan prima terdekat dan lebih besar daripada 8.
4. Nilai *d* harus dipilih sehingga,

$$\frac{(ed-1)}{(p-1)(q-1)}$$

adalah sebuah integer. Lalu nilai

(11 *d* - 1) / [(2)(4)] = (11d - 1) / 8

juga merupakan integer. Setelah melalui proses penghitungan, salah satu nilai yang mungkin adalah $d = 3$.

5. Lalu kita masukkan kata yang akan dienkripsi, "SECRET". Kita akan mengkonversi string ini ke representasi desimal menggunakan nilai karakter ASCII, yang akan menghasilkan nilai ASCII 83 69 67 82 69 84
6. Pengirim akan mengenkripsi setiap digit angka pada saat

yang bersamaan menggunakan nilai kunci publik (*e, n*) = (11,15). Lalu setiap karakter *ciphertext* akan masuk ke persamaan $C_i = M_i^{11} \bmod 15$. Yang akan menghasilkan nilai digit masukan adalah 0x836967826984 yang akan dikirim sebagai 0x2c696d286924.

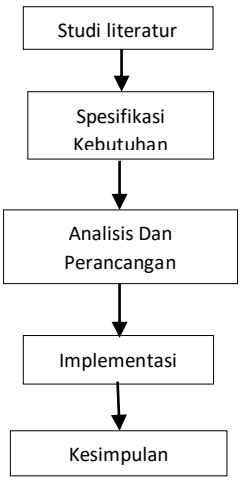
7. Penerima akan mendekripsi setiap digit angka menggunakan nilai kunci privat (*d, n*) = (3, 15). Lalu, setiap karakter plaintext akan masuk persamaan $M_i = C_i^3 \bmod 15$. String masukan yang bernilai 0x2c696d286924, akan dikonversi kembail menjadi 0x836967826984, dan akhirnya angka-angka tersebut akan diubah kembali menjadi bentuk string *plaintext* yang bernilai "SECRET".

Dari contoh di atas kita dapat menangkap suatu kelemahan dari pemakaian *p* dan *q* yang bernilai kecil yaitu bisa kita lihat di digit ke-4, ke-6 dan ke-9 tidak berubah saat dienkripsi, dan nilai 2 dan 8 dienkripsi menjadi 8 dan 2, yang berarti dienkripsi menjadi kebalikannya. Tapi kesimpulan yang bisa diambil dari contoh yang sederhana ini adalah RSA dapat digunakan dalam penyandian dalam pengiriman informasi.

III. METODOLOGI PENELITIAN

Tahapan Penelitian

Dalam pengerjaan Tugas Akhir ini diperlukan langkah-langkah kegiatan penelitian untuk mendapatkan hasil yang maksimal. Untuk itu penulis merencanakan suatu langkah-langkah untuk dapat memaksimalkan dalam pengerjaan Tugas Akhir ini. Langkah-langkah tersebut adalah sebagai berikut :



Gambar 3.1 Tahapan Penelitian

Studi Literatur

Penelitian ini dimulai dengan melakukan studi literatur, yaitu proses pengumpulan data sebagai bahan referensi baik dari buku, artikel, jurnal, makalah, atau situs internet yang berkaitan dengan pelabelan dokumen, android,sertifikat, *GPS*, *QR Code* dan sandi *algoritma RSA*.

Analisis dan Perancangan

3.4.1 Analisis

Masalah yang ada pada pencacatan SHM (*Sertifikat Hak Milik Tanah*) saat ini masih mengandalkan sistem manual yang tentunya memakan waktu yang cukup lama, tidak efisien dan tidak jarang pula terdapat banyak kecurangan oknum-oknum karena dilakukan dengan cara manual dengan menggunakan alat ukur. Meskipun menggunakan bantuan GPS (*Global Positioning System*) namun penyimpanan datanya masih belum maksimal. Proses yang memakan waktu lama, dan tidak jarang adanya kecurangan saat pengukuran dapat diatasi dengan adanya pengambilan

gambar tanah/bidang disebut NIB (*Nomor Identifikasi Bidang)* menggunakan kamera smartphone dan fitur lokasi atau GPS yang hasilnya telah di enkripsi dalam bentuk *QR Code* sebagai pelabelan dokumen SHM (*Sertifikat Hak Milik Tanah*). Dengan adanya pelabelan dokumen menggunakan teknologi *QR Code* , memungkinkan pembuatan dokumen SHM (*Sertifikat Hak Milik Tanah*) menjadi lebih cepat, mudah dan valid status keaslian dokumennya.

3.4.2 Perancangan Sistem

Prosedur yang akan digunakan untuk pelabelan dokumen adalah :

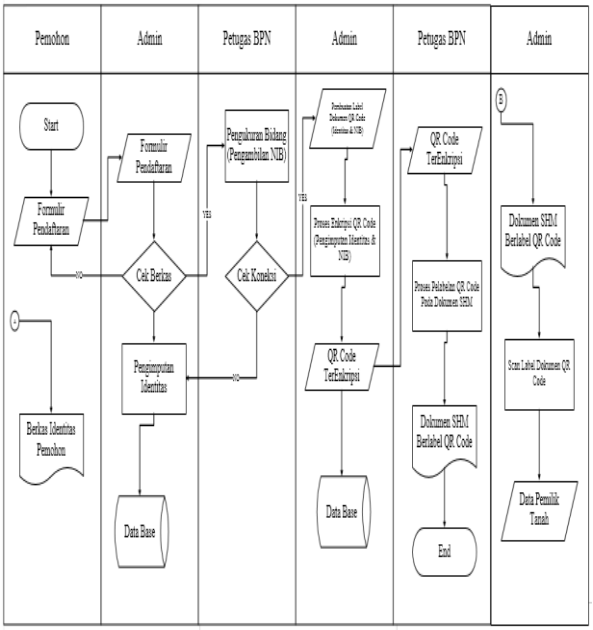
1. Setiap pembuat dokumen SHM (*Sertifikat Hak Milik Tanah*) akan diberikan formulir pendaftaran dan mengisi identitas diri (KTP) sebagai data awal yang akan di enkripsi bersama NIB (*Nomor Ideentifikasi Bidang*) menggunakan *algoritma RSA.* Yang nantinya akan menjadi *QR Code* sebagai label setiap dokumen.
2. Format data *QR Code* sebelum di sandikan oleh *algoritma RSA* berupa, Nama , Tempat/Tanggal Lahir, Jenis Kelamin, Alamat, Agama, Kewarganegaraan, NIB, dan Tanggal Pembuatan. Fungsi dari data *QR Code* ini adalah untuk mengetahui identitas dan bidang tanah yang dimiliki oleh pembuat dokumen SHM (*Sertifikat Hak Milik Tanah*).
3. Dalam proses pelabelan dokumen, petugas BPN, PPAT atau Notaris harus memiliki perangkat android dengan aplikasi pemindai *QR Code* khusus.

Pada sistem pelabelan dokumen ini, sandi *algoritma RSA* yang digunakan untuk menyandikan data di dalam *QR Code* adalah sandi *algoritma RSA* dengan 160 karakter.

3.4.3 Arsitektur Sistem

Arsitektur sistem digunakan untuk menerjemahkan bagian-bagian dari keseluruhan sistem yang lebih bersifat khusus secara terstruktur dan bertujuan menjawab kebutuhan sistem.

Arsitektur sistem pada penelitian ini dapat di lihat pada gambar berikut ini :



Gambar 3.2 Arsitektur Sistem Pelabelan Dokumen

Pada proses arsitektur sistem pelabelan dokumen ini, proses pertama ialah “Pemohon” melakukan pengisian formulir pendaftaran, yang berisi Nama, Tempat/Tanggal Lahir, Jenis Kelamin, Alamat, Agama, Kewarganegaraan,

setelah berkas telah dilengkapi maka berkas diserahkan kepada admin untuk dicek kembali.

jika berkas belum lengkap maka akan dikembalikan kepada pemohon, jika lengkap maka berkas akan diimputkan lalu disimpan ke database, setelah proses pengimputan selesai, petugas bpn akan melakukan pengukuran bidang/pengambilan NIB sebagai *Nomor Identifikasi Bidang* tanah milik pemohon, pada proses ini memerlukan koneksi internet agar data dapat langsung tersimpan ke database, jika tidak ada koneksi maka pengimputan dilakukan dengan manual.

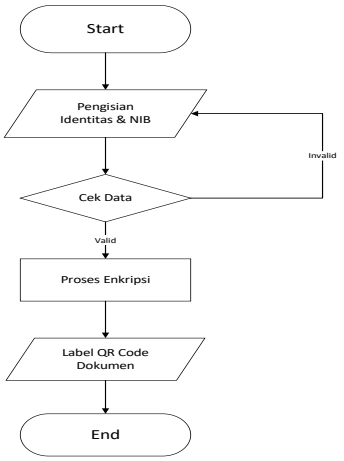
Jika kedua proses telah dilakukan baik pengisian identitas dan pengambilan NIB, maka data *QR Code* telah diperoleh, sehingga proses pembuatan label dokumen berupa *QR Code* yang telah dienkripsi dapat dilakukan. Pada proses akhir yang tergambar pada arsitektur ini yaitu pemasangan label dokumen berupa QR Code yang telah dienkripsi Sertifikat Hak Milik Tanah.

3.4.4 Flowchart Diagram

Flowchart atau diagram aliran adalah langkah-langkah prosedur sistem yang digambarkan secara grafik. Flowchart dapat memberi solusi untuk menyelesaikan masalah dalam proses atau algoritma program dalam sistem.

Berikut adalah flowchart sistem yang akan dibuat pada penelitian ini :

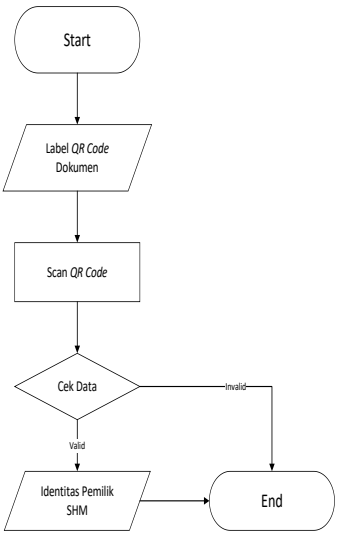
1. Flowchart Proses Enkripsi Pembuatan Label menggunakan *Algoritma RSA*



Gambar 3.3 Flowchart Proses Enkripsi Pembuatan Label Dokumen

Pada proses enkripsi ini, data yang akan dienkripsi adalah berupa Identitas pemohon dan NIB pemohon. Jadi, nantinya identitas dan NIB tersebut akan diekripsi kedalam *Algoritma RSA* .pertama, data keduanya akan dicek apakah ada atau tidak. Jika keduanya ada maka akan dilanjutkan kedalam proses penyandian *Algoritma RSA* sampai mengeluarkan Label *QR Code* Dokumen.

2. Flowchart Scan *QR Code*

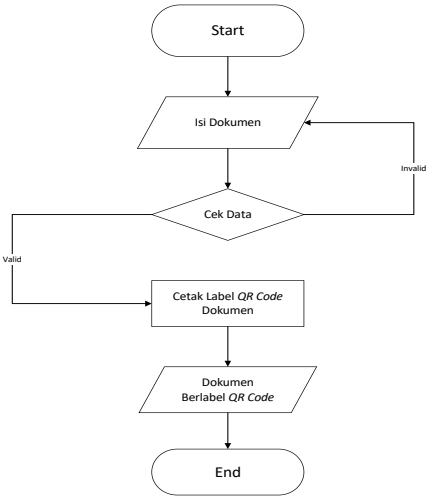


Gambar 3.4 Flowchart Scan QR Code

Flowchart pada gambar 3.4 adalah flowchart saat melakukan scan qr code pada label dokumen. Generate

dari *QR Code* dilakukan dengan menggunakan library Zxing. Pada proses scanning *Qr Code* yang otomatis terhubung dengan database sistem. Jika data yang discan sesuai maka system akan mengidentifikasi identitas data pemilik SHM yang valid. Namun jika data tidak valid maka proses akan langsung terhenti tanpa mengetahui identitas pemilik.

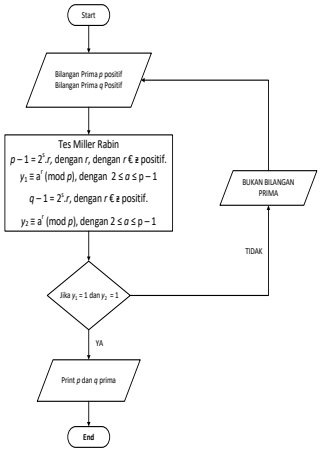
3. Flowchart cetak label dokumen



Gambar 3.5 Flowchart Cetak Label Dokumen.

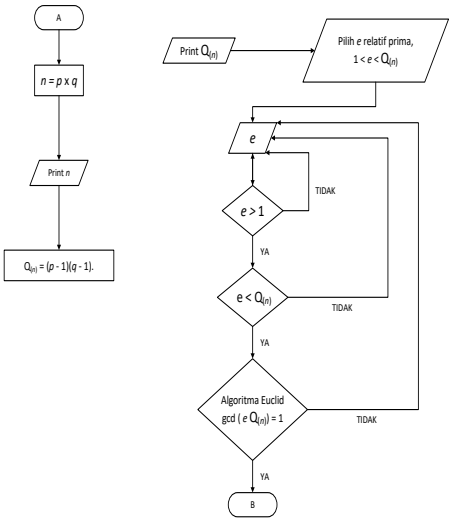
Pada flowchart cetak label Dokumen, langkah yang dilakukan adalah melihat data valid atau belum. Pemohon SHM (*Sertifikat Hak Milik Tanah*) yang telah melengkapi data dapat melakukan pencetakan label dokumen berupa *QR Code* tersebut. Jika data pemohon belum valid, maka tidak bisa melakukan proses cetak label dokumen. Jika pemohon telah melengkapi persyaratan isi data secara lengkap proses pencetakan label dokumen akan dilakukan dan menghasilkan dokumen yang mempunyai label *QR Code*.

4. Flowchart Algoritma Pembangkit Kunci



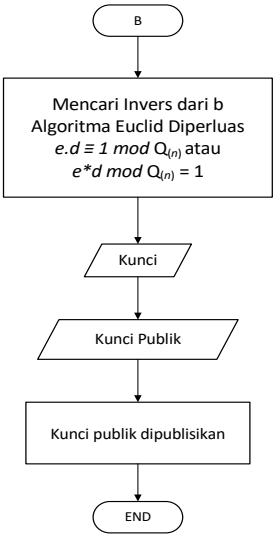
Gambar 3.6 Flowchart Algoritma Pembangkit Kunci

5. Flowchart Algoritma Pembangkit Kunci Lanjutan



Gambar 3.7 Flowchart Algoritma Pembangkit Kunci Lanjutan.

6. Flowchart Algoritma Pembangkit Kunci Lanjutan



Gambar 3.8 Flowchart Algoritma Pembangkit Kunci Lanjutan

Algoritma RSA memiliki dua kunci yang berbeda untuk proses enkripsi dan dekripsi. Dalam menentukan dua bilangan prima sebagai kunci adalah bilangan prima yang besar, karena pemfaktoran bilangan dari dua bilangan prima yang besar sangat sulit, sehingga keamanan pesan lebih terjamin. Pasangan kunci adalah elemen penting dari algoritma RSA.

Berikut ini langkah- langkah dalam membangkitkan dua kunci algoritma RSA.

1. Pilih dua bilangan prima sembarang, *p* dan *q*.
2. Hitung $n = p.q$
3. Hitung $Q_{(n)} = (p - 1)(q - 1)$.
4. Pilih kunci publik e, yang relatif prima terhadap $Q_{(n)}$.
5. Bangkitkan kunci pribadi dengan menggunakan $e.d \equiv 1 \ mod \ Q_{(n)}$ atau $e*d \ mod \ Q_{(n)} = 1$

Hasil dari algoritma tersebut akan menghasilkan dua kunci, yaitu kunci public (*e*,*n*) dan kunci private (*d*,*n*).

Cntoh Perhitungan Pembangkit Kunci Algoritma RSA.

Misalkan B akan membangkitkan kunci publik dan kunci pribadi miliknya. B memilih $p = 7$ dan $q = 13$ (keduanya prima). Selanjutnya B menghitung.

$$n = 7 \times 13 = 91$$

Dan

$Q_{(n)} = (7-1)\ (13-1) = 72$

B memilih $e = 5$ karena 5 relatif prima terhadap 72. B mengumumkan nilai *e* dan *n*.

Selanjutnya B menghitung nilai dengan algoritma Euclid yang diperluas menjadi

$72 = 14.5 + 2$ $n = 1, a_1 = 5, q_1 = 14$

$5 = 2.2 + 1$ $n = 2, a_2 = 2, q_2 = 2$

$2 = 2.1$

$n = 3, a_3 = 1, q_3 = 2$

$t_2 = t_0 – q_1.t_1 = 0 – 14(10) = -14 = 58$

$t_3 = t_1 – q_2.t_2 = 1 – 2.(-14) = 29.$

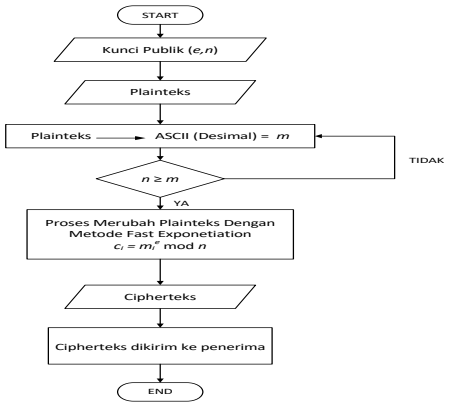
Karena $e.d \equiv 1 \bmod Q_{(n)}$ dapat ditulis menjadi $e^{-1} \ mod \ Q_{(n)} = d$, maka didapat $5^{-1} \ mod \ 72 = 29$. Sehingga diperoleh $d = 29$. Ini adalah kunci pribadi untuk mendekripsikan pesan dan harus dirahasiakan oleh B. Dari perhitungan tersebut didapat kunci publik dan kunci pribadi berturut- turut adalah

($e = 5, n = 91$)

Dan

($d = 29, n = 91$)

7. Flowchart Proses Enkripsi Algoritma RSA



Gambar 3.9 Flowchart Proses Enkripsi Algoritma RSA

Langkah-langkah dalam melakukan proses enkripsi adalah sebagai berikut:

1. Ambil kunci public penerima pesan, e, dan modulus n.
2. Plainteks dibuat menjadi blok-blok m_1, m_2, m_3, m_4, ……sedemikian sehingga setiap blok merepresentasikan nilai di selang [0, n – 1].

Setiap blok m_i dienkripsi menjadi blok c_i dengan rumus

$c_i = m_i^e \bmod n$

Contoh Perhitungan :

Misalkan A akan mengirim pesan ke B. Pesan (Plainteks) yang akan dikirim adalah m = DONI

atau dalam sistem desimal pengkodean ASCII adalah

68797873

A memecah m menjadi blok yang lebih kecil, misalkan membagi menjadi 5 blok yang berukuran 2 digit $m_1 = 68$

$m_2 = 79$

$m_3 = 78$

$m_4 = 73$

Nilai-nilai m_i ini masih terletak di selang [0,91 – 1] agar transformasi menjadi satu-ke-satu. A mengetahui kunci publik B adalah e = 5 dan n = 91. A dapat mengenkripsikan setiap blok plainteks sebagai berikut :

$c_1 = 68^5 \ mod \ 91 = 87$

$c_2 = 79^5 \ mod \ 91 = 53$

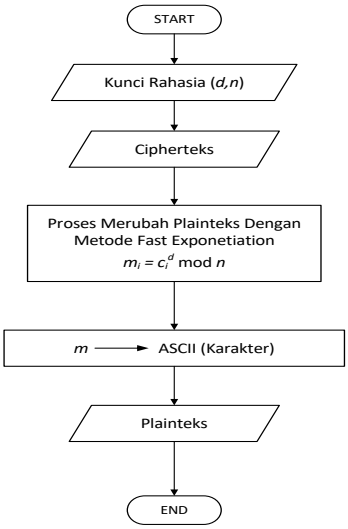
$c_3 = 78^5 \ mod \ 91 = 78$

$c_4 = 73^5 \ mod \ 91 = 47$

Jadi chiperteks yang dihasilkan adalah

c = 87537847

8. Flowchart Proses Dekripsi Algoritma RSA



Gambar 3.10 Flowchart Proses Dekripsi Algoritma RSA

Langkah-langkah dalam melakukan proses dekripsi adalah sebagai berikut:

1. Setiap blok chiperteks c_i didekripsi kembali menjadi blok m_i dengan rumus :
   $m_i = c_i^d \bmod n$
2. Blok - blok m_1, m_2, m_3, m_4, ...diubah kembali menjadi bentuk huruf dengan kode ASCII.

Contoh Perhitungannya : B akan mendekripsi pesan dengan menggunakan kunci pribadi (d = 29, n = 91). Blok – blok chiperteks didekripsikan dengan cara :

$c_1 = 87^{29} \ mod \ 91 = 68$

$c_2 = 53^{29} \ mod \ 91 = 79$

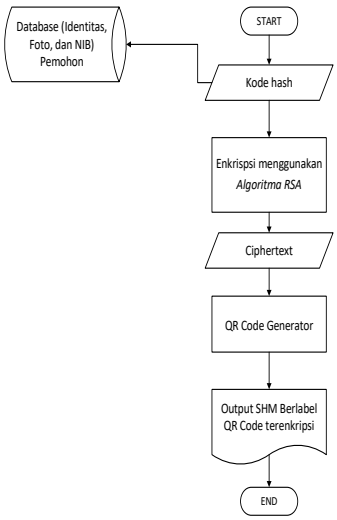
$c_3 = 78^{29} \ mod \ 91 = 78$

$c_4 = 47^{29} \ mod \ 91 = 73$

Akhirnya diperoleh plainteks semula yaitu m = 68797873 yang dalam

sistem karakter pengkodean ASCII *m* = DONI.

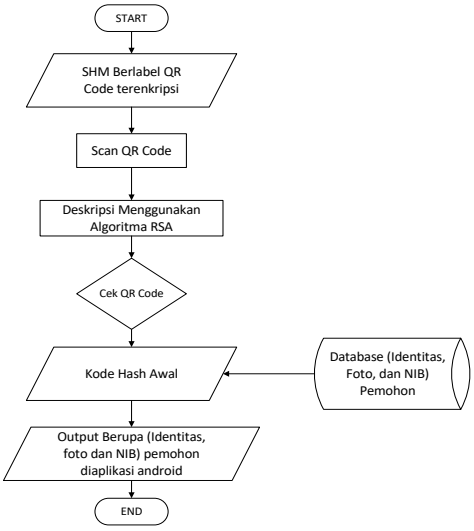
9. Flowchart Proses Enkripsi Pembuatan Label Dokumen.



Gambar 3.11 Flowchart Proses Enkripsi Pembuatan Label

Pada proses enkripsi pembuatan label dokumen memasukkan kode hash yang nanti akan memanggil data yang ada didatabase yang akan dienkripsi dengan *Algoritma RSA*, lalu akan menghasilkan ciphertext sebagai data yang akan dijadikan label *QR Code* dengan menggunakan QR Code generator, yang hasilkan akan langsung ditempelkan ke dalam documen SHM (*Sertifikat Hak Milik Tanah*).

10. Flowchart Proses Dekripsi Label Dokumen.



Gambar 3.12 Flowchart Proses Deskripsi Label Dokumen

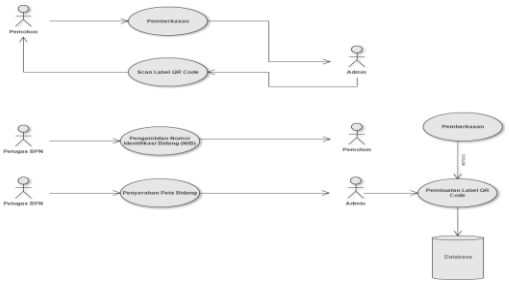
Dalam proses deskripsi ini pemohon memberikan dokumen SHM(*Sertifikat Hak Milik Tanah*) yang sudah diberi label *QR Code*, lalu label *QR Code* akan discanning oleh admin, data tersebut berupa ciphertext yang akan diterjemahkan ke dalam plaintext menggunakan aplikasi scanning adroid yang telah menggunakan Algoritma RSA, sehingga proses scanning nantinya berupa kode hash awal yang akan mengeluarkan data pemilik, yang berada didalam database

3.4.5 Use Case Diagram

Use case merupakan gambaran dari sebuah sistem dari sudut pandang pengguna. Diagram use case digunakan untuk menggambarkan fungsi-fungsi dari aspek perilaku sebuah sistem tersebut.

Pada sistem ini aktor dibagi menjadi 3 bagian yaitu pemohon, petugas bpn, admin. User merupakan pengguna pada mobile device yaitu petugas bpn. Sedangkan admin adalah petugas administrator yang menginput data pemohon pembuat dokumen SHM (*Sertifikat Hak Milik Tanah*). Dan terakhir adalah Petugas BPN sebagai orang yang menscan *QR Code* pada saat penunjukan kevalidtan isi dokumen.

Diagram use case sistem dapat dilihat pada gambar 3.6



Gambar 3.13 Use case diagram

Penjelasan dari use diatas adalah sebagai berikut :

1. Terdapat tiga aktor yaitu pemohon,admin dan petugas bpn
2. Terdapat 6 use case dimana ada : pemberkasan, , scan label *QR Code*, pengambilan nomor NIB, penyerahan peta bidang,pembuatan label *QR Code,* penyimpanan ke database.

Pertama pemohon terlebih dulu melakukan pemberkasan dalam proses ini pemohon diminta untuk mengisi formulir pendaftaran, administrasi dan mengisi identitas diri. Jika sudah melakukan pemberkasan maka admin akan mengecek kelengkapan berkas, jika berkas sudah lengkap, petugas bpn akan melakukan pengambilan nomor bidang bersama pemohon yang disebut NIB, gunanya nanti untuk dijadikan nomor code disetiap sertifikat, setelah melakukan proses pengambilan nomor bidang, petugas bpn akan membuat peta bidang dari tanah milik pemohon, kemudian diserahkan kepada admin untuk diinclude kan dengan berkas yang nantinya akan dijadikan label dokumen berupa *QR Code,* dan akan disimpan ke database. Kemudian jika label sudah dibuat maka admin akan mengecek kebenaran isi label berupa *QR Code* dengan menggunakan perangkat androidnya menggunakan QR Code scanner. Dalam proses ini admin bertugas memantau keseluruhan kegiatan pada sistem, misal : input data, edit, hapus, dan lihat data.

3.6 Implementasi.

Implementasi sistem pelabelan dokumen berupa *QR Code* yang telah dienkripsi ini, dilakukan pada pembuatan SHM (*Sertifikat Hak Milik Tanah*). Sistem pelabelan dokumen ini akan terintegrasi dengan pihak BPN (*Badan Pertanahan Nasional*). Pada implementasinya, untuk mengolah gambar penanda *QR Code* digunakan sebuah library open source bernama *Zxing.* Sistem generator *QR Code* dan data dienkripsi menggunakan open source Php (*php hypertext preprocessor*), dan *Smartphone Android* dengan bahasa pemrogaman java.

Pada sistem pelabelan dokumen dibutuhan beberapa aplikasi pendukung seperti : *Android Studio, Qr Code generator, sublime text.* Pada tahap uji coba akan diimplementasikan pada dokumen SHM (*Sertifikat Hak Milik Tanah*) yang sudah diduplikat dan telah melalui proses pelabelan *QR Code.* Data yang dienkripsi pada *QR Code* adalah Nama , Tempat/Tanggal Lahir, Jenis Kelamin, Alamat, Agama, Status Perkawinan, Pekerjaan, Kewarganegaraan, NIB, dan Tanggal Pembuatan. Kemudian dengan adanya pelabelan dokumen menggunakan *QR Code* ini, dapat mempercepat proses pembuatan,

mempermudah pihak BPN,PPAT atau Notaris untuk mengecek dan menyimpan data, dan tentu lebih terjaga keaslian isi dokumen karena menggunakan label *QR Code* yang telah diekripsi.

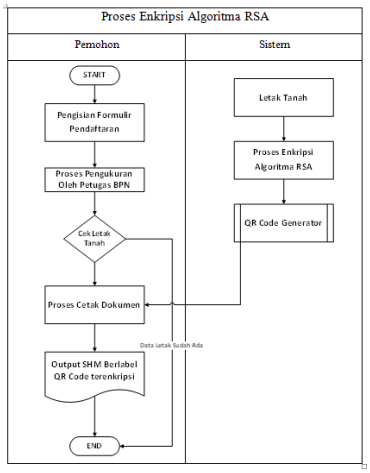
IV. HASIL DAN PEMBAHASAN

Pada bab ini akan dijelaskan tentang proses pengimplementasian integrasi sistem antara SHM (*Sertifikat Hak milik*

Tanah) yang berlabel *QR Code* yang telah terenkripsi *algortima RSA* dengan aplikasi scan *QR Code algoritma RSA* berbasis android , sesuai perancangan sisetem yang telah dibahas pada bab 3 serta melakukan pengujian sistem yang telah dibangun.

4.1 Proses Sandi *Algoritma RSA*

Pada proses sandi *Algoritma RSA* ini, akan dilakukan beberapa ujicoba enkripsi pada identitas lengkap pemohon, foto bidang dan nomor identifikasi bidang, dengan titik koordinatnya yang akan dienkripsi. Adapun prosesnya seperti gambar 4.1 dibawah ini :

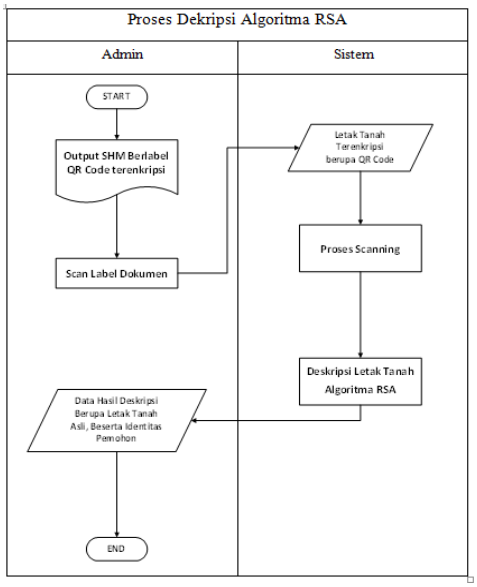


Gambar 4.1 Flowchart Proses Sandi *Algoritma RSA*

Penjelasan pada proses enkripsi *algoritma RSA* ini dilakukan oleh sistem, dimana nantinya pemohon atau pembuat SHM yang telah mengisikan identitas diri dan petugas BPH yang telah mengambil nomor identifikasi bidang akan menjadi data yang dienkripsi dengan *algoritma RSA* sehingga sistem akan otomatis langsung mengenerate data enkripsi tersebut menjadi kode batang *QR Code* Scanner. Yang nantinya akan menghasilkan output berupa kode batang *QR Code* yang terenkripsi pada SHM (*Sertifikat Hak Milik Tanah*) pemohon.

4.2 Proses Dekripsi *Algoritma RSA*

Pada proses desripsi algoritma RSA ini, data yang telah dienkripsi berupa string koordinat enkripsi. Selanjutnya akan didekripsi kembali dengan kunci key berupa NIB yang nantinya akan kembali kepada koordinat asal, seperti pada gambar 4.3 berikut ini :



Gambar 4.3 Flowchart Proses Dekripsi *Algoritma RSA*

Penjelasan pada proses deskripsi ini, dilakukan oleh sistem. Dimana nantinya SHM (*Surat Hak Milik Tanah*) yang telah disisipi kode *QR Code*, langsung discan menggunakan aplikasi android scanner. Proses deskripsi ini dimulai dengan menscan SHM berlabel *QR Code* yang nantinya output dari hasil scan tersebut adalah koordinat asli yang akan memanggil seluruh identitas, foto bidang dan NIB pomohon tersebut.

4.3 Contoh Kasus Kecurangan Manipulasi *QR Code*

Contoh kasus yang dimanipulasi oleh orang lain. Misalkan ada oknum ataupun pemohon/pembuat akta palsu yang ingin menggadakan dan membuat data *QR Code* palsu. Maka jika terjadi

pemalsuan ataupun penggandaan dokumen, sistem akan dapat mengetahui sehingga, misalkan data *QR Code* yang dibuat itu palsu ketika dilakukan proses scanning menggunakan *Algoritma RSA* output yang dikeluarkan akan berbeda pada perangkat android.

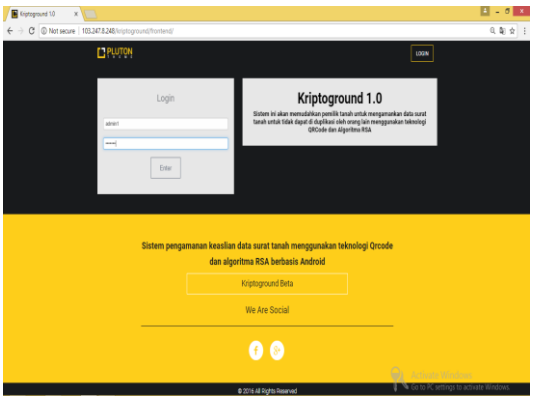
Gambar 4.5 Data *QR Code* tanpa enkripsi *Algoritma RSA*

Dan apabila data tersebut tidak terenkripsi, maka hasil output data yang akan dikeluarkan tidak berupa koordinat asli yang nantinya tidak akan bisa memanggil seluruh identitas, foto maupun NIB pomohon, contoh gambar seperti dibawah ini :

Gambar 4.6 Data Dekripsi Dengan Data Palsu/Manipulasi

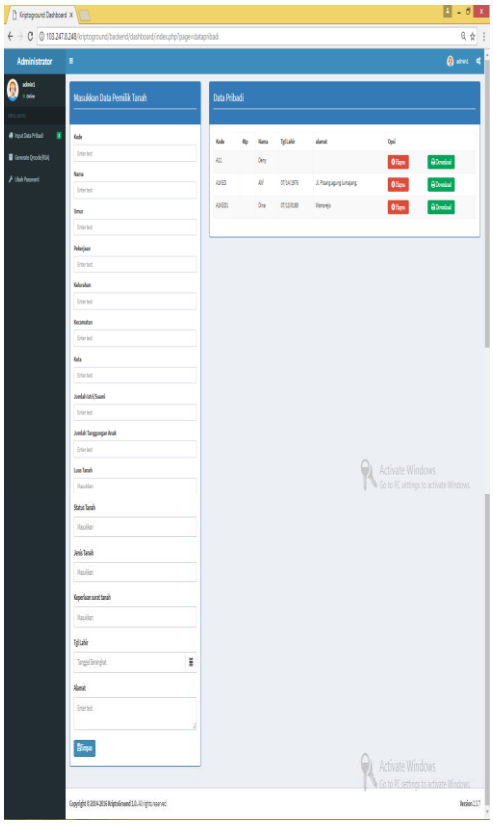
4.4 Proses Pengimputan Data Pada Website Pembuatan Label SHM

Pada proses desain login, dosen akan memasukkan user dan password yang telah ada pada sistem scanner Dokumen SHM untuk melanjutkan proses scanner, dapat dilihat pada gambar 4.7 berikut ini :



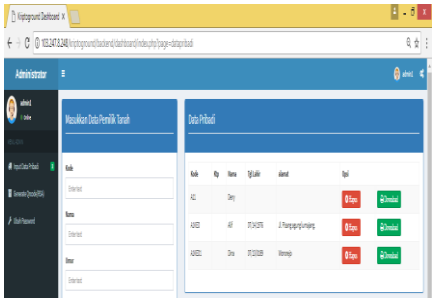
Gambar 4.7 Proses Login Admin Website

Pada desain sistem login admin, admin memasukkan user dan password yang telah ada pada sistem. Dan kemudian melanjutkan proses penginputan data setting pertama bisa dilihat pada gambar 4.8.



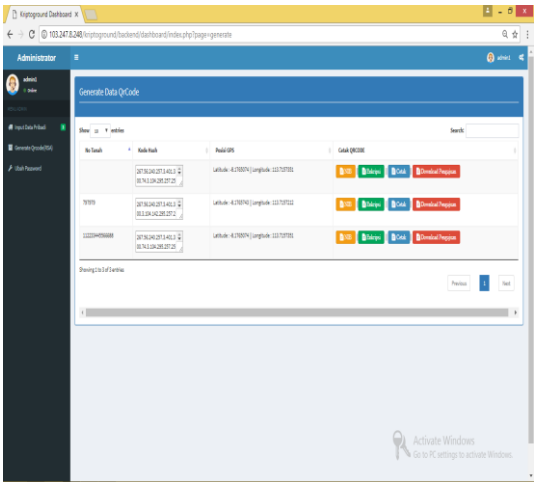
Gambar 4.8 Menu Pengimputan Identitas Pemohon

Pada menu pengimputan data berisi identitas pemohon, baik admin atau pemohon harus mengimputkan identitas sesuai dengan formulir yang telah dibuat, ketika proses pengimputan telah sesuai maka langkah selanjutnya yaitu menyimpannya, dengan menekan tombol simpan, maka akan muncul data yang telah disimpan seperti gambar 4.9 dibawah ini :



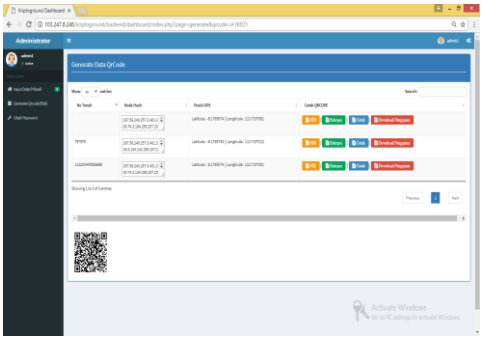
Gambar 4.9 Data Pribadi Yang Tersimpan

Data Pribadi tersebut berisikan data identitas pemohon yang nantinya akan dienkripsi menggunakan algoritma RSA beserta NIB dan letak tanah pemohon. Pengambilan letak tanah dilakukan oleh petugas ukur BPN dengan menggunakan aplikasi kriptoground yang telah terinstall pada smartphone android petugas ukur tersebut, sehingga jika pengambilan letak tanah sudah dilakukan maka proses selanjutnya ialah mengenkripsi data tersebut dengan memilih tombol Ganerate QR Code (RSA), seperti gambar 4.10 dibawah ini :



Gambar 4.10 Generate Kode QR Code (Algoritma RSA)

Pada menu ini terdapat banyak tombol yaitu NIB, Enkripsi, Cetak QR, dan Download Pengajuan. Pada posisi GPS, data ini muncul ketika petugas ukur BPN telah melakukan proses pengukuran, jika posisi tersebut belum diukur maka langkah selanjutnya akan bisa melakukan proses download pengajuan untuk mendapatkan NIB, tapi jika tanah itu telah diukur dan telah didaftarkan maka sistem tidak akan bisa mencetak pengajuan, karena terdapat data letak yang sama, dalam proses ini dilakukan investigasi apakah tanah tersebut sudah terdaftar atau belum, sehingga dalam proses ini dapat mengetahui dan mengurangi adanya duplikasi dokumen sertifikat tanah. Jika tanah itu belum terdaftar maka langkah selanjutnya yaitu mencetak data yang telah dienkripsi menjadi QR Code, seperti gambar dibawah ini :



Gambar 4.11 Cetak QR Code dan Cetak Dokumen Berlabel QR Code Terenkripsi

Pada menu ini menampilkan hasil enkripsi berupa cetakan QR Code yang nantinya akan dilabelkan disetiap sertifikat tanah yang dimiiliki pemohon. Seperti pada gambar 4.12 berikut ini :

4.5 Perbandingan Sistem

Integrasi pada sistem pembuatan label QR Code ini dikembangkan untuk mempermudah pembuat dokumen atau pemohon Sertifikat Hak Milik Tanah dan petugas pembuat dokumen Sertifikat Hak Milik Tanah yaitu BPN dalam melakukan pencacatan dokumen SHM. Data pengembangan sistem dan perbedaan sistem lama dengan sistem baru dapat dilihat pada tabel 4.1.

No.	Modul	Sistem Lama	Sistem Baru
1.	Pembuatan Dokumen Sertifikat Hak Milik.	A. Pembuatan dokumen masih menggunakan sistem manul dan tidak terkoneksi internet. B. Kemungkinan duplikasi dan pemalsuan dokumen masih dapat dilakukan karena keamanan data pada dokumen masih kurang.	A. Pembuatan dilakukan dengan komputerisasi dan online. B. Kemungkinan akan adanya duplikasi dan pemalsuan dapat teratasi dengan menggunakan pelabelan dokumen berupa kode *QR Code* terenkripsi.

Tabel 4.1 Perbandingan Sistem.

4.6 Pengujian

A. Pengujian Black Box

Pengujian black box merupakan metode pengujian yang berfokus pada kebutuhan fungsional dari aplikasi. pengujian black box dilakukan dengan focus pada hasil keluaran yang diharapkan dari sistem yang diuji, apakah dapat berjalan sesuai yang diharapkan atau tidak. Tabel pengujian black box dapat dilihat pada tabel 4.2.

No.	Skenario Pengujian	Hasil Yang Diharapkan	Hasil Pengujian
1.	*Scanning QR Code* pada SHM.	Aplikasi masuk ke halaman *Scanning*.	Berhasil
2.	Mendapatkan data dari hasil *Scanning*.	Aplikasi Menampilkan data Pemohon atau pemilik SHM.	Berhasil
3.	Dekripsi *QR Code* melalui aplikasi android.	Dekripsi Berupa titik koordinat lokasi Tanah asli Serta Pemilik	Berhasil
4.	Proses Pelabelan *QR Code* terenkripsi *Algoritma RSA* pada dokumen SHM.	Sertifika Hak Milik Tanah telah tersisipi otomatis Kode *QR Code*	Berhasil

PENGUJIAN BLACK BOX

Tabel 4.2 Pengujian Black Box

V. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan uraian permasalahan dan pembahasa pada bab sebelumnya mengenai *"Pengembangan Quick Response Code Pada Pelabelan Dokumen Sertifikat Tanah Menggunakan Kriptografi RSA Berbasis Service",* Maka dapat diambil kesimpulan bahwa :

1. Implementasi *QR Code* yang telah terenkripsi menggunakan *Algoritma RSA* pada pelabelan dokumen SHM *(Sertifikat Hak Milik Tanah)* dapat menjaga keamanan dan kerahasian isi dokumen.
2. Sistem atau Aplikasi yang digunakan dapat mempermudah pihak BPN *(Badan Pertanahan Nasional)*, dalam proses pembuatan dan pengamanan isi dokumen SHM.
3. Sistem atau Aplikasi yang dikembangkan dapat menguji kecurangan akan adanya duplikasi ataupun pemalsuan dokumen SHM, dikarenakan pada proses scanner, jika dokumen tersebut palsu maka identitas pemilik dokumen yang sah tidak akan muncul.

5.2 Saran

Pada penelitian ini masih sangat jauh dari nilai sempurna, penulis menyarankan bagi peneliti selanjutnya agar :

1. Sistem ini dikembangkan lagi dengan menggunakan program bantu yang lebih komplek yaitu *Android Studio.*
2. Pada Sistem ini enkripsi yang diterapkan adalah enkripsi *Algoritma RSA*, dan disarankan untuk lebih memilih enkripsi terbaru lalu dimodifikasi.
3. Pada proses enkripsi *Algoritma RSA*, disarankan kunci/key yang digunakan dinamis dan bilangan-bilangan bernilai besar.

DAFTAR PUSTAKA

Suyanto Agus. 2017. *Pengertian Dokumen-Dokumen Tanah & Cara Melakukan Pembuatan Sertifikat Tanah,* Badan Pertanahan Nasional Kabupaten Lumajang, www.bpn.go.id.

Devha, Canda P. 2013. *Pengamanan Pesan Rahasia Menggunakan Algoritma Kriptografi Rivest Shank Adleman*

(RSA), Universitas Pendidikan Indonesia.

Asmono. 2013. *Pemanfaat Komponen Layer Dalam Sistem Operasi Android,* Universitas Indonesia.

Yusran Paris. 2014. *Pengaruh Pelayanan Bidang Penerbitan Sertifikat Tanah Terhadap Kepuasan Masyarakat Pada Kantor Badan Pertanahan Nasional Kota Makassar,* Yusran Paris/ Jurnal Administrasi Publik, Volume 4 No. 1

Ariadi. (2011). *Analisis dan Perancangan Kode Matriks Dua Dimensi Quick Response (QR) Code.* Skripsi. Universitas Sumatera Utara.

Ashford, Robin. 2010. *QR Code and academic libraries reaching mobile users. (Online)* http://crln.acrl.org/content/71/10/526.full

Bruen, Aiden. A & Forcinito, Mario. A. 2011. *Cryptography, Information Theory, and Error-Correction: A Handbook for the 21st Century*. John Wiley & Sons : Canada.

Edy Winarno. 2009. *Penggunaan XML Database Xindice pada Aplikasi Kriptografi menggunakan Data XML untuk Keamanan Distribusi Data,* Jurnal Teknologi Informasi DINAMIK Volume XIV, No.2.

Bunafit Nugroho. 2004. *PHP dan MySQL dengan editor Dreamweaver MX*. ANDI Yogyakarta, Yogyakarta.

Denso Wave Incorporated. 2013. Answers to your question about the QR Code. (Online) http://www.qrcode.com/en/

Denso ADC. 2011. *QR Code Essentials*. http://www.nacs.org /LinkClick. aspx?fileticket=D1FpVAvvJuo%3D&tabid=1426&mid=4802.

Munir, Rinaldi. 2006. *Kriptografi, Algoritma RSA & ElGamal*. Dapartemen Teknik Informatika, ITB : Bandung.

Savitri, Ayunda W. 2013. *Android kian mengepakkan sayapnya di Indonesia.* Sumber : Okezone.com.

Jurnal Sarjana Teknik Informatika e-ISSN: 2338-5197 Volume 1 Nomor 1,

Pemanfaatan Google Maps Api Untuk Pembangunan Sistem Informasi Manajemen Bantuan Logistik Pasca Bencana Alam Berbasis Mobile Web. Juni 2013.

Wildan, Habibi. 2011. *Undergraduate Thesis Google Maps.* ITS : Surabaya.

Yuhana, Laili Umi. 2010. *Pemanfaatan Google Maps Untuk Pemetaan & Pencarian Data Perguruan Tinggi Negeri Di Indonesi,* ITS : Surabaya.

Abdul, Kadir. 2003. *Pengenalan Sistem Informasi*. ANDI Yogyakarta, Yogyakarta.

Rifki Sadikin. 2012. *Kriptografi untuk Keamanan Jaringan*. Edisi Pertama. Penerbit ANDI, Yogyakarta.

Shodiq, Amri. 2008. *Pemrograman Google Maps API*. ITB : Bandung