PEMANFAATAN TEKNOLOGI QR CODE UNTUK VERIFIKASI ANGGOTA MENGGUNAKAN ALGORITMA ELIPTIK PADA ORGANISASI IPKIN (IKATAN PROFESI KOMPUTER DAN INFORMATIKA INDONESIA)

Meta Eri Safitri

28 April 2015

PEMANFAATAN TEKNOLOGI QR CODE UNTUK VERIFIKASI ANGGOTA MENGGUNAKAN ALGORITMA ELIPTIK PADA ORGANISASI IPKIN (IKATAN PROFESI KOMPUTER DAN INFORMATIKA INDONESIA)

Oleh

META ERI SAFITRI

TESIS

Untuk memenuhi salah satu syarat guna memperoleh gelar
Magister Sistem Informasi pada
Program Pasca Sarjana
Universitas Gunadarma

PROGRAM PASCA SARJANA
UNIVERSITAS GUNADARMA
JAKARTA
2015

Pernyataan Orisinalitas dan Publikasi

Saya yang bertanda tangan di bawah ini:

Nama	:	Meta Eri Safitri
NPM	:	92313085
NIRM	:	92313085
Judul skripsi	:	PEMANFAATAN TEKNOLOGI QR CODE UNTUK VERIFIKASI ANGGOTA MENGGUNAKAN ALGORITMA ELIPTIK PADA ORGANISASI IPKIN (IKATAN PROFESI KOMPUTER DAN INFORMATIKA INDONESIA)
Tanggal Sidang	:	30 April 2015
Tanggal Lulus	:	30 April 2015

menyatakan bahwa tulisan di atas merupakan hasil karya saya sendiri dan dapat dipublikasikan sepenuhnya oleh Universitas Gunadarma. Segala kutipan dalam bentuk apapun telah mengikuti kaidah dan etika yang berlaku. Semua

hak cipta dari logo serta produk yang disebut dalam buku ini adalah milik masing-masing pemegang haknya, kecuali disebutkan lain. Mengenai isi dan tulisan merupakan tanggung jawab Penulis, bukan Universitas Gunadarma.

Demikianlah pernyataan ini dibuat dengan sebenarnya dan dengan penuh kesadaran.

Jakarta, 30 April 2015

(Meta Eri Safitri)

Lembar Pengesahan

Judul Penelitian	:	**PEMANFAATAN TEKNOLOGI QR CODE UNTUK VERIFIKASI ANGGOTA MENGGUNAKAN ALGORITMA ELIPTIK PADA ORGANISASI IPKIN (IKATAN PROFESI KOMPUTER DAN INFORMATIKA INDONESIA)**
Nama Mahasiswa	:	**Meta Eri Safitri**
Nomor Pokok/NIRM	:	**92313085**

Menyetujui

Komisi Pembimbing:

Dr. Asep Juarna, SSi, Mkom (Ketua)

Prof. Dr. Yuhara Sukra, MSc (Anggota)

Program Pasca Sarjana

Prof. Dr. Ir. Bambang Suryawan, MT
(Direktur)

Tanggal Lulus: 30 April 2015

Abstraksi

Meta Eri Safitri. 92313085
PEMANFAATAN TEKNOLOGI QR CODE UNTUK VERIFIKASI ANGGOTA MENGGUNAKAN ALGORITMA ELIPTIK PADA ORGANISASI IPKIN (IKATAN PROFESI KOMPUTER DAN INFORMATIKA INDONE-
SIA).
Skripsi, Fakultas Pasca Sarjana, Jurusan Perangkat Lunak Sistem Informasi, Universitas Gunadarma, 2015.
Kata Kunci: Pendaftaran Online. Verifikasi Menggunakan QR Code, Organisasi IPKIN

(13+ 51+ lampiran)

Quick Response Code atau yang sering disingkat dengan qr code merupakan sebuah barcode dua dimensi yang diperkenalkan oleh Perusahaan Jepang Denso Wave pada tahun 1994. Jenis barcode ini awalnya digunakan untuk melacak persediaan di bagian manufaktur kendaraan dan sekarang sudah digunakan dalam berbagai industri perdagangan dan jasa. Saat ini, untuk penggunaan qr code telah banyak diimplementasikan dalam bentuk aplikasi qr code Reader dan qr code Generator, sehingga seseorang akan sangat mudah untuk membuat informasi dalam bentuk qr code dan mendapatkan informasi yang ingin diketahuinya, hanya dengan melakukan proses scanning dan pemindaian data melalui media dari kamera handphone (Anastasia, Istiadi, dan Hidayat, 2010).

Aplikasi pendaftaran online Organisasi IPKIN (Ikatan Profesi Komputer dan Informatika Indonesia) penulis akan mengimplementasikan model verifikasi dengan menggunakan qr code untuk kegiatan yang diselenggarakan oleh organisasi terkait. Dengan demikian, fisik dari surat atau dokumen tersebut dapat dienkripsi terlebih dahulu selanjutnya diberi digital signature. Melalui cara ini, dokumen tidak hanya dapat diamankan tetapi juga dapat menunjang terhadap administrasi keaslian dokumen pada saat verifikasi yang langsung terhubung dengan database. Daftar Pustaka (2007-2012)

Abstract

Meta Eri Safitri. 92313085
USE OF TECHNOLOGY QR CODE FOR MEMBERS VERIFICATION USING ELLIPTIC ALGORITHM THE ORGANIZATION IPKIN (IKATAN PROFESI KOMPUTER DAN INFORMATIKA).
Bachelor thesis, Fakultas Pasca Sarjana, Jurusan Perangkat Lunak Sistem Informasi, Universitas Gunadarma, 2015.
Keyword: Online Registration. Verification Using QR Code, Organization IPKIN

(13+ 51+ appendix)

Quick Response Code or often abbreviated with a qr code is a twodimensional barcode which was introduced by the Japanese company Denso Wave in 1994. This barcode type originally used to track inventory in the manufacturing of vehicles and is now used in various industrial trades and services. Currently, for the use of the qr code has been widely implemented in the application form and qr code Reader qr code Generator, so that someone will be very easy to make the information in the form of a qr code and get the information you want to know, just to make the process of scanning and scanning data through the media from a camera phone (Anastasia, Istiadi, and Hidayat, 2010).

Online registration application IPKIN Organization (Professional Association of Computer and Information Indonesia) authors will implement the model verification by using the qr code to activities organized by related organizations. Thus, the physical of letters or documents can subsequently be encrypted first digital signature. Through this way, the document can not only be secured, but also to support the administration of the authenticity of the document at the time of verification that is directly connected to the database.

References (2007-2012)

Riwayat Hidup

Penulis dilahirkan di Bandar Lampung pada tanggal 23 April 1991 dengan nama Meta Eri Safitri dari ayah yang bernama M. Trio Cahyono dan ibu Erna Sofia, NS dan merupakan anak pertama dari dua bersaudara. Penulis menyelesaikan pendidikan Sekolah Dasar di SDN 2 Rawalaut pada tahun 2003. Kemudian melanjutkan pendidikan di SLTPN 4 B. Lampung dan lulus pada tahun 2006. Penulis melanjutkan pendidikannya di SMA Al – Kautsar B. Lampung dan lulus pada tahun 2009. Setelah tamat SMA, penulis melanjutkan pendidikan S1 Fakultas Ilmu Komunikasi dan Teknologi Informasi di Universitas Gunadarma Depok, Informatika kemudian lulus pada tanggal 09 November 2013 dengan gelar Sarjana Komputer. Selama masa perkuliahan, penulis aktif sebagai asisten di Laboratorium Sistem Informasi dan Paduan Suara Swaradarmagita Universitas Gunadarma. Pada bulan Oktober tahun 2013, penulis melanjutkan pendidikannya ke jenjang Pasca Sarjana Jurusan Perangkat Lunak Sistem Informasi di Universitas Gunadarma Depok dan sejak Maret 2014 aktif sebagai dosen di Universitas Gunadarma sampai saat ini.

Kata Pengantar

Assalamualaikum Wr, Wb.

Segala puji dan syukur penulis panjatkan kehadirat ALLAH SWT yang telah melimpahkan rahmat dan karunia-NYA, serta kepada junjungan kita Nabi besar Muhammad SAW, sehingga penulis dapat menyelesaikan Tugas Akhir ini yang bertujuan untuk membuat dan memahami tentang verifikasi dokumen; Adapun penulisan ini disusun untuk melengkapi syarat program jenjang Pasca Sarjana pada jurusan Manajemen Sistem Informasi, Fakultas Ilmu Komputer dan Teknologi Informasi Universitas Gunadarma.

Penulis menyadari bahwa penyusunan Tugas Akhir ini tidak lepas dari bantuan semua pihak yang telah memberikan bantuan, baik moril maupun materil hingga selesainya penulisan ini. Pada kesempatan ini penulis mengucapkan terima kasih yang sebesar-besarnya kepada semua pihak yang telah membantu dalam menyelesaikan penulisan ini, terutama kepada:

1. Ibu Prof. Dr. E.S. Margianti, SE. MM, selaku Rektor Universitas Gunadarma.
2. Bapak Prof. Dr. Ir. Bambang Suryawan MT, selaku Direktur ProgramPasca Sarjana Universitas Gunadarma.
3. Bapak Dr. rer. nat. I Made Wiryana, SKom, SSi, MAppSc, selakuKetua Komisi Pembimbing Penulisan Tugas Akhir Jurusan Manajemen Sistem Informasi.
4. Bapak Dr. Asep Juarna, SSi, Mkom selaku dosen pembimbing yang selalu meluangkan waktu, tenaga dan ilmunya untuk membimbing penulis dari awal pengerjaan hingga terselesainya penulisan ini.
5. Ibu Anthi Hasibuan, yang telah menjadi orangtua kedua selama menempuh pendidikan pasca ini, atas segala kasih sayang, motivasi dan bimbingannya bagi penulis.

6. Suamiku tercinta, terkasih dan tersayang Aditya Irham dan Calon Anakkami yang selalu membuat semangat dalam penulisan dan selalu menjadi penghibur disaat lelah.
7. Kedua Orang Tuaku, bapak Rio dan mami Erna, Mertuaku bapak onodan ibu etty, serta adikku M. Andika Wicaksono, Gitra taufiq dan Ridwan Budiman, serta sodara - sodara terdekat yang telah memberikan perhatian, penghiburan, dukungan dan doa yang tak terukur selama ini.
8. Semua Staf Dosen Universitas Gunadarma yang telah memberikan bekalilmu kepada penulis.
9. Tim di UGBBSDM Mami rence, ka Andreas, ka Tresna, ka Junaedi(guru), ka Bayu, ka Evans, ka Mara, ka Iman, ka Andre, ka Ovan, Astie, Lulu, Keke, Saarah fadilah, temen – temen FT2, temen – temen FT3 atas motivasinya yang sangat berharga selama menempuh pasca sarjana ini.
10. Teman-teman alumni kelas 4KA08 angkatan 2009 serta semua mahasiswa/ i jurusan Sistem Komputer, Manajemen Informatika dan Teknik Informatika, Universitas Gunadarma.

Dengan segala kerendahan hati, penulis menyadari bahwa masih banyak terdapat kekurangan dalam penulisan dan penyusunan Tugas Akhir dan juga penulisan Tugas Akhir ini masih jauh dari kesempurnaan, untuk itu penulis mengharapkan kritik dan saran yang bersifat membangun demi sempurnanya penulisan ini. Akhirnya penulis berharap semoga tulisan ini bermanfaat bagi diri pribadi penulis maupun para pembaca.

Jakarta, April 2015

Penulis

Daftar Isi

Daftar Gambar

Daftar Tabel

Bab 1

Pengantar

1.1 Latar Belakang Masalah

Model verifikasi dokumen saat ini sangat berkembang pesat, verifikasi dokumen digunakan untuk memastikan keaslian sebuah berkas yang berbentuk sebuah data dan gambar, serta untuk membuktikan siapa pemilik yang sah atas dokumen tersebut. Verifikasi dapat dilakukan dengan beberapa cara. Misalnya text integrity verification pada dokumen yang dikirim melalui fax, menggunakan teknik pixel reorganizing dengan memanfaatkan kamera untuk mengambil citra dokumen yang diperkenalkan (Pramoun & Amornraksa, 2013).

Model verifikasi dokumen ini tidak hanya meguntungkan satu pihak saja, tapi membantu kedua belah pihak dalam pembangunan dan keberhasilannya seperti yang akan penulis implementasikan kedalam sistem pendaftaran online Organisasi IPKIN. Model verifikasi anggota digunakan untuk menvalidasi data keanggotan pada saatn kegiatan IPKIN. IPKIN adalah sebuah organisasi yang berdiri pada tahun 1974 didirikanlah organisasi Ikatan Pengguna Komputer Indonesia yang merupakan organisasi nirlaba independent yang beranggotakan para profesional dalam bidang Komputer dan Informatika. IPKIN bertujuan untuk meningkatkan pemanfaatan dan pengembangan teknologi Komputer dan Informatika di Indonesia guna menunjang Pembangunan Nasional. Untuk itu IPKIN berupaya berperan sebagap wadah komunikasi, konsultasi dan koordinasi antar anggota. Pada pengembangan sistem ini penulis akan menggunakan Quick Response (QR) Code pada tahap verifikasi dokumen. Quick Response (QR) Code adalah suatu jenis kode matriks atau kode batang dua dimensi yang dikembangkan oleh Denso Wave, sebuah divisi Denso Corporation yang merupakan sebuah perusahaan Jepang dan dipublikasikan pada tahun 1994. Pada dasarnya bahwa qr code dikembangkan sebagai suatu ko-

de yang memungkinkan isinya untuk dapat diterjemahkan dengan kecepatan tinggi (Rouillard, 2008).

Dari paparan di atas, keaslian dari sebuah dokumen itu sangat penting karena pemalsuan dan manipulasi dokumen dapat menyebabkan kerugian yang signifikan dilihat dari segi kepercayaan dengan relasi, serta keabsahan sebuah dokumen fisik. Pemalsuan yang biasa dilakukan terbagi menjadi dua jenis pemalsuan dengan menerbitkan dokumen serupa, dan pemalsuan dengan menggunakan pemindai dan printer dari sebuah dokumen asli (Beusekom & Shafait, 2011). Pada model verifikiasi dokumen pada ipkin tanda tangan digital (digital signature) akan dikonversikan dalam model Quick Response (QR) Code dari nilai hasil enkripsi digital signature dengan metode kurva eliptik, dan barcode ini akan dibaca kembali oleh Quick Response (QR) Code reader dengan menterjemahkan informasi yang ada pada Quick Response (QR) Code menjadi informasi yang dapat membuktikan keaslian data anggota pada saat kegiatan
IPKIN sepertit pertemuan, conference ataupun seminar yang diselenggarakan.

1.2 Rumusan Masalah

Beberapa masalah yang diangkat sehubungan dengan uraian di atas sebagai berikut:

Bagaimana merancang pengamanan dokumen dengan menggunakan digital signature dan algoritma kurva eliptik pada model verifikasi dokumen pada IPKIN ?

Bagaimana membuat sistem pendaftaran online dengan output Quick Response (QR) Code yang berfungsi pada model verifikasi dokumen pada IPKIN?

Bagaimana keberhasilan model verifikasi pada mobile menggunakan Quick Response (QR) Code pada IPKIN ?

Bagaimana performa dari model verifikasi dokumen Quick Response (QR) Code pada IPKIN?

1.3 Batasan Masalah

Sistem verifikasi dokumen merupakan sebuah penelitian dengan cakupan yang luas, untuk itu perlu ditetapkan sejumlah batasan masalah dan asumsi, antara lain:

Studi kasus pada sistem informasi untuk Organisasi IPKIN di desain dengan pengamanan berkas elektronik dengan menggunakan tanda tangan digital (digital signature) dan menggunakan algoritma kurva eliptik.

Perancangan sistem pendaftaran online ditujukan kepada anggota baru atau anggota lama dalam perpanjangan anggota.

Perancangan model verifikasi pada mobile digunakan oleh panitia yang ditugaskan untuk sistem absensi yang diselenggarakan IPKIN untuk mengkoreksi.

Aplikasi mobile verification akan berjalan hanya pada saat admin yang diperintahkan menggunakan aplikasi mobile verikasi pada sistem absensi kegiatan IPKIN yang berlangsung.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah merancang sebuah sistem pendaftaran online berbasis web dengan pemanfaatan Quick Response (QR) Code sebagai output dari kartu member yang akan diicetak setiap anggota yang dapat digunakan untuk verifikasi dokumen dengan algoritma eliptik pada kegiatan yang diselenggarakan oleh IPKIN (Ikatan Profesi Komputer dan Informatika Indonesia) dengan menggunakan *mobile verification*.

1.5 Metode Penelitian

Dalam penelitian ini penulis menggunakan beberapa metodologi sebagai berikut:

1. Studi Pustaka

Penulis melakukan studi kepustakaan yaitu dengan cara mengumpulkan dan membaca literatur - literatur dan jurnal dari internet serta buku buku yang relevan dengan penulisan tugas akhir ini.

2. Diskusi

   Berdiskusi dengan dosen pembimbing dan nara sumber lain berkaitan dengan proses pengerjaan dan penyelesaian setiap masalah - masalah yang ditemukan selama proses penyusunan tugas akhir berlangsung.

1.5. Metode Penelitian

3. Perancangan

   Pembuatan perancangan web dan model verifikasi dokumen pada mobile dengan mengimplemntasikan algoritma eliptik.

4. Implementasi

   Penerapan model verifikasi pada website dan mobile.

5. Uji Coba

   Menguji model verifikasi anggota yang telah terdaftar dan mengukur seberapa besar keberhasilan model verifikasi dengan kesensitifan *qr code*.

Bab 2

Tinjauan Pustaka

2.1 Organisasi IPKIN (Ikatan Profesi Komputer dan Informatika Indonesia)

IPKIN Pada perkembangannya, teknologi mengalami kemjuan dengan cepat. Tentunya di setiap Negara mempunyai teknologi yang baik. Di Indonesia pun kemajuan teknologinya sudah baik, kemajuan teknologi melahirkan berbagai macam organisasi yang mempunyai hubngan dengan dunia teknologi salah satunya yang lahir adalah IPKIN Sekilas tentang sejarah IPKIN Organisasi ikatan pengguna komputer Indonesia yang di kenal dengan sebutan IPKIN berdiri sejak tahun 1974 Dengan berjalannya waktu organisai ini berganti nama menjadi ikatan profesi computer dan informatika Indonesia.

2.1.1 Keanggotaan IPKIN

Anggota IPKIN terdiri dari berberapa golongan, anggota ini digolongkan berdasarkan kriteria tersendiri. Berikut adalah keanggotaan dari IPKIN:

1. Anggota Biasa (Pendidikan Formal/Non Formal).
2. Anggota Muda (Hobi).
3. Anggota Kehormatan.
4. Anggota Perusahaan.

2.1.2 Tata Organisasi IPKIN

Setiap organisasi harus memiliki tata organisasi yang baik, agar organisasi ini dapat berjalan dengan baik dan mencapai tujuan bersama. disetiap organisasi memiliki tata organisasi yang berbeda-beda sesuai dengan kebutuhan dan jenis organisasi tersebut. Begitu pula dalam organisasi IPKIN, dibawah ini merupakan tata organisasi dalam IPKIN:

1. Rapat Anggota (pemegang kekuasaan tertinggi).
2. Dewan Pengurus (D.Pembina, D.Pengurus Pusat/cabang/harian).
3. Dewan Pengurus .
4. Ketua - Pemimpin IPKIN merupakan penanggung jawab umum ataspelaksanaan dan jalannya IPKIN.
5. Sekretaris Jendral - Pusat koordinasi dalam pengaturan ketatausahaanserta kegiatan kesekretariatan, dokumentasi.
6. Ketua Bidang (Tekhnologi, Pembinaan, Program, Pendidikan dan Latihan).

2.1.3 Kegiatan yang di selenggarakan oleh IPKIN

Berikut adalah kegiatan yang dilakukan oleh IPKIN:

1. Menyelenggarakan Kegiatan Ilmiah spt pendidikan, latihan, seminar, diskusi, yang berhubungan dengan komputer dan informatika.
2. Menghimpun, mengelola dan mengembangkan bahan kepustakaan.
3. Menerbitkan buletin IPKIN, buku, jurnal profesi.
4. Mengadakan kerja sama dgn organisasi sejenis.
5. Menyelenggarakan usaha lain yg dianggap perlu oleh IPKIN dan tidakbertentanga dgn AD/ART.

2.2 Tinjauan Pustaka

Menurut (Rinaldi Munir, 2006), Integritas berkas perangkat lunak berkaitan dengan keaslian berkas program, keutuhan, dan keabsahan pengembang perangkat lunak sangat rentan pada transaksi di internet. Berkas program dapat

dimodifikasi oleh pihak ketiga (menjadi tidak asli) atau mengalami kerusakan (corrupt) oleh virus atau gangguan selama transmisi dari komputer server ke komputer client (menjadi tidak utuh). Selain itu, pengguna perangkat lunak perlu memastikan bahwa program yang ia download dibuat oleh pengembang program yang sah, dan bukan pengembang lain yang menyamar sebagai pengembang program yang asli. Masalah integritas berkas perangkat lunak ini dapat diselesaikan dengan menggunakan tanda tangan digital. Tanda tangan digital dibangkitkan dengan algoritma kriptografi kunci-publik. Tanda tangan digital bergantung pada isi berkas program dan kunci pengembang perangkat lunak. Melalui proses verifikasi, pengguna dapat membuktikan integritas berkas perangkat lunak yang ia downlaod dari situs web pengembang.

(Chao-Yong Hsu dan Chun-Shien Lu, 2005) meneliti tentang perbedaan berbagai model tipe kompresi terhadap kualitas warna dan mencari warna yang paling efektif untuk watermarking. Percobaan yang dilakukan dengan mengambil sebuah gambar dan melakukan manipulasi pada gambar tersebut dengan metode memberikan tekanan pada halftone warna serta kualitas resolusi dan menghasilkan beberapa model gambar yang telah di modifikasi. Hasil dari modifikasi kemudian di analisis.

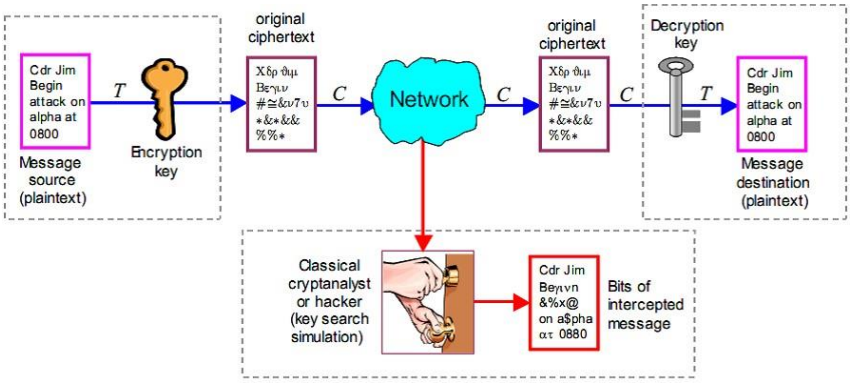
(El-Affendi, 2008) yaitu penerapan watermarking untuk mengamankan tanda tangan fisik yang disertai dengan stempel dalam aplikasi e-government. Setiap berkas/surat elektronik yang telah ditanda tangani oleh pihak yang berwenang dan distempel, pada setiap tanda tangan dan stempelnya diselipkan kriptografi watermarking. Setiap dokumen dikirim bersamaan dengan contoh hasil tanda tangan dan stempel fisik yang tidak disandikan dengan watermarking yang berfungsi sebagai pembanding dari tandatang dan stempel pada dokumen yang telah di enkripsi dengan algoritma tertentu.

(Don Johnson dan Alfred Menezes, 2001) mencoba menganalisis kelebihan dari model Elliptic Curve Digital Signature Algorithm (ECDSA), dari beberapa perbandingan parameter dengan persamaan diskrit biasa akan didapat beberapa kemudahan dalam faktorisasi. Selain itu keamanan yang tinggi serta implementasi yang mudah menjadikan algoritma ini bisa dijadikan dalam satu model algoritma pada digital signature yang handal.

2.3 Konsep Kriptografi

Kriptografi klasik yang mulai digunakan dari jaman Yunani kuno seperti oleh raja Julius Caesar, menggunakan metode subtitusi yang paling sederhana yaitu Caesar cipher. Kriptografi klasik lain yang digunakan oleh raja Yunani kuno menggunakan Scytale terdiri dari sebuah kertas panjang dari daun papyrus yang dililitkan pada sebuah silinder dengan diameter tertentu (diameter silender menyatakan kunci penyandian), dan masih banyak kriptografi klasik lainnya.

Kriptografi pada abad modern menggunakan matematika untuk melakukan enkripsi dan dekripsi. Data teks asli yang dapat dibaca atau dipahami disebut plaintext. Metode penyandian teks asli dengan menggunakan kunci sebagai informasi tambahan sedemikian hingga isi data aslinya tersembunyi disebut enkripsi. Enkripsi digunakan untuk menyembunyikan informasi dari orang yang tidak dikehendaki. Data hasil enkripsi disebut ciphertext. Proses mengembalikan ciphertext menjadi plaintext disebut dekripsi atau de-enkripsi seperti yang dijelaskan pada gambar 2.1.



Gambar 2.1: Konsep Dasar Proses Enkripsi dan Dekripsi

Kriptografi dibagi menjadi dua golongan besar yaitu kriptografi kunci simetris (symmetric-key cryptography) dan kriptografi kunci asimetris (asymmetric-key cryptography).

2.3.1 *Symmetric Algorithms*

Algoritma kriptografi simetris atau disebut juga algoritma kriptografi konvensional adalah algoritma yang menggunakan kunci untuk proses

enkripsi sama dengan kunci untuk proses dekripsi. Algoritma kriptografi simetris dibagi menjadi 2 kategori yaitu algoritma aliran (Stream Ciphers) dan algoritma blok (Block Ciphers). Pada algoritma aliran, proses penyandiannya berorientasi pada satu bit atau satu byte data. Sedang pada algoritma blok, proses penyandiannya berorientasi pada sekumpulan bit atau byte data (per blok).

Contoh algoritma kunci simetris yang terkenal adalah DES (Data Encryption Standard).

2.3.2 *Asymmetric Algorithms*

Algoritma kriptografi asimetrik adalah algoritma yang menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsinya. Algoritma ini disebut juga algoritma kunci umum (public key algorithm) karena kunci untuk enkripsi dibuat umum (public key) atau dapat diketahui oleh setiap orang, tapi kunci untuk dekripsi hanya diketahui oleh orang yang berwenang mengetahui data yang disandikan atau sering disebut kunci pribadi (private key). Contoh algoritma terkenal yang menggunakan kunci asimetris adalah RSA dan ECC.

2.3.3 Aspek-aspek Keamanan pada Kriptografi

Inti dari kriptografi adalah menjaga kerahasiaan plaintext atau kunci dari penyadapan. Penyadap berusaha mendapatkan data yang digunakan untuk kegiatan pencurian data atau biasa disebut kriptanalisis (cryptanalysis). Kriptanalisis bertujuan untuk memecahkan cipherteks menjadi plainteks semula tanpa memiliki akses ke kunci yang digunakan hingga berhasil menemukan kelemahan dari sistem kriptografi yang pada akhirnya mengarah untuk menemukan kunci dan mengungkap plainteks. Aspek-aspek yang diamankan pada sistem kriptografi agar sistem dapat berjalan sempurna menurut (Dony Ariyus, 2006) ada delapan aspek yang perlu diperhatikan antara lain:

1. Authentifikasi: agar penerima informasi dapat memastikan pesan tersebut datang dari orang yang dimintai informasi, dengan kata lain informasi tersebut benar-benar datang dari orang yang dikehendaki.

2. Integrity: keaslian pesan yang dikirim melalui sebuah jaringan dan dapatdipastikan bahwa informasi yang dikirim tidak dimodifikasi oleh orang lain yang tidak berhak dalam perjalanan informasi tersebut.

3. Nonrepudiation: menyatakan pesan yang dikirim dari orang yang asli, artinya si pengirim pesan tidak dapat mengelak bahwa dialah yang mengirimkan informasi tersebut.

4. Authority: informasi yang berada pada sistem jaringan tidak dapat dimodifikasi oleh pihak yang tidak berhak atas akses tersebut.
5. Confidentiality: merupakan usaha untuk menjaga informasi dari orangyang tidak berhak mengakses.

6. Privacy: merupakan data-data yang sifatnya rahasia dan tidak bolehdiketahui oleh pihak lain.

7. Availability: Sistem yang diserang atau di jebol dapat menghambat ataumeniadakan akses ke informasi.

8. Access Control: Aspek ini berhubungan dengan cara pengaturan siapasiapa saja yang berhak mengakses sistem, mengetahui sistem keamanannya.

2.3.4 Teori Bilangan Modulo

Pada proses pembangkitan kunci pada kurva eliptik terdapat operator modulo. Aritmatika modulo merupakan salah satu dari teori bilangan bulat yang penting yang digunakan untuk perhitungan bilangan bulat pada kurva ellipstik. Adapun fungsi modulo didefinisikan sebagai berikut:

1. Misalkan a adalah bilangan bulat, dan m bilangan bulat > 0. Operasi a mod m memberikan sisa jika a dibagi dengan m.

2. a mod m dibaca 'a modulo m'

3. notasi a mod $m = r$ sehingga $a = mq + r$, dengan $0 \leq r < m$.

4. m disebut modulus atau modulo, dan hasil modulo m terletak di dalamhimpunan$0,1,2,...,m + 1$

Contoh dari fungsi modulo misalnya 23*...mod...*5 = 3,27*...mod...*3 = 0*.*

Untuk dua buah bilangan*a* dan *b* yang berbeda, bisa saja memiliki sisa yang sama jika dibagi dengan bilangan positif m. Hal ini bisa disebut bahwa *a* dan*b* kongruen dalam modulo m, yang dilambangkan dengan *a* ≡ *b*(*mod...m*).

Misalnya 38*...mod...*5 dan13*...mod...*5, hasil dari dua operasi tersebut adalah 3. Maka dapat dikatakan 38 ≡ 13(*mod...*5).

2.3.5 Teori Bilangan Prima

Pada proses pembangkitan kunci pada kurva eliptik terdapat bilangan prima. Bilangan prima adalah bilangan integer positif, $p > 1$ adalah prima jika hanya dapat dibagi oleh 1 dan p (bilangan prima itu sendiri). Karena bilangan prima harus lebih besar dari 1, maka barisan bilangan prima dimulai dari 2, yaitu 2,3,5,7,11,13,.... Seluruh bilangan prima adalah bilangan ganjil kecuali 2.

Bilangan selain prima disebut bilangan komposit. Misal 20 adalah bilangan komposit karena 20 dapat dibagi oleh 2,4,5 dan 10 selain 1 dan 20 sendiri.

Menurut (Stalling, 2004) Dua buah bilangan bulat a dan p dikatakan relatif prima/koprima (coprime) jika faktor persekutuan terbesar (*FPB*)(*a,p*) = 1. Sehingga jika a dan b relatif prima, maka terdapat bilangan bulat m dan n sedemikian. Sehingga ma + nb = 1. Contoh: Bilangan 20 dan 3 adalah relatif prima karena *PBB*(20,3) = 1, atau dapat ditulis 2.20 + (−13).3 = 1

2.3.6 Fungsi HASH

Dalam peneltian ini digunakannya fungsi Hash untuk menentukan string yang berukuran apapun diubah menjadi message digest dengan bit yang konstan. Secara sederhana fungsi hash ditujukan untuk pengalamatan record di memori.

Bentuk dari fungsi hash adalah sebagai berikut:

$$h(k) = k \bmod m$$

dengan k adalah kunci bilangan bulat dan m adalah jumlah lokasi memori yang tersedia. Sedangkan hasilnya h(k) adalah lokasi memori untuk record dengan kunci k. (Munir, 2005).

Contoh: m = 11 mempunyai sel+sel memori yang diberi indeks 0 sampai 10. Akan disimpan data record yang masing+masing mempunyai kunci 15,558,32,132,102, dan 5.

Maka:

$h(15) = 15 \text{ mod } 11 = 4$ $h(558) = 558 \text{ mod } 11 = 8$ $h(32) = 32 \text{ mod } 11 = 10$ $h(132) = 132 \text{ mod } 11 = 0$ $h(102) = 102 \text{ mod } 11 = 3$ $h(5) = 5 \text{ mod } 11 = 5$

Penempatan record pada memori dengan fungsi hash menjadi:

132			102	15	5			32		558
0	1	2	3	4	5	6	7	8	9	10

Fungsi hash sering juga disebut sebagai cryptographic checksum karena bisa digunakan untuk mentransformasi masukan string dengan panjang sembarang menjadi sebuah string lain dengan panjang tetap. Hasil dari transformasi tersebut biasanya berukuran lebih pendek dibanding string masukannya. Hasil transformasi ini disebut juga nilai hash atau message digest. Jika dituliskan dalam notasi matematis akan jadi seperti:

$$MD = Hash(M)$$

dengan MD adalah message digest, dan M adalah string masukan.

Oleh fungsi hash sebuah string yang berukuran apapun diubah menjadi message digest yang berukuran tetap (128+512 bit). Adapun sifat+sifat yang dimiliki oleh fungsi hash adalah sebagai berikut:

Fungsi H dapat diterapkan pada blok data yang berukuran berapa saja.

Nilai hash yang dihasilkan memiliki panjang yang tetap.

Untuk setiap h yang diberikan, tidak mungkin menemukan suatu x sedemikian sehingga $H(x) = h$. Fungsi H tidak dapat mengembalikan nilai hash menjadi masukan awal.

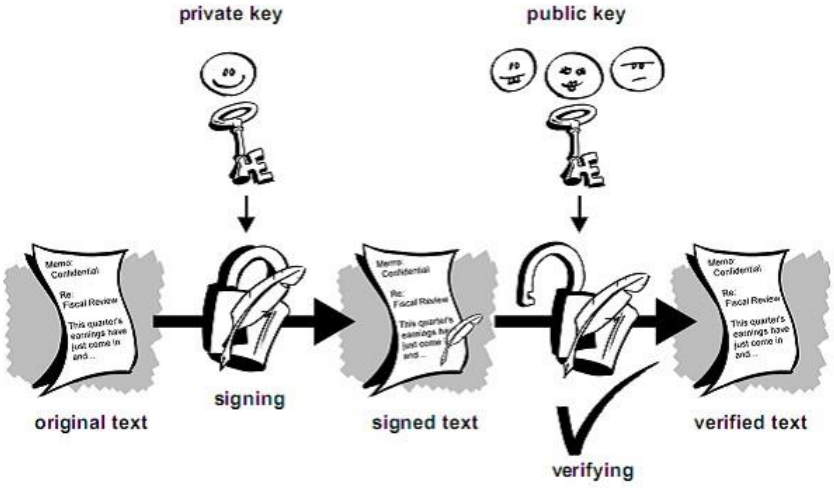
Untuk setiap x yang diberikan, tidak mungkin mencari pasangan x 6= y sedemikian sehingga $H(x) = H(y)$.

2.4 *Digital Signature*

Tanda tangan digital (*Digital Signature*) adalah suatu mekanisme untuk menggantikan tanda tangan secara manual pada dokumen kertas. Yang dimaksud dengan tanda tangan digital menurut (Rinaldi Munir, 2005) bukanlah tanda tangan yang di-digitalisasi dengan alat scanner, tetapi suatu nilai kriptografis yang bergantung pada pesan dan pengirim pesan. Kegunaan tanda tangan digital adalah menyatakan pengesahan (data integrity) atas apa yang tercatum dalam dokumen tersebut, dan menyatakan pertanggung

jawaban penandatangan (data originality) atas apa yang tertulis dalam dokumen tersebut, serta untuk mencegah satu saat penandatangan mengingkari apa yang tertulis didokumen bertanda tangan (non repudiation).

Adapun aspek keamanan kerahasiaan (confidentality) bukan disediakan dengan sistem tanda tangan digital, tetapi tanda tangan yang telah dienkripsikan terlebih dahulu dan menghasilkan sebuah publick key serta tanda tangan dengan algoritma tertentu. Jika Digital Signature yang telah di enkripsi menggunakan kunci publik X, maka pada proses mendeskripsikan kembali dengan kunci pribadi X. Tidak akan terbuka dengan kunci pribadi Y seperti pada gambar 2.2



Gambar 2.2: Proses Pengabsahan Pada Tanda Tangan Digital.

Penandatanganan pesan dengan cara mengenkripsikannya selalu memberikan dua fungsi berbeda, yaitu kerahasiaan pesan dan otentifikasi. Pada beberapa kasus, seringkali otentifikasi yang diperlukan tetapi kerahasiaan tidak. Maksudnya pesan tidak perlu dienkripsikan, sebab yang diperlukan hanya otentikasi saja.

Hanya sistem kriptografi kunci publik yang cocok dan alami untuk pemberian tanda tangan digital dengan menggunakan fungsi hash. Hal ini karena disebabkan karena skema tanda tangan digital berbasis sistem kunci publik dapat menyediakan masalah non-repudiation (baik penerima dan pengirim pesan mempunyai pasangan kunci masing-masing).

Teknik yang umum digunakan untuk membentuk tanda tangan digital adalah dengan fungsi hash dan melibatkan algoritma kriptografi kunci-publik. Mula-mula pesan M ditransformasi oleh fungsi hash H menjadi pesan ringkas

h. Pesan ringkas tersebut dienkripsi dengan kunci private (PK) pengirim pesan:

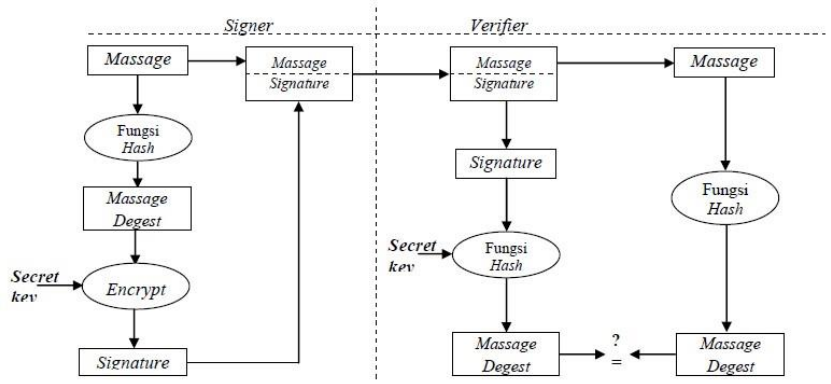
$S = ESK(h)$. Hasil enkripsi (S) inilah yang disebut tanda-tangan digital. Tanda-tangan digital dapat ditambahkan pada pesan atau terpisah dari pesan dan dikirim secara bersamaan. Di tempat penerima, tanda tangan diverifikasi untuk dibuktikan keotentikannya dengan cara berikut:

1. Tanda tangan digital S didekripsi dengan menggunakan kunci publik(PK) pengirim pesan, menghasilkan pesan-ringkas semula, h, sebagai berikut: $h = DPK(S)$

2. Pengirim kemudian mengubah pesan *M* menjadi pesan ringkas *h*' dengan menggunakan fungsi hash satu-arah yang sama dengan fungsi hash yang digunakan oleh pengirim.

3. Jika *h*' = *h*, berarti tanda-tangan yang diterima otentik dan berasal dari pengirim yang benar.

Gambar 2.3 memperlihatkan proses pembangkitan tanda tangan digital (signing) dan verifikasi tanda tangan digital (verivying).



Gambar 2.3: Otentifikasi Dengan Tanda Tangan Digital

Otentikasi pesan dapat dijelaskan sebagai berikut:

1. Apabila pesan *M* yang diterima sudah berubah, maka *h*' yang dihasilkan dari fungsi hash berbeda dengan h semula. Ini berarti pesan tidak asli lagi.

2. Apabila pesan *M* tidak berasal dari orang yang sebenarnya, maka *h* yang dihasilkan berbeda dengan *h*' yang dihasilkan pada proses verifikasi (hal

ini karena kunci publik yang digunakan oleh penerima pesan tidak berkoresponden dengan kunci privat pengirim).

3. Bila $h = h'$, ini berarti pesan yang diterima adalah pesan yang asli dan orang yang mengirim adalah orang yang sebenarnya.

Beberapa parameter dasar pada Digital Standard Algorithm (DSA) (Munir, 2005) seperti berikut ini:

1. p, adalah bilangan prima dengan panjang L bit, yang dalam hal ini$512 < L < 1024$ dan L harus kelipatan 64. Parameter p bersifat publik dan dapat digunakan bersama-sama oleh orang di dalam kelompok.
2. q, bilangan prima 160 bit, merupakan faktor dari $p-1$. Dengan kata lain, $(p-1) mod ... q = 0$. Parameter q berisfat publik.
3. $g = h^{(p-1)/q} \bmod p$, yang dalam hal ini $h < p-1$ sedemikian sehingga $h^{(p-1)/q} \bmod p > 1$. Parameter g bersifat publik.
4. x adalah bilangan bulat kurang dari q. Parameter x adalah kunci rahasia.
5. $y = g^X mod ... p$, adalah kunci publik.
6. m, pesan yang akan diberi tanda tangan.

Proses pembangkitan sepasang kunci adalah sebagai berikut:

1. Pilih bilangan prima p dan q, yang dalam hal ini $(p - 1) \bmod q = 0$.
2. Hitung $g = h^{(p-1)/q} \bmod p$, yang dalam hal ini $1 < h < p - 1$ dan $h^{(p-1)/q} \bmod p > 1$.
3. Tentukan kunci rahasia x, yang dalam hal ini $x < q$.
4. Hitung kunci publik $y = g^x \bmod p$.

Prosedur di atas menghasilkan:

1. Kunci publik dinyatakan sebagai (p,q,g,y)
2. Kunci private dinyatakan sebagai (p,q,g,x)

Prosedur pembangkitan tanda tangan (Signing):

1. Ubah pesan m menjadi massage digest dengan fungsi hash *SHA,H.*

2. Tentukan bilangan acak$k < q$.
3. Tanda tangan dari pesan m adalah bilangan r dan s. Hitunglah r dan s sebagai berikut:

   $r = (g^k mod...p) mod...q \quad s =$

   $(k^{-1}(H(m) + x * r)) mod...q$

4. Kirimkan pesan m beserta tanda tangan r dan s.

Prosedur verifikasi keabsahan tanda tangan (Verifing):

1. Hitung$w = s^{-1} mod...q \; u1 = (H(m) * w) mod...q \; u2 = (r *$

   $w) mod...q \; v = ((q^{u1} * y^{u2}) mod...p) mod...q)$

2. Jika v = r, maka tanda tangan sah, yang berarti bahwa pesan masih aslidan dikirim oleh pengirim yang benar.

2.4.1 Algoritma Tanda Tangan Digital Kurva Eliptik

Kriptosistem kurva eliptik (*Elliptic Curves Cryptosystem*) di perkenalkan oleh Neil Koblitz dan Viktor Miller pada tahun 1985 yang menggunakan masalah logaritma diskrit pada titik-titk kurva eliptik yang disebut dengan ECDLP (*Elliptic Curves Discrete Logarithm Problem*) (www.wikipedia.org). Kriptosistem kurva eliptik ini dapat digunakan pada beberepa keperluan antara lain Skeme enkripsi (ElGamal ECC) dan Tanda tangan digital (*ECDSA–Elliptic Curves Digital Signature*).

Pada tanda tangan digital, pendekatan yang dilakukan untuk menghasilkan algoritma kurva eliptik adalah dengan meggunakan struktur matematika yang sangat unik yang memungkinkan memrosesan titik dengan memiliki dua buah titik dalam sebuah kurva eliptik dan menghasilkan sebuah titik lain yang ada pada kurva tersebut. Struktur yang unik ini memberikan keuntungan dalam kriptografi dikarenakan kesulitan untuk menemukan 2 buah titik yang menentukan sebuah titik tertentu tersebut tidak dapat ditemukan dengan mudah. Tingkat kesulitan untuk menemukan 2 buah titik termasuk dalam golongan yang rumit sama seperti kesulitan untuk memperhitungkan variasi

eksponensial yang digunakan dalam algoritma RSA yang telah banyak diimplementasikan. Sehingga tanda tangan digital dengan algoritma kurva eliptik ini lebih aman terhadap sniffing yang mencoba untuk mendapatkan informasi dari pesan yang terenkripsi.

Menurut Certicom, parameter-parameter domain kriptografi kurva eliptik pada bidang *Fp* didefinisikan sebagai six-tuple T, yaitu:

$$T = (p,a,b,G,n,h)$$

Dimana:

Fp: Lapangan berhingga prima yang memiliki *p* elemen *Fp* = 0,1,...,*p* − 1 *p*: bilangan prima *a,b*: koefisien

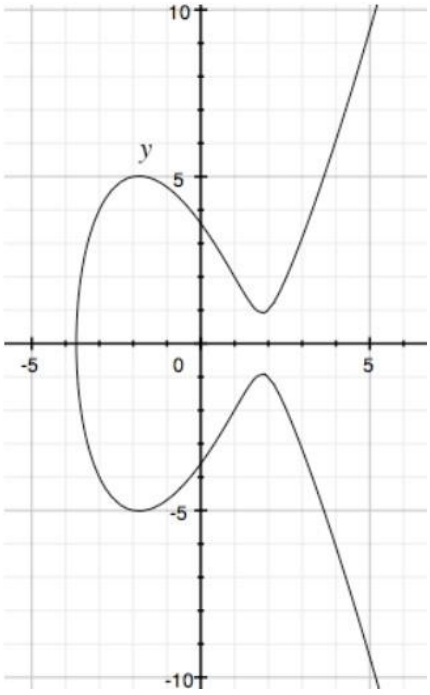
persamaan kurva eliptik

$$y^2 = x^3 + ax + b(mod...p) \quad (2.1)$$

G: basic point, yaitu elemen pembangun grup eliptik $E_p(a,b)$ atas F_P *n*: order basic point, yaitu bilangan bulat positip terkecil *n.G* = *O h*: kofaktor, *h* = #...*E*/*n*, dengan #E adalah banyaknya titik dalam grup eliptik

Setiap perubahan nilai dari '*a*' dan '*b*' akan menghasilkan kurva eliptik yang berbeda.

Contoh pada persamaan $Y^2 = X^3 - 10X + 13$ maka akan menghasilkan grafik seperti pada gambar 2.4



Gambar 2.4: Grafik Kurva Eliptik dengan Persamaan

Setiap kurva eliptik akan mendefinisikan kumpulan titik pada bidang dan dapat membentuk kumpulan albelian (kumpulan titik dengan titik tak hingga sebagai elemen identitas). Jika nilai x dan y yang dipilih adalah daerah finit yang besar, solusi akan menghasilkan suatu albelian finite.

Proses pembuatan tanda tangan, hingga pengujian tanda tangan digital dengan algoritma kurva eliptik menurut aturan standar (certicom, 2000) adalah sebagai berikut:

Proses pembangkitan sepasang kunci:

1. Menentukan sebuah bilangan bulat random d_A, yang nilainya diantara $[1,n-1]$
2. Menghitung

$$Q_A = d_A * G + G[(x_1,y_1)] \tag{2.2}$$

dengan $y^2 = x^3 + ax + b(mod...p)$ d_A=

kunci rahasia

Q_A= kunci publik.

Prosedur pembangkitan tanda tangan (Signing):

1. Memilih sebuah bilangan bulat random k, yang nilainya diantara $[1,n-1]$
2. Menghitung

$$Q_A = k * G = (x_1,y_1) \tag{2.3}$$

dan

$$r = x_1 mod...n \tag{2.4}$$

jika $r = 0$ maka kembali ke langkah a

3. Menghitung

$$k^{-1} mod...n \tag{2.5}$$

(2.5)

4. Menghitung

$$e = HASH(m) \tag{2.6}$$

(dimana m adalah pesan yang akan di signing)

5. Menghitung

$$s = k^{-1}e + d_A * r mod...n \tag{2.7}$$

6. Tanda tangan untuk massage *m* adalah (*r,s*)

Prosedur verifikasi keabsahan tanda tangan (Verifing)

1. Memverifikasi bahwa *r* dan *s* adalah bilangan bulat antara [1,$n-1$]
2. Menghitung $e = HASH(m)$
3. Menghitung

$$w = s^{-1} mod...n \tag{2.8}$$

4. Menghitung

$$u_1 = ew \ldots mod...n \tag{2.9}$$

dan

$$u_2 = rw \ldots mod...n \tag{2.10}$$

5. Menghitung

$$u_1 * G + u_2 * QA = (x_1,y_1) \tag{2.11}$$

6. Menghitung

$$v = x_1 mod...n \tag{2.12}$$

Jika $v = r$**, maka tanda tangan adalah sah**

Seperti dengan kriptografi pada umumnya, ukuran bit dari kunci publik diyakini diperlukan untuk tanda tangan digital kurva eliptik adalah sekitar dua kali ukuran tingkat keamanan dalam bit. Sebagai perbandingan, pada tingkat keamanan 80 bit, berarti penyerang memerlukan sekitar setara dengan sekitar 280 generasi tanda tangan untuk menemukan kunci pribadi, ukuran kunci DSA publik setidaknya 1024 bit, sedangkan ukuran sebuah kunci publik
ECDSA akan menjadi 160 bit seperti contoh pada tabel 2.1

Tabel 2.1: Panjang Bit Publick dan Private Key ECDSA dan RSA

	ECDSA and ECES over GF(q)	RSA 1024-bit n and e=216+1
system parameters	(4 x 160)+1 = 641	0
public key	160+1 = 161	1024 + 17 = 1041
private key	160 (801 with system parameters)	2048 (or 2560 with CRT information)

2.5 *Quick Response (QR) Code*

Barcode memiliki sejarah panjang dan perkembangannya didorong oleh kebutuhan mendasar untuk mempercepat proses pembelian dan pelacakan persediaan (Gura et al., 2011). Usaha pertama untuk mengembangkan sistem pembelian mirip dengan barcode dengan menggunakan kartu punch yang memiliki pola yang unik. Namun sistem ini cukup rumit dan mahal. Pada tahun 1960, barcode modern dimulai evolusinya ketika laser pertama kali digunakan untuk memindai garis hitam dengan berbagai ketebalan. Laser digunakan untuk mengukur ketebalan dari garis hitam sedangkan ruang putih diantaranya mengindikasikan dimana satu garis hitam diakhiri dan garis yang lain dimulai. Ketebalan setiap garis hitam berkorespondensi dengan nomor alfanumerik tertentu. Dengan diadopsi secara luas, barcode tradisional memiliki sistem standar berdasarkan kode 11-digit yang mewakili suatu produk yang unik. *qr code* sangat mirip dengan barcode, namun memiliki manfaat tambahan yang berbeda yaitu kode ini memiliki format matriks yang memungkinkannya untuk menyimpan sejumlah besar data yang unik. Barcode linier standar berbentuk satu dimensi dan hanya dapat menyimpan hingga 20 digit alfanumerik, tetapi qr code merupakan bentuk dua dimensi (2D) sehingga dapat menyimpan hingga 7.089 karakter numerik dan 4.296 karakter alfanumerik (Pcmag.com, ND). *qr code* adalah simbol dua dimensi yang dikembangkan oleh Denso Wave 1994 dengan tujuan utama sebagai simbol yang dapat dengan mudah diinterpretasikan oleh alat scanner (Denso Wave, ND).

QR adalah merek dagang terdaftar dari perusahaan Jepang Denso Wave, anak perusahaan dari Toyota, yang menemukan teknologi tersebut pada tahun

1994 untuk melacak bagian dalam perakitan kendaraan. Denso Wave memilih untuk tidak melaksanakan paten atas teknologi ini dan mempromosikan penggunaannya secara luas . Di Jepang, *qr code* telah digunakan secara luas dalam kegiatan pemasaran sejak awal 1990 karena kemampuannya untuk menciptakan interaksi langsung dengan konsumen seperti contoh pada gambar
2.5 tampilan dari Quick Response (QR) Code.

Gambar 2.5: *Quick Response (QR) Code*

Penggunaan *qr code* dalam kehidupan sehari-hari di Jepang bisa meluas disebabkan karena beberapa alasan berikut: (Soon, 2008)

1. Beberapa keunggulan *qr codes* dibandingkan barcode linear: data density yang lebih tinggi, mendukung karakter Kanji/Chinese, dll.
2. Dapat digunakan oleh semua orang secara gratis karena Denso telahmembuat patennya untuk umum.
3. Standar struktur data bukan merupakan kebutuhan awal dari penggunaannya
4. Kebanyakan ponsel di Jepang telah dilengkapi dengan kamera yang memungkinkan pembacaan qr codes dapat digunakan untuk mengakses alamat Internet dengan membaca URL yang dikodekan dalam *qr code* secara otomatis.

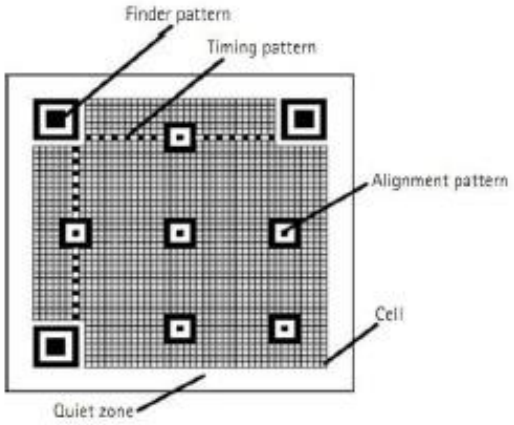
Qr code mempunyai karakteristik yang berbeda dengan barcode tradisional, antara lain:

1. Mampu menyimpan data tersandi dalam kapasitas besar *qr code* mampu menyandikan berbagai macam tipe data seperti numeris, karakter, Kanji,

Hiragana, simbol, biner, bahkan mampu menyandikan 7089 karakter hanya dalam satu simbol. Berbeda dengan barcode biasa yang hanya mampu menyimpan informasi sebesar 20 digit.

2. Ukuran printout yang kecil *qr code* mampu menyandikan data hanya dengan membutuhkan sepersepuluh ruangan yang dibutuhkan oleh barcode biasa
3. Mampu menyandikan Kanji dan Kana
4. Tahan terhadap kotoran dan kerusakan *qr code* mempunyai koreksi error, dimana data dapat direstore walaupun sebagian simbol kotor ataupun rusak.
5. Mampu terbaca pada arah manapun (360 derajat) *qr code* mampu dibaca dalam berbagai arah (omni direksional) secar cepat. *qr code* mempunyai pola untuk mendeteksi posisi pada tiga pojok simbol.
6. Kepadatan yang tinggi (rata-rata 100 kali lebih tinggi daripada barcodelinear.
7. Pembacaan berkecepatan tinggi.
8. Memiliki keunggulan dalam unjuk kerja dan aspek fungsional.

Struktur qr code yang terdiri dari finder patterns, alignment patterns, timing patterns, dan quiet zone ditunjukkan pada Gambar 2.6.



Gambar 2.6: Struktur *Quick Response (QR) Code*

Keterangan gambar:

Finder Pattern

Merupakan pola untuk mendeteksi posisi *qr code*. Dengan mengatur pola ini pada tiga sudut simbol, posisi, ukuran, dan sudut dari simbol dapat dideteksi. Finder pattern ini terdiri dari sebuah struktur yang dapat dideteksi dari semua arah (360).

Alignment Pattern

Merupakan pola untuk mengoreksi distorsi dari *qr code*. Ini sangat efektif untuk mengkoreksi distorsi non linear. Koordinat pusat dari alignment pattern akan diidentifikasi untuk mengoreksi distorsi simbol. Untuk tujuan ini, sebuah sel hitam terisolasi ditempatkan di alignment pattern untuk membuatnya lebih mudah untuk mendeteksi koordinat pusat dari alignment pattern.

Timing Pattern

Merupakan pola untuk mengidentifikasi koordinat pusat untuk setiap sel di *qr code* dengan pola hitam dan putih yang disusun berselang-seling. Ini digunakan untuk mengoreksi koordinat pusat dari sel data jika simbol terdistorsi atau jika ada error untuk setiap area sel. Pola ini disusun dengan arah vertikal dan horizontal.

Quiet Zone

Ruang margin diperlukan untuk membaca *qr code*. Quiet zone membuat simbol lebih mudah untuk dideteksi diantara gambar-gambar yang dibaca oleh sensor CCD. Empat atau lebih sel dibutuhkan untuk quiet zone.

Data Area

Data *qr code* akan disimpan (dikodekan) ke area data. Bagian abu-abu pada gambar 2 mewakili area data. Data akan dikodekan ke bilangan biner ‘0’ dan ‘1’ berdasarkan aturan pengkodean. Bilangan biner ‘0’ dan ‘1’ akan dikonversikan ke sel hitam dan putih dan akan disusun. Area data akan memiliki kode Reed- Solomon yang digunakan untuk data yang tersimpan dan fungsionalitas pengkoreksian error.

2.5.1 Penggunaan *Quick Response (QR) Code*

qr code yang berisi informasi dapat ditempatkan pada kemasan, majalah, tanda-tanda, bis, kartu nama, atau dimana saja pengguna mungkin memerlukan informasi. Dalam bidang bisnis hal ini membuka luas berbagai kemungkinan bagi penjual untuk berhubungan dengan pelanggan mereka dan berbagi informasi terkait mengenai produk mereka. *qr code* memberikan para penjual kemampuan untuk mengukur kecepatan respon dengan presisi yang tinggi, mempermudah perhitungan ROI (return on investment), sehingga membantu menjustifikasi pengeluaran atas budget yang diberikan. *qr code* telah dimanfaatkan di berbagai bidang, antara lain:

1. Bidang kesehatan. Pemanfaatan *qr code* untuk aplikasi kesehatan berbasis mobile di Mexico (Vazquez-Briseno et al., 2010). Aplikasi ini bertujuan untuk meningkatkan gaya hidup sehat dengan membantu orang untuk merekam informasi makan yang telah dikonsumsi beserta kadar kalori yang mereka makan. Perangkat mobile dimanfaatkan untuk aplikasi ini. Namun karena kelemahan dari ukuran alat input/keyboard dari ponsel, maka *qr code* dimanfaatkan untuk meng-capture informasi nutrisi daripada harus melakukan entri data secara manual.

2. Bidang perdagangan. (Lundahl, 2009) memaparkan bagaimana perangkat mobile diintegrasikan dengan *NFC technology* dan *qr code* untuk menghasilkan suatu aplikasi mobile yang dapat mendukung proses belanja.

3. Bidang pendidikan. (Law & So, 2010) menawarkan saran dan implementasi pemanfaatan qr code pada institusi pendidikan. Law dan So menawarkan tiga kegiatan pemanfaatan *qr code* yaitu untuk aktivitas belajar matematika di luar ruangan, belajar bahasa Inggris pada aktivitas pembelajaran multimedia, dan aktivitas latihan mandiri.

4. Bidang marketing. (Erickson, 2011) menawarkan penggunaan *qr code* untuk firma-firma hukum dalam rangka menggapai pelanggan dan calon pelanggan *qr code* dapat dicetak pada kartu bisnis yang berisi informasi kontak dan URL situs web perusahaan, situs web, artikel, dan lain sebagainya.

5. *Qr code* untuk tandatangan digital Pada penelitian ini, peneliti menggunakan *qr code* untuk tanda tangan digital. Data yang di-encode adalah message digest dari artikel atau tulisan yang akan dibuat tanda tangan digitalnya. Pada penelitian ini juga dibuat sebuah perangkat lunak yang langsung men-generate qr code dari masukan berupa tulisan/artikel yang akan dibuat tanda tangan digiltalnya.

6. *Qr code* untuk autentikasi novel user. Pada penelitian ini, *qr code* digunakan sebagai autentikasi user pada sebuah jaringan internet untuk mobile phone.

7. Q*r code* untuk edukasi, Pada penelitian ini dijelaskan manfaat *qr code* untuk edukasi, karena peneliti mengungkapkan bahwa selama ini qr code kebanyakan hanya digunakan untuk kepentingan komersil. Contohnya adalah penggunaan *qr code* untuk katalog perpustakaan.

Berkaitan dengan bidang pendidikan, *qr code* dapat dimanfaatkan juga untuk mendukung layanan perpustakaan. The University of Huddersfield menggunakan qr code untuk "link ke sumber daya elektronik, video instruksional, situs-situs web untuk informasi lebih lanjut, secara langsung berisi detil kontak, dan sebagai cara untuk menyimpan informasi untuk referensi kedepan" (Walsh, 2010) serta untuk "menemukan bantuan yang diperlukan menyediakan alternatif buku berbentuk elektronik daripada bentuk fisik" dan ujuan-tujuan yang lain (Walsh, 2011). Di kasus-kasus ini, qr code mewakili informasi tekstual yang menunjuk ke sumberdaya (URL) atau menyimpan informasi telepon untuk penggunaan nantinya.

The University of Bath telah memenangkan sebuah hibah, yang dikelola oleh Andy Ramsden, untuk meneliti penggunaan qr code di seluruh universitas. qr code digunakan di Bath "untuk menggabungkan layanan perpustakaan dengan 16 teknologi dan peralatan yang digunakan oleh siswa" (Robinson, 2010a). Penelitian ini dilakukan untuk menemukan apakah qr code adalah teknologi yang akan digunakan oleh siswa. Penggunaan ini mencakup sebuah projek untuk memandu siswa mencari lokasi perpustakaan dengan bantuan audio. Dilakukan pemindaian qr code "dengan ponsel yang kompatibel, sehingga seseorang dapat mengunduh petunjuk tur dalam bentuk audio ke lantai ke tiga" perpustakaan. qr code juga digunakan untuk mentransfer "jumlah kelas, penulis dan judul" dari item-item pada katalog. qr

code untuk katalog dibuat secara dinamis menggunakan sebuah program yang ditulis oleh pustakawan (Robinson,2010b). Di perpustakaan Rector Gabriel Ferrat´e milik Technical University of Catalonia, qr code digunakan pada "poster untuk mempromosikan layanan web yang baru" dan untuk menunjuk ke "form registrasi untuk

menggunakan fasilitas komputer di perpustakaan". Penggunaan ini membantu untuk "menghindari pengenalan data secara manual di ponsel user", sehingga memfasilitasi transfer informasi yang dilakukan siswa pada ponsel mereka. Idenya adalah untuk membuat pengguna lebih mudah dan lebih akurat sehingga mereka tidak perlu mengingat-ingat data atau menggunakan kertas. (Walsh, 2010). Pada Brigham Young University (BYU), qr code digunakan untuk memberikan panduan tur dalam bentuk audio kepada para siswa yang akan mengunjungi perpustakaan Harold B. Lee Library (HBLL) (Whitchurch, 2011). Pada papernya, Pons et al. (2011) menjelaskan tantang penggunaan *qr code* di perpustakaan Universitat Polit`ecnica de Val`encia (UPV) di Spanyol. Disana qr code digunakan untuk mendapatkan akses ke situs web mobile, untuk mengunduh dokumen-dokumen, dan untuk mempromosikan blog literatur mereka.

2.5.2 *Qr code Reader* dan *Qr code Generator*

Code yang diambil dari sistem operasi komputer. Kemudian perangkat lunak ini akan membaca qr code tersebut untuk kemudian menampilkan hasilnya kepada user, baik itu berupa teks maupun berupa gambar. Seperti halnya qr code generator, pada qr code reader user juga dapat menyimpan dan atau mencetak hasil pembacaan *qr code*.

qr code generator akan meminta masukan sebuah file image yang dapat diambil dari sistem operasi komputer. Kemudian file gambar tersebut dibaca sebagai byte stream sebelum diubah menjadi representasi byte, numerik, atau alfanumerik dengan algoritma tertentu untuk kemudian diubah menjadi qr code dengan algoritma yang sudah tersedia. Berdasarkan analisis sebelumnya, maka representasi data yang digunakan adalah alfanumerik.

2.6 Verifikasi Dokumen

Dalam era serba elektronik seperti saat ini, penggunaan dokumen tercetak memang masih memegang peranan yang tak bisa diabaikan. Dokumen fisik ini dimanfatkan untuk mencetak berkas penting seperti sertifikat, ijazah, transkrip akademik, kontrak kerjasama, surat perjanjian, dan akta

kepemilikan tanah. Namun, beberapa kasus pamalsuan dokumen cetak telah ditemukan beberapa tahun belakangan. Dokumen palsu dibuat untuk mengelabuhi orang yang tidak memperhatikan keaslian dokumen asli. Seorang pejabat Amerika dibuat malu ketika laporan penting yang diterima menyatakan Irak telah mengembangkan senjata pemusnah masal, adalah laporan yang telah dipalsukan. Pada kasus lain, dua orang polisi ditahan selama beberapa waktu karena telah mengubah surat pernyataan saksi mata, dan menggunakan surat palsu tersebut pada kantor Departemen Investigasi Kriminal (Criminal Investigation Department - CID) di Malaysia (Salleh & Yew, 2009).

Pemalsuan dan manipulasi dokumen dapat menyebabkan kerugian yang signifikan dilihat dari segi kepercayaan dengan relasi, serta keabsahan sebuah dokumen fisik. Adalah tindakan yang penting, untuk memastikan sebuah dokumen agar terhindar dari implikasi dokumen penting, yang dilakukan oleh pihak tanpa kepentingan. Pemalsuan yang biasa dilakukan terbagi menjadi dua jenis: pemalsuan dengan menerbitkan dokumen serupa, dan pemalsuan dengan menggunakan pemindai dan printer dari sebuah dokumen asli (Beusekom & Shafait, 2011).

Verifikasi dokumen diperlukan untuk memastikan keaslian sebuah berkas, serta untuk membuktikan siapa pemilik yang sah atas dokumen tersebut. Verifikasi dapat dilakukan dengan beberapa cara. Misalnya text integrity verification pada dokumen yang dikirim melalui fax, menggunakan teknik pixel reorganizing. Teknik ini diusulkan oleh (Pramoun & Amornraksa, 2013) dengan memanfaatkan kamera untuk mengambil citra dokumen yang dikirim dengan fax. Dokumen diteliti dan diverifikasi berdasarkan algoritma MAC, untuk mendeteksi adakah isi teks telah diubah. Hasil manunjukkan metode yang diusulkan berhasil mendeteksi teks yang telah diubah meski ukuran huruf berbeda. Metode serupa juga digunakan oleh (Thongkor, Pramoun, Chaisri, & Amornraksa, 2012).

2.7 Bahasa Pemograman PHP

Aplikasi yang di buat pada penelitian ini menggunakan bahasa pemograman PHP, karena bahasa pemograman ini bekerja pada sisi server sehingga dari segi keamanan kriptografi yang di gunakan lebih terjamin kerahasiaannya

karena user hanya terhubung di sisi client nya. Untuk disain tampilan digunakan juga cascading style sheets (CSS) sebagai dinamisasi tampilan web.

PHP merupakan kependekan dari Personal Home Page (Situs personal). PHP pertama kali dibuat oleh Rasmus Lerdorf pada tahun 1995. Pada waktu itu PHP masih bernama Form Interpreted (FI), yang wujudnya berupa sekumpulan skrip yang digunakan untuk mengolah data formulir dari web. Selanjutnya Rasmus merilis kode sumber tersebut untuk umum dan menamakannya PHP/FI. Dengan perilisan kode sumber ini menjadi sumber terbuka, maka banyak pemrogram yang tertarik untuk ikut mengembangkan PHP. Pada November 1997, dirilis PHP/FI 2.0. Pada rilis ini, interpreter PHP sudah diimplementasikan dalam program C. Dalam rilis ini disertakan juga modul-modul ekstensi yang meningkatkan kemampuan PHP/FI secara signifikan. Pada tahun 1997, sebuah perusahaan bernama Zend menulis ulang interpreter PHP menjadi lebih bersih, lebih baik, dan lebih cepat. Kemudian pada Juni 1998, perusahaan tersebut merilis interpreter baru untuk PHP dan meresmikan rilis tersebut sebagai PHP 3.0 dan singkatan PHP diubah menjadi akronim berulang PHP: Hypertext Preprocessing. Pertengahan tahun 1999, Zend merilis interpreter PHP baru dan rilis tersebut dikenal dengan PHP 4.0. PHP 4.0 adalah versi PHP yang paling banyak dipakai pada awal abad ke-21. Versi ini banyak dipakai disebabkan kemampuannya untuk membangun aplikasi web kompleks tetapi tetap memiliki kecepatan dan stabilitas yang tinggi.

Pada Juni 2004, Zend merilis PHP 5.0. Dalam versi ini, inti dari interpreter PHP mengalami perubahan besar. Versi ini juga memasukkan model pemrograman berorientasi objek ke dalam PHP untuk menjawab perkembangan bahasa pemrograman ke arah paradigma berorientasi objek. Saat ini banyak aplikasi yang telah dibuat dengan PHP. Baik sifatnya yang komersil maupun free. Salah satu aplikasi yang cukup terkenal dilingkungan open source adalah web portal PHP Nuke yang dibuat oleh komunitas open source dapat diperoleh secara gratis di internet. Software ini dapat di download di http://www.phpnuke.org. Selain PHP Nuke banyak lagi software web portal yang sejenis seperti Post Nuke yang merupakan turunan dari PHP Nuke. Aplikasi-aplikasi seperti e-commerce juga banyak dikembangkan dengan PHP, aplikasi e-learning, aplikasi *search engine*, bahkan aplikasi ERP (Enterprise Resource Plan) yang banyak digunakan oleh perusahaan-perusahaan besar juga sudah ada yang dikembangkan dengan PHP.

Ketika akan membuat aplikasi dengan PHP. Supaya PHP dapat dijalankan tentunnya kita perlu memiliki software pendukung yang biasanya sering digunakan. Seperti web server, database server, teks editor, dan web browser. Istilah yang sering gunakan untuk kombinasi software untuk keempat aplikasi di atas di dunia open source dikenal dengan LAMP (Linux Apache MySQL dan PHP). Jika kita menggunakan sistem operasi windows, kita bisa menggunakan PHP Triad. Software ini telah menyertakan ketiga komponen software untuk pemrograman PHP. Yakni PHP itu sendiri, Apache dan MySQL.

2.7.1 *Web Server*

Web server adalah software yang menjadi tulang punggung dari *world wide web* (www). Web server menunggu permintaan dari client yang menggunakan browser seperti Netscape Navigator, Internet Explorer, Modzilla, dan program browser lainnya. Jika ada permintaan dari browser, maka web server akan memproses permintaan itu kemudian memberikan hasil prosesnya berupa data yang diinginkan kembali ke browser. Data ini mempunyai format yang standar, disebut dengan format SGML (standar general markup language). Data yang berupa format ini kemudian akan ditampilkan oleh browser sesuai dengan kemampuan browser tersebut. Contohnya, bila data yang dikirim berupa gambar, browser yang hanya mampu menampilkan teks (misalnya lynx) tidak akan mampu menampilkan gambar tersebut, dan jika ada akan menampilkan alternatifnya saja. Web server, untuk berkomunikasi dengan client-nya (web browser) mempunyai protokol sendiri, yaitu HTTP (*hypertext transfer protocol*). Dengan protokol ini, komunikasi antar web server dengan client-nya dapat saling dimengerti dan lebih mudah. Seperti telah dijelaskan diatas, format data pada world wide web adalah SGML. Tapi para pengguna internet saat ini lebih banyak menggunakan format HTML (*hypertext markup language*) karena penggunaannya lebih sederhana dan mudah dipelajari. Kata HyperText mempunyai arti bahwa seorang pengguna internet dengan web browsernya dapat membuka dan membaca dokumen-dokumen yang ada dalam komputernya atau bahkan jauh tempatnya sekalipun. Hal ini memberikan cita rasa dari suatu proses yang tridimensional, artinya pengguna internet dapat membaca dari satu dokumen ke dokumen yang lain hanya dengan mengklik beberapa bagian dari halaman-halaman dokumen (web) itu. Proses yang dimulai dari permintaan webclient (browser), diterima web server, diproses, dan dikembalikan hasil prosesnya oleh *web server* ke web client lagi dilakukan secara transparan. Setiap orang dapat dengan mudah

mengetahui apa yang terjadi pada tiap-tiap proses. Secara garis besarnya web server hanya memproses semua masukan yang diperolehnya dari web clientnya.

Apache merupakan web server yang paling banyak dipergunakan di Internet. Program ini pertama kali didesain untuk sistem operasi lingkungan UNIX. Namun demikian, pada beberapa versi berikutnya Apache mengeluarkan program yang dapat dijalankan di Windows. Apache mempunyai program pendukung yang cukup banyak, hal ini memberikan layanan yang cukup lengkap bagi penggunanya.

2.7.2 *Java Script*

Java Script adalah bahasa pemrograman yang bisa disisipkan ke HTML seperti halnya PHP akan tetapi javascript berjalan di sisi Client. Misalnya, jam ditampilkan pada halaman yang update sendiri untuk menunjukkan waktu saat ini pada komputer pengguna. Desain JavaScript dipengaruhi oleh banyak bahasa pemrograman, termasuk C, tetapi dimaksudkan untuk lebih digunakan oleh non-programmer. JavaScript tidak didasarkan pada atau terkait ke Java, ini adalah kesalahpahaman umum. JavaScript seringkali disertakan dalam file HTML atau link dari file HTML dan dijalankan secara lokal oleh web browser. Ini berarti bahwa server bebas untuk mengerjakan sesuatu yang lain daripada pemrosesan instruksi untuk setiap klien. Hal ini telah membuat JavaScript pilihan yang lebih populer daripada bahasa yang memerlukan server untuk melakukan pengolahan.

2.7.3 HTML

HyperText Markup Language (HTML) adalah sebuah bahasa markah yang digunakan untuk membuat sebuah halaman web, menampilkan berbagai informasi di dalam sebuah penjelajah web Internet dan pemformatan hiperteks sederhana yang ditulis dalam berkas format ASCII agar dapat menghasilkan tampilan wujud yang terintegerasi. Dengan kata lain, berkas yang dibuat dalam perangkat lunak pengolah kata dan disimpan dalam format ASCII normal sehingga menjadi halaman web dengan perintah-perintah HTML. Bermula dari sebuah bahasa yang sebelumnya banyak digunakan di dunia penerbitan dan percetakan yang disebut dengan SGML(Standard Generalized Markup Language), HTML adalah sebuah standar yang digunakan secara luas untuk menampilkan halaman web. HTML saat ini merupakan

standar Internet yang didefinisikan dan dikendalikan penggunaannya oleh World Wide Web Consortium (W3C). HTML dibuat oleh kolaborasi Caillau TIM dengan Berners-lee Robert ketika mereka bekerja di CERN pada tahun 1989 (CERN adalah lembaga penelitian fisika energi tinggi di Jenewa).

2.7.4 Basis Data (Database)

Data merupakan sekumpulan dari lambang-lambang yang teratur dan mewakili/ merepresentasikan sebuah obyek atau benda. Sedangkan yang dimaksud dengan data base atau basis data adalah gabungan dari beberapa data yang diolah dan diorganisasikan sedemikian rupa, sehingga didapatkan suatu hubungan atau relasi antara kedua data tersebut serta dapat dipakai secara bersama oleh beberapa pengguna aplikasi. Terdapat dua cara yang dilakukan dalam menggunakan basis data, yaitu:

Modus langsung, dilakukan dengan mengetikkan perintah langsung setelah munculnya dot prompt.

Modus Program: dilakukan dengan menuliskan rangkaian perintah dalam program.

Basis data diperlukan karena data dapat diterjemahkan kedalam sebuah aplikasi program, dibandingkan terpisah atau diolah masing-masing. Kontrol akses luas dan manipulasi pada data dapat dilakukan oleh sebuah aplikasi program. Sebuah basis data dapat di-generate atau di-maintain secara manual atau terkomputerisasi. Contoh kartu katalog perpustakaan. Basis data yang terkomputerisasi data dibuat dan dimaintain oleh program aplikasi yang secara khusus ditulis untuk itu atau oleh sistem manajemen basis data.

2.7.5 *Mysql*

MySQL adalah sebuah perangkat lunak system manajemen basis data SQL (DBMS) yang multithread, dan multi-user. MySQL adalah implementasi dari system manajemen basisdata relasional (RDBMS). MySQL dibuah oleh TcX dan telah dipercaya mengelola system dengan 40 buah database berisi 10.000 tabel dan 500 di antaranya memiliki 7 juta baris. MySQL AB merupakan perusahaan komersial Swedia yang mensponsori dan yang memiliki MySQL. Pendiri MySQL AB adalah dua orang Swedia yang bernama David Axmark, Allan Larsson dan satu orang Finlandia bernama Michael “Monty”.

Setiap pengguna MySQL dapat menggunakannya secara bebas yang didistribusikan gratis dibawah lisensi GPL(General Public License) namun tidak boleh menjadikan produk turunan yang bersifat komersial. Pada saat ini MySQL merupakan database server yang sangat terkenal di dunia, semua itu tak lain karena bahasa dasar yang digunakan untuk mengakses database yaitu SQL. SQL (Structured Query Language) pertama kali diterapkan pada sebuah proyek riset pada laboratorium riset San Jose, IBM yang bernama system R. Kemudian SQL juga dikembangan oleh Oracle, Informix dan Sybase. Dengan menggunakan SQL, proses pengaksesan database lebih user-friendly dibandingan dengan yang lain, misalnya dBase atau Clipper karena mereka masih menggunakan perintah-perintah pemrograman murni. SQL dapat di-

gunakan secara berdiri sendiri maupun di lekatkan pada bahasa pemograman seperti C, dan Delphi.

2.8 Android

Android adalah sebuah tumpukkan software untuk perangkat mobile yang termasuk di dalamnya sistem operasi, middleware, dan aplikasi-aplikasi kunci. Sejak kemunculan perdananya, Android menarik perhatian banyak perusahaan, pengembangan, dan masyarakat lainnya. Android menyediakan platform terbuka bagi para pengembangnya untuk menciptakan aplikasi mereka sendiri untuk digunakan oleh berbagai macam piranti bergerak. Adapun bahasa pemograman yang diperlukan untuk membangun aplikasi pada platform Android adalah bahasa pemograman Java. Beberapa bagian penting dalam mengembangkan aplikasi Android adalah sebagai berikut:

1. Android Software Development Kit (SDK)
2. Android Emulator

2.9 *Library ZXing*

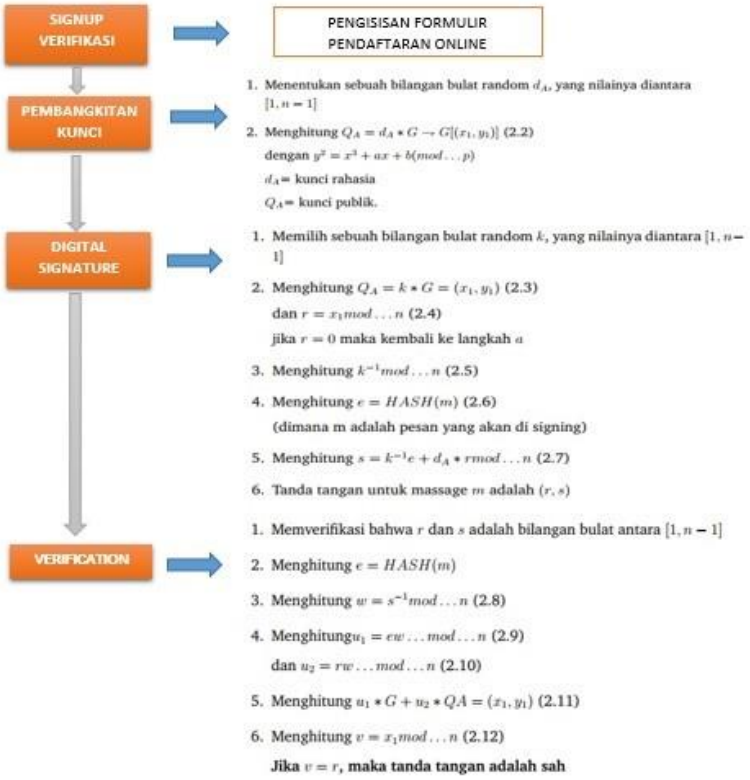
ZXing adalah sebuah open-source, dan library Java yang dapat memproses berbagai format gambar barcode 1D/2D. Fokus dari library ini adalah untuk menggunakan kamera dari telepon selular untuk melakukan *scan* dan *decode barcode*, tanpa harus berkomukasi dengan server. Biarpun begitu, *ZXing* juga dapat digunakan untuk meng-encode dan decode barcode untuk dekstop dan server juga.

Bab 3

Model Verifikasi

3.1 Alur Proses Model Verifikasi Dengan Algortima Eliptik

Pada penelitin model verifikasi dalam penelitian ada 4 alur proses dengan pengimplemntasian model algoritma eliptik. Pada gambar 3.1berikut merupakan alur proses dari sistem:



Gambar 3.1: Alur Proses Model Algoritma Eliptik

33

Keterangan Alur Proses Model Algoritma Elitptik seperti pada Gambar 3.1:

1. *Signup Verifikasi*

   Pada tahap *signup* pada alur proses gambar 3.1, merupakan langkah awal dalam keberhasilan proses verifikasi. Dengan memasukkan data

kedalam data base yang akan diproses dengan model sistem keamanan data dengan memasukkan dokumen data pribadi anggota.

2. **Pembangkitan Kunci**

   Pada tahap pembangkitan kunci pada gambar 3.1 menjelaskan tentang pengimplemntasian algoritma eliptik pada tahap pembangkitan kunci dengan algoritma elipttik pada tahap database memproses data untuk mengeluarkan nomor anggota masing - masing anggota yang mendaftar kedalam sistem.

3. *Digital Signature*

   Pada tahap *Digital Signature* pada gambar 3.1menjelaskan dari alur algoritma untuk memberikan tanda tangan digital berupa nomor anggota yang telah diproses pada pembangkitan kunci untuk mempunyai kode unik masing - masing setiap anggota berupa nomor anggota dan qr_code.

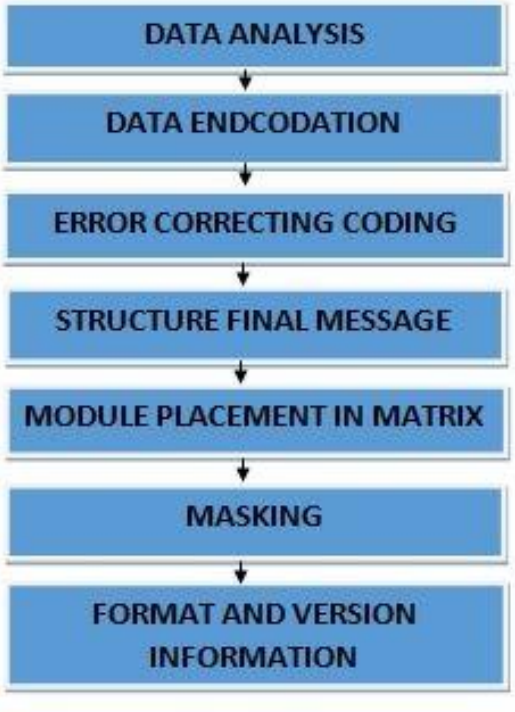
4. *Verification*

   Pada tahap *Verification* pada gambar 3.1 menjelaskan tentang tahapan pengujian tanda tangan *digital* berupa *qr code* masing - masing anggota dengan alur algoritma eliptik dengan kondisi Jika $v = r$, maka tanda tangan adalah sah.

3.2 Diagram Alir *Quick Response (QR) Code*

3.2.1 Diagram Alir *Encoding Qr Code*

Pada Gambar 3.2 menjelaskan tentang proses encoding *Quick Response (QR) Code.* Proses encoder adalah proses dimana input data text sampai menjadi *qr code* dengan tahapan-tahapannya, sebelum masuk ke tahapan-tahapan user harus menentukan tipe data, versi data dan tingkat koreksi error yang akan dibuat menjadi *qr code*.



Gambar 3.2: Diagram Alur Encoding *Qr Code*

Keterangan diagram alir pada Gambar 3.2:

1. *Data Analysis*

   Pada alur proses *Data Analysis* menjelaskan tentang alur proses pemilihan data masukkan yang dibutuhkan untuk diproses dalam tahapan *encoding.* Pada tahap ini peneliti mendapatkan data langsung dari pihak organisasi IPKIN tentang data apa saja yang dibutuhkan dalam formulir pendaftaran pada *website online* yang sudah terlebih dahulu dianalisis pihak organisasi. Menentukan kapasitas data adalah proses awal sebelum proses pembuatan QR Code, untuk lebih memahaminya penulis memasukan contoh data yang di buat menjadi QR Code.

   (a) **Tipe data.**

   Tipe data dalam QR Code sebagai berikut:

   Numerik

   Alfanumerik

Biner

Kanji

(a) **Versi data.**

Versi data dalam QR Code telah dipaparkan dalam pembahasan dan tabel sebelumnya.

2. *Data Endcodation*

Pada alur proses *Data Endcodation* menjelaskan tentang tahapan di mana data yang telah dianalisis diubah menjadi kode unik sebagai pembangkit kunci pada proses verifikasi untuk difungsikan menjadi nomor anggota yang diwakili pula dengan tampilan output berupa *qr code*.

3. *Error Correcting Coding*

Pada alur proses *Error Correcting Coding* menjelaskan tentang tahapan di mana sistem mengkoreksi kembali struktur pemrograman yang dibuat untuk menghasil output pada *qr code module.* Kapasitas data dalam *qr code* cukup banyak, tetapi terkadang hasil cetakan dari qr Code mengalami kerusakan yang di akibatkan atau kotor. Data di dalamnya dapat dipulihkan dalam kisaran tertentu dengan kemampuan koreksi kesalahan yang bahkan jika simbol sebagian hilang. PadaTabel3.1, terdapat empat tingkat koreksi kesalahan dan *qr code* dapat memulihkan q*r code*.

Tabel 3.1: Tabel Koreksi *Error Qr code*

Level L	7% dari kode yang hilang dapat dikembalikan
Level M	15% dari kode yang hilang dapat dikembalikan
Level Q	25% dari kode yang hilang dapat dikembalikan
Level H	30% dari kode yang hilang dapat dikembalikan

4. *Strukture Final Message*

Pada alur proses *Strukture Final Message* menjelaskan tentang tahapan di mana struktur tampilan *qr code* di berikan message sebagai output yang akan ditampilkan pada *qr code module*.

5. *Module Placement In Matrix*

   Pada alur proses *Module Placement In Matrix* menjelaskan tentang tahapan tampilan *qr code* pada *module* program.

6. *Masking*

   Pada alur proses *Masking* menjelaskan tentang proses menghilangkan bagian yang bukan merupakan modul data yang diharapkan kedalam output program, terdapat delapan jenis indikator pola mask dalam *qr code* seperti pada Tabel 3.2.

Tabel 3.2: Tabel Indikator Pola Mask

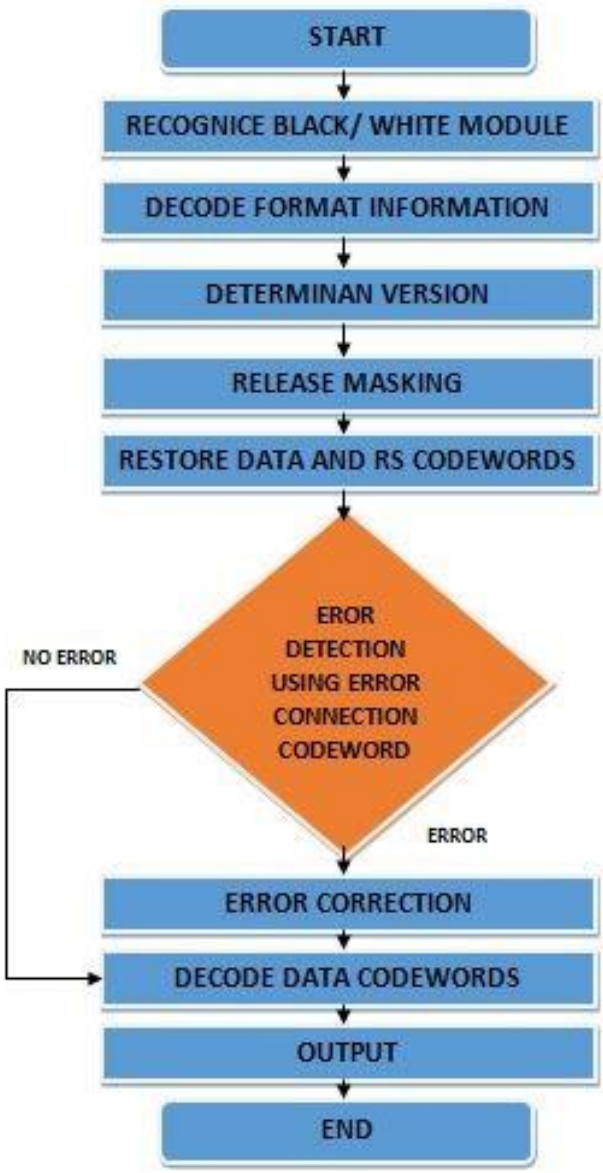
Pola *Mask*	Aturan
000	Jika (x+y) mod = 0, maka isi matrik mask pada posis tersebut dengan 1 (true)
001	Jika y mod 2 = 0, maka isi matrik mask pada posisi tersebut dengan 1 (true)
010	Jika x mod 3 = 0, maka isi matrik mask pada posisi tersebut dengan 1 (true)
011	Jika (x+y) mod 3 = 0, maka isi matrik mask pada posisi tersebut dengan 1 (true)
100	Jika ((x/3)+(y/2 mod 2 = 0, maka isi matrik mask pada posisi tersebut dengan 1 (true)
101	Jika ((x*y) mod 2 + (x*y) mod 3=0), maka isi matrik mask pada posisi tersebut dengan 1 (true)
110	Jika (((x*y) mod 3 + (x+y) mod 2) mod 2 = 0), maka isi matrik mask pada posisi tersebut dengan 1 (true)
111	Jika (((x*y) mod 3 + (x+y) mod 2) mod 2 = 0), maka isi matrik mask pada posisi tersebut dengan 1 (true)

7. *Format And Version Information*

Pada alur proses *Format And Version Information* menjelaskan tentang format *outpur qr code* dan versi tanpilan *qr code modelu.*

3.2.2 Diagram Alir Decoding *Qr Code*

Pada *Decoding* menjelaskan tentang kebalikan alur prose Gambar *3.2. Module qr code* tidak hanya dapat dibuat saja, tetapi juga dapat dibaca dengan melalui beberapa proses dan algoritma pembacaannya. Proses-proses ini secara umum merupakan kebalikan dari proses pembuatan qr code. Diagram alur untuk membaca sebuah *qr code* dapat dilihat pada Gambar 3.3.



Gambar 3.3: Diagram Alur Decoding qr code

Keterangan alur proses *Decoding* pada Gambar 3.3:

1. *Recognice Black/ White Module*

   Pada alur proses decoding kita akan memulai dengan proses *Recognice Black/ White Module* pada ini kita akan kembali mengenali kode yang telah menjadi output pada tahapan *Encoding* dengan kembali titik hitam dan putih yang ada pada *module*.

2. *Decode Format Information*

   Pada alur proses *Decode Format Information* menjelaskan tentang alur proses pengaturan format pada pembacaan informasi kembali.

3. *Determinan Version*

   Pada alur proses *Determinan Version* menjelaskan tentang faktor penentu yang akan di keluarkan sebagai informasi untuk dikeluarkan pada *output* tahapan masking,

4. *Release Masking*

   Pada alu proses *Release Masking* menjelaskan tentang tampilan *output masking* yang akan diproses dan dibaca kembali.

5. *Restore Data And RS Codeword*

   Pada alur proses *Restore Data And RS Codeword* menjelaskan tentang pengembalian data yang yang tersimpan pada *memory* program/ *database* program.

6. *Error Detection Using Error Connection Codeword*

   Pada alur proses *Error Detection Using Error Connection Codeword* menjelaskan tentang proses *decission* untuk hasil output dari database jika *error* program akan mengulangi proses jika *no error* program akan melanjutkan tahap *decoding*.

7. *Error Correction*

Pada alur proses *Error Correction* menjelaskan tentang kondisi di mana pengoreksian ulang data pada database yang akan ditampilkan pada *output decoding*.

8. *Decode Data Codeword*

   Pada alur prose *Decode Data Codeword* menjelaskan tentang pengembalian data - data yang telah dikorekasi dari berupa code menjadi data anggota kemabali yang akan menjadi *output* program.

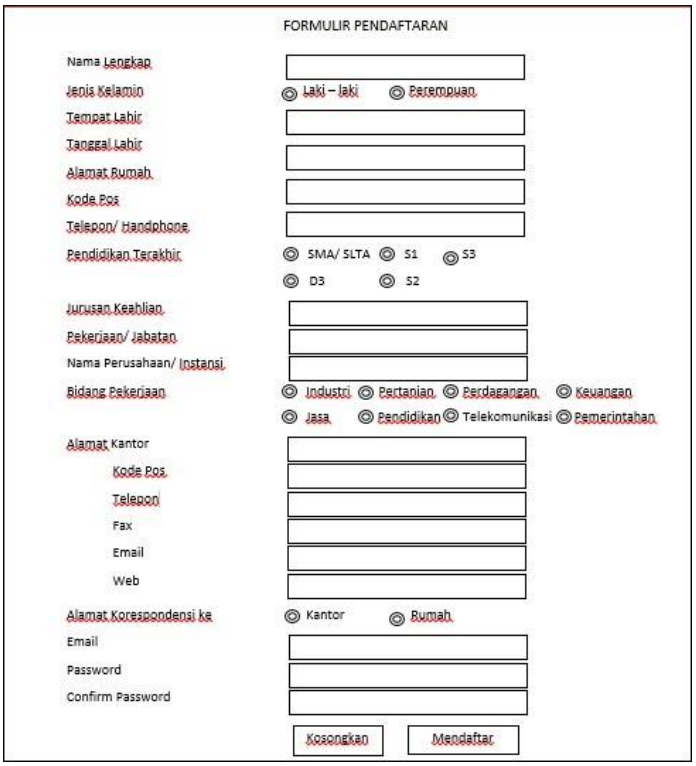
9. *Output*

   Pada alur proses *Output* menjelaskan tentang tampiilan data anngota yang telang berhasil dalam proses *decoding*.

3.3 Tampilan Halaman Model Verifikasi

3.3.1 Desain Tampilan Halaman Signup Verifikasi

Pada Gambar 3.4 menjelaskan tentang gambaran desain tampilan formulir pendaftaran online pada website IPKIN. Desain formulir yang ditampilkan merupakan rujukan dari perwakilan pengurus IPKIN yang merekomendasikan tampilan formulir online terpacu kepada informasi data yang ada pada formulir manual.



Gambar 3.4: Tampilan Form Signup

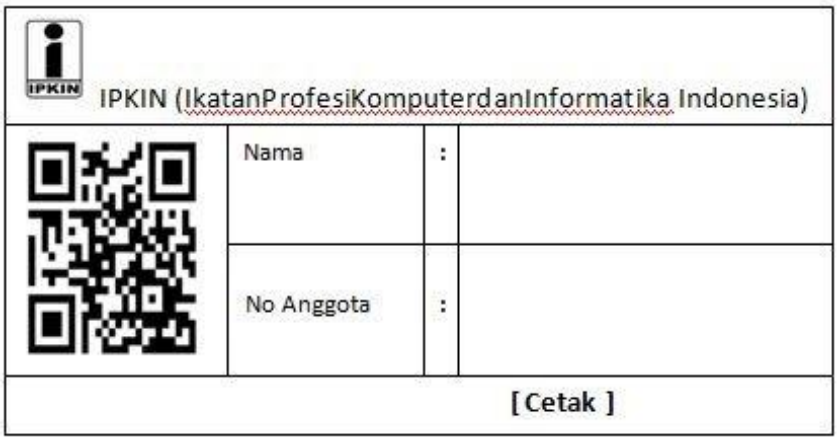
3.3.2 Desain Tampilan Halaman Notifikasi Pembangkitan Kunci

Pada Gambar 3.5 menjelaskan tentang pesan pembangkitan kunci pada tampilan websit bahwa data yang didaftarkan telah sukses terdaftar.

Gambar 3.5: Notifikasi Proses Pembangkitan Kunci

3.3.3 Desain Tampilan Halaman Pemberian Digital Signature

Pada Gambar 3.6 menjelaskan tentang desain tampilan *message digital signature* yang akan diproses cetak pada halam website.



Gambar 3.6: Desain Halaman Digital Signature

3.3.4 Tampilan Hamalan Objek Verifikasi

Pada Gambar 3.7 menjekaskan tentang desain tampilan output kartu member yang akan digunakan sebagai objek verifikasi pada kegiatan IPKIN yang sedang berlangsung.

Gambar 3.7: Desain Halaman Objek Verifikasi (Kartu Member)

Bab 4

Implementasi

4.1 Pembuatan Alur Sistem Model Verifikasi

Pada proses ini akan dilakukan implementasi arsitektur sistem yang mendukung keberhasilan dari model verifikasi.. Seperti yang sudah dijelaskan sebelumnya, terdapat beberapa faktor yang diperlukan sebagai *input* untuk model verifikasii, yaitu pendaftaran online pada website, cetak kartu member dan mengikuti kegiatan yang diselenggerkan organisasi IPKIN untuk anggota yamg telah terdaftar. Oleh karena itu, pada sistem ini juga dibuat *interface* serta pengujian model verifikasi seperti pada Gambar 4.1.

Gambar 4.1: Gambaran Alur Sistem

4.2 Proses Sirkulasi Data

Pada proses sirkulasi data pada model verifikasi terdapat dua alur sistem yaitu:

1. Alur sistem *Encoding* yang diproses pada aplikasi website IPKIN yang dijelaskan pada Gambar .4.2.

2. Alur sistem Decoding yang diproses pada aplikasi *mobile* verifikasi IPKIN yang dijelaskan pada Gambar 4.7.

4.2.1 Proses Pengolahan Data Pada Website

Pada aliran arus data website pada Gambar 4.2 menjelaskan tentang proses data input dengan pengisian formulir online sampai output program berupa kartu member sebai objek atau media yang diverifikasi.

Gambar 4.2: Aliran Arus Data Website

4.2.1.1 Tampilan Formulir Online Pada Website

Pada Gambar 4.3 merupakan tampilan dari formulir online pada website.

Gambar 4.3: Tampilan Formulir Online

4.2.1.2 Tampilan Message Encoding Pada Website

Pada Gambar 4.4 menjelaskan tentang message output *encoding* pada website untuk melanjutkan user yang mendaftar dapat mengklik kotak dengan perontah ok.

Gambar 4.4: Tampilan Message Encoding

4.2.1.3 Tampilan Digital Signature Pada Website

Pada Gambar 4.5 menjelaskan tentang *output* hasil *encoding* data yang dirujukkan sebagai *digital signature* masing - masing anggota.

Gambar 4.5: Tampilan Digital Signature

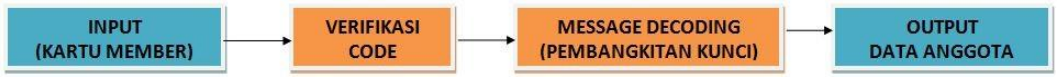
4.2.1.4 Tampilan Kartu Member Pada Website

Pada Gambar 4.6 merupakan tampilan *output* tahapan *encoding* berupa kartu member anggota yang akan diproses pada model verifikasi dengan teknik *decoding*.

Gambar 4.6: Tampilan Kartu Member

4.2.2 Proses Pengolahan Data Pada *Mobile*

Pada aliran arus data *mobile* pada Gambar 4.7 menjelaskan tentang proses verifikasi kartu member sebagai objek dengan verifikasi kartu member dengan scanning *qr code* dengan teknik *decoding* untuk pembacaan data kembali sebagai *output* model verifikasi.



Gambar 4.7: Aliran Arus Data Mobile

4.2.2.1 Tampilan Objek Verifikasi

Pada Gambar 4.8 merupakan tampilan kartu member sebagai objek verifikasi pada aplikasi *mobile*.

Gambar 4.8: Tampilan Objek Verifikasi

4.2.2.2 Tampilan Penerapan Proses Verfikasi Code Pada Mobile Pada Gambar 4.9 menjelaskan tentang alur proses verifikasi yaitu:

1. **Kegiatan IPKIN**

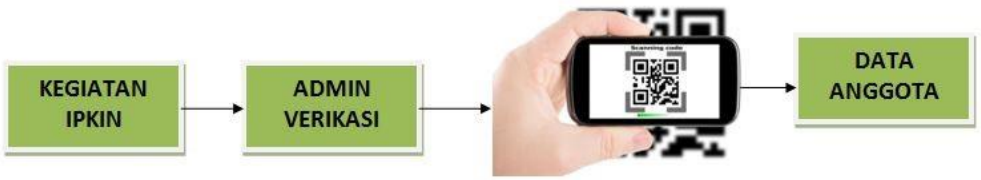
   Pada tahapan model verifikasi, model verifikasi dapat diimplementasikan dan diuji coba pada saat kegiatan IPKIN yang sedang berlangsung seperti pertemuan - pertemuan conference maupun seminar dalam bidang komputer dan teknologi informasi.

2. **Admin Verifikasi**

   Pada tahapan admin verifikasi dalam alur proses menjelaskan tentang alur verfikasi yang membutuhkan *user* sebagai *admin* untuk menvalidasi kebenaran keanggotaan dengan menscanning kartu member anggota dengan aplikasi *mobile* verifikasi.

3. **Data Anggota**

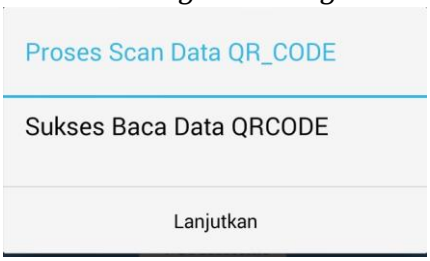
   Pada tahapan ini merupakan *output* dari model verifikasi berupa data anggota yang terdapat pada database *website* dengan kondisi sistem dalam keadaan *online*.



Gambar 4.9: Tampilan Proses Sistem Verifikasi

4.2.2.3 Tampilan Message Decoding Pada Mobile

Pada Gambar merupakan *4.10 message decoding* bahwa kode berhasil terbaca.



Gambar 4.10: Tampilan Message Decoding

4.2.2.4 Tampilan Data Anggota Pada Mobile

Pada Gambar 4.11 merupakan tampilan *output* model verifikasi yang data berhasil terbaca dengan teknik *decoding*.

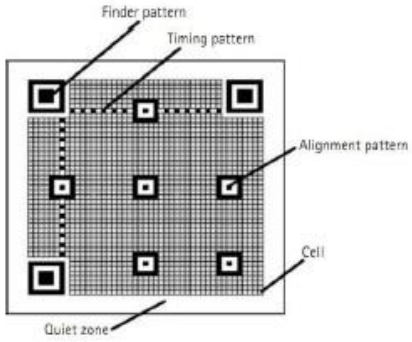
Gambar 4.11: Tampilan Data Aggota

Pada Gambar 4.12 merupakan data selengkapnya dari Gambar 4.11 pada model verifikasi.

Gambar 4.12: Tampilan Data Selengkapnya

4.3 Pengujian Model Verifikasi

Pada pengujian model verifikasi, tahapan selanjutnya adalah pengujian kartu member dengan menguji beberapa kerusakkan pada *qr code* yang terbagi menjadi beberapa bagian seperti Gambar *2.6.*



Gambar 4.13: Struktur *Module Qr Code*

Pada pengujian model verifikasi dengan kerusakkan beberapa bagian pada Module Qr Code, ada beberapa titik pada *module* yang tetap diterima sistem dan beberapa titik pada *module* yang ditolak oleh sistem atau tidak terbaca dengan hasil pengujian seperti pada Tabel 4.1

Tabel 4.1: Tabel Pengujian

Deskripsi	Kesimpulan
Menguji pembacaan dengan *QR Code* yang bagus dan benar	Diterima
Menguji pembacaan dengan *QR Code* yang kotor sebagian kecil pada bagian pojok bawah	Diterima
Menguji pembacaan dengan *QR Code* yang kotor sebagian kecil secara vertikal	Diterima
Menguji pembacaan dengan *QR Code* yang kotor sebagian kecil secara horizontal	Diterima
Menguji pembacaan dengan *QR Code* yang kotor sebagian kecil pada bagian pojok atas	Diterima
Menguji pembacaan dengan *QR Code* yang kotor sebagian	Ditolak
Menguji pembacaan dengan *QR Code* yang kotor sebagian besar	Ditolak
Menguji pembacaan dengan *QR Code* yang rusak sebagian kecil	Diterima
Menguji pembacaan dengan *QR Code* yang rusak sebagian	Diterima
Menguji pembacaan dengan *QR Code* yang rusak sebagian besar	Ditolak
Menguji pembacaan dengan *QR Code* yang kotor di 1 bagian finder pattern	Diterima
Menguji pembacaan dengan *QR Code* yang kotor di 2 bagian finder pattern	Ditolak
Menguji pembacaan dari *QR Code* dengan arah terbalik	Diterima

Bab 5

Kesimpulan dan Saran

5.1 Kesimpulan

Pembuatan model verfikasi dengan pemanfaatan *Qr Code* dan Algoritma Eliptik memiliki tingkat ketepatan yang cukup baik. Namun hal ini harus diseimbangi dengan output *qr code* yang handal dan aplikasi untuk menverifikasi data dengan sistem yang baik. Semakin handal output *qr code* dan aplikasi, akan menghasilkan model verifikasi yang tepat, namun sebaliknya semakin tidak baik hasil output qr code dan aplikasi verifikasi semakin menghambat kegiatan yang diselenggarakan oleh IPKIN (Ikatan Profesi Komputer dan Informatika Indonesia).

Dalam keberhasilan model verifikasi pada kegiatan IPKIN dibutuhkan pula seorang user sebagai admin yang dapat dipercaya, karena bukan hanya faktor sistem yang baik dan benar saja dalam kerhasilan model verifikasi dalam penelitian ini, Akan tetapi sumber daya manusia yang baik dan juga menentukan keberhasilan dari model verikasi.

5.2 Saran

Dalam Pembuatan model verfikasi ini masih menggunakan pengujian kehandalaan kerukkan pada *module qr code* secara manual . Belum terdapatnya aplikasi pengujian *image* juga salah satu kekurangan dalam pembuatan sistem model verifikasi ini agar lebih mempermudah dalam pengujian akhir seperti aplikasi *image correction* pada aplikasi Java Dekstop maupun aplikasi dengan Program Matlab.

Bibliografi

[Afrianto, 2012] Afrianto, I, H. A. F. A. (2012). ”pemanfaatan qrcode sebagai akses cepat verifikasi ijazah unikom”. Seminar Nasional Teknologi Informasi dan Komunikasi, Universitas Komputer Indonesia.

[Bachtiar, 2012] Bachtiar, M, d. M. S. A. (2012). ”smart login pada situs web menggunakan qr-code”. volume 1, 1-4. Jurnal Teknik Pomits.

[Falas, 2007] Falas, T., K. (2007). Two-dimensional barcode decoding with camera equipped mobile phones. Proceedings of the Fifth Annual IEEE International Conference on Pervasive Computing and Communications Workshops.

[Gandhewar, 2010] Gandhewar, N., S. R. (2010). An emerging software platform for mobile devices. International Journal on Computer Science and Engineering (IJSCE).

[ITSC, 2998] ITSC (2998). Qr code. Synthesis Journal. Information Technology Standards Committee Singapore.

[Law, 2007] Law, C.-Y. . S. S. (2007). Qr codes in education. volume 3, pages 85 – 100. Journal of Educational Technology Development and Exchange,. [Soon, 2011] Soon, T. J. (2011). Qr code. EPCglobal Singapore Council.

[ZXing, 2011] ZXing (2011). Zebra crossing (zxing). http://code.google.com/p/zxing/.