IMPLEMENTASI ALGORITMA *RIVEST CIPHER 4* DALAM MENGAMANKAN HASIL *E-VOTING* PEMILIHAN KEPALA DESA BERBASIS JAVA

SKRIPSI

Oleh:

ACHMAD CHAFIDHI

06550107

JURUSAN TEKNIK INFORMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI
MAULANA MALIK IBRAHIM MALANG
2013

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

IMPLEMENTASI ALGORITMA *RIVEST CIPHER 4* DALAM MENGAMANKAN HASIL *E-VOTING* PEMILIHAN KEPALA DESA BERBASIS JAVA

SKRIPSI

Diajukan kepada
Universitas Islam Negeri Maulana Malik Ibrahim Malang
Untuk Memenuhi Salah Satu Persyaratan
Dalam Memperoleh Gelar Sarjana Komputer (S.Kom)

Oleh:
ACHMAD CHAFIDHI
06550107

JURUSAN TEKNIK INFORMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI
MAULANA MALIK IBRAHIM MALANG
2013

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

LEMBAR PERSETUJUAN

IMPLEMENTASI ALGORITMA *RIVEST CIPHER 4* DALAM MENGAMANKAN HASIL *E-VOTING* PEMILIHAN KEPALA DESA BERBASIS JAVA

SKRIPSI

Oleh:

ACHMAD CHAFIDHI
06550107

Telah Disetujui,
15 Juli 2013

Telah disetujui oleh:

Pembimbing I	Pembimbing II
Ririen Kusumawati, M.Kom	Totok Chamidy, M.Kom
NIP. 197203092005012002	NIP. 196912222006041001

Mengetahui,
Ketua Jurusan Teknik Informatika
Fakultas Sains dan Teknologi
Universitas Islam Negeri (UIN) Maulana Malik Ibrahim Malang

Ririen Kusumawati, M. Kom
NIP. 197203092005012002

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

LEMBAR PENGESAHAN

IMPLEMENTASI ALGORITMA *RIVEST CIPHER 4* DALAM MENGAMANKAN HASIL *E-VOTING* PEMILIHAN KEPALA DESA BERBASIS JAVA

SKRIPSI

Dipersiapkan dan disusun oleh:

Achmad Chafidhi
NIM. 06550107

Telah Dipertahankan Di Depan Dewan Penguji Skripsi
Dan Dinyatakan Diterima Sebagai Salah Satu Persyaratan
Untuk Memperoleh Gelar Sarjana Komputer (S.Kom)
Tanggal, 20 Juli 2013

1.	Penguji Utama	:	Zainal Abidin, M.Kom NIP. 197606132005011004	( )
2.	Ketua Penguji	:	M. Ainul Yaqin, M.Kom NIP. 19761013 200604 1 004	( )
3.	Sekretaris Penguji:		Ririen Kusumawati, M.Kom NIP. 197203092005012002	( )
4.	Anggota Penguji	:	Totok Chamidy, M.Kom NIP. 196912222006041001	( )

Mengetahui dan Mengesahkan
Ketua Jurusan Teknik Informatika
Universitas Islam Negeri Maulana Malik Ibrahim Malang

Ririen Kusumawati, M.Kom
NIP. 197203092005012002

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

LEMBAR PERNYATAAN

Saya yang bertanda tangan dibawah ini:

Nama : Achmad Chafidhi

NIM : 06550107

Jurusan : Teknik Informatika

Judul Skripsi :Implementasi Algoritma *Rivest Cipher 4* Dalam Mengamankan Hasil *E-Voting* Pemilihan Kepala Desa Berbasis Java

Menyatakan dengan sebenar-benarnya bahwa hasil penelitian yangpenulis buat initidak terdapat unsur-unsur penjiplakan karya penelitian atau karya ilmiah yang pernah dibuat oleh orang lain, baik sebagian maupun seluruhnya, kecuali dalam bentuk kutipan dan disebutkan dalam sumber kutipan tersebut didalam daftar pustaka.

Apabila ternyata hasil penelitian ini terbukti terdapat unsur-unsur jiplakan, maka semua akibat dari hal tersebut akan menjadi tanggung jawab saya sepenuhnya, tanpa melibatkan dosen pembimbing atau pihak lain.

Demikian pernyataan ini dibuat dengan segala kesadaran.

Malang, 20 Juli 2013

Yang membuat pernyataan,

Mahasiswa

Achmad Chafidhi
06550107

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

MOTTO

بِسْمِ ٱللَّهِ ٱلرَّحْمَٰنِ ٱلرَّحِيمِ

وَٱلْعَصْرِ ﴿١﴾ إِنَّ ٱلْإِنسَٰنَ لَفِى خُسْرٍ ﴿٢﴾ إِلَّا ٱلَّذِينَ ءَامَنُوا۟ وَعَمِلُوا۟ ٱلصَّٰلِحَٰتِ وَتَوَاصَوْا۟ بِٱلْحَقِّ وَتَوَاصَوْا۟ بِٱلصَّبْرِ ﴿٣﴾

1. demi masa.
2. Sesungguhnya manusia itu benar-benar dalam kerugian,
3. kecuali orang-orang yang beriman dan mengerjakan amal saleh dan nasehat menasehati supaya mentaati kebenaran dan nasehat menasehati supaya menetapi kesabaran.(QS al-Asr)

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

PERSEMBAHAN

Yang utama dari segalanya

Sembah sujud serta syukur kepada Allah SWT. Taburan cinta kasih dan sayang-Mu telah memberikanku kekuatan, membekaliku dengan ilmu. Atas Karunia serta kemudahan yang Engkau berikan akhirnya skripsi yang sederhana ini dapat terselesaikan. Sholawat dan salam selalu terlimpahkan keharibaan Rasulullah Muhammad SAW.

Kupersembahkan karya sederhana ini kepada orang yang sangat kukasihi dan kusayangi

Ayah dan Bu Kaji

Sebagai tanda bakti, hormat, dan rasa terima kasih yang tiada terhingga saya haturkan kepada Abah dan Bu Kaji yang telah memberikan dukungan, dan cinta kasih yang tiada terhingga yang tiada mungkin dapat saya balas, hanya dengan selembar kertas yang bertuliskan kata cinta dan persembahan.

Semoga ini langkah awal untuk membuat ibu bahagia dan bangga karena saya sadar, selama ini saya belum bisa berbuat yang lebih. Untuk Bu Kaji yang selalu mendoakan, dan untuk ibuku yang selalu membuat neng termotivasi serta selalu menjadi inspirasiku, untuk ibuku yang selalu menyirami kasih dan menjadi persinggahanku saat suka ataupun dukaku. ”*Semoga Allah Selalu Menyayangi, Menjaganya dan memberikan kekuatan untuknya*”

keluarga besarku terimah kasih atas doa dan motivasinyaselama ini. Buat kakak Islahuddin yang telah menuntun mulai awal sampai akhir, buat sahabatku *Icha husnia anggraini*, *vianisti*, *ellen*yang telahmenemani selama ini.

Teman-Teman Terbaik

Para sahabat angkatan ’06 Hilmi, Faisol, Adi,Ridho, Aziz, Jamil,Putra, Jundi,Tegar, Hendra, Nizar, Hariadi, Zaqia, Ulin, Ulil, Mas Mahyadan Musrif 2007 Ginanjar, Nafi’, Icha Husnia, Dika. Bimbel *Cemerlang* Zila, Furi, Winda, Ali, Rosi, Diah, Darul, Santri *KENIA*, Santri Komplek Maliki Pondok Gading Kamal, Rizal, Beqi, Santri, Sukron semoga sukses dan terus maju.

Semua rekan seperjuangan yang tidak bisa disebutkan satu persatu, yang telah membantu penulis selama ini.

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

KATA PENGANTAR

Segala puji bagi Allah SWT yang telah melimpahkan karunia-Nya kepada penulis sehingga bisa menyelesaikan skripsi dengan judul "Implementasi Algoritma *Rivest Cipher 4* Dalam Mengamankan Hasil *E-Voting* Pemilihan Kepala Desa Berbasis Java"

Sholawat dan salam semoga selalu tercurah kepada Nabi Muhammad SAW karena bimbingan beliau, Islam telah disampaikan dan membawa umat dari kegelapan menuju zaman yang terang benderang.

Penyelesaian skripsi ini akan sulit terwujud tanpabantuan dan sumbangsih berbagai pihak karena penulis memiliki keterbatasan kemampuan dan pengetahuan. Untuk itu, dengan segala kerendahan hati maka penulis mengucapkan terima kasih kepada:

1. Prof. Dr. H. Mudjia Rahardjo M.Sc selaku Rektor Universitas Islam Negeri Maulana Malik Ibrahim Malang
2. Dr. Drh. Bayyinatul Muchtaromah, M.Si, selaku Dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang
3. Ririen Kusumawati, M.Kom selaku pembimbing dan Ketua Jurusan yang telah meluangkan banyak waktu untuk membimbing dan mengarahkan dalam penyelesaian skripsi
4. Totok Chamidy, M.Kom selaku pembimbing agama dan Dosen Wali Jurusan Teknik Informatika, yang membantu penulis serta banyak memberikan petunjuk dan nasehat dalam penyelesaian skripsi

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

5. Segenap Dosen Teknik Informatika yang telah memberikan bimbingan keilmuan kepada penulis selama masa studi.
6. Keluarga besar Perpustakaan Pusat Universitas Islam Negeri Maulana Malik Ibrahim Malang yang telah memberikan dukungan pustaka kepada penulis untuk menyelesaikan penyusunan skripsi.
7. Abah dan ibu, yang selalu memberikan dorongan moral, spiritual, dan material sehingga penulisan skripsi ini dapat terselesaikan dengan baik.
8. Teman-teman jurusan Teknik Informatika dan untuk seluruh civitas akademika Universitas Islam Negeri Maulana Malik Ibrahim Malang yang telah banyak membantu perjuangan dan berbagi pengalaman dalam kehidupan sehari-hari.
9. Semua pihak yang tidak mungkin penulis sebutkan satu persatu, atas segala yang telah diberikan kepada penulis dan dapat menjadi pelajaran.

Sebagai penutup, penulis menyadari masih banyak kekurangan dalam skripsi ini. Semoga apa yang menjadi kekurangan bisa disempurnakan oleh peneliti selanjutnya. Harapan penulis selanjutnya adalah semoga karya ini bermanfaat bagi kita semua. Aamiin.

Malang, 20 Juli 2013

Penulis,

Achmad Chafidhi

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

DAFTAR ISI

HALAMAN JUDUL ..... **i**
HALAMAN PENGAJUAN ..... **ii**
LEMBAR PERSETUJUAN ..... **iii**
LEMBAR PENGESAHAN ..... **iv**
LEMBAR PERNYATAAN ..... **v**
MOTTO ..... **vi**
PERSEMBAHAN ..... **vii**
KATA PENGANTAR ..... **viii**
DAFTAR ISI ..... **x**
DAFTAR TABEL ..... **xii**
DAFTAR GAMBAR ..... **xiii**
ABSTRAK ..... **xiv**
BAB I: PENDAHULUAN **1**
1.1 Latar Belakang 1
1.2 Rumusan Masalah 5
1.3 Tujuan Penelitian 5
1.4 Manfaat Penelitian 5
1.5 Batasan Masalah 6
1.6 Sistematika Penulisan 7
BAB II: TINJAUAN PUSTAKA **8**
2.1.Kriptografi 8
2.1.1 Istilah kriptografi 8
2.1.2Klasifikasi Kriptografi 10
2.1.3Kunci Simetrik 12
2.1.4Algoritma RC 4 14
2.2*E-Voting*. 22
2.2.1 Definisi *E-Voting* 22
2.2.2Macam-Macam *E-Voting* 23
2.2.3Tehnik Pengiriman*E-Voting* 25

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

2.2.4 Prinsip-Prinsip *E-Voting* 27
2.2.5 Contoh Penerapan *E-Voting* 28
2.2.6 Pilkades 30
2.3. Software 30
2.3.1. Netbeans 33
2.3.2. MySQL 33
2.4.QR Code 34
BAB III: ANALISIS DAN PERANCANGAN SISTEM 41
3.1Tahapan Penelitian 41
3.2 Deskripsi Perangkat Lunak 42
3.3 AnalisaSistem 43
3.2.1 *Use Case Diagram* 43
3.2.2 *Activity Diagram* 45
3.2.3 *Flowcard* *54*
3.3 Perancangan Design 55
3.3.1 Design Admin 55
3.3.2 Design Kandidat 56
3.3.3 Design Pemilihan 57
3.5 Spesifikasi data base 57
3.4 Software 59
3.5 Hardware 60
BAB IV: HASIL PEMBAHASAN 61
4.1 Implementasi 61
4.1.1 Ruang Lingkup Perangkat Keras 61
4.1.2 Ruang Lingkup Perangkat Lunak 62
4.2 Implementasi Desain *Interface* 63
4.2.1 Menu Beranda 63
4.2.2 Menu Pendaftaran Pemilih 64
4.2.3 Menu Admin Pemilih 64
4.2.4 Menu Cetak Kartu Pemilih 65

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

4.2.5 Menu Edit Pemilih 664.2
.6 Menu Barcode 67
4.2.7 Menu Upload Foto 674.2
.8 Menu Proses Pemilihan 67
4.2.9 Menu Calon Pemilihan 68
4.2.10 Menu Enkripsi Pemilihan 68
4.2.11 Menu Deskripsi Pemilihan 68
4.2.12 Menu Konfirmasi 68
4.2.13 Menu Calon Kades 68
4.2.14 Menu Admin Kades 70
4.2.15 Menu Foto Kades 71
4.2.16 Menu Edit Kades 71
4.2.17Menu Grafik Rekapitulasi Pemilihan 72
4.3 Menu Control Database 72
4.3.1 Menu Database *E-voting* 72
4.3.2 Menu Database Pemilih 73
4.3.3 Menu Database Kandidat 74
4.3.4 Menu Database Agama 74
4.3.5 Menu Database Hasil 75
4.4 Pengujian Sistem 75
4.4.1 Pendaftaran 75
4.4.2 Pemilihan 76
4.4.3 Enkripsi Data 77
4.4.4 Uji Coba 79
4.5 Kriptografi Dalam Al-Quran 80
BAB V: PENUTUP 83
5.1 Kesimpulan 83
5.2 Saran 83
DAFTAR PUSTAKA 72

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

DAFTAR TABEL

Tabel 2.1 Serangan Brute Force Pada DES 17
Tabel 2.2 Serangan Brute Force Pada RC 4 18
Tabel 3.17 Tabel db Pemilih 56
Tabel 3.18 Tabel db Hasil 56
Tabel 3.19 db Agama 56
Tabel 3.20 Tabel db Pilihan 57

DAFTAR GAMBAR

Gambar 2.1 Klasifikasi Kriptografi 13
Gambar 2.2 Enkripsi Simetris 14
Gambar 2.5 Tingkatan Data 30
Gambar 2.6 QR Code 33
Gambar 2.7 Kode Dimensi 34
Gambar 2.8 Struktur QR Code 35
Gambar 2.9 bagian-bagian QR Code 36
Gambar 3.1 Gambaran Umum System 39
Gambar 3.2 *Use Case* Diagram *E-Voting* Pilkades Kedungdowo 40
Gambar 3.3 Keterangan Diagram *E-Voting* 41
Gambar 3.4 Activity Diagram Manage Kandidat 42
Gambar 3.5 Gambar *Manage* Pemilih 43
Gambar 3.6 *Manage* Data Admin 44
Gambar 3.7 *Manage* Membaca QR Code 45
Gambar 3.8 *Manage* Data Login Admin 46
Gambar 3.9 *Manage* Membaca QR Code 47
Gambar 3.10 Gambar Aplikasi Pemilihan 48
Gambar 3.11 Gambar Aplikasi Pemilihan 49
Gambar 3.12 Gambar Aplikasi Pemilihan 50
Gambar 3.13 Flowchar *E-Voting* 52
Gambar 3.14 Manage Tampilan Admin Edit,Delete,Uplode,Cetak 53
Gambar 3.15 Manage Tampilan Kandidat Edit,Delete,Uplode Dan Cetak 54
Gambar 3.16 Tampilan Pemilihan 55
Gambar 4.1 Menu Beranda 62
Gambar 4.2 Pendaftaran Pemilih 63
Gambar 4.3 Menu Admin Pemilih 63
Gambar 4.4 Menu kartu pemilih 64
Gambar 4.5 Menu Edit Pemilih 64
Gambar 4.6 Menu QR Code 64
Gambar 4.7 Menu Upload Foto 65
Gambar 4.8 Menu Proses Voting 65
Gambar 4.9 Menu Data Kandidat 66
Gambar 4.10 Menu Enkripsi 66
Gambar 4.11 Menu Konfirmasi Sudah Memilih 67

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

Gambar 4.12 Menu Kades 67
Gambar 4.13 Admin Calon Kandidat 68
Gambar 4.14 Menu Upload Kades..... 68
Gambar 4.15 Menu Edit Calon Kandidat..... 69
Gambar 4.16 Menu Grafik Pemilihan..... 70
Gambar 4.17 Menu apache 71
Gambar 4.18 Menu Data Base Admin..... 72
Gambar 4.19 Menu Data Pemilih 73
Gambar 4.20 Menu Beranda 73
Gambar 4.21 Menu Data Base Agama..... 73
Gambar 4.22 Menu DataBase Hasil Pilihan 73

DAFTAR KODE

Gambar 4.1 Koding QR Code..... 76
Gambar 4.2 Koding Pemilihan 77
Gambar 4.3 Koding RC 4 78

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

ABSTRAK

Chafidhi, Achmad. 2013. 06550107**.** Implementasi Algoritma *Rivest Cipher 4* Dalam Mengamankan Hasil *E-Voting* Pemilihan Kepala Desa Berbasis Java . Jurusan Teknik Informatika Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang. Pembimbing : (I) Ririen Kusumawati, M.Kom (II) Totok Chamidy, M.Kom

Kata Kunci : Kriptografi, *RC4, QR Code, E-voting.*

Pemungutan suara secara konvensional atau *voting* adalah proses pemungutan suara dan aspirasi serta keputusan penting untuk beberapa pihak. Tetapi pemungutan secara konvensional membutuhkan waktu yang lama dan sangat melelahkan untuk menunggu hasil *voting***.** *e-voting* menjadi alternatif proses pemungutan suara yang lebih mudah dan cepat serta dapat menurunkan tingkat kesalahan. Tetapi penerapan e-*voting* menyisakan persoalan terkait soal keamanan informasi yaitu keutuhan data (*integrity*), kerahasiaan informasi (*confidentiality*), dan ketersediaan informasi (*availability*). Kriptografi dapat dimanfaatkan untuk menjawab pertanyaan terkait dengan keamanan informasi berupa kerahasiaan, keutuhan data, serta otentikasi. Pada skripsi ini dijelaskan bagaimana QR Code mampu mengautentikasi daftar pemilih agar tidak ganda, dan algoritma *stream cipher* berupa RC4 digunakan untuk mengenkripsi plaintexs dan mendeskripsi ciphertext berupa hasil pemilihan. Algoritma RC4 merupakan enkripsi simetris golongan stream cipher yang mudah dipelajari, ciri khas RC4 memiliki dua fase yaitu setup kunci dan pengenkripsian dengan panjang kunci 1024 bit. Pada waktu proses enkripsi dan deskripsi membutuhkan waktu yang relative singkat. Dalam implementasinya sangat relevan untuk meningkatkan keamanan aplikasi e-voting pemilihan kepala Desa Kedungdowo.

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

ABSTRAK

Chafidhi, Achmad. 2013. 06550107. *RivestCipher4AlgorithmImplementationInSecuringE-Voting ElectionResultsVillage HeadJava based.* Department of Informatics, Faculty of Science and Technology of the State Islamic University of Maulana Malik Ibrahim Malang. Supervisor: (I) Ririen Kusumawati, M.Kom (II) totok Chamidy, M.Kom

Kata Kunci : Kriptografi, *RC4, QR Code, E-voting.*

Conventional ballot or voting is the voting process and aspirations as well as important decisions for some parties. But the conventional collection takes a long time and very tiring to wait for the results of voting. e-voting into alternative voting process easier and faster, and can reduce the error rate. But the application of e-voting leaves about information security issues related to the integrity of the data (integrity), confidentiality (confidentiality), and the availability of information (availability). Cryptography can be used to answer questions related to information security such as confidentiality, integrity of data, and authentication. In this paper described how a QR Code is able to authenticate the voter list so as not to double, and the form of the RC4 stream cipher used to encrypt and decrypt ciphertext plaintexs form of election results. RC4 symmetric encryption algorithm is a class of stream ciphers are easy to learn, the hallmark has two phases namely RC4 key setup and pengenkripsian with 1024 bit key length. At the time of the encryption process and the description requires a relatively short time. In its implementation is very relevant to improve the security of e-voting election Kedungdowo village.

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

BAB I

PENDAHULUAN

1.1 Latar Belakang

Demokrasi secara harfiah berasal dari kata *demos* yang berarti rakyat dan *kratos* atau *kratein* yang berarti kekuasaan atau berkuasa. Sehingga sistem pemerintahan dimana kekuasaan terletak pada mayoritas rakyat dan pelaksanaan dilaksanakan melalui wakil yang terpilih. Menurut Puspowati demokrasi dapat dikatakan secara sederhana sebagai pemerintahan rakyat yaitu suatu pemerintah dengan rakyat memiliki peranan yang sangat menentukan dalam mengambil kebijakan-kebijakan sebuah desa (2005 : 1). Abraham Linchon berpendapat demokrasi berarti pemerintahan yang di selenggarakan "dari rakyat, oleh rakyat, untuk rakyat". Sehingga kekuasaan tertinggi berada di tangan rakyat. (1861 : 1).

Sistem pemilihan kepala desa masih menggunakan sistem pemilihan konvensional, proses pemungutan dan perhitungan suara secara sistem konvensional tersebut memiliki beberapa kelemahan. Menurut Azhari Beberapa kelemahan sistem voting pemilihan kepala desa kenvensional (2005 : 1) antara lain sebagai berikut :

a. Banyak terjadi kesalahan dalam proses pendaftaran pemilih. Dikarenakan banyak menggunakan kartu identitas. Sehingga banyaknya pemilih yang memiliki kartu suara yang lebih dari satu. Keadaan ini biasanya dimanfaatkan oleh salah satu pihak tertentu untuk meningkatkan jumlah suara pilihan sehingga dapat meningkatkan suara voting calon kepala desa.

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

b. Pemilih salah dalam memberikan tanda suara, karena ketentuan keabsahan yang kurang jelas serta kurangnya sosialisasi yang dilakukan panitia mengakibatkan banyak suara yang tidak sah. Pada saat verifikasi keabsahan surat suara sering terjadi kontrovesi peraturan.

c. Proses pengumpulan suara yang berjalan lambat karena badan permusyawarahan desa harus menghitung manual kertas suara yang telah masuk.

d. Kurang terjaminnya kerahasiaan dari pemilih dalam memberikan suara voting. Dikarenakan adanya intimidasi dan *monay politic* dari pihak tertentu untuk memberikan suara.

Seiring dengan perkembangbiakan teknologi informasi yang sangat pesat. Berbagai masalah-masalah pemilihan kepala desa dapat diatasi dengan sistem *electronic voting*. Dalam dunia teknologi informasi sering kali muncul masalah yang berkenaan dengan kerahasian data. Seperti adanya penyadapan data, virus yang dapat menggandakan data orang lain, ataupun dengan menyewa jasa hacker agar dapat mengetahui data yang di inginkan. Dengan adanya kemungkinan penyadapan data tersebut maka aspek keamanan menjadi sangat penting karena suatu kerahasian pemilih menjadi harga mati. Rahasia adalah sebuah amanat dan menjaga rahasia sangat dianjurkan oleh Allah seperti dalam firman-Nya:

۞ إِنَّ ٱللَّهَ يَأۡمُرُكُمۡ أَن تُؤَدُّواْ ٱلۡأَمَٰنَٰتِ إِلَىٰٓ أَهۡلِهَا وَإِذَا حَكَمۡتُم بَيۡنَ ٱلنَّاسِ أَن تَحۡكُمُواْ بِٱلۡعَدۡلِۚ إِنَّ ٱللَّهَ نِعِمَّا يَعِظُكُم بِهِۦٓۗ إِنَّ ٱللَّهَ كَانَ سَمِيعَۢا بَصِيرٗا ٥٨

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

58. "*Sesungguhnya Allah menyuruh kamu menyampaikan amanat kepada yang berhak menerimanya, dan (menyuruh kamu) apabila menetapkan hukum di antara manusia supaya kamu menetapkan dengan adil. Sesungguhnya Allah memberi pengajaran yang sebaik-baiknya kepadamu. Sesungguhnya Allah adalah Maha mendengar lagi Maha melihat". (QS.An-Nisa' ; 58)*

Dari ayat di atas, menurut 'Aidh al-Qarni dalam buku Tafsir Muyassar jilid.1 dijelaskan bahwa Allah menyuruh kalian agar senantiasa menyampaikan amanat kepada yang berhak menerimanya. Sehingga ayat tersebut menganjurkan agar kita menjaga amanat yang dititipkan kepada kita dan tidak memberitahukan amanat tersebut kepada orang yang tidak berhak menerimanya, dan salah satu jenis dari amanat tersebut adalah rahasia. Dan rahasia tersebut, dimana rahasia tersebut dapat disampaikan dalam bentuk pesan tertulis.

Dikarenakan rahasia merupakan amanat, maka kita juga berkewajiban menjaga rahasia yang telah dititipkan kepada kita dan janganlah menghianati amanah tersebut dengan memberitahukannya kepada orang yang tidak berhak. Seperti dijelaskan dalam al-qur'an sebagai berikut:

يَٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُواْ لَا تَخُونُواْ ٱللَّهَ وَٱلرَّسُولَ وَتَخُونُوٓاْ أَمَٰنَٰتِكُمۡ وَأَنتُمۡ تَعۡلَمُونَ ٢٧

Hai orang-orang yang beriman, janganlah kamu mengkhianati Allah dan Rasul (Muhammad) dan (juga) janganlah kamu mengkhianati amanat-amanat yang dipercayakan kepadamu, sedang kamu mengetahui.(QS. Al-Anfal; 27)

Menurut 'Aidh al-Qarni dalam buku Tafsir Muyassar jilid2, ayat diatas menjelaskan bahwa janganlah kalian menghianati setiap amanat yang diberikan kepada kalian, seperti hak, kewajiban, rahasia. Sedangkan kalian mengetahui penghianatan amanah ini hukumnya haram.

Ayat di atas menganjurkan kepada kita agar tidak menghianati setiap amanat yang diberikan kepada kita. Salah satu dari jenis amanah tersebut adalah

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

rahasia. Sehingga menjaga rahasia juga sangat diwajibkan dan apabila kita memberitahukan rahasia tersebut berarti sama dengan kita menghianati amanah yang diberikan kepada kita. Sedangkan menghianati amanah hukumnya adalah haram.

Ayat tersebut juga dikuatkan dengan hadits Rasulullah yang ditulis oleh Imam Nawawi dalah bukunya Riyadhus Sholihin sebagai berikut:

وَ عَنْ ثَابِتٍ عَنْ أَنَسٍ رَضِىَ اللهُ عَنْهُ قَالَ : أَتَى عَلَيَّ رَسُوْلُ اللهِ صَلَّى اللهُ عَلَيْهِ وَسَلَّمَ وَأَنَا أَلْعَبُ مَعَ الْغِلْمَانِ ، فَسَلَّمَ عَلَيْنَا فَبَعَثَنِى فِى حَاجَةٍ ، فَأَبْطَأْتُ عَلَى أُمِّى . فَلَمَّا جِئْتُ قَالَتْ : مَا حَبَسَكَ ؟ فَقُلْتُ : بَعَثَنِى رَسُوْلُ اللهِ صَلَّى اللهُ عَلَيْهِ وَسَلَّمَ لِحَاجَةٍ ، قَالَتْ : مَا حَاجَتُهُ ؟ قُلْتُ : إِنَّهَا سِرٌّ . قَالَتْ : لاَ تُخْبِرَنَّ بِسِرِّ رَسُوْلُ اللهِ صَلَّى اللهُ عَلَيْهِ وَسَلَّمَ أَحَدًا . قَالَ أَنَسٌ : وَاللهِ لَوْ حَدَّثْتُ بِهِ أَحَدًا لَحَدَّثْتُكَ بِهِ يَا ثَابِتُ . (رواه مسلم)

"Dari Tsabit dari Anas R.A, dia berkata : "Saya didatangi oleh Rasulullah ketika itu aku sedang bermain- main dengan anak- anak. Beliau mengucapkan salam kepada kami lalu menyuruh saya untuk suatu keperluan, akhirnya saya terlambat menemui ibuku. Ketika saya datang ibuku bertanya: "apa yang membuatmu terlambat?". Saya menjawab: "saya disuruh oleh Rasulullah SAW untuk suatu keperluan". Ibu bertanya: "apa keperluan beliau?" saya menjawab: "itu rahasia". Ibu berkata: "jangan sekali- kali kau memberitahukan rahasia Rasulullah SAW kepada siapapun". Anas berkata: "demi Allah seandainya aku memberitahukannya kepada seseorang tentu aku telah memberitahukannya kepadamu wahai Tsabit". (HR. Muslim)

Hadits tersebut mengajarkan kepada kita bahwa menjaga rahasia telah diajarkan oleh Nabi Muhammad SAW kepada para sahabat. Dan janganlah melakukan penghianatan terhadap rahasia yang diamanatkan kepada kita karena sesungguhnya menghianati amanah dengan menyampaikan rahasia adalah haram hukumnya, seperti yang telah dijelaskan pada surat Al-Anfal.

Berbagai cara yang dilakukan untuk menjamin keamanan informasi*e-voting*. Dan dengan berkembangnya cara pengiriman *e-voting* nantinya, berkembangpula cara menyembunyikan pesan kriptografi dan bagaimana agar

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

orang lain tidak mengetahui isi pesan atau informasi walaupun pesan tersebut telah ditemukan. Salah satunya adalah dengan menyandikan informasi menjadi suatu kode-kode yang tidak dimengerti, sehingga apabila disadap akan kesulitan untuk mengetahui informasi yang sebenarnya. Dari sinilah lahir suatu ilmu yang disebut kriptografi.

1.2 Rumusan Masalah

1. Bagaimana merancang *e-voting* pemilihan kepala desa kedungdowo yang sesuai dengan UU No 4 Tahun 2007 tentang pilkades.
2. Bagaimana merancang keamanan data pemilih saat melakukan pencoblosan agar tetap terjaga kerahasiaanya

1.3 Tujuan Penelitian

1. Membuat aplikasi *e-voting* pemilihan kepala desa kedungdowo agar sesuai dengan UU No 4 Tahun 2007 tentang pilkades.
2. Membuat keamanan data pemilih e-voting pilkades menggunakan algoritma RC 4.

1.4 Manfaat Penelitian

1. Menghasilkan aplikasi e-voting pemilihan kepala desa Kedungdowo yang sesuai dengan UU No 4 tahun 2007.
2. Menghasilkan keamanan data pemilih e-voting pilkades menggunakan algoritma RC 4

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

1.5 Batasan Masalah

a. Sistem *e-voting* dalam pemilihan kepala desa Kedungdowo.
b. Input pemilihan *e-voting* menggunakan nomer induk kependudukan yang tertera pada KTP yang telah dikodekan dengan *QR cod*e.
c. Sistem menggunakan bahasa pemrograman *java server page* (JSP) dan menggunakan database MySQL.
d. Sistem e-voting menggunakan algoritma *Rivest Cipher* (*RC4)* dalam mengamankan data hasil pemilih.

1.6 Sistematika Pembahasan

Dalam penulisan skripsi ini, secara keseluruhan terdiri dari lima bab yang masing-masing bab disusun dalam sistematika sebagai berikut:

1. BAB I: Pendahuluan, membahas tentang latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika pembahasan.
2. BAB II :Tinjauan Pustaka, membahas tentang teori yang berhubungan dengan permasalahan penelitian yang berkenaan dengan e-voting, Kriptografi *Rivest Cipher 4*, QR Code.
3. BAB III:Analisis dan Perancangan Sistem, membahas tentang pembuatan desain dan perancangan sistem *e-voting* pemilihan kepala desa menggunakan metode *Rivest Cipher* 4.

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

4. BAB IV: Hasil Dan Pembahasan, membahas hasil yang dicapai dari perancangan sistem dan implementasi program, yaitu dengan melakukan pengujian sehingga dapat ditarik kesimpulan.
5. BAB V: Penutup, membahas kesimpulan berdasarkan hasil yang telah dicapai dari pembahasan. Serta berisi saran yang diharapkan sebagai bahan oleh pihak yang akan melakukan pengembangan terhadap program aplikasi ini ke depannya.

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

BAB II

TINJAUAN PUSTAKA

Bab ini menjelaskan teori dan konsep yang menjadi landasan materi dari sistem yang akan dibuat. Beberapa teori dan konsep yang akan dibahas antara lain pembahasan konsep dasar *e-voting*, kriptografi, algoritma *Rivest Cipher* 4, QR Code.

2.1 Kriptografi

Kriptografi (*cryptography*) berasal dari bahasa Yunani, *cryptos* artinya *secret* (rahasia), sedangkan *graphien* artinya *writing* (tulisan). Jadi, kriptografi berarti *secret writing* (tulisan rahasia). Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain (Ariyus, 2008 : 13). Kata seni didalam definisi tersebut berasal dari fakta sejarah bahwa pada masa awal-awal sejarah kriptografi, setiap orang mungkin mempunyai cara yang unik untuk merahasiakan pesan. Cara-cara unik tersebut mungkin berbeda-beda pada setiap pelaku kriptografi, sehingga setiap cara menulis pesan rahasia mempunyai nilai estetika tersendiri, sehingga kriptografi berkembang menjadi sebuah seni merahasiakan pesan (kata *graphy* di dalam *cryptography* itu sendiri sudah mengisyaratkan sebuah seni).

Dalam sumber yang lain, kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi (Munir, 2006 : 2). Sebuah pesan rahasia harus terjaga keamanannya, salah satu caranya adalah dengan penyandian

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

pesan yang bertujuan meyakinkan privasi dengan menyembunyikan informasi dari orang- orang yang tidak ditujukan informasi tersebut kepadanya.

وَلَقَدْ جَعَلْنَا فِي ٱلسَّمَآءِ بُرُوجًا وَزَيَّنَّٰهَا لِلنَّٰظِرِينَ ﴿١٦﴾ وَحَفِظْنَٰهَا مِن كُلِّ
شَيْطَٰنٍ رَّجِيمٍ ﴿١٧﴾ إِلَّا مَنِ ٱسْتَرَقَ ٱلسَّمْعَ فَأَتْبَعَهُۥ شِهَابٌ مُّبِينٌ ﴿١٨﴾

16. dan Sesungguhnya Kami telah menciptakan gugusan bintang-bintang (di langit) dan Kami telah menghiasi langit itu bagi orang-orang yang memandang (Nya),
17. dan Kami menjaganya dari tiap-tiap syaitan yang terkutuk,
18. kecuali syaitan yang mencuri-curi (berita) yang dapat didengar (dari malaikat) lalu Dia dikejar oleh semburan api yang terang.(QS Al-Hijr, 16-18)

Allah telah menjadikan Lauh Mahfuzh ini sebagai tempat untuk menyimpan segala rahasia dilangit dan di bumi.Jin dari golongan setanakan berusaha untuk mencuri segala rahasia yang tertulis di dalamnya untuk menipu manusia. Disamping itu, mereka juga memiliki tujuan untuk memainkan aqidah manusia. Sebab itu Allah melarang manusia untuk mengetahui ramalan nasib, karena peramal itu dibantu oleh jin dan jin itu akan membisikkan hasil curian itu kedalam hati peramal. Jika ada setan yang berusaha mencuri berita, maka malaikat penjaga Luh Mahfuzh akan melemparkan bintang ke arah pencuri berita tersebut, pelemparan ini yang kadang-kadang kita lihat dengan adanya bintang jatuh atau meteor.Penyandian pesan yang bertujuan untuk menyembunyikan informasi tersebut diperbolehkan dalam Islam karena tujuannya adalah untuk menjaga rahasia dari pesan yang disampaikan. Hal tersebut dikarenakan dalam al-qur'an telah dijelaskan tentang perintah menjaga rahasia, dimana rahasia juga termasuk dalam kategori amanat. Sebagaimana telah dijelaskan dalam firman-Nya sebagai berikut:

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

۞ إِنَّ ٱللَّهَ يَأۡمُرُكُمۡ أَن تُؤَدُّواْ ٱلۡأَمَٰنَٰتِ إِلَىٰٓ أَهۡلِهَا وَإِذَا حَكَمۡتُم بَيۡنَ ٱلنَّاسِ أَن تَحۡكُمُواْ بِٱلۡعَدۡلِۚ إِنَّ ٱللَّهَ نِعِمَّا يَعِظُكُم بِهِۦٓۗ إِنَّ ٱللَّهَ كَانَ سَمِيعَۢا بَصِيرٗا ٥٨

"Sesungguhnya Allah menyuruh kamu menyampaikan amanat kepada yang berhak menerimanya, dan (menyuruh kamu) apabila menetapkan hukum di antara manusia supaya kamu menetapkan dengan adil. Sesungguhnya Allah memberi pengajaran yang sebaik-baiknya kepadamu. Sesungguhnya Allah adalah Maha mendengar lagi Maha Melihat".(QS. An-Nisa'/4 : 58)

Dari ayat di atas, menurut 'Aidh al-Qarni dalam buku Tafsir Muyassar jilid.1 dijelaskan bahwa Allah menyuruh kalian agar senantiasa menyampaikan amanat kepada yang berhak menerimanya. Sehingga ayat tersebut menganjurkan agar kita menjaga amanat yang dititipkan kepada kita dan tidak memberitahukan amanat tersebut kepada orang yang tidak berhak menerimanya, dan salah satu jenis dari amanat tersebut adalah rahasia. Dan rahasia tersebut dapat berupa pesan tertulis. Untuk itulah, kriptografi dapat digunakan sebagai sarana untuk menjaga keamanan pesan, yakni pesan yang bersifat rahasia.

2.1.1 Istilah-Istilah Dalam Kriptografi

a. Pesan, Plainteks, Dan Chipertext

Pesan (message) adalah data atau informasi yang dapat dibaca dan dimengerti maknanya. Nama lain untuk pesan adalah plaintext. Pesan dapat berupa data atau informasi yang dikirim melalui kurir atau media telekomunikasi lainatau yang di dalam media penyimpanan *(storage).* Agar pesan tidak dapat dimengerti maknanya oleh pihak lain, maka pesan harus disandikan kebentuk lain yang tidak dapat difahami. Bentuk pesan tersandikan

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

disebut dengan cipertext.Chipertext harus dapat dikembalikan menjadi plaintext semula agar dapat di baca oleh orang yang seharusnya menerima pesan.

b. Pengirim Dan Penerima

Pengirim dan penerima komunikasi data yang menggunakan kriptografi selalu menggunakan 2 pihak atau entitas. Pengirim *(sender)*adalah entitas yang mengirim pesan kepada entitas lain. Penerima *(receiver)* adalah entitas yang menerima pesan entitas.Disini dapat berupa orang,mesin maupun Komputer.

c. Enkripsi Dan Deskripsi

Enkripsi *(encryption)* atau *enciphering* standart nama menurut ISO 7498-2 merupakan proses penyandian plaintext menjadi chipertext. Sedangkan deskripsi adalah (*deskription*) standart nama menurut ISO 7498-2 merupakan proses pengembalian chipertext menjadi plaintext semula (A Darto Iwan S, 2009, dan Rinaldi Munir, 2004)

d. Cipher

Algoritma kriptografi disebut juga cipher yaitu aturan untuk encipheringdan decipheringatau fungsi matematika yang digunakan untuk enkripsi dan deskripsi. Konsep matematis yang mendasari algoritma kriptografi adalahrelasi antara dua buah himpunan yaitu himpunan yang berisi elemen elemen plaintexs dan himpunan dan himpunan yang berisi chipertext. Enkripsi dan deskripsi merupakan fungsi yang memetakan elemen-elemen antara kedua

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

himpunan tersebut,misalnya P menyatakan plaintext dan C menyatakan chipertext maka fungsi enkripsi E memetakan P ke C

E(P) = C

Dan fungsi deskripsi D memetakan C ke P:

D(C) = P

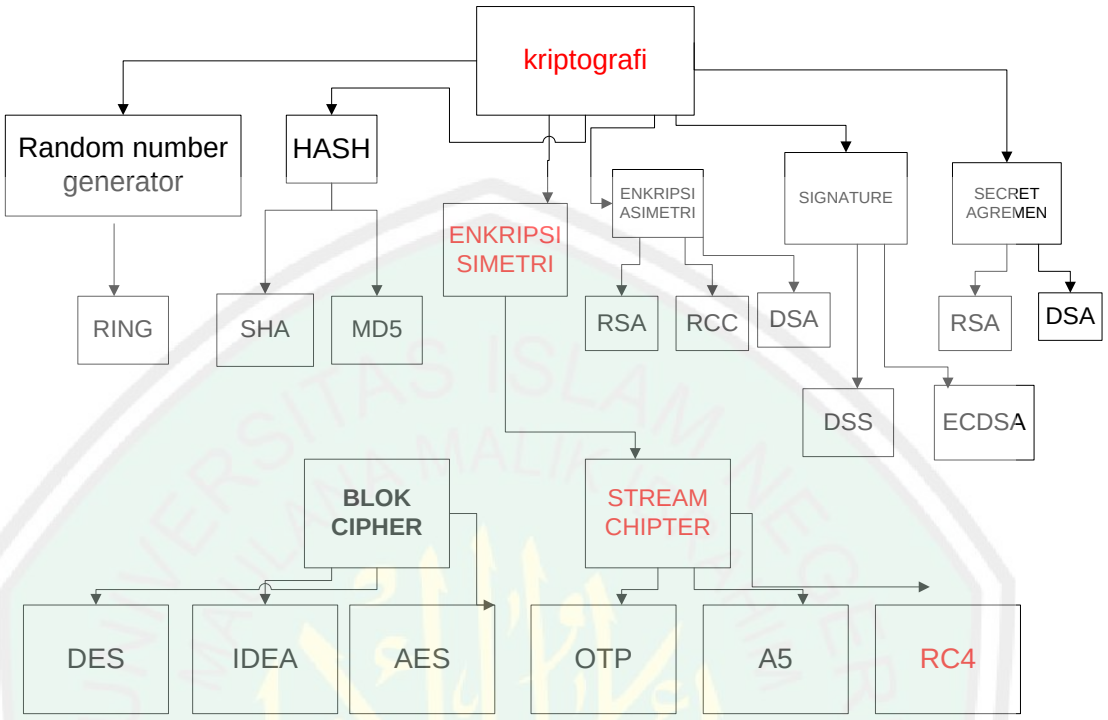
karena proses enkripsi kemudian deskripsi mengembalikan pesan ke pesan awal, maka kesamaan berikut harus benar :

D(E(C)) : P

2.1.2 Klasifikasi Kriptografi

Menurut Rinaldi Munir terdapat enam kasifikasi kriptografi namun berdasarkan jenis kunci yang digunakan, dikenal dua buah algoritma yaitu algoritma kriptografi simetris atau private key algorithm. Algoritma kriptografi asimetris atau key public algorithm (2004 : 12) seperti Nampak pada gambar 2.1. Berikut ini adalah klasifikasi kriptograsi dimana salah satunya terdapat RC4 yang merupakan enkripsi simetri jenis stream chipter.

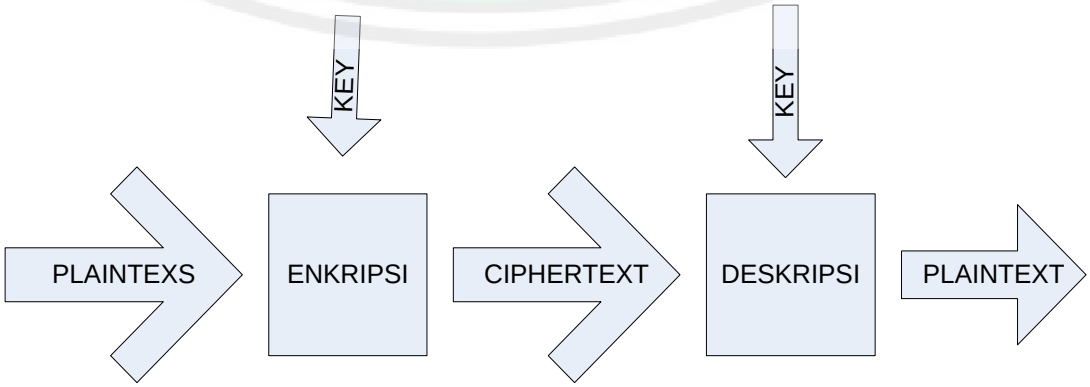
CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG



Gambar 2.1 Klasifikasi Kriptografi

2.1.3 Kunci Simetrik

Kunci Simetrik yang sering disebut algoritma konvensional adalah algoritma yang menggunakan kunci yang sama untuk proses enkripsi dan dekripsinya (Schneier, 1996). Dari gambar ini terlihat bahwa untuk mengenkripsi dan mendekripsinya pesan hanya menggunakan satu buah kunci saja (K) saja :



Gambar 2.2 Enkripsi Simetris

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

Untuk menjaga kerahasiaan pesan antar komunikan pada kriptografi ini dibutuhkan sebuah kunci untuk tiap pasangan komunikan. Sehingga untuk *n* komunikan jumlah kunci yang dibutuhkan adalah: $\frac{n(n-1)}{2}$

Kelebihan kriptografi kunci simetri adalah:

a. Proses enkripsi atau dekripsi kriptografi kunci simetri membutuhkan waktu yang singkat.
b. Ukuran kunci simetri relatif lebih pendek.
c. Otentikasi pengiriman pesan langsung diketahui dari cipherteks yang diterima, karena kunci hanya diketahui oleh pengirim dan penerima saja.

Sedangkan kelemahan kriptografi kunci simetri adalah:

a. Kunci simetri harus dikirim melalui saluran komunikasi yang aman, dan kedua entitas yang berkomunikasi harus menjaga kerahasiaan kunci.
b. Kunci harus sering diubah setiap kali melakukan komunikasi.

Beberapa algoritma yang memakai kunci simetri adalah Data Encryption Standard (DES), RC2, RC4, RC5, RC6, International Data Encryption Algorithm (IDEA), Advanced Encryption Standard (AES), One Time Pad (OTP), Blowfish, dan lain sebagainya.

2.1.4 Algoritma RC 4

Algoritma RC4 adalah algoritma kriptografi simetrik. Disebut algoritma kriptografi simetrik karena menggunakan kunci yang sama untuk mengenkripsi ataupun mendekripsi suatu pesan, data, ataupun informasi. Kunci enkripsi didapat dari sebuat 256 bit *state-array* yang di inisialisasi dengan sebuah *key* tersendiri

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

dengan panjang 1-256 bit. Setelah itu, *state-array* tersebut akan diacak kembali dan diproses untuk menghasilkan sebuah kunci enkripsi yang akan di-*XOR*-kan dengan plainteks ataupun cipherteks.

Secara umum, algoritma RC4 terbagi menjadi dua, inisalisasi *state-array* dan penghasilan kunci enkripsi serta pengenkripsiannya.

a. **Penginisialisasian *State-Array***

Dalam penginisialisasian *state-array*, terdapat 2 *state array* yang harus diinisialisasi, S dan K. Array S sebesar 256 bit di inisialisasi dengan angka dari 0 sampai dengan 255. Sedangkan array K sebesar 256 bit diisi dengan key dengan panjang 1-256 bit secara berulang sampai seluruh array K terisi penuh. Setelah itu, dilakukan *Key Scheduling Algorithm* untuk menghasilkan permutasi dari array S berdasarkan key yang tersedia.

```
for i from 0 to 255
S[i] := i
endfor
j := 0
for i from 0 to 255
j := (j + S[i] + key[i mod
keylength]) mod 256
swap(&S[i],&S[j])
endfor
```

2.3 Gambar inisialisasi state array

Proses swap di atas adalah proses menukar nilai antara S[i] dengan S[j].

Proses swap memiliki algoritma sebagai berikut.

```
temp = s[i];
s[i] = s[j];
s[j] = temp;
```

2.4 Gambar proses swap

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

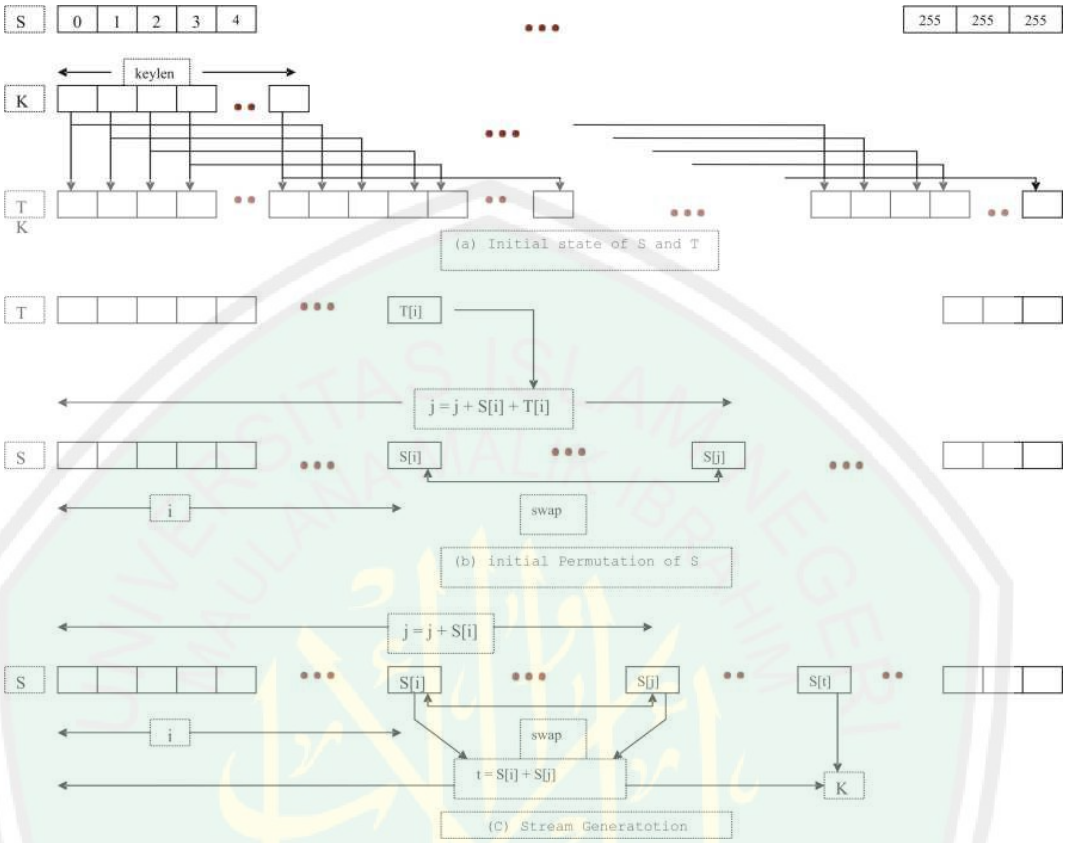
b. Penghasilan Kunci Enkripsi dan Pengenkripsian

Setelah memiliki *state array* yang telah teracak, maka kita akan menginisialisasi kembali i dan j dengan 0. Setelah itu, kita lakukan *pseudo-random generation algorithm* atau PRGA untuk menghasilkan kunci enkripsi (dalam hal ini cipher_byte) yang akan di-*XOR*-kan dengan plainteks. Untuk menghasilkan kunci enkripsi, PRGA meng-*incremen* i, menambahkan nilai S[i] dan S[j] menukar nilai keduanya, dan nilai kunci yang dihasilkan adalah S dengan indeks yang sama dengan jumlah S[i] dan S[j] di-modulo dengan 256.

```
i := 0
j := 0
while GeneratingOutput:
i := (i + 1) mod 256
j := (j + S[i]) mod 256
swap(&S[i],&S[j])
byte_cipher := S[(S[i] + S[j])
mod 256]
result_ciphered := byte_cipher
XOR byte_message
endwhile
```

2.5 Gambar PRGA

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG



Gambar 2.6 Ilustrasi Algoritma RC4

c. Contoh Enkripsi dengan metode RC4

Untuk menunjukkan bagaimana RC4 bekerja pada tingkat dasar, mari kita state-array 4 bit. Hal ini dikarenakan akan sangat sulit menggambarkan proses RC4 secara manual dengan state-array 256 bit. Kali ini, kita akan mengenkripsi kata HALO dengan kunci 3123.

Pertama, kita menginisialisasi array S 4 bit sehingga terbentuk state-array S dan state-array K sebagai berikut,

Array S

0	1	2	3

Array K

2	5	7	3

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

Inisialisasi i dan j dengan 0 kemudian dilakukan KSA agar tercipta state-array yang acak. Penjelasan iterasi lebih lanjut dapat dijelaskan sebagai berikut.

Iterasi 1
i = 0
j = (0 + S[0] + K [0 mod 4]) mod 4
= (0 + 0 + 2) mod 4 = 2
Swap (S[0],S[2])

Hasil Array S

2	1	0	3

Iterasi 2
i = 1
j = (2 + S[1] + K [1 mod 4]) mod 4
= (2 + 1 + 5) mod 4 =0
Swap (S[1],S[0])

Hasil array S

1	2	0	3

Iterasi 3
i = 2
j = (0 + S[2] + K [2 mod 4]) mod 4
= (0 + 0 + 7) mod 4 = 3
Swap (S[2],S[3])

Hasil

1	2	3	0

Iterasi 4
i = 3
j = (3 + S[3] + K [3 mod 4]) mod 4
= (3 + 0 + 3) mod 4 = 2
Swap (S[3],S[2])

Hasil Array S

1	2	0	3

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

Setelah melakukan KSA, akan dilakukan PRGA. PRGA akan dilakukan sebanyak 4 kali dikarenakan plainteks yang akan dienkripsi berjumlah 4 karakter. Hal ini disebakan karena dibutuhkan 1 kunci dan 1 kali pengoperasian XOR untuk tiap-tiap karakter pada plainteks.

Berikut adalah tahapan penghasilan kunci enkripsi dengan PRGA.

Array S

1	2	0	3

Inisialisasi
i = 0
j = 0

Iterasi 1
i = (0 + 1) mod 4 = 1
j = (0 + S[1]) mod 4 = (0+ 2) mod 4 = 2
swap (S[1],S[2])

1	0	2	3

K1 = S[(S[1]+S[2]) mod 4] = S[2 mod 4] = 2
K1 = 00000010

Iterasi 2
i = (1 + 1) mod 4 = 2
j = (2 + S[2]) mod 4 = (2+ 2) mod 4 = 0
swap (S[2],S[0])

2	0	1	3

K2 = S[(S[2]+S[0]) mod 4] = S[3 mod 4] = 3
K2 = 00000011
Iterasi 3
i = (2 + 1) mod 4 = 3

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

j = (0 + S[3]) mod 4 = (0+ 3) mod 4 = 3
swap (S[3],S[3])

1	0	2	3

K3 = S[(S[3]+S[3]) mod 4] = S[6 mod 4] = 2
K3 = 00000010
Iterasi 4
i = (3 + 1) mod 4 = 0
j = (3 + S[0]) mod 4 = (3+ 1) mod 4 = 0
swap (S[0],S[0])

1	0	2	3

K1 = S[(S[0]+S[0]) mod 4] = S[2 mod 4] = 2
K1 = 00000010

Setelah menemukan kunci untuk tiap karakter, maka dilakukan operasi XOR antara karakter pada plaintext dengan kunci yang dihasilkan. Berikut adalah tabel ASCII untuk tiap-tiap karakter pada plaintks yang digunakan.

Tabel 2.1 Kode ASCII untuk setiap karakter plainteks yang digunakan

Huruf	Kode ASCII (Binary 8 bit)
H	01001000
A	01000001
L	01001100
O	01001111

Proses XOR dari kunci bisa dilihat pada tabel 2.

Tabel 2.2 Proses XOR kunci enkripsi dengan plainteks pada enkripsi

	H	A	L	O
Plainteks	01001000	01000001	01001100	01001111
Key	00000010	00000011	00000010	00000010
Cipherteks	01001010 (L)	01000010 (B)	01001110 (N)	01001101 (M)

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

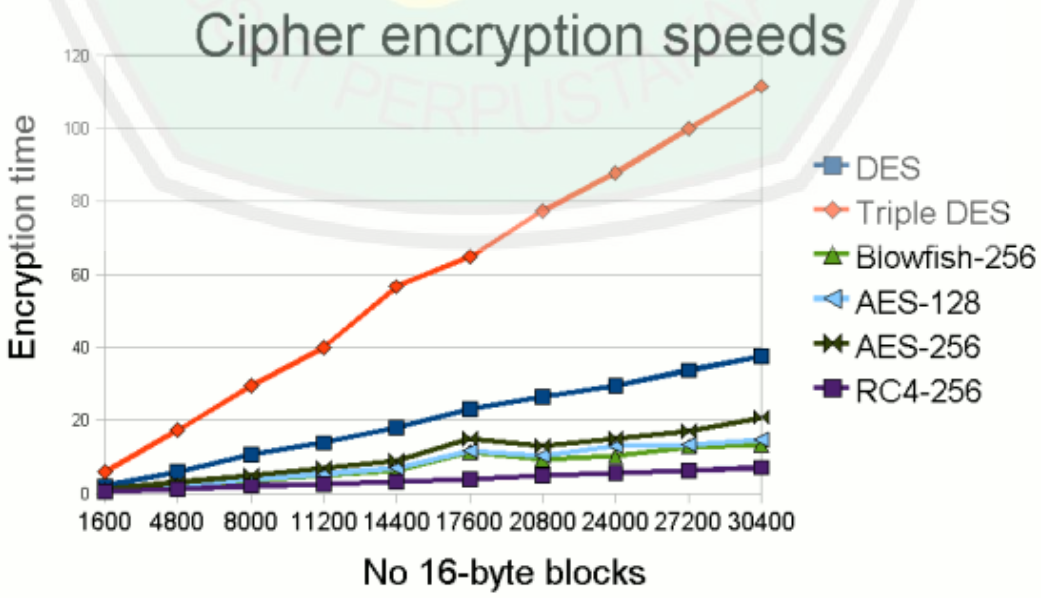
Setelah terkirim, pesan yang telah dienkripsi akan didekripsikan. Proses pendekripsian dilakukan dengan proses XOR antara kunci dekripsi yang sama dengan kunci dekripsi dengan cipherteks yang dapat dilihat di tabel 3.

Tabel 2.3 Proses XOR kunci dekripsi dengan cipherteks pada dekripsi

	L	B	N	M
Cipherteks	01001010	01000010	01001110	01001101
Key	00000010	00000011	00000010	00000010
Plainteks	01001000 (H)	01000001 (A)	01001100 (L)	01001111 (O)

d. Kecepatan RC4 Sebagai Salah Satu Metode Enkripsi

Kinerja RC4 sebagai metode enkripsi tergolong sangat cepat. Selain cepat, waktu RC4 tidak terpengaruh dengan panjang keylength yang dipakai. Berikut adalah perbandingan waktu yang digunakan untuk enkripsi dari berbagai metode.



Gambar 2 Perbandingan waktu enkripsi dari berbagai metode

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

2.2 *E-Voting*

2.2.1 Definisi *E-Voting*

a. *E-Voting*

adalah suatu metoda pengumpulan suara dengan menggunakan perangkat elektronik

b. *Remote voting*

adalah suatu cara/metoda pemberian suara pemilih padasuatu tempat dimana saja, seperti di rumah, di kantor atau dijalan, artinyadilokasi mana saja asal ada kesempatan bisa melakukan pemilihan suara.

c. *Supervised voting*

adalah suatu proses pemilihan suara (memberikansuara) yang diawasi oleh petugas atau pejabat pemilihan umum (KPU).

d. *Remote electronic voting*

adalah pemilihan suara pada suatu tempatdengan menggunakan perangkat elektronik, tanpa pengawasan petugas/pejabat pemilihan umum (KPU)

e. *Internet Voting*

adalah pemilihan suara melalui media internet, bisa dimana saja seperti dirumah, diperjalanan atau di tempat yang sudah disediakan

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

2.2.2 Macam-Macam Teknologi Voting

Ada enam macam teknologi voting yang umum digunakan yaitu:

1. **Kertas Suara/ Surat Pemilihan (*Paper Ballots*)**

Tekonologi ini adalah teknologi yang pertama dalam peradaban umat manusia dalam berdemokrasi, dimana kertas suara dijadikan dasar untuk menghitung suara pemilih. Cara melakukan pemilihan adalah pemilih mengambil kertas suara yang sudah disediakan dalam bentuk formulir, nama-nama calon dan gambarnya sudah tercetak, setelah itu pemilih tinggal menusuk atau mencoblos photo atau symbol calon pilihannya dan memasukkannya kedalam suatu kotak suara yang sudah disediakan oleh petugas. Selanjutnya team atau anggota panitia akan melakukan penghitungan suara.

2. ***Lever Machines***

Teknologi berikutnya (*Technological advance*) adalah *Lever Machines* yang dimulai diperkenalkan pada tahun 1892.Teknologi ini tidak terdapat dokumen suara.Pemilih memasukkan suara dalam suatu tempat dengan memilih daftar calon dan mengumpulkan masing-masing calon terpilih. Suara dicatat dan dihitung dengan *Lever Machines*

3. ***Punchcards***

Teknologi *punchcard,* pertama kali dipakai untuk menghitung suara dengan menggunakan komputer yang dimulai pada tahun 1964. Dalam sistem ini, suara dicatat dengan memilih lubang-lubang padu kartu atau kertas komputer dan selanjutnya komputer akan membaca kartu suara. Kartu suara

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

adalah sebagai dokumen suara pemilih yang tercatat. Ada dua tipedari sistem *punchcard*yaitu kotak nomor dicetak pada kartu suara, dimana setiap kotak untuk pemilihan suara. Dan yang lainnya disebut *Datavote* yang mempunyai lubang-lubang pemilih yang menyatakan nama-nama kandidat atau memilih kandidatnya dengan cara melubangi kertas *punchcard* yang dicetak pada kartu suara.

4. Marksense Form

Teknologi ini dinamakan *optical scan* yang dimulai digunakan pada tahun 1980.Pada sistem ini pemilih menggunakan bentuk kertas dan menulis pada kotak atau bentuk oval berikut arah panah untuk mengarahkan calon pemilih.Jika suara sudah lengkap ditulis kemudian dibaca oleh komputer. Tulisan pemilih ditempatkan pada suatu tempat perhitungan dan selanjutnya akan dibaca melaluiproses *optical scanning* dan langsung dihitung dengan bantuan mesin penghitung. Kira-kira 25 persen dari seluruh Negara telah menggunakan alat dengan cara seperti ini. Pada tahun 1992 telah meningkat dua kali lipat penggunaannya dan terus meningkat pemakainya

5. Electronic Voting

Teknologi *electronic voting* dimulai pada tahun 1970 yang disebut teknologi pencatatan langsung secara elektronik atau lebih dikenal dengan istilah DRE (*direct recording electronic*). Cara memilih dengan sistem ini adalah dengan memilih kandidat yang sudah tercetak pada layar komputer. Pemilih hanya menekan tombol pada display atau pada alat atau piranti yang mirip.

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

Contoh dari *electronic voting* adalah dengan menekan tombol suara pemilih langsung disimpan pada suatu piranti memori atau pada sirkit memori *non volatile*. Jika peralatan pemilihan menggunakan *keyboard* tulisan suara akan dicatat secara elektronik. Salah satu bentuk *electronic voting electronic voting* yang sedang dikembangkan adalah *Internet Voting.*

6. Remote Voting

Remote voting adalah suatu tempat pemungutan suara yang letaknya berjauhan atau pada tempat yang berbeda, teknologi ini bias menggunakan kertas yang dikirim melalui surat suara atau kartu suara, atau menggunakan suatu perangkat dengan kata lain bagaimana dokumen suara bisa dikirim ke suatu tempat untuk dihitung ditempat yang lain, cara ini tidak ada bedanya denganpemungutan suara melalui surat, jadi *remote voting* adalah pemungutan suara dari tempat yang berbeda hanya saja cara atau media yang berbeda atau perangkat yang digunakan bisa berbeda-beda.

2.2.3 Tehnik Pengiriman *E-Voting*

Pengiriman e-v*oting* dapat dilakukan dengan berbagai metoda atau dengan berbagai perangkat elektronik yang menjadi sarana pendukungnya

a. Pemilih dapat memberikan suara melalui Internet

Dengan menggunakan bentuk web yaitu berupa halaman web di internet maka dapat mengirimkan input data dalam bentuk *alphanumeric*. Data yang dikirim sudah di enkripsi terlebih dahulu untuk menghindari dari penyadapan atau perubahan data.

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

b. Pemilih dapat memberikan suara melalui telepon

Dalam pesawat telepon terbaru menggunakan sistim digital, pada tombol tombolnya berbasis angka, tetapi dapat mengidentifikasi pernyataan yes atau no, satu, dua,tiga.

c. **Pemilih dapat memberikan suara melalui pesan *Text SMS***

Pemilih diberikan dokumen petunjuk, user name dan PIN terlebih dahulu. Selanjutnya, sebelum mengirimkan pilihannya, pemilih juga diminta untuk memberikan nomor identitas atau nomor KTP sebagai salah satu usaha untuk mencegah pencurian identitas oleh orang lain. Jika pemilih sudah memberikan suara sebelumnya, tentu saja akan ditolak oleh sistem. Setelah mengirimkan SMS dengan format tersebut, pemilih akan mendapatkan SMS balasan berisi konfirmasi bahwa pilihan mereka telah diterima.

d. Pemilih dapat memberikan suara melalui TV digital dengan menggunakan *remote control* TV digital.

e. **Pemilih dapat memberikan suara melalui surat dan dikirim melalui *post***

f. Pemilih dapat memberikan suara melalui Kios (bilik suara)

Pemilih menyalurkan suaranya dengan cara datang ke suatu tempat yang sudah disediakan oleh panitia dan pemilih menyalurkan suaranya di bilik suara yang tertutup agar hasil pilihannya tidak diketahui oleh orang lain. Cara pemilihan seperti ini di sudah tidak asing lagi di Indonesia sudah.

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

2.2.4 Prinsip-Prinsip *E-Voting*

Supaya *e-voting* dapat diterapkan dengan efektif dan menghasilkan hasil penghitungan suara yang dapat diakui oleh seluruh lapisan masyarakat, di samping prinsip langsung, umum, bebas, rahasia, jujur, adil (Luber Jurdil) yang ada pada sistem pemilu sekarang, maka penerapan *e-voting* harus berdasarkan prinsip-prinsip sebagai berikut.

a. ***Eligibility and Authentication***

Hanya pemilih terdaftar yang dapat memberikan suara.

b. ***Uniqueness***

Pemilih hanya dapat memilih sekali.

c. ***Accuracy***

Sistem harus dapat menyimpan pilihan dengan benar.

d. ***Integrity***

Sistem harus menjamin pilihan tidak dapat diubah, dipalsu dan dihapus tanpa deteksi.

e. ***Verifiability and Auditability***

Sistem memungkinkan pengecekan pilihan untuk memeriksabahwa semua pilihan telah dihitung dengan benar dan harus ada rekaman pilihan yang asli danterpercaya.

f. ***Secrecy and Non-Coercibilit***

Sistem harus menjamin kerahasiaan setiap pemilih untukmencegah terjadinya penjualan atau pemaksaan suara.

g. ***Convenience*sistem**

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

Pemilih dapat memberikan pilihannya secara cepat dengan peralatan dan kemampuan minimal.

h. *Certifiability*

Sistem harus dapat diujicobakan sehingga penyelenggara pemungutan suara memiliki kepercayaan terhadap sistem.

i. *Transparency*

Pemilih harus memiliki pengetahuan umum dan pehamaman terhadap proses pemungutan suara.

j. *Cost-effectiveness*

Sistem harus dapat dibiayai dengan dana terbatas dan efisien.

2.2.5 Penerapan *E-Voting*

Pemanfaatan *e-voting* sudah dimulai dilakukan pada beberapa Negara, Berikut ini beberapa contoh Negara yang telah memanfaatkan teknologi *e-voting.*

a) Brazil

Brazil adalah salah satu negara yang masuk sepuluh besar jumlah penduduk terbesar di dunia selain Indonesia.Brazil telah mulai memperkenalkan sistem *e-voting*pada awal tahun 1990an pada kota-kota dengan penduduk sekitar 200.000 orang. Kemudian pada tahun 1998, system *e-voting* telah digunakan pada proses pemilihan umum dengan skala yang lebih tinggi. Pada tahun 2002, lebih dari 100 juta penduduk Brazil memasukan suara mereka menggunakan mesin *e-voting* yang berjumlah lebih dari 400.000 yang tersebar di seluruh bagian Negara. Keberhasilan Brazil tersebut

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

menunjukan bahwa Negara dengan jumlah penduduk yang sangat besar juga mampu memanfaatkan system *e-voting*.

b) Jepang

Jepang mulai memanfaatkan *e-voting* secara resmi pada tahun 2002 pada pemerintah lokal kota Niimi. Penggunaan *e-voting* tersebut cukup sukses karena diikuti oleh 96% warga kota tersebut dari total 25.000 penduduk kota. Pelaksanaan *e-voting* di kota tersebut serupa dengan pelaksanaan *e-voting* di Brazil dengan menggunakan mesin *e-voting*.

c) Estonia

Estonia adalah sebuah negara di Eropa dengan jumlah penduduk lebih dari satu juta jiwa.Estonia telah berhasil memanfaatkan teknologi *e-voting* berbasis internet pada tahun 2005 pada Pemilu lokal dengan jumlah warga yang memanfaatkan teknologi tersebut sebanyak 9.317 orang.Pada tahun 2007, Estonia telah menjadi Negara pertama di dunia yang berhasil memanfaatkan teknologi *e-voting* berbasis internet untuk melakukan Pemilu secara nasional.Jumlah warga negara yang memanfaatkan teknologi tersebut adalah 30.275 orang.Pada saat pemanfaatan teknologi *e-voting* berbasis internet, pemerintah Estonia juga tempat pemungutan suara (TPS) seperti biasa. Jadi warga bebas memilih akan melakukan pemungutan suara menggunakan teknologi *e-voting* berbasis internet maupun menggunakan TPS.

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

2.2.6 Penerapan Pilkades

a) Pilkades di Jembrana Bali

Penggunaan *e-voting* untuk pemilihan kepala daerah di Kabupaten Jembrana dilandasi oleh tiga pemikiran.Pemikiran pertama, dalam rangka pertanggungjawaban ke publik.Pemerintah Kabupaten Jembrana seharusnya melakukan optimalisasi anggaran yang telah dilakukan secara efektif dan efisien, seperti yang diamanatkan dalam Undang-Undang No 32 tahun 2004 pasal 20 ayat 1.Anggaran yang harus di alokasikan untuk penyelengaraan pemilihan kepala desa dirasa cukup berat bagi kabipaten jembrana yang memiliki pendapatan asli daerah (PAD) cukup kecil.Pemikiran kedua, proses perhitungan suara yang bertahap dari Tempat Pemungutan Suara (TPS) kemudian ke Kantor Kecamatan hingga di Kabupaten rentan terhadap kecurangan atau manipulasi perolehan suara.Sehingga dengan *e-voting*, diharapkan suara dari TPS bisa langsung ke kabupaten. Pemikiran ketiga, esensi penandaan dalam pemilu pada prinsipnya adalah untuk mengoptimalkan kerja manusia dalam hal ini petugas pemilihan, maupun mempermudah proses perhitungan hasi perolehan suara, sehingga pelaksanaan *e-voting* mestinya merupakan sebuah tahap tranformasi metode pemilihan modern yang mengedepankan teknologi informasi.

Tahapan pemilihan dengan *e-voting* di jembrana :

a. Pemilih mendatangi tempat pemungutan suara membawa J-ID menuju terminal verifikasi

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

b. Pada terminal J-ID pemilih memverifikasikan J-Id. Jika terdaftar dalam daftar pemilih otomasis akan muncul nomer induk kewarganegaraan, nama pemilih, dan foto pemilih
c. Pemilih menuju terminal pemilihan memilih cukup dengan menyentuh gambar calon kepala desa
d. Presentase pemilih akan tampil dalam grafik di layar
e. Jika batas akhir pelaksanaan *e-voting* selesai masyarakat akan mengetahui pemenang secara langsung(I putu agus swastika; 2011)

b) Pilkades di Kebonlimo Boyolali

Pelaksanaan *e-voting* Kebonlimo boyolali dilaksanakan pada kamis, 7 Maret 2013 di ikuti oleh 2461 daftar calon pemilih. Pilkades kebon limo merupakan desa kedua di Boyolali yang menerapkan sistem *e-voting*.Sebelumnya, pilkades *e-voting* dilaksanakan di desa Kebon Gula Boyolali.Dalam pelaksanaan *e-voting*, panitia telah menyiapkan sebanyak enam perangkat computer, lima untuk pencoblosan, sedangkan satu komputer untuk uji coba bagi warga yang sebelum memberikan suara.Dalam pelaksanaan *e-voting* ini hanya di ikuti satu calon incumbent Soeherman,S.Pd dengan kemenangan mutlak.

Selain contoh Negara dan Desa, sebenarnya masih banyak negara lain yang sudah mulai *e-voting* dalam proses pemungutan suara antara lain India, Irlandia, Amerika, Perancis, dan lain-lain. Seperti halnya negara Jepang, hampir semua Negara tersebut memanfaatkan teknologi *e-voting* masih dalam tingkat

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

pemilihan umum lokal, belum bersifat nasional.Masih ada kekhawatiran yang cukup besar terkait dengan keamanan sistem *e-voting*. Brazil dan Estonia adalah contoh negara yang telah berani memanfaatkan teknologi *e-voting* untuk pemilihan umum nasional.

Penerapan *e-voting* akan membuat pesta demokrasi menjadi semakin efisien dan efektif dan hasilnya lebih cepat diketahui kurang dari 24 jam. Tetapi pentingnya kerahasiaan dan keamanan *electronic elevation system* juga harus diperhatikan Artinya, jika kerahasiaan dan keamanan terpenuhi, maka *e-voting* sangatlah tepat digunakan. Berikut sejumlah aspek manfaat dari penerapan *e-voting* adalah

1. **Biaya**

   Terkait sumber daya dan investasi yang lebih hemat dibanding dengan sistem tradisional yang ribet, kompleks dan tidak efisien.

2. **Waktu**

   Terkait waktu pelaksanaan pemilihan yang lebih cepat dan kalkulasi hasil yang lebih tepat dibandingkan sistem yang tradisional.

3. **Hasil**

   Terkait dengan hasil kalkulasi yang lebih tepat dan akurat serta minimalisasi terjadinya kasus human *error* selama sistem yang dibangun terjamin dari berbagai ancaman kejahatan.

4. **Transparansi**

   Terkait dengan transparansi dari semua proses karena semua dilakukan oleh suatu sistem yang otomatis dan *real time online*.

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

2.3 Software Pendukung

a. Netbeans 7.3

Netbeans sebagai *IDE* ditujukan untuk memudahkan pemrograman Java.Dalam Netbeans, pemrograman dilakukan berbasiskan visual dan *event driven*.Seperti *IDE* lain, misalnya Borland Delphi dan Microsoft Visual Studio. Untukmembuat dialog atau *User Interface*, kita tidak perlu membuat teks programsecara manual baris per baris, tetapi cukup klik pada *component pallete*. Teksprogram akan dihasilkan secara otomatis.Untuk memakai Netbeans *IDE* maka kita harus terlebih dahulumempunyai driver JDK yang akan mendukung pembuatan perangkat lunakdengan menggunakan Netbeans *IDE*, maka sebelum meng*install* Netbeansterlebih dahulu kita harus menginstal driver JDK. Netbeans yang dipakai padapengembangan perangkat lunak ini adalah Netbeans 6.5 dan JDK 1.7.

b. MySQL

MySQL adalah perangkat lunak *Relational Database Management System*(RDBMS) yang didistribusikan secara gratis dibawah lisensi *GPL* (*GeneralPublic License*).Dimana setiap orang bebas untuk menggunakannya, tapi tidakboleh dijadikan produk turunan yang bersifat *Closed Source* atau komersial.MySQL sebenarnya merupakan turunan salah satu konsep utama dalam*database* sejak lama, yaitu *SQL* (*Structure Query Language*).*SQL* adalah sebuahkonsep pengoperasian *database*, terutama untuk pemilihan atau seleksi danpemasukan data, yang memungkinkan pengoperasian data dikerjakan denganmudah secara otomatis.Keandalan suatu sistem *database*

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

(DBMS) dapat diketahui dari cara kerja*Optimizer*-nya dalam melakukan proses perintah-perintah *SQL*, yang dibuat oleh*user* maupun program-program aplikasinya. Sebagai *database server*, MySQLdapat dikatakan lebih unggul dibanding *database server* lainnya dalam *query* data.Hal ini terbukti untuk *query* yang dilakukan oleh *single user*, kecepatan *query*MySQL bisa sepuluh kali lipat lebih cepat dari PostgreSQL dan lima kali lebihcepat dibanding Interbase.

2.4 *QR Code (Quick Response Code)*

Ada banyak standar *Barcode* 2D yang ada saat ini, diantaranya adalah PDF417, Data Matrix, Maxi Code dan *QR Code*. Namun diantara standar-satandar *Barcode* 2D tersebut hanya *Barcode* 2D dengan standar *QR Code* yang memiliki keunggulan lebih di banding yang lainnya. Hal ini dapat dilihat pada *tabe l*2.1.

Gambar 2.4: *QR Code*

Huruf-huruf yang dapat ditangani oleh *QR Code* adalah sebagai berikut:

1. Numerik (0….9), setiap tiga angka akan disimpan dalam ukuran 10 bit. Secara teori *QR Code* dapat menampung total 7089 angka. Untuk tipe ini pada *QR Code* diberi tanda deret bit 0001 pada awal data dan dilanjutkan dengan 10 buah deret bit tambahan yang menyimpan jumlah angka yang

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

disimpan dalam *QR Code*. Misal data yang akan disimpan adalah 123987, maka ketika dilakukan proses penyimpanan data ke dalam *QR Code* setiap 3 karakter dari data tersebut akan disimpan dalam ukuran 10 bit, hasilnya dari contoh data tersebut adalah 0001111011 1111011011.

2. Alphanumerik, setiap 2 karakter disimpan dalam ukuran 11 bit. Secara teori *QR Code* dapat menampung total 4296 huruf dengan jenis seperti ini. Untuk tipe ini pada *QR Code* diberi tanda deret bit 0010 pada awal data dan dilanjutkan dengan 9 buah deret bit tambahan yang menyimpan jumlah karakter yang disimpan dalam *QR Code*.

Tabel 2.2: Daftar *Index* dan Karakter Tipe *Alphanumerik* (Yeni Dwi Rahayu, 2010)

Index	Karakter	Index	Karakter
0	0	23	N
1	1	24	O
2	2	25	P
3	3	26	Q
4	4	27	R
5	5	28	S
6	6	29	T
7	7	30	U
8	8	31	V
9	9	32	W
10	A	33	X
11	B	34	Y
12	C	35	Z
13	D	36	Blank
14	E	37	$
15	F	38	%
16	G	39	*
17	H	40	+
18	I	41	-
19	J	42	.
20	K	43	/
21	L	44	:
22	M		

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

Misal data yang akan disimpan adalah ABCD, maka ketika dilakukan proses penyimpanan data ke dalam *QR Code* setiap 2 karakter dari data tersebut akan disimpan dalam ukuran 11 bit, dengan cara sebagai berikut:

AB ≥ 45 * 10 + 11 ≥ 462 ≥ 00111001110

CD ≥ 45 * 12 + 13 ≥ 553 ≥ 01000101001

Maka hasilnya adalah 00111001110001000101001

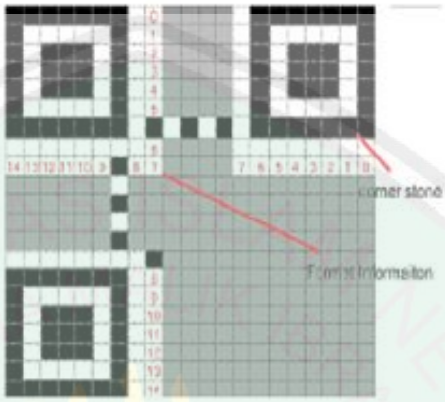
Data *oktet*, setiap huruf disimpan dalam ukuran 8 bit. Secara teori *QR Code* dapat menampung total 2953 huruf dengan jenis seperti ini. Untuk tipe ini pada *QR Code* diberi tanda deret bit 0100 pada awal data dan dilanjutkan dengan 8 buah deret bit tambahan yang menyimpan jumlah karakter yang disimpan dalam *QR Code*.

Karakter huruf Kanji, setiap huruf disimpan dalam ukuran 13 bit. Secara teori *QR Code* dapat menampung total 1817 huruf dengan jenis seperti ini. Untuk tipe ini pada *QR Code* diberi tanda deret bit 1000 pada awal data dan dilanjutkan dengan 8 buah deret bit tambahan yang menyimpan jumlah karakter yang disimpan dalam *QR Code*.

Dalam penanganan koreksi kesalahan *QR Code* menyerahkannya pada *Algoritma Reed Solomon Code*. Level perbaikan error yang dapat dipilih ketika membuat *QR Code* terdapat empat buah level yang masing-masing level adalah L, M, Q dan H dimana masing-masing level dapat memperbaiki error hingga 7%, 15%, 25%, 30% dari ukuran datanya (Nokia Forum Development, 2010). Ciri-ciri sebuah *barcode QR Code* dapat dilihat dari tiga buah corner stone (tanda sudut)

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

yang dimilikinya dan setiap tanda memiliki cirri lebar sebesar 7 satuan bit data atau blok matrik *QR Code*.



Gambar 2.5: Simbol *QR Code*

Blok yang diberi nomor merupakan blok data format information yang terdiri dari informasi level koreksi error (bit 0 dan 1), untuk level koreksi L diwakilkan dengan bit 01, M dengan 00, Q dengan 11 dan H dengan 10. Informasi mask (bit 2 – 4) yang digunakan oleh *QR Code* tersebut (bit 5 – 14 merupakan bit tambahan untuk koreksi kesalahan pada data bit 0 – 4). Blok yang berwarna abu-abu merupakan blok data sebenarnya yang terkandung dan blok data tambahan untuk koreksi kesalahan. Mask berguna untuk menghilangkan bagian yang bukan merupakan blok data yang diinginkan.

QR Code memiliki versi 1 – 40, semakin besar versi maka semakin besar pula ukuran matriknya dan semakin besar pula ukuran data yang dapat ditampungnya,

Untuk membaca sebuah *QR Code* langkah-langkah yang harus dilakukan adalah:

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

1. Tentukan versi *QR Code*, dengan melihat ukuran matrik *QR Code* yang akan dikenali.
2. Tentukan koreksi kesalahan dan mask yang digunakan *QR Code*.
3. Membuat pola mask sesuai dengan mask yang digunakan oleh *QR Code* yang akan dikenali, yaitu dengan membuat sebuah matrik baru berukuran sama dengan matrik *QR Code*, tetapi isi matrik mask pada posisi selain area data adalah 0 (false) dan mengisi matrik mask pada area data dengan aturan berikut:

Tabel 2.3: Aturan pada Area Data

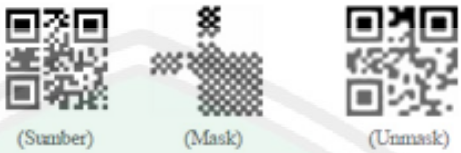
No	Biner	Aturan
0	0	Jika (x + y) mod 2 = 0, maka isi matrik mask pada posisi tersebut dengan 1 (true).
1	1	Jika y mod 2 = 0, maka isi matrik mask pada posisi tersebut dengan 1 (true).
2	10	Jika x mod 3 = 0, maka isi matrik mask pada posisi tersebut dengan 1 (true).
3	11	Jika (x + y) mod 3 = 0, maka isi matrik mask pada posisi tersebut dengan 1 (true).
4	100	Jika ((x/3)+(y/2)) mod 2 = 0, maka isi matrik mask pada posisi tersebut dengan 1 (true).
5	101	Jika ((x * y) mod 2 + (x * y) mod 3 = 0), maka isi matrik mask pada posisi tersebut dengan 1 (true).
6	110	Jika (((x * y) mod 2 + (x * y) mod 3) mod 2 = 0), maka isi matrik mask pada posisi tersebut dengan 1 (true).
7	111	Jika (((x * y) mod 3 + (x + y) mod 2) mod 2 = 0), maka isi matrik mask pada posisi tersebut dengan 1 (true).

4. Lakukan proses unmask, yaitu dengan cara melakukan operasi logika NOT pada setiap posisi matrik *QR Code* dimana pada posisi tersebut dalam matrik mask bernilai 1 (true).

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

5. Lakukan pembacaan data

Berikut ini adalah gambar proses pembacaan *QR Code*:



Gambar 2.6: Pengenalan *QR Code*

Pada contoh sumber *QR Code* diatas, dapat dilihat bahwa matrik *QR Code* berukuran 21x21 bit. Berarti matrik tersebut merupakan versi 1, kemudian jika diambil data bit format informasinya yaitu 001011000001001 (untuk bit nomor 6-8 disi 0) kemudian lakukan proses logika XOR dengan deret biner 101010000010010, sehingga dihasilkan deret biner 110110000100001, dimana bit ke 0 dan 1 adalah 10 merupakan tanda level koreksi kesalahan yang digunakan adalah H dan bit ke 2 – 4 adalah 000 merupakan kode pola mask yang digunakan. Setelah kode pola mask didapat kemudian lakukan pembuatan matrik pola mask sesuai dengan aturan yang ada. Kemudian buat sebuah matrik unmask dengan melakukan proses logika NOT pada matrik *QR Code* pada posisi yang bersesuaian dengan matrik mask dimana pada posisi tersebut nilai data matrik mask adalah 1 (true). Jika matrik unmask telah dibuat selanjutnya lakukan proses pembacaan data dimulai dari bit 20, 20 ke kiri 1 bit, kemudian ke kanan dan ke atas 1 bit, kemudian ke kiri lagi satu bit, hingga didapat deret bit sebagai berikut :

010000011011100000000110111100011000000001000

Pada 4 bit pertama, yaitu bit 0 – 3 terdapat deret biner 0001. Hal ini menandakan bahwa tipe data *QR Code* adalah numerik. Karena tipe datanya adalah numerik. Kemudian jika diambil 10 bit berikutnya, didapat deret biner

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

0000000011. Hal ini menandakan bahwa jumlah data angka yang tersimpan dalam *QR Code* adalah 3 buah angka. Selanjutnya jika diambil 10 bit berikutnya, didapat deret biner 0001111011 yang jika diubah kedalam decimal menjadi 123. Untuk sisa deret biner berikutnya hanya data koreksi kesalahan. Jadi data yang terkandung dalam *QR Code* tersebut adalah 123.

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

BAB III

ANALISA DAN PERANCANGAN SISTEM

3.1 Tahapan Penelitian

Penelitian yang dilakukan untuk merancang sistem diperoleh dari pengamatan data-data yang ada. Tahap-tahap yang dilakukan untuk penelitian guna perancangan (pendesainan sistem) secara terstruktur sebagai berikut:

a. Observasi

Mengadakan penelitian dan menganalisa secara langsung kondisi di Desa Kedungdowo Kaliwungu Kudus. Observasi ini mencakup pencarian dan pengambilan data, serta pengamatan terhadap pola sosial, kehidupan masyarakat, dan sebagainya.

b. Studi Literatur

Mempelajari data manual dan referensi yang berhubungan dengan masalah yang dihadapi dalam perencanaan dan perancangan aplikasi yang akan dibuat.

c. Interview

Melakukan interview dengan catatan penduduk sipil, badan permusyawaratan desa, maupun dengan pihak-pihak yang berkaitan di Desa Kedungdowo Kaliwungu Kudus untuk memperoleh data dan informasi dalam pembuatan aplikasi *e-voting*.

d. Analisa Sistem

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

Membuat analisa terhadap data yang sudah diperoleh dari hasil observasi yaitu Perancangan Sistem e-voting Kepala Desa Kedungdowo Kudus.

Pemodelan sistem ini dengan didukung pembuatan flowchard, *Use Case Diagram*, *Activity Diagram*

e. Evaluasi Program

Menguji coba seluruh spesifikasi terstruktur dan sistem secara keseluruhan. Pada tahap ini, dilakukan uji coba sistem yang telah selesai disusun. Proses uji coba ini diperlukan untuk memastikan bahwa sistem yang telah dibuat telah sesuai dengan kriteria-kriteria dan tidak ada kesalahan-kesalahan yang terkandung di dalamnya.

f. Pembuatan Laporan Skripsi

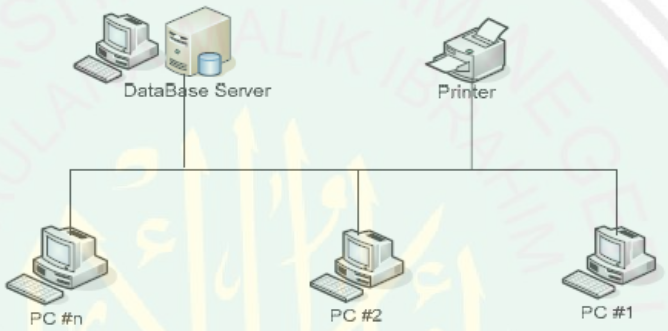
Pembuatan laporan berdasarkan penelitian yang telah dilakukan dan dari hasil program.

3.2 Deskripsi Umum Perangkat Lunak

Aplikasi yang dibangun dalam laporan ini adalah sebuah aplikasi *e-voting* pemilihan kepala desa Kedungdowo Kaliwungu Kudus berbasis java dengan metode algoritma RC4. Konsep *e-voting* ini nantinya sangat bermanfaat karena menjamin adanya prinsip-prinsip dalam pemilu. pemilih akan memilih calon kepala desa yang diinginkan pada tempat yang telah ditentukan. Hasil suara pilihan pemilih dalam bentuk enkripsi dengan maksud untuk meningkatkan keamanan datanya.pemilih dapat mengdeskripsikan data pilihanya untuk mengecek autentikasi data pemilih. Hasil suara pilihan pemilih kemudian akan

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

ditampilkan di sebuah grafik rekapitulasi calon kepala desa. *e-voting* berjalan pada jaringan *Local Area Network* (LAN). Jaringan LAN adalah suatu kumpulan komputer, dimana terdapat beberapa unit komputer (*client*) dan satu unit komputer untuk bank data (*server*). Antara masing-masing komputer yang terhubung pada jaringan LAN dapat saling menggunakan printer secara bersamaan.



Gambar 3.1 Gambaran Umum Sistem

3.3 Analisa Sistem

Untuk mendapatkan gambaran mengenai sistem yang digunakan saat ini, kami melakukan analisa terhadap sistem dan memodelkannya dengan menggunakan *functional modeling*. Proses dan data model dari sistem dimodelkan dengan diagram *Use Case Diagram, Activity Diagram*.

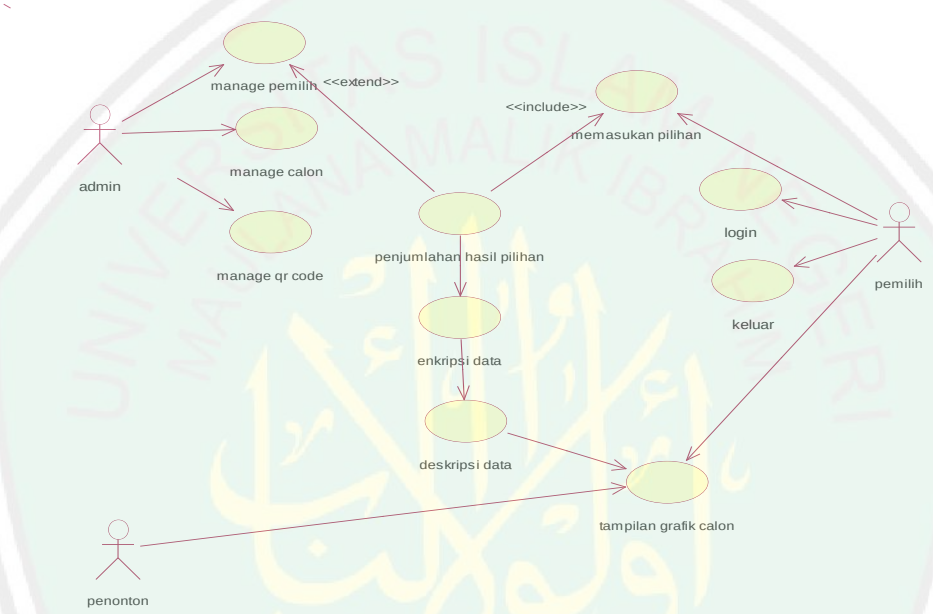
3.3.1. Use Case Diagram

Use Case adalah peringkat tertinggi dari fungsionalitas yang dimiliki sistem, dengan memberi gambaran bagaimana seseorang akan menggunakan atau memanfaatkan sistem. *Use Case* menampilkan spesifikasi fungsional yang diharapkan dari system perangkat lunak yang kelak akan dikembangkan. *Use*

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

Case sangat penting dimanfaatkan untuk menangkap seluruh kebutuhan dan harapan pengguna (*user needs and expectation*). (Adi Nugroho, 2005 : 51 - 52).

Dengan diagram *use case* ini dapat diketahui proses yang terjadi pada *e-voting* pilkades di kudus, seperti gambar 3.1.



Gambar 3.2 *Use Case* Diagram *E-Voting* Pilkades Kedungdowo

Tabel 3.1 Keterangan Diagram *E-Voting*

Aktor	Nama Use Case	Deskripsi Use Case
Admin	Manage pemilih	Use case ini untuk mengatur daftar pemilih berhak mencontreng
Admin	Manage calon kades	Use case ini mengatur calon kepala desa
Admin	Manage qr code	Use case ini mengatur barcode untuk identitas pemilih
Pemilih	login	Use case ini memverifiksi login masuk *e-voting*
pemilih	Logout	Use case ini keluar dari halaman web *e-voting*
Pemilih	Memilih calon kades	Use case ini untuk memberikan suara kepada calon kades
pemilih	Melihat grafik kades	Use case ini memberikan data perolehan suara masing-masing calon
penonton	Melihat grafik kades	Use case ini memberikan data perolehan suara masing-masing calon
Admin	Enkripsi data	Use case ini untuk mengkodekan hasil pemilihan agar tidak di ketahui orang lain
Admin	Deskripsi data	Use case ini untuk menampilkan data yang telah di kodekan sehingga Nampak pilihan aslinya

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

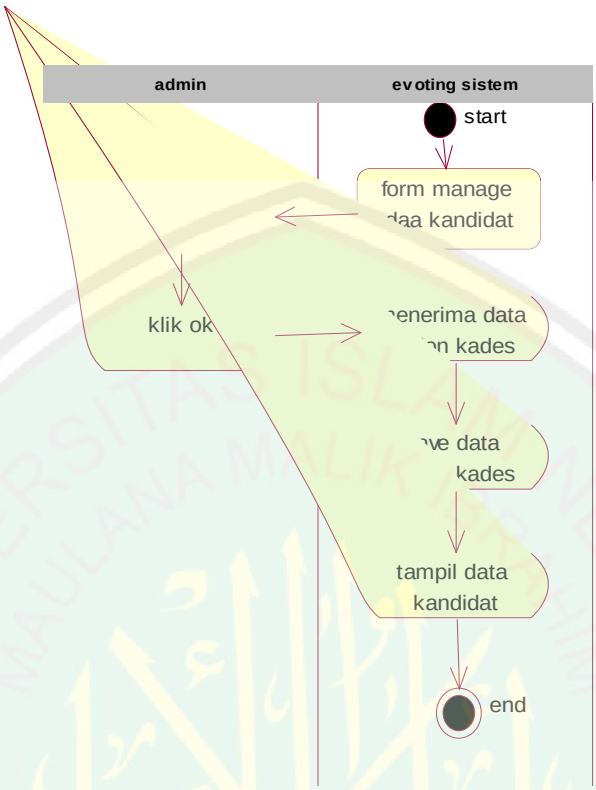
3.3.2. Activity Diagram

Activity diagram merupakan suatu bentuk *flow diagram* yang memodelkan alur kerja (*workflow*) sebuah urutan aktifitas sebuah proses sistem. Diagram ini sangat mirip dengan *flowchart*, sehingga dapat dimodelkan sebuah alur kerja dari sebuah aktifitas lainnya kedalam keadaan sesaat. *Activity diagram* juga sangat berguna untuk menjelaskan bagaimana perilaku dalam berbagai *use case* berinteraksi. Berkaitan dengan *use case diagram*, maka terdapat beberapa buah *activity diagram* yang dapat digambarkan, yaitu:

a) Proses Manage Data Kandidat

Pertama kali sistem akan menampilkan form manage data kandidat yang isinya daftar calon kepala desa dengan menginputkan data seperti nama, alamat, jeni kelamin, dll data inputan ini nanti akan di simpat dalam database db_jspevotting data calon ini akan dijadikan sebagai kandidat calon kepala Desa Kedungdowo data kandidat. Bagi admin yang ingin memanage data kandidat maka semua data harus diisi secara lengkap. Jika data telah diisi secara lengkap, admin dapat memilih

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG



Gambar 3.4 *Activity Diagram Manage Kandidat*

Pada gambar 3.4 dijelaskan manage kandidat sebagai berikut :

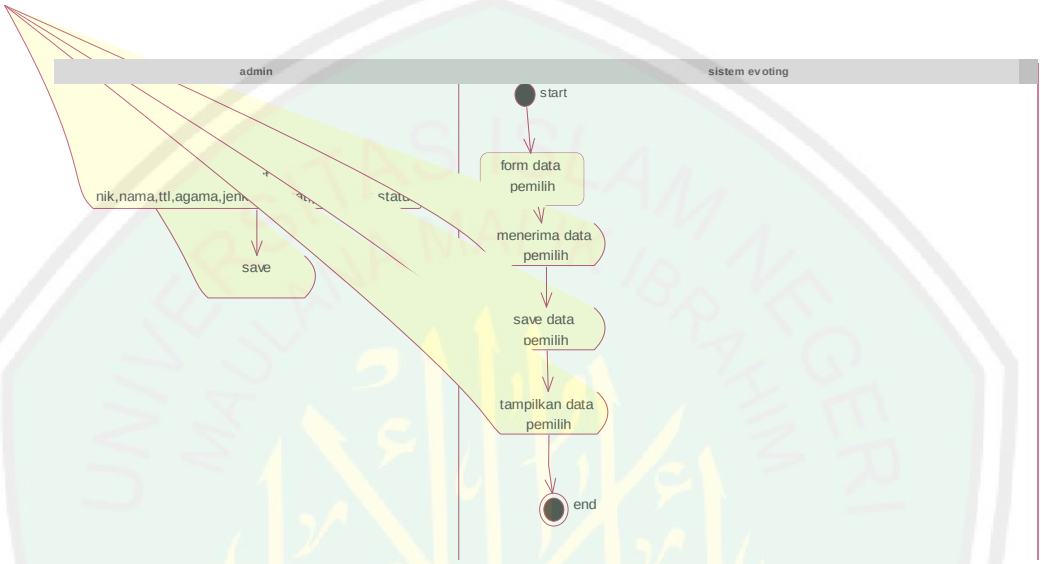
a. System memberika form data calon kandidat
b. Admin akan menginputkan data kandidat
c. Admin Klik tombol save atau OK
d. System akan menerima data calon kepala desa
e. System lalu menyimpan data pemilih
f. System akan menampilkan data pemilih

b) Proses Registrasi Data pemilih

Pertama kali sistem akan menampilkan form manage data pemilih yang isinya daftar pemilih tetap dengan menginputkan data seperti nama, alamat, jeni kelamin, dll data inputan ini nanti akan di simpan dalam database

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

db_jspevotting data pemilih ini akan dijadikan sebagai daftar pemilih tetap dalam melakukan penjoblosancalon kepala desa kedungdowo. admin dapat mendelete maupun mengedit data pemilih apabila ada kesalahan.



Gambar 3.5 Gambar *Manage* Pemilih

Pada gambar 3.5 dijelaskan manage pemilih sebagai berikut :

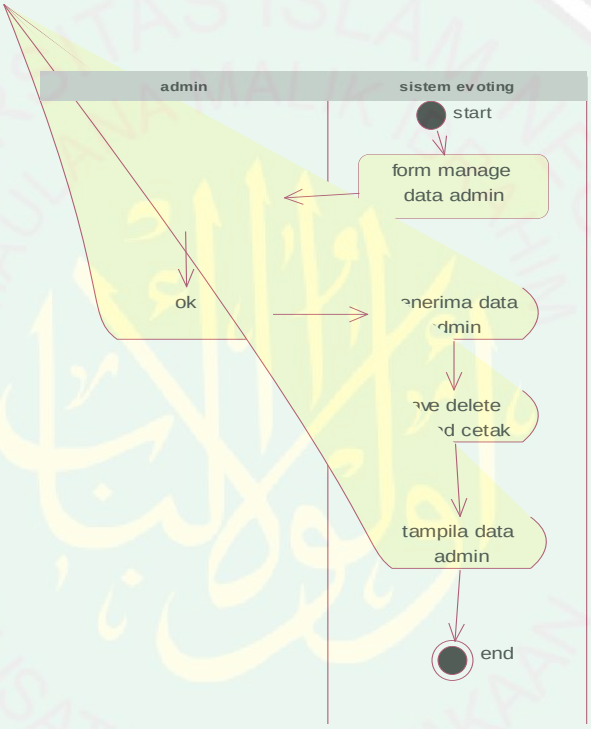
a. System memberika form pengisian data pemilih
b. Admin menginputkan data pemilih
c. Klik tombol save atau OK
d. Sistem akan menerima data pemilih
e. Sistem akan menyimpan data pemilih
f. Sistem akan menampilkan data pemilih

c) Proses Manage Data admin

Pertama kali sistem akan menampilkan form manage data admin yang berisi beberapa inputan yaitu *username* dan *password*. Jika semua data telah

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

diisi secara lengkap maka admin dapat memilih dapat menambah data inputan. Tetapi apabila admin ingin mengedit atau menghapus data, maka admin harus memilih data mana yang akan diedit atau dihapus. Sistem akan menerima data inputan admin kemudian data inputan dan hasil editan disimpan dalam database.



Gambar 3.6 *Manage* Data Admin

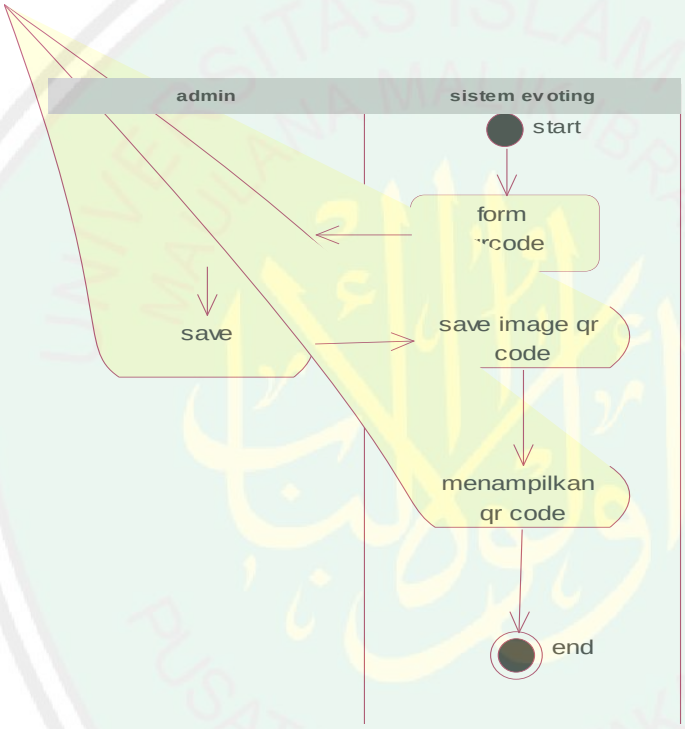
Pada gambar 3.6 dijelaskan sebagai berikut :

a. System menyediakan form admin
b. Admin akan input username, password
c. Admin akan mengklik tombol save atau OK
d. System akan menerima data admin
e. System akan menyimpan data admin
f. System akan menampilkan data admin

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

d) Proses Cetak Barcode

Pertama kali sistem akan menampilkan form cetak barcode yang berisi beberapa *textbox* inputan. Teks inputan disini tidak diinputkan secara manual tetapi admin tinggal memilih data yang akan dibuat *image* barcodenya dengan cara memilih NIK



Gambar 3.7 *Manage* Membaca QR Code

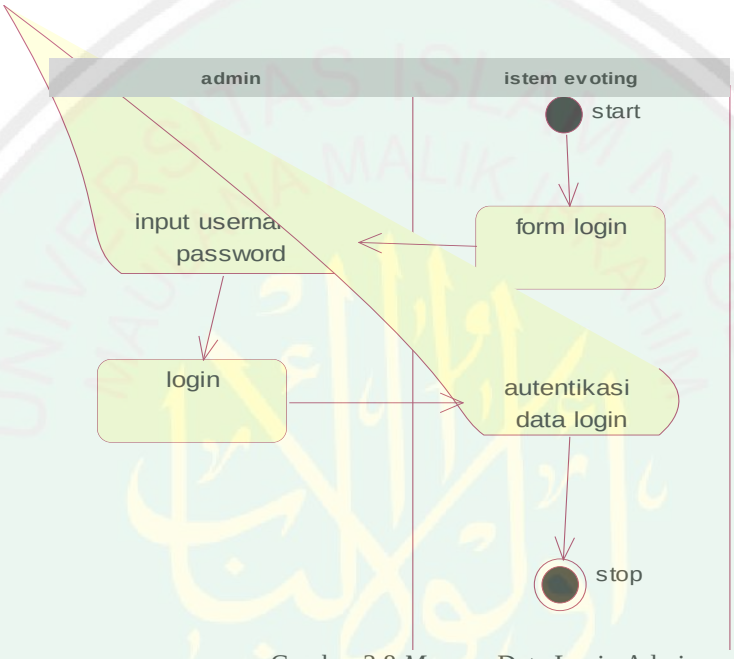
Pada gambar 3.7 dijelaskan manage QR Code

a. System memberikan form QR Code
b. Admin akan menginoutkan data pada QR Code
c. Admin akan menampilkan data QR Code
d. System akan menyimpan data gambar QR Code
e. System juga akan menampilkan QR Code

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

e) Proses Login Admin

Pertama kali sistem akan menampilkan form *login* yang tediri dari dua *textbox* inputan yaitu input *username* dan *password*.proses ini digunakan agar setiap orang tidak dapat masuk dengan mudah



Gambar 3.8 *Manage* Data Login Admin

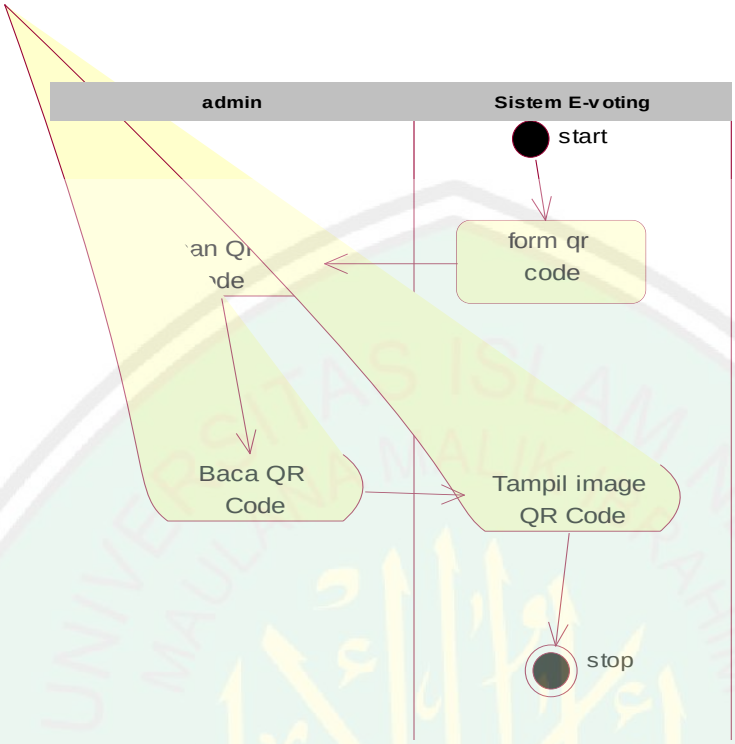
Pada gambar 3.8 di jelaskan sebagai berikut :

a. System *e-voting* menyediakan form login admin
b. Admin akan memasukan username, password
c. Jika username dan password sesuai dengan data maka system akan mengautentikasikan data login admin

f) Proses Baca QR Code

Sistem akan menampilkan form baca QR Code yang berisi beberapa *textbox* inputan. *Textbox* ini tidak diinputkan secara manual, tetapi diinputkan dengan cara men-scan barcode dengan alat scanner.

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

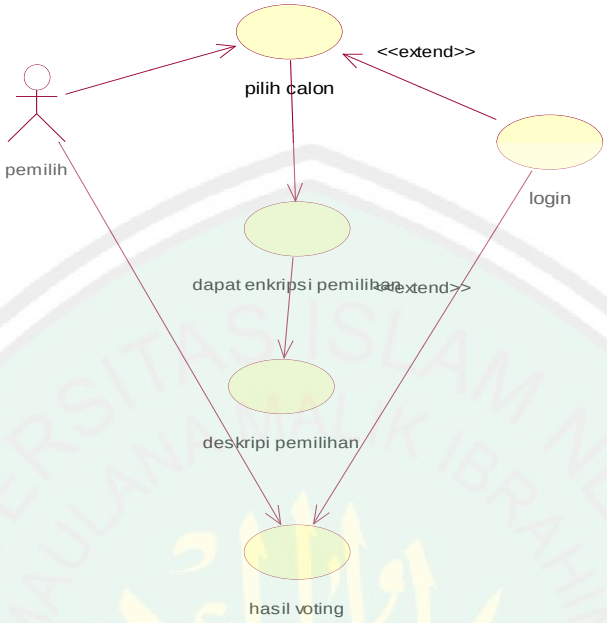


Gambar 3.9 *Manage* Membaca QR Code

Pada gambar 3.9 dijelaskan manage QR Code

a. System *e-voting* menyediakan form QR Code
b. Admin akan membaca QR code menggunakan barcode reader
c. System akan menerima data QR Code
d. System akan menampilkan data QR code

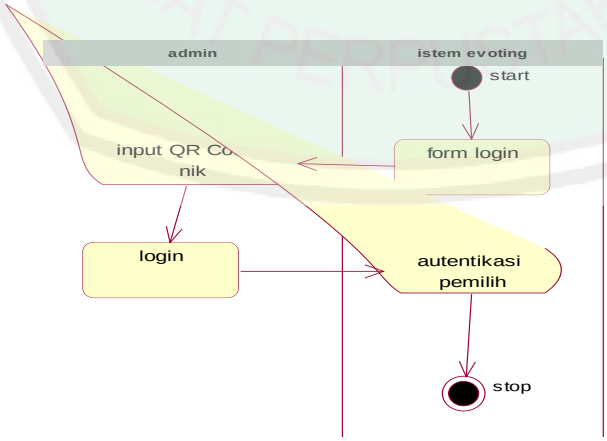
CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG



Gambar 3.10 Gambar Aplikasi Pemilihan

Gambar 3.10 dijelaskan sebagai berikut :

pemilih login dengan menscan QR code, lalu masuk dihalaman daftar pemilih, pemilih lalu menvoting kandidat,datanya akan tersimpan dalam enkripsi RC4,pemilih dapat mendeskripsikan dalam bentuk plainteks.

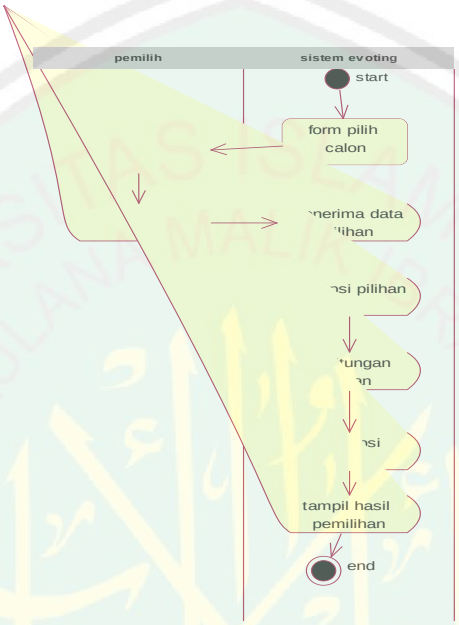


Gambar 3.11 Gambar Aplikasi Pemilihan

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

Gambar 3.11 dijelaskan sebagai berikut :

System menyediakan form input, pemilih menscan QR Code kedalam Barcode reader,system akan mengautentikasi data pemilih



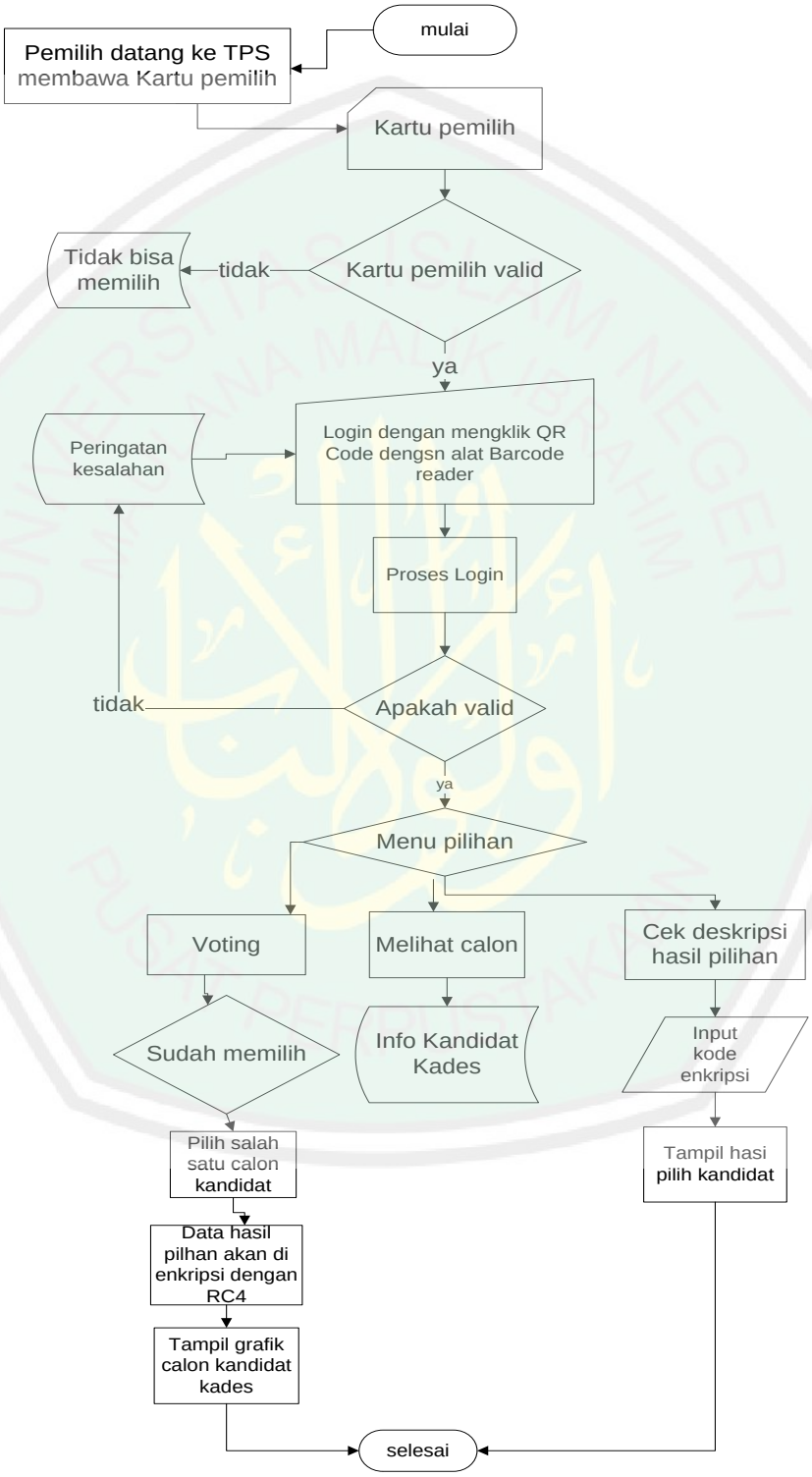
Gambar 3.12 Gambar Aplikasi Pemilihan

Gambar 3.12 dijelaskan sebagai berikut

System memberikan form voting, pemilih akan memberikan pemilihan, data tersimpan dan terenkripsi dalam bentuk symbol, pemilih dapat mendeskripsikan data menggunakan algoritma RC 4, tampil hasil pemilihan.

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

3.3.3. Flow Card *e-voting* pilkades

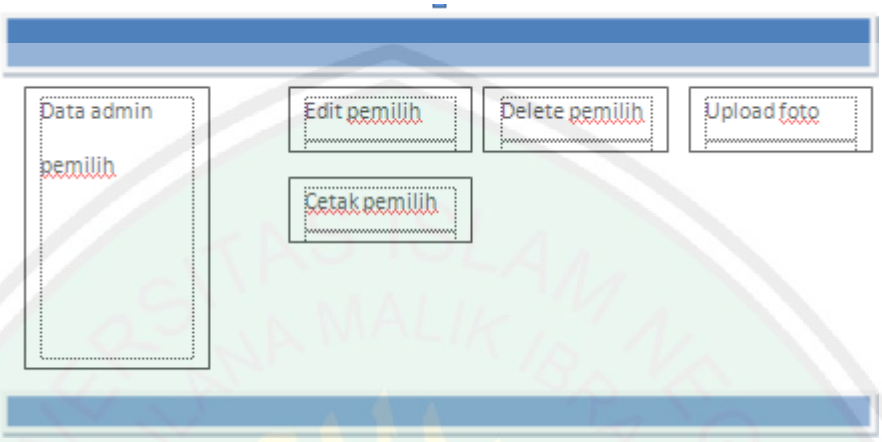


Gambar 3.13 Flowchar *E-Voting*

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

3.4 Rancangan Antarmuka

3.4.1. Design Tampilan Admin



Gambar 3.14 Manage Tampilan Admin Edit, Delete, Upload, Cetak

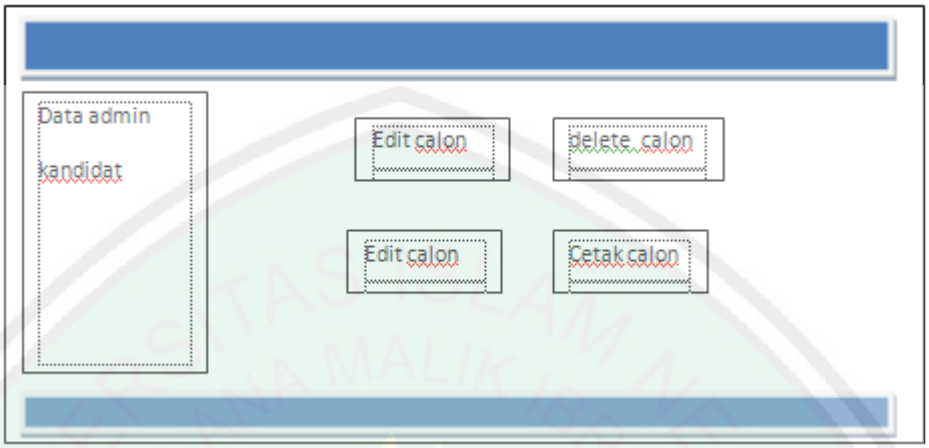
Gambar 3.14 dijelaskan sebagai berikut

a. Admin akan menginputkan data pemilih
b. Edit admin digunakan untuk mengedit data apabila terjadi kesalah dalam profil pemilih
c. Delete admin digunakan untuk menghapus data kandidat apabila telah tidak aktif (meninggal, pindah alamat)
d. Uplode admin digunakan untuk memberikan identitas pengenal dalam profile pemilih
e. Cetak admin digunakan untuk mencetak data pemilih berupa profile pemilih, foto, dan QR Code

Dalam rancangan tampilan manage admin pemilih nantinya admin bisa mengedit dan memperbaiki data pemilih, admin juga bisa mengupload foto untuk identifikasi seseorang, admin dapat mendelete apabila calon apabila telah meninggal atau sudah pindah alamat

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

3.4.2. Design Tampilan kandidat



Gambar 3.15 Manage Tampilan Kandidat Edit, Delete,Upload Foto Dan Cetak

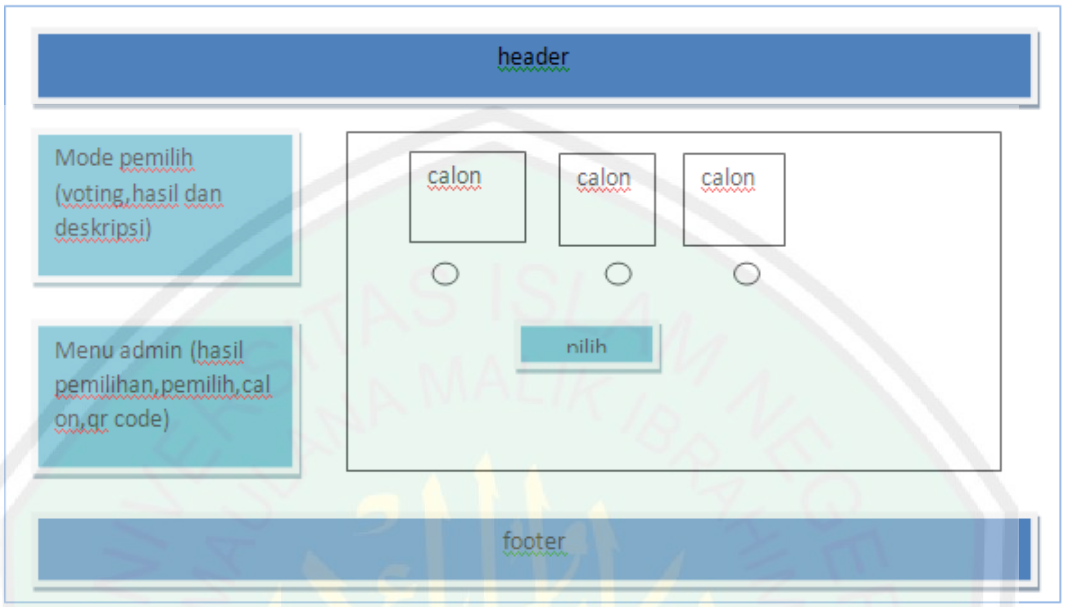
Gambar 3.15 dijelaskan sebagai berikut

a. Admin akan menginputkan dan data kandidat
b. Edit admin digunakan untuk mengedit data apabila terjadi kesalah dalam profile kandidat
c. Delete admin digunakan untuk menghapus data kandidat apabila telah tidak aktif (meninggal,pindah alamat)
d. Uplode admin digunakan untuk memberikan identitas pengenal dalam profile kandidat
e. Cetak admin digunakan untuk mencetak data kandidat berupa profile foto, dan QR Code

Dalam rancangan tampilan manage admin kandidat nantinya admin bisa mengedit dan memperbaiki data pemilih, admin juga bisa mengupload foto untuk identifikasi seseorang, admin dapat mendelete apabila calon apabila telah meninggal atau sudah pindah alamat

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

3.4.3. Rancangan Pemilihan



Gambar 3.16 Tampilan Pemilihan

Gambar 3.16 Menampilkan tampilan pemilihan

Pemilih melakukan identifikasi pemilih dengan membaca QR Code pada alat Barcode Reader, setelah login pemilih akan masuk ke halaman voting,lalu memilih salah satu kandidat, lalu hasil pemilihan voting tadi di enkripsi sehingga terbentuk atas kode-kode acak, untuk membaca kode acak pemilih melakukan deskripsi data untuk mengecek pilihan, lalu pemilih dapat melihat grafik rekapitulasi pemilihan.

3.5 Spesifikasi Database

Rancangan kode pembuatan desain sistem dari aplikasi ini dapat dibuat table-tabel database yang akan dikelola dan digunakan untuk menjalankan aplikasi ini. Database yang digunakan dalam skripsi ini adalah *Mysql* dengan file

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

databasenya “db_sertifikasi”. Berikut ini nama-nama table yang digunakan beserta *field-field* yang terdapat pada masing-masing table.

a. Tabel Pemilih.

Tabel 3.2 Tabel db Pemilih

No	Field	Type	Size
1	Nik	varchar	16
2	Nama	varchar	255
3	Tempat lahir	varchar	255
4	Tanggal	varchar	10
5	Kd_agama	int	11
6	Jk	varchar	1
7	Pekerjaan	varchar	255
8	Kawin	varchar	1
9	Alamat	varchar	255
10	Status	int	11
11	Fnama	varchar	255

b. Table Hasil

Tabel 3.3 Tabel Db Hasil

No	Field	Type	Size
1	Id_hasil	int	11
2	Nik	varchar	16
3	Pilihan	varchar	255
4	Tanggal	date	

c. Table Agama

Table 3.4 Tabel db Agama

No	Field	Type	Size
1	Kd_agama	Int	11
2	Agama	varchar	255

d. Table Pilihan

Tabel 3.5 db Pilihan

No	Field	Type	Size
1	Nik	varchar	16

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

2	Nama	varchar	255
3	Tempat lahir	varchar	255
4	Tanggal	varchar	10
5	Kd_agama	int	11
6	Jk	varchar	1
7	Pekerjaan	varchar	255
8	Kawin	varchar	1
9	Alamat	varchar	255
10	Status	int	11
11	Fnama	varchar	255
12	Nomer	Int	11

3.6 *Software*

Software adalah program atau aplikasi kompter lain yang dibutuhkan untuk membangun sebuah sistem. *Software* yang dibutuhkan dalam pembuatan aplikasi *e-voting* antara lain:

1. **Windows XP**

   Windows XP merupakan sistem operasi yang menjembatani antara komputer dan *user*. Sistem operasi ini digunakan karena *support* dan *compatible* dengan *software* lain yang dibutuhkan dalam pembuatan aplikasi *e-voting* pilkades ini.

2. ***Java Development Kit* (JDK) versi 1.7.**

   JDK merupakan paket *platform* java yang terdiri dari berbagai macam *library*, JVM, *compiler*, dan *debuger*.

3. **XAMPP control panel 1.8.1**

   Digunakan untuk managemen database e-voting

4. ***NetBeans IDE* 7.3**

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

NetBeans IDE 7.3 merupakan editor java, dimana didalamnya juga terdapat fitur *mobility* yang digunakan dalam pembuatan program *e-voting* pilkades.

5. **Dreamweaver 8**

   Digunakan untuk mengedit tampilan website

6. **Rational rose 2000**

7. **Microsof office visio**

3.7 *Hardware*

Hardware adalah perangkat keras atau *device* yang digunakan untuk menunjang dalam pembuatan sebuah sistem. Dalam pembuatan aplikasi *e-voting* pilkades, *hardware* yang digunakan antara lain:

Perangkat keras yang digunakan dalam penelitian ini adalah dengan spesifikasi sebagai berikut:

1. Prosesor Intel Core2Duo T6400 @ 2.00 GHz
2. RAM 2.00 GB
3. HardDisk 120 GB
4. VGA 358 MB
5. Monitor 14”
6. Keyboard
7. Mouse

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

BAB IV

HASIL DAN PEMBAHASAN

4.1 Implementasi

Implementasi merupakan proses pembangunan komponen-komponen pokok sistem berdasarkan desain yang sudah di buat. Implementasi sistem juga merupakan sebuah proses pembuatan dan penerapan sistem secara utuh baik dari sisi perangkat keras maupun perangkat lunaknya.

4.1.1 *Hardware* dan *Software* Untuk Pembuatan Aplikasi

a. Hardware

Perangkat keras yang digunakan dalam pembuatan aplikasi Sistem *e-voting* pemilihan kepala desa Kedungdowo adalah sebagai berikut:

1. Prosesor Intel Core2Duo T6400 @ 2.00 GHz
2. RAM 2.00 GB
3. HardDisk 120 GB
4. VGA 358 MB
5. Monitor 14”
6. Keyboard
7. Mouse

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

b. Software

Perangkat Lunak yang digunakan dalam pembuatan aplikasi Sistem *e-voting* pemilihan kepala desa Kedungdowo adalah sebagai berikut:

1. **Windows XP**

   Windows XP merupakan sistem operasi yang menjembatani antara perangkat Perangkat keras yang digunakan dalam pembuatan aplikasi Sistem *e-voting* pemilihan kepala desa Kedungdowo adalah sebagai berikut: ini.

2. ***Java Development Kit* (JDK) versi 1.7.**

   JDK merupakan paket *platform* java yang terdiri dari berbagai macam *library*, JVM, *compiler*, dan *debuger*.

3. **XAMPP Control Panel 1.8.1**

   Digunakan untuk managemen database *e-voting*

4. ***NetBeans IDE* 7.3**

   *NetBeans IDE*7.3 merupakan editor java, dimana di dalamnya juga terdapat fitur *mobility* yang digunakan dalam pembuatan program *e-voting* Pilkades.

5. **Dreamweaver 8**
6. **Rational Rose 2000**
7. **Microsof Office Visio**

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

4.2 Implementasi Desain *Interface*

Berikut implementasi antarmuka yang terdapat di aplikasi *e-voting* pilkades Kedungdowo kaliwungu kudus.

4.2.1 Menu Beranda

Menu Beranda adalah tampilan awal program dimana pada menu utama ini merupakan salam pembuka dari aplikasi ini. Adapun tampilan menu beranda dapat dilihat pada gambar 4.1

Gambar 4.1 Menu Beranda

Tampilan menu utama *e-voting* pilkades

a. Menu Home untuk tampilan halaman muka
b. Menu voting untuk tampilan pemilihan

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

c. Menu hasil untuk tampilan hasil pemilihan

d. Menu data pemilih untuk memanagemen daftar pemilih

e. Menu data pilihan untuk menampilkan calon kepala desa

4.2.2 Menu Pendaftaran Pemilih

Menu pendaftaran pemilih digunakan untuk membuat daftar pemilih. Data ini digunakan untuk untuk pemilihan kepala desa kedungdowo.

Gambar 4.2 Pendaftaran Pemilih

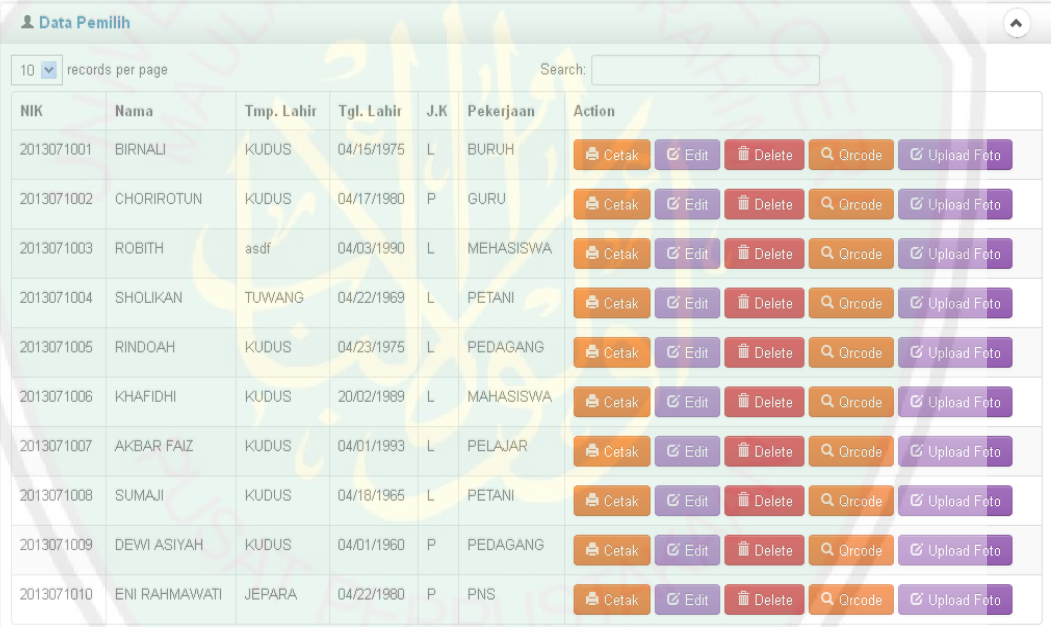
4.2.3 Menu Admin Pemilih

Data pemilih admin berisi tsebagai berikut :

1. Cetak digunakan untuk mencetak daftar pemilih. Dalam cetak ini berisi QR Code, foto, identitas pemilih

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

2. Delete digunakan untuk menghapus daftar pemilih apabila daftar pemilih telah menginggal, pindah alamat.
3. Edit digunakan untuk mengedit data pemilih apabila ada kesalahan ketik dalam identitas pemilih
4. Upload foto digunakan untuk mengambil foto untuk identifikasi pemilih
5. QR Code digunakan untuk kode agar tidak terjadi pemilih ganda



Gambar 4.3 Menu Admin Pemilih

4.2.4 Menu Cetak Kartu Pemilih

Digunakan untuk melakukan login pemilihan pemilihan, data pemilih dilengkapi QR Code agar data pemilih tidak ganda

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

Gambar 4.4 Menu Kartu Pemilih

4.2.5 Menu Edit Pemilih

Menu edit pemilih digunakan untuk mengedit data pemilih apabila terjadi kesalahan dalam pencetakan kartu pemilih

Gambar 4.5 Menu Edit Pemilih

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

4.2.6 Menu Barcode Pemilih

Barcode yang digunakan adalah QR Code. QR Code ini digunakan agar tidak terjadi pemilih ganda

Gambar 4.6 Menu QR Code

4.2.7 Menu Upload Foto Pemilih

Menu upload pemilih digunakan untuk memasukan foto daftar pemilih. Foto ini untuk inisialisasi dan gambar pemilih

Gambar 4.7 Menu Upload Foto

4.2.8 Menu Pemrosesan Pemilihan

Menu pemrosesan pemilih dengan cara kita memasukan NIK dan juga inisisalisasi barcode reader apabila data kita telah tersedia maka akan masuk

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

halaman voting tetapi apabila kita tidak terdaftar maka kita tidak dapat melakukan pencoblosan

Gambar 4.8 Menu Proses Voting

4.2.9 Menu Calon Pemilihan

Menu calon pemilihan digunakan untuk pencoblosan *e-voting* disini ada tiga calon yang yakni bapakm Ali Ahmadi, Susilowati, Chamdik.

Gambar 4.9 Menu Data Kandidat

4.2.10 Menu Enkripsi Data Pemilihan

Menu enkripsi data pemilihan digunakan untuk mengkodekan data pemilih.agar kerahasiaan data pemilihan dapat terjaga keasliannya.

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

Gambar 4.10 Menu Enkripsi

4.2.11 Menu Pesan Anda Sudah Pernah Memilih Sebelumnya

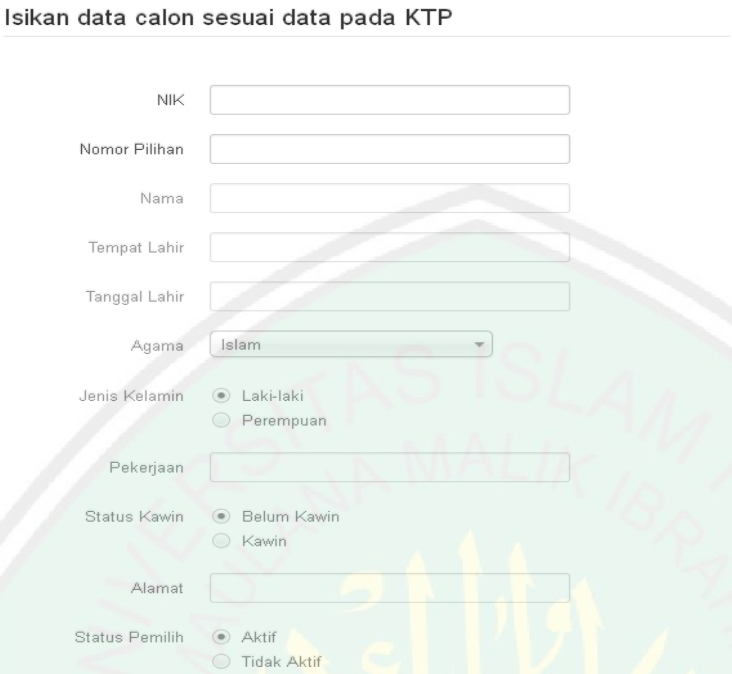
Menu peringatan ini digunakan apabila seseorang yang sudah melakukan pemilihan tidak dapat lagi melakukan pemilihan karena datanya sudah tersimpan dalam data base.

Gambar 4.11 Menu Konfirmasi Sudah Memilih

4.2.12 Menu Calon Kades

Menu pendaftaran calon kades digunakan untuk inputan calon kepala desa. Data ini digunakan untuk untuk pemilihan kepala desa kedungdowo

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

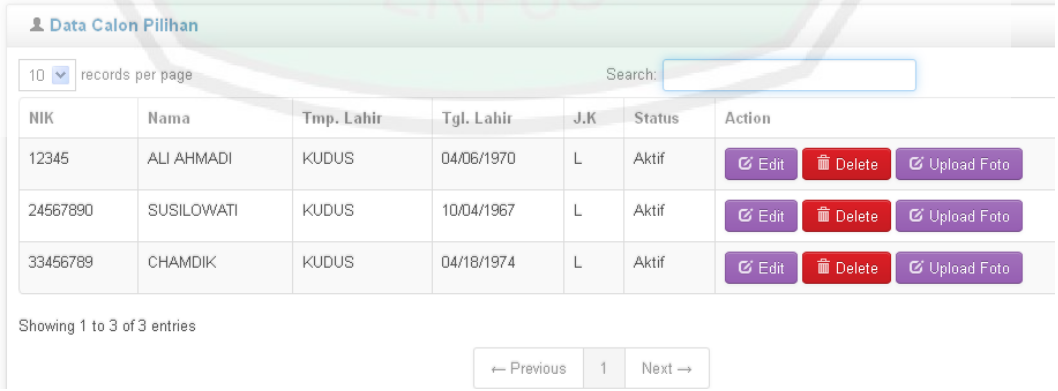


Gambar 4.12 Menu Kades

4.2.13 Menu Admin Calon Kades

Menu admin calon kepala desa berisi sebagai berikut:

1. Edit digunakan untuk mengedit data calon pemilih
2. Delete digunakan untuk menghapus calon pemilih
3. Upload foto digunakan untuk memasukan foto



\ Gambar 4.13 Admin Calon Kandidat

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

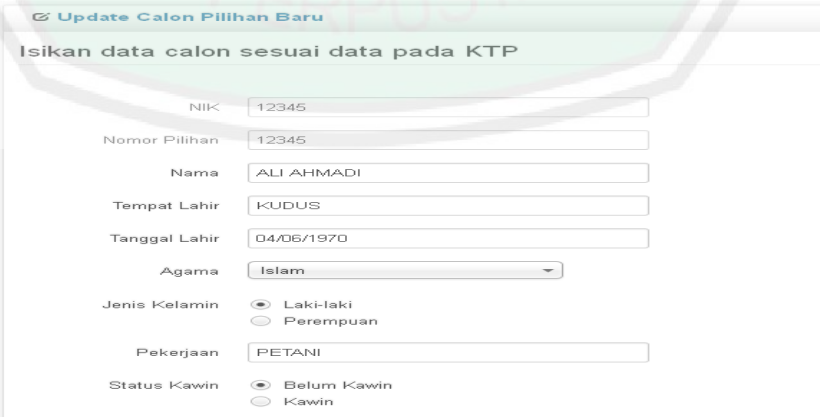
4.2.14 Menu Upload Foto Kades

Menu Upload foto untuk memasukan foto kandidat

Gambar 4.14 Menu Upload Kades

4.2.15 Menu Edit Kades

Menu edit kades digunakan untuk mengedit apabila terjadi kesalhan dalam mencetak identitas calon kepala desa



Gambar 4.15 Menu Edit Calon Kandidat

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

4.2.16 Menu Grafik Rekapitulasi Pemilihan

Menu grafik rekapitulasi pemilihan digunakan untuk melihat hasil perolehan suara selama pemilihan,

Gambar 4.16 Menu Grafik Pemilihan

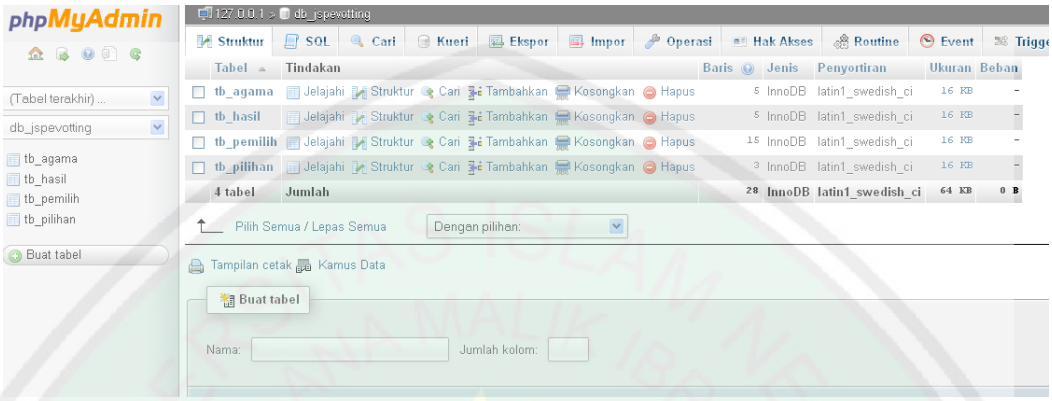
4.3 Menu Mengatur Data Base

Gambar 4.17 Menu Apache

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

.3.2 Menu Data Base

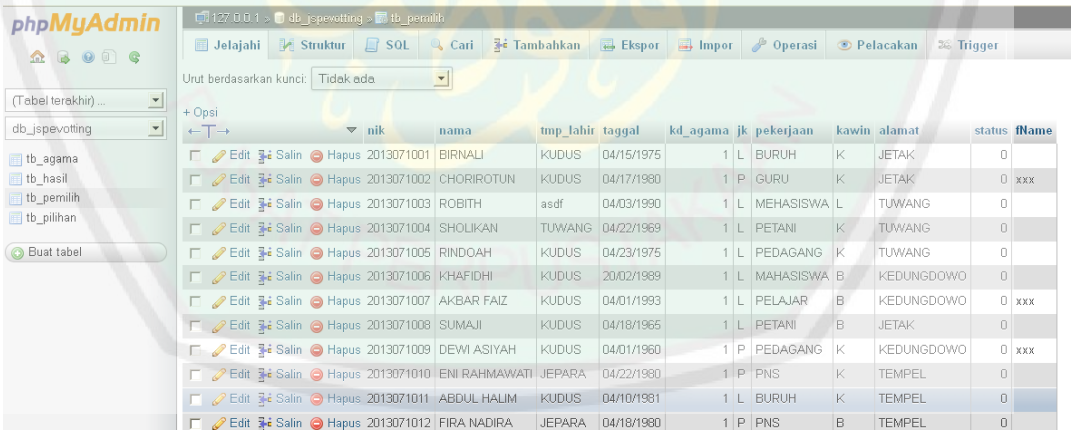
Menu ini digunakan untuk managemen data base



Gambar 4.18 Menu DataBase Admin

4.3.3 Menu Data Base Pemilih

Menu database pemilih berisi NIK, nama, tempat,tanggal lahir,Kd_agama, JK, Pekerjaan, status, alamat, status, foto



Gambar 4.19 Menu Data Pemilih

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

4.3.4 Menu Calon Kepala Desa

Menu database kepala desa berisi NIK, nama, tempat ,tangggal lahir, Kd_agama, JK, pekerjaan, Status, alamat, foto.

Gambar 4.20 Menu Beranda

4.3.5 Menu Data Base Agama

Data base agama berisi macam-macam agama : islam, Kristen, katolik, hindu, budha.

Gambar 4.21 Menu Database Agama

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

4.3.6 Menu Data Base Hasil Pilihan

Menu database hasil pemilihan berisi id_hasil, NIK, pilihan, tanggal.

Gambar 4.22 Menu Database Hasil Pilihan

4.4 Pengujian Sistem

Sistem yang baik perlu dilakukan pengujian kepada sebagian orang untuk mendapat gamabar umum pada pemakaian sistem tersebut nantinya kepada khalayak yang lebih luas lagi. Implementasi *e-voting* dimulai dari penetapan pendaftaran, autentikasi pemilih, pemilihan calon kepala desa, dan penerapan hasil pemilihan dengan algoritma RC 4.

4.4.1 Pendaftaran

Sebelum melakukan pemilihan kepala desa, daftar colon pemilih harus mendaftar ke panitia pemilihan. Untuk mengatasi agar pemilih tidak ganda maka menggunakan QR Code.

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

```
public class QRCodeGen extends HttpServlet {
        @Override
        protected void doGet(HttpServletRequest request,
                        HttpServletResponse response) throws ServletException,
IOException {
                String qrtext = request.getParameter("kode");
                ByteArrayOutputStream out = QRCode.from(qrtext).to(
                                ImageType.PNG).stream();
                response.setContentType("image/png");
                response.setContentLength(out.size());
                OutputStream outStream = response.getOutputStream();
                outStream.write(out.toByteArray());
                outStream.flush();
                outStream.close();
        }
}
```

Gambar 4.1 koding qr code

4.4.2 Pemilihan

Setelah pemilih sukses mendaftar langkah selanjutnya adalah pemilihan kepala desa. Pemilih tinggal mengklik foto calon kandidat yakni susilowati, chamdik dan ali ahmadi, setelah sukses nanti data hasil pemilihan akan langsung terakumulasi kedalam grafik rekapitulasi pemilih

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

```
public static double hasilPemilih(String id) {
    int jml =0;
    int All =0;
    try {
       Class.forName("com.mysql.jdbc.Driver");
       Connection con = DriverManager.getConnection(url, "root", "");
       Statement stmt = con.createStatement();
       System.out.println("id :" + id);
       ResultSet result = stmt.executeQuery("SELECT * FROM tb_hasil where pilihan =
'" + id + "' ");

       while(result.next())
       {
          jml++;
       }
       System.out.println("jml :" + jml);
       stmt = con.createStatement();
       result = stmt.executeQuery("SELECT * FROM tb_hasil  ");

       while(result.next())
       {
          All++;
       }
       System.out.println("All :" + All);
       con.close();
    } catch (Exception ex) {
       Logger.getLogger(Pemilih.class.getName()).log(
                  Level.SEVERE, null, ex);
       return 0;
    }
    double ret = 100/All * jml;
    return  ret   ;
`
```

Gambar 4.2 koding pemilihan

4.4.3 Enkripsi data hasil pemilihan

Setelah pemilih melakukan pencoblosan, maka pemilih akan mendapatkan kode enkripsi yang telah di kodekan agar tidak ada orang yang tahu. Pemilih juga dapat mengecek deskripsi hasil pilihan.

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

```
public RC4(byte[] key) throws NullPointerException {
    for (int i=0; i < 256; i++) {
        state[i] = (byte)i;
    }
    x = 0;
    y = 0;
    int index1 = 0;
    int index2 = 0;
    byte tmp;
    if (key == null || key.length == 0) {
        throw new NullPointerException();
    }
    for (int i=0; i < 256; i++) {
        index2 = ((key[index1] & 0xff) + (state[i] & 0xff) + index2) & 0xff;
        tmp = state[i];
        state[i] = state[index2];
        state[index2] = tmp;
        index1 = (index1 + 1) % key.length;
    }
}
public byte[] rc4(String data) {
    if (data == null) {
        return null;
    }
    byte[] tmp = data.getBytes();
    this.rc4(tmp);
    return tmp;
}
public byte[] rc4(byte[] buf) {
    int xorIndex;
    byte tmp;
    if (buf == null) {
        return null;
    }
    byte[] result = new byte[buf.length];
    for (int i=0; i < buf.length; i++) {
        x = (x + 1) & 0xff;
        y = ((state[x] & 0xff) + y) & 0xff;
        tmp = state[x];
        state[x] = state[y];
        state[y] = tmp;
        xorIndex = ((state[x] &0xff) + (state[y] & 0xff)) & 0xff;
        result[i] = (byte)(buf[i] ^ state[xorIndex]);
    }
    return result;
}
}
```

Gambar 4.3 koding rc 4

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

4.4.4 Hasil uji coba

NIK	Nama	Alamat	Hasil
2013071001	BIRNALI	JETAK	BAGUS
2013071002	CHORIROTUN	JETAK	BAGUS
2013071003	ROBITH	KEDUNGDOWO	CUKUP
2013071004	SHOLIKAN	TUWANG	CUKUP
2013071005	RINDOAH	TUWANG	BAGUS
2013071006	CHAFIDHI	JETAK	BAGUS
2013071007	AKBAR FAIS	KEDUNGDOWO	BAGUS
2013071008	SUMAJI	KEDUNGDOWO	BAGUS
2013071009	DEWI ASIYAH	JETAK	BAGUS
2013071010	ENI	JETAK	BAGUS

Tabel 4.1 uji coba pemilihan

Berdasarkan pengamatan terhadap beberapa pemilih dalam melakukan pemilihan kepala desa kedungdowo system ini dapat disimpulkan mudah untuk digunakan. Akan tetapi beberapa pemilih masih kesulitan dalam memahami kode enkripsi hasil pemilihan dan deskripsi pemilihan. Untuk itu perlu adanya sosialisasi yang lebih banyak

4.5 Kriptografi Dalam Pandangan Al-Quran

وَلَقَدْ جَعَلْنَا فِي ٱلسَّمَآءِ بُرُوجًا وَزَيَّنَّٰهَا لِلنَّٰظِرِينَ ﴿١٦﴾ وَحَفِظْنَٰهَا مِن كُلِّ
شَيْطَٰنٍ رَّجِيمٍ ﴿١٧﴾ إِلَّا مَنِ ٱسْتَرَقَ ٱلسَّمْعَ فَأَتْبَعَهُۥ شِهَابٌ مُّبِينٌ ﴿١٨﴾

16. *dan Sesungguhnya Kami telah menciptakan gugusan bintang-bintang (di langit) dan Kami telah menghiasi langit itu bagi orang-orang yang memandang (Nya),*
17. dan Kami menjaganya dari tiap-tiap syaitan yang terkutuk,
18. kecuali syaitan yang mencuri-curi (berita) yang dapat didengar (dari malaikat) lalu Dia dikejar oleh semburan api yang terang.

Allah telah menjadikan Lauh Mahfuzh ini sebagai tempat untuk menyimpan segala rahasia dilangit dan di bumi. Jin dari golongan setan akan berusaha untuk mencuri segala rahasia yang tertulis di dalamnya untuk menipu manusia. Disamping itu, mereka juga memiliki tujuan untuk memainkan aqidah manusia.

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

Rahasia adalah sebuah amanat dan menjaga rahasia sangat dianjurkan oleh Allah seperti dalam firman-Nya:

۞ إِنَّ ٱللَّهَ يَأۡمُرُكُمۡ أَن تُؤَدُّواْ ٱلۡأَمَٰنَٰتِ إِلَىٰٓ أَهۡلِهَا وَإِذَا حَكَمۡتُم بَيۡنَ ٱلنَّاسِ أَن تَحۡكُمُواْ بِٱلۡعَدۡلِۚ إِنَّ ٱللَّهَ نِعِمَّا يَعِظُكُم بِهِۦٓۗ إِنَّ ٱللَّهَ كَانَ سَمِيعَۢا بَصِيرٗا ٥٨

58. *"Sesungguhnya Allah menyuruh kamu menyampaikan amanat kepada yang berhak menerimanya, dan (menyuruh kamu) apabila menetapkan hukum di antara manusia supaya kamu menetapkan dengan adil. Sesungguhnya Allah memberi pengajaran yang sebaik-baiknya kepadamu. Sesungguhnya Allah adalah Maha mendengar lagi Maha melihat". (QS.An-Nisa' ; 58)*

Dari ayat di atas, menurut 'Aidh al-Qarni dalam buku Tafsir Muyassar jilid.1 dijelaskan bahwa Allah menyuruh kalian agar senantiasa menyampaikan amanat kepada yang berhak menerimanya. Sehingga ayat tersebut menganjurkan agar kita menjaga amanat yang dititipkan kepada kita dan tidak memberitahukan amanat tersebut kepada orang yang tidak berhak menerimanya, dan salah satu jenis dari amanat tersebut adalah rahasia. Dan rahasia tersebut, dimana rahasia tersebut dapat disampaikan dalam bentuk pesan tertulis.

Dikarenakan rahasia merupakan amanat, maka kita juga berkewajiban menjaga rahasia yang telah dititipkan kepada kita dan janganlah menghianati amanah tersebut dengan memberitahukannya kepada orang yang tidak berhak. Seperti dijelaskan dalam al-qur'an sebagai berikut:

يَٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُواْ لَا تَخُونُواْ ٱللَّهَ وَٱلرَّسُولَ وَتَخُونُوٓاْ أَمَٰنَٰتِكُمۡ وَأَنتُمۡ تَعۡلَمُونَ ٢٧

Hai orang-orang yang beriman, janganlah kamu mengkhianati Allah dan Rasul (Muhammad) dan (juga) janganlah kamu mengkhianati amanat-amanat yang dipercayakan kepadamu, sedang kamu mengetahui.(QS. Al-Anfal; 27)

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

Menurut ‘Aidh al-Qarni dalam buku Tafsir Muyassar jilid2, ayat diatas menjelaskan bahwa janganlah kalian menghianati setiap amanat yang diberikan kepada kalian, seperti hak, kewajiban, rahasia. Sedangkan kalian mengetahui penghianatan amanah ini hukumnya haram.

Ayat di atas menganjurkan kepada kita agar tidak menghianati setiap amanat yang diberikan kepada kita. Salah satu dari jenis amanah tersebut adalah rahasia. Sehingga menjaga rahasia juga sangat diwajibkan dan apabila kita memberitahukan rahasia tersebut berarti sama dengan kita menghianati amanah yang diberikan kepada kita. Sedangkan menghianati amanah hukumnya adalah haram.

Ayat tersebut juga dikuatkan dengan hadits Rasulullah yang ditulis oleh Imam Nawawi dalah bukunya Riyadhus Sholihin sebagai berikut:

وَ عَنْ ثَابِتٍ عَنْ أَنَسٍ رَضِى اللهُ عَنْهُ قَالَ : أَتَى عَلَيَّ رَسُوْلُ اللهِ صَلَّى اللهُ عَلَيْهِ وَسَلَّمَ وَأَنَا أَلْعَبُ مَعَ الْغِلْمَانِ ، فَسَلَّمَ عَلَيْنَا فَبَعَثَنِى فِى حَاجَةٍ ، فَأَبْطَأْتُ عَلَى أُمِّى . فَلَمَّا جِئْتُ قَالَتْ : مَا حَبَسَكَ ؟ فَقُلْتُ : بَعَثَنِى رَسُوْلُ اللهِ صَلَّى اللهُ عَلَيْهِ وَسَلَّمَ لِحَاجَةٍ ، قَالَتْ : مَا حَاجَتُهُ ؟ قُلْتُ : إِنَّهَا سِرٌّ . قَالَتْ : لاَ تُخْبِرَنَّ بِسِرِّ رَسُوْلُ اللهِ صَلَّى اللهُ عَلَيْهِ وَسَلَّمَ أَحَدًا . قَالَ أَنَسٌ : وَاللهِ لَوْ حَدَّثْتُ بِهِ أَحَدًا لَحَدَّثْتُكَ بِهِ يَا ثَابِتُ . (رواه مسلم)

“Dari Tsabit dari Anas R.A, dia berkata : “Saya didatangi oleh Rasulullah ketika itu aku sedang bermain- main dengan anak- anak. Beliau mengucapkan salam kepada kami lalu menyuruh saya untuk suatu keperluan, akhirnya saya terlambat menemui ibuku. Ketika saya datang ibuku bertanya: “apa yang membuatmu terlambat?”. Saya menjawab: “saya disuruh oleh Rasulullah SAW untuk suatu keperluan”. Ibu bertanya: “apa keperluan beliau?” saya menjawab: “itu rahasia”. Ibu berkata: “jangan sekali- kali kau memberitahukan rahasia Rasulullah SAW kepada siapapun”. Anas berkata: “demi Allah seandainya aku memberitahukannya kepada seseorang tentu aku telah memberitahukannya kepadamu wahai Tsabit”. (HR. Muslim)

Hadits tersebut mengajarkan kepada kita bahwa menjaga rahasia telah diajarkan oleh Nabi Muhammad SAW kepada para sahabat. Dan janganlah

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

melakukan penghianatan terhadap rahasia yang diamanatkan kepada kita karena sesungguhnya menghianati amanah dengan menyampaikan rahasia adalah haram hukumnya, seperti yang telah dijelaskan pada surat Al-Anfal.

Berbagai cara yang dilakukan untuk menjamin keamanan informasi *e-voting*. Dan dengan berkembangnya cara pengiriman *e-voting* nantinya, berkembangpula cara menyembunyikan pesan kriptografi dan bagaimana agar orang lain tidak mengetahui isi pesan atau informasi walaupun pesan tersebut telah ditemukan. Salah satunya adalah dengan menyandikan informasi menjadi suatu kode-kode yang tidak dimengerti, sehingga apabila disadap akan kesulitan untuk mengetahui informasi yang sebenarnya. Dari sinilah lahir suatu ilmu yang disebut kriptografi.

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

BAB V

PENUTUP

5.1. Kesimpulan

Dari penelitian yang telah dilakukan, maka dapat diambil beberapa kesimpulan sebagai berikut:

1. Untuk menjaga kerahasiaan hasil pemilihan dapat menggunakan cara mengenkripsi data pilihan. Sehingga kerahasiaan pemilihan dapat terjaga. Pada aplikasi ini metode yang digunakan untuk proses enkripsi simetri menggunakan algoritma RC4.
2. QR Code menjaga agar tidak terjadi pemilih ganda.
3. Dengan melakukan proses *e-voting,* nantinya akan berjalan dengan cepat, dan aman

5.2. Saran

Untuk pengembangan lebih lanjut, maka terdapat beberapa saran yang perlu dipertimbangkan untuk pengembang selanjutnya, antara lain:

1. Hendaknya dalam melakukan autentifikasi pemilih menggunakan Chip.
2. Dilakukan suatu pengembangan Aplikasi *e-voting* yang berbasis *client server* ini sehingga keberadaannya bisa lebih *user friendly*.
3. Dalam penelitian berikutnya, sebaiknya menggunakan algoritma enkripsi yang lain, yang menggunakan kunci publik. Sehingga dapat diketahui lebih efektif mana penggunaan algoritma kunci publik dan kunci privat.

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

DAFTAR PUSTAKA

Al-Qarni, ‘Aidh. 2007. *Tafsir Muyassar Jilid 1*. Jakarta: Qisthi Press

Al-Qarni, ‘Aidh. 2007. *Tafsir Muyassar Jilid 2*. Jakarta: Qisthi Press

Ariyus, Doni. 2008. *Pengantar Ilmu Kriptografi (Teori, Analisis, dan Implementasi).* Yogyakarta: Andi

Azhari, Rahmad. 2005. *E-Voting*. Jakarta; Universitas Indonesia.

Febrianto, Anjar. 2012. *Aplikasi E-Voting Berbasis Client-Server*.Jakarta

Fiansah, Endang. 2008. *Implementasi Algoritma Dasar RC4 Stream Cipher Dan Pengacakan Plaintext Dengan Dinamit Teknik Blocking*.IPB

Helena, Apriza. 2009. *Simulasi E-Voting system menggunakan metode scratch and vote* .Surabaya; Institute Teknologi Sepuluh Novenber

Khairul, Ahmad. 2010. *Tutorial Rational Rose.*

Munir, Rinaldi dan Nugraha, pasca. 2011. *Pengembangan Aplikasi QR Code Generator dan QR Code Reader dari Data Berbentuk Image*. Bandung; ITB

Munir, Rinaldi. 2004. “*Pengolahan Citra Digital dengan Pendetakan Algoritmik*”. Informatika Bandung, Bandung.

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

Nugroho, Adi. 2005. *Rational Rose Untuk Pemodelan Berorientasi Obyek*. Bandung: Informatika

Nugraha, Agung. 2010. *Penerapan Kriptografi Pada Aplikasi Java E-Voting*. Bogor; Jurusan Teknik Persandian

Rahayu, Dwi Yeni. 2010. *Pembuatan Aplikasi Pembacaan Quick Response Code Menggunakan Perangkat Mobile Berbasis J2ME Untuk Identifikasi Suatu Barang. Tugas akhir* Tidak Diterbitkan. Surabaya: Jurusan Teknik Informatika Politeknik Elektronika Negeri Surabaya Institut Teknologi Sepuluh Nopember.

Schneier, B., 1996. *Applied Cryptography, Second Edition: Protocols, Algorithms and Source Code in C.* John Willey & Sons, Inc.

Sholahuddin, M. dan Rosa A.S. 2008. *Pemrograman J2ME (Belajar Cepat Pemrograman Perangkat Telekomunikasi Mobile*). Informatika:Bandung.

Sholahudin, Muhamad. 2008. *Pembuatan Modul E-Voting Berbasis Web*. Bandung; Institute Teknologi Bandung.

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

Suharto, Ansar Rizal. 2011. *Implementasi algoritma RC4 untuk keamanan login pada system pembayaran uang sekolah*. Bontang: Jurusan Elektro Politeknik Negeri

Sulistiyani, Sri. 2008. *Membuat aplikasi database dengan java dan MySQL* Semarang; Wahana Komputer

Undang-Undang No 4 Tahun 2007 *Tentang Pemilihan Kepala Desa*.

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG