BAB III

ANALISA DAN PERANCANGAN

3.1 Analisi Sistem

Sistem pemungutan suara secara elektronik sama dengan pemungutan suara secara konvensional, yang membedakan pada peralatan pendukung pelaksanaan pemungutan suara. Dalam pelaksanaan pemungutan suara secara konvensioanal peralatan pendukung berupa alat-alat manual (bukan mesin), sedangkan dalam pemungutan suara elektronik peralatan pendukungnya berupa mesin dalam hal ini adalah komputer. Pelaksanaan voting yang konvensioanl, sering terjadi kesalahan-kesalahan yang disebabkan oleh *human error*, atau disebabkan karena sistem pendukung pelaksanaan voting yang tidak berjalan dengan baik, kesalahan dalam proses pendaftaran pemilih, pemilih salah dalam memberi tanda pilihanya, lamanya proses pengumpulan kartu suara, lamanya proses perhitungan suara,permasalahan-permasalahan tersebut yang membuat keabsahan hasil voting diragukan.

3.1.1 Tahap Pelaksanaan Pemungutan dan Penghitungan Suara Pilkada

Pelaksanaan pemungutan dan perhitungan suara dibagi menjadi dua tahapan yakni persiapan dan pelaksanaan.

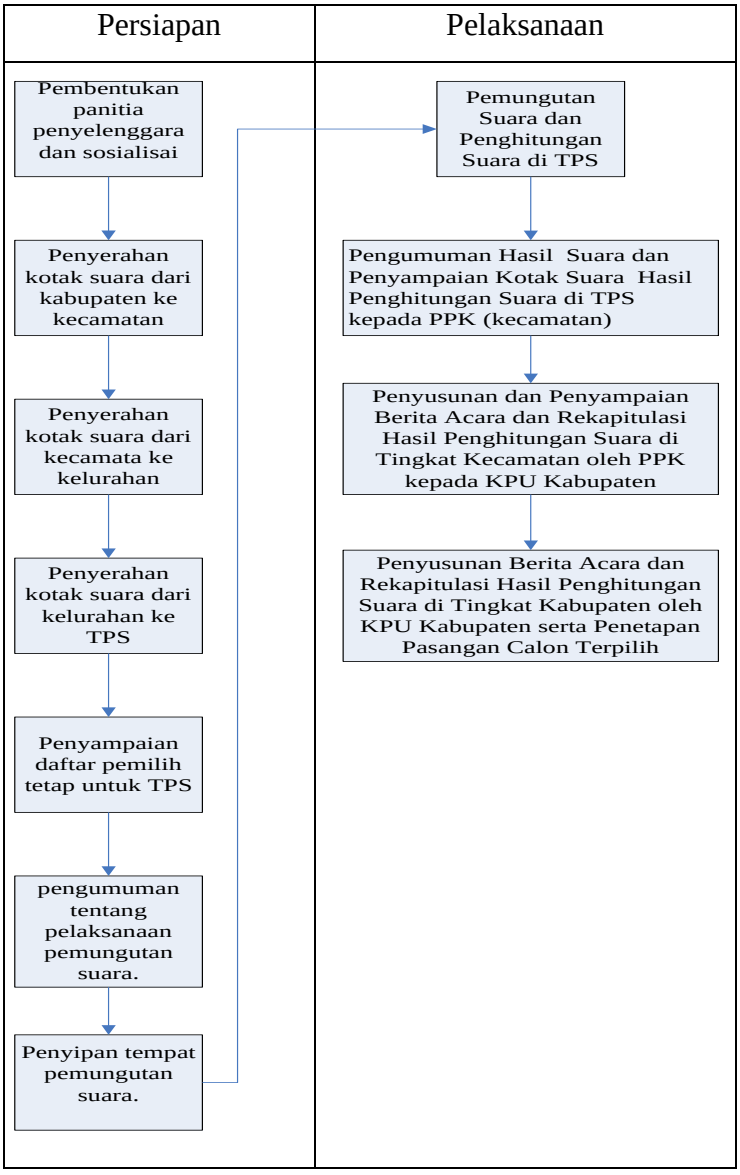
Dalam tahap persiapan dilaksanakan beberapa kegiatan yakni:

1. Pembentukan panitia penyelenggara dan sosialisai
2. Penyerahan kotak suara dari kabupaten ke kecamatan
3. Penyerahan kotak suara dari kecamata ke kelurahan
4. Penyerahan kotak suara dari kelurahan ke TPS (tempat pemungutan suara)
5. Penyampaian daftar pemilih tetap untuk TPS
6. Penyampaian pengumuman tentang pelaksanaan pemungutan suara.
7. Penyipan tempat pemungutan suara.

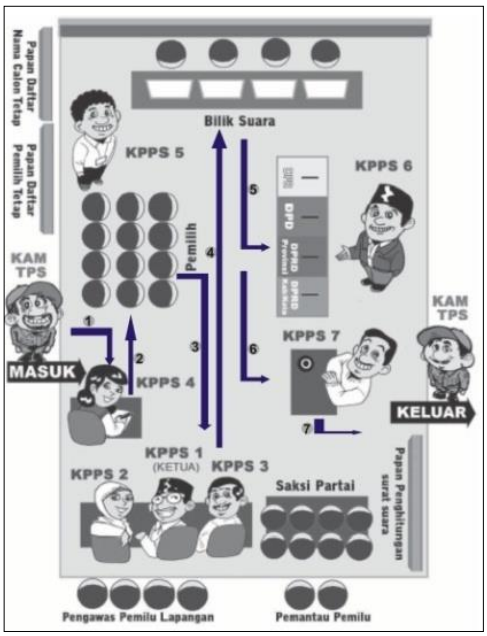
Sedangakan dalam tahap pelaksanaan dilaksanakan beberapa kegiatan yakni:

1. Pemungutan Suara dan Penghitungan Suara di TPS serta Penyusunan Berita Acara serta Sertifikat Hasil Penghitungan Suara oleh KPPS

2. Pengumuman Hasil Penghitungan Suara dan Penyampaian Kotak Suara yang Masih Dikunci dan Disegel yang Berisi Berita Acara dan Sertifikasi Hasil Penghitungan Suara di TPS kepada PPK (kecamatan)
3. Penyusunan dan Penyampaian Berita Acara dan Rekapitulasi Hasil Penghitungan Suara di Tingkat Kecamatan oleh PPK kepada KPU Kabupaten
4. Penyusunan Berita Acara dan Rekapitulasi Hasil Penghitungan Suara di Tingkat Kabupaten oleh KPU Kabupaten serta Penetapan Pasangan Calon Terpilih



Gambar 3.1 Tahap Pelaksanaan Pilkada Secara Konvensional



Gambar 3.2 Alur Pemungutan Suara di TPS

Keterangan gambar:

1. Pemilih mendaftarkan diri di meja Anggota KPPS ke empat dengan menunjukkan surat pemberitahuan.
2. Pemilih menunggu giliran untuk dipanggil di tempat duduk pemilih.
3. Pemilih dipanggil ketua KPPS dengan menyerahkan formulir dan menunjukkan Kartu Pemilih kepada anggota KPPS kedua, kemudian diberi satu lembar surat suara oleh anggota KPPS ketiga dalam keadaan terbuka (tidak dilipat).
4. Pemilih memberikan suara di bilik suara yang diatur oleh anggota KPPS ke lima. Bila surat suara rusak atau keliru dicoblos dapat meminta ganti sebanyak satu kali.
5. Pemilih memasukan surat suara ke dalam kotak suara yang diperlihatkan kepada anggota KPPS ke enam.
6. Pemilih sebelum keluar ditandai dengan tinta khusus pada salah satujari tangannya oleh anggota KPPS ke tujuh.
7. Pemilih selesai memberikan suara dan meninggalkan lokasi TPS melalui pintu keluar

3.2 Hasil Analisis

Hasil dari analisis yang telah dilakukan dari proses penelitian pemilihan umum secara konvensional dihasilkan keputusan perlunya suatu sistem elektronik voting untuk pemilihan kepala daerah, dari proses pemilihan kepala daerah secara elektronik adalah didapatkanya data pemilih tetap untuk TPS serta data pasangan calon kandidat. informasi ini dapat membantu pihak TPS untuk memudahkan dalam proses pemilihan suara dan pengumuman hasil suara yang telah dihitung secara otomatis oleh sistem di TPS serta penyampaian informasi hasil rekapitulasi perolehan suara oleh KPPS ke PPS (Kelurahan),PPS kepada PPK (kecamatan), PPK kepada KPU Kabupaten.

Berikut ini yang terlibat secara langsung dalam pemilihan kepala daerah secara elektronik :

a. PEMILIH
    1) Fungsi : meverifikasi saat pemilihan kedalam system serta melakukan pemilihan.
    2) Alur Proses : Pemilih memasukkan nomor pemilih dan PIN.
    3) Item Data : data pemilih, data pasangan calon kandidat
    4) Hasil : Pilihan pemilih yang tersimpan.

b. TPS (tempat pemungutan suara)
    1) Fungsi : Sebagai aktivasi pemilihan dalam sistem, memasukkan daftar kandidat dan daftar pemilih dari KPU Kabupaten, aktivasi pemilih serta perhitungan suara di TPS.
    2) Alur Proses : Dalam aktifasi pemilihan ini petugas melakukan pembukaan dan penutupan sistem, memasukkan daftar pemilih dan daftar kandidat yang diperoleh dari KPU Kabupaten, mengaktifasi pemilih dengan memeriksa nomor pemilih dan memberikan PIN yang terdapat pada database sistem pemilihan.
    3) Item Data : daftar data pemilih, daftar data kandidat, aktivasi, hasil perhitungan suara.

4) Hasil : Pemilihan tidak dapat dilakukan sebelum aktifasi pemilihan dibuka, import daftar kandidat dan daftar pemilih, Hasil perhitungan suara tidak dapat dilakukan sebelum pemilihan selesai. Pengumuman Hasil Suara yang dihitung secara otomatis oleh sistem di TPS dan mengirimkan hasil perolehan suara kepada kelurahan untuk proses rekapitulasi, Data prolehan suara dienkripsikan sebelum dikirimkan. Penutupan sistem saat pemilihan selesai dengan batas waktu yang telah ditentukan.

c. Kelurahan (PPS)
   1) Fungsi : mengumpulkan data hasil rekapitulasi perolehan suara dari TPS yang ada di kelurahan
   2) Alur Proses : meeknripsikan dan menadatangani secara digital hasil rekapitulasi perolehan suara dari seluruh TPS
   3) Hasil : dari hasil rekapitulasi perolehan suara dari seluruh TPS yang ada di kelurahan data tidak dibuka atau didekripsi, hanya mengumpulkan data dari TPS yang ada di kelurahan tersebut dan menyerahkan data yang terkumpul dieknripsi dan ditandatangani secara digital oleh PPS kepada KPU Kecamatan (PPK) setempat.

d. KPU Kecamatan (PPK)
   1) Fungsi : Penyampaian informasi hasil rekapitulasi perolehan suara dari seluruh TPS.
   2) Alur Proses : meeknripsikan dan menadatangani secara digital hasil rekapitulasi perolehan suara dari seluruh TPS
   3) Hasil : dari hasil rekapitulasi perolehan suara dari seluruh TPS yang telah dieknripsi dan ditandatangani secara digital oleh PPK kepada KPU Kabupaten

e. KPU Kabupaten
    1) Fungsi : input data calon kandindat dan data pemilih serta menentukan hasil rekapitulasi perolehan suara.
    2) Alur Proses : input data calon kandindat dan data pemilih serta penyusunan berita acara dan rekapitulasi hasil perhitungan suara di tingkat kabupaten dalam penetapan calon terpilih.
    3) Item Data : daftar data calon kandidat, daftar data pemilih, rekapitulasi hasil perhitungan suara.
    4) Hasil : penyusunan berita acara dan rekapitulasi hasil perhitungan suara di tingkat kabupaten oleh KPU Kabupaten serta penetapan calon terpilih.

Sama halnya dengan pemungutan suara konvensional maka dalam pemungutan suara elektronik ada tahap persiapan dan pelaksanaan, berikut gambaran alur pemungutan suara yang dilaksanakan secara elektronik.

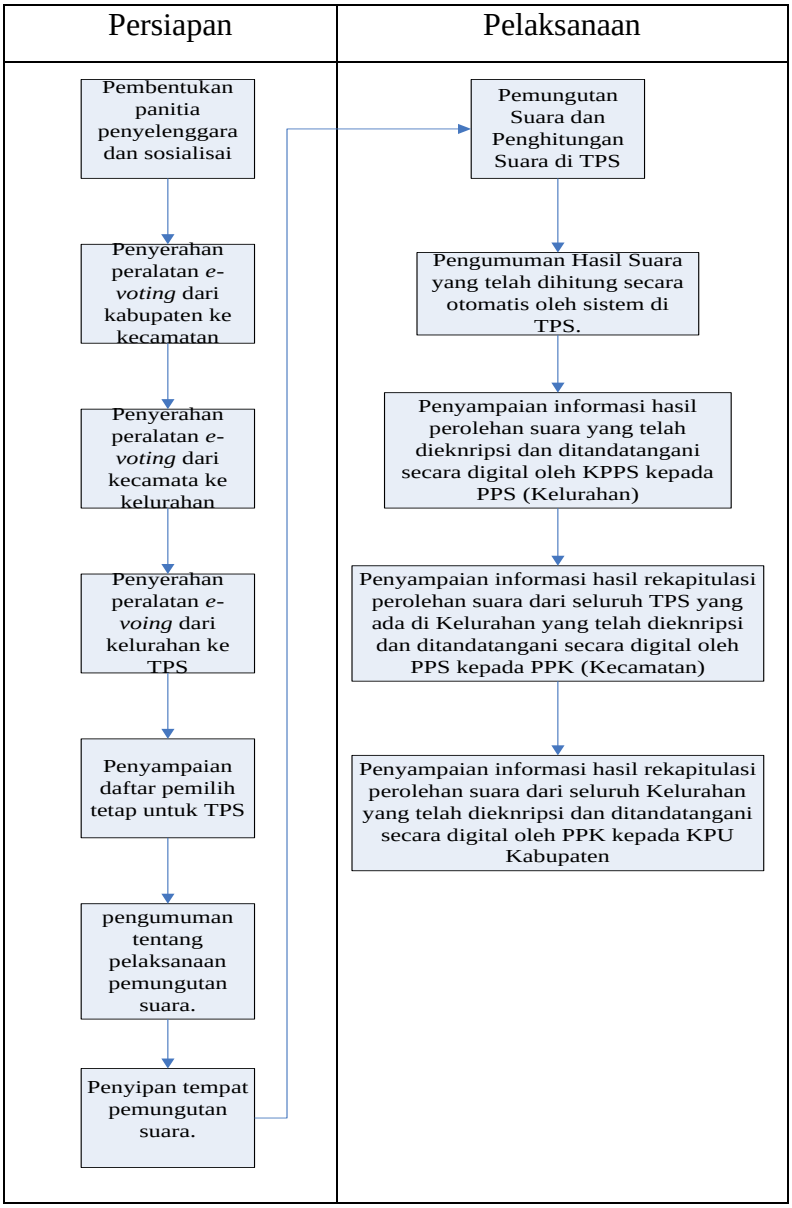
Dalam tahap persiapan dilaksanakan beberapa kegiatan yakni:

1. Pembentukan panitia penyelenggara dan sosialisai
2. Penyerahan peralatan *e-voting* dari kabupaten ke kecamatan
3. Penyerahan peralatan *e-voting* dari kecamata ke kelurahan
4. Penyerahan peralatan *e-voing* dari kelurahan ke TPS (tempat pemungutan suara)
5. Penyampaian daftar pemilih tetap untuk TPS.
6. Penyampaian pengumuman tentang pelaksanaan pemungutan suara.
7. Penyiapan tempat pemungutan suara.

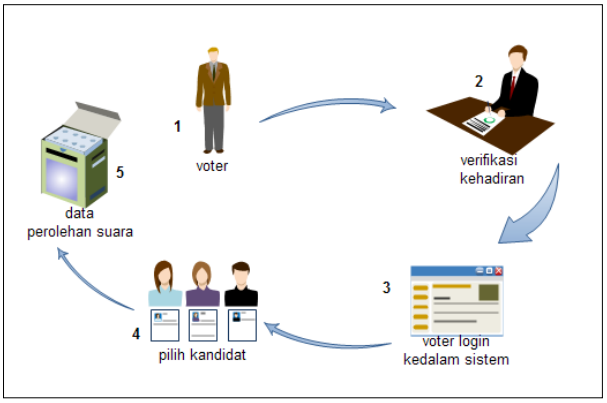
Sedangkan dalam tahap pelaksanaan dilaksanakan beberapa kegiatan yakni:

1. Pemungutan Suara di TPS oleh KPPS
2. Pengumuman Hasil Suara yang telah dihitung secara otomatis oleh sistem di TPS.

3. Penyampaian informasi hasil perolehan suara yang telah dieknripsi dan ditandatangani secara digital oleh KPPS kepada PPS (Kelurahan)
4. Penyampaian informasi hasil rekapitulasi perolehan suara dari seluruh TPS yang telah dieknripsi dan ditandatangani secara digital oleh PPK kepada KPU Kabupaten
5. Penyusunan Berita Acara dan Rekapitulasi Hasil Penghitungan Suara di Tingkat Kabupaten oleh KPU Kabupaten serta Penetapan Pasangan Calon Terpilih.



Gambar 3.3 tahap pelaksanaan pemilihan secara elektronik



Gambar 3.4 Alur Pelaksanaan Pemungutan Suara elektronik

Keterangan :

1. Calon pemilih datang ke tempat pemilihan suara
2. Calon pemilih melakukan verifikasi kehadiran terhadap petugas TPS dengan menunjukan kartu pemilih kemudian akan mendapatkan PIN dari petugas.
3. Pemilih masuk ke sistem dengan mengisi nomor pemilih dan PIN yang telah diberikan oleh petugas sebelumnya
4. Pemilih melakukan pemilihan kandidat
5. Data pemilihan dienkripsi dan disimpan di database TPS

Aplikasi yang akan dibangun merupakan aplikasi analisis sistem yang dibutuhkan untuk pemilihan umum secara elektronik. Aplikasi yang akan dibuat adalah sebagai berikut :

1. Desain input

   Desain input pada sistem ini terdiri dari input data pemilih, nomor pemilih, dan pilihan pemilih. Input data diri pemilih dilakukan pada saat sebelum pemilihan di TPS dibuka.

   Pada tahap ini petugas yang berada di TPS memasukan data pemilih yang telah ditetapkan oleh kelurahan, setelah data pemilih telah tersimpan dalam database selanjutnya petugas akan melakukan aktivasi data pemilih yang akan melakukan pemilihan.

Pemilih langsung menuju bilik suara setelah data dirinya diaktivasi untuk malakukan pemungutan suara, pemilih memasukan nomor pendaftaran dan PIN yang telah diberikan petugas untuk masuk kedalam sistem.

2. Desain output

   Desain output pada sistem ini terdiri dari informasi calon Bupati dan Wakil Bupati pada Pilkada, informasi pilihan pemilih, dan informasi hasil perhitungan suara. Pemilih dapat melihat informasi calon berupa nama, visi dan misi, serta partai pengusung calon. informasi hasil perhitungan dapat dilihat setelah pemilihan selesai dilakukan. Hasil perolehan suara di tingkat TPS.

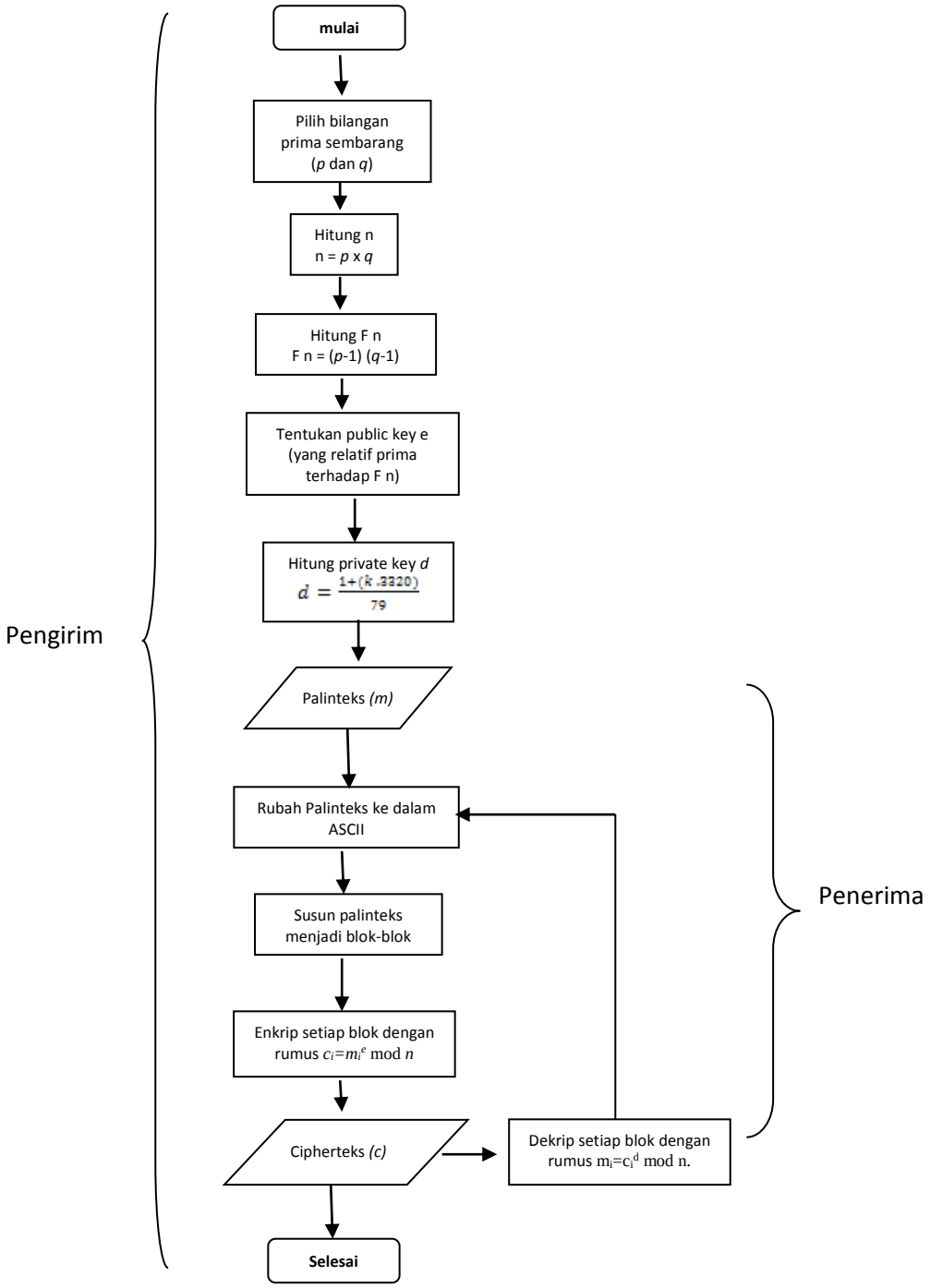
3. Desain basis data

   Desain basis data yang disusun berupa tabel-tabel yang dibutuhkan oleh sistem berdasarkan skema *e-voting*.

   Basis data terdiri dari dua bagian, yaitu basis data pada Tps yang berisi hasil perhitungan perolehan suara pada Tps dan basis data pusat yang berisi data calon pemilih dan data calon pemilih.

3.2.1 Flowchart Metode algoritma RSA

Algoritma pembangkit kunci pada algoritma RSA dapat dilihat pada gambar dibawah, dalam *flowchart* tersebut digambarkan cara pembuatan kunci publik serta pembangkitan pasangan kunci yakni kunci privat.



Gambar 3.5 Flowchat metode algoritma RSA

3.2.2 Batasan Sistem

Sistem ini memiliki batasan, yaitu:

a. Group blind digital signature metode algoritma RSA digunakan untuk menganalisis keamanan pengiriman data hasil perolehan suara.
b. Program ini berisi tentang system elektronik pemilihan umum kepala daerah.
c. Analisis yang digunakan dalam system elektronik pemilihan umum kepala daerah adalah pemilihan kepala daerah dan wakil kepala daerah serta penentuan hasil suara pemilihan kepala daerah di tingkat TPS.
d. Data-data yang dikelola adalah data pemilih, data kandidat, dan data hasil perhitungan suara di TPS.

3.3 Representasi Model *algoritma RSA*

Adapun langkah-langkah Perhitungan enkripsi pesan dengan *RSA* yang akan digunakan untuk *digital signature* dalam pendistribusian data tahap pengiriman adalah sebagai berikut :

1) *p* : bilangan yang dipilih oleh pengirim dan dijaga kerahasiaanya
2) *q* : bilangan yang dipilih oleh pengirim dan dijaga kerahasiaanya
3) *n* : Besaran n tidak dirahasiakan
4) $\Phi(n) = (p-1)(q-1)$: sekali $\Phi(n)$ dapat dihitung, *p* dan *q* dapat dihapus untuk mencegah tidak diketahui oleh orang lain (rahasia)
5) *e* : bilangan bulat untuk kunci publik yang relatif prima terhadap $\Phi(n)$ (tidak rahasia)
6) *d* : kunci privat, dihitung dari d = e^{-1} mod ($\Phi(n)$)(rahasia)
7) *m* : plainteks (rahasia)
8) *c* : cipherteks (tidak rahasia)

Pada awalnya kita tentukan kunci privat, kuci publik, dan modulus dengan menggunakan algoritma pembangkit kunci yang telah dijelaskan sebelumnya. misalkan kita memilih *p*= 47 dan *q*=71 selanjutnya kita menghitung

n=47 x 71

n=3337

dan $\Phi(n) = (p-1)(q-1)$

$\Phi(n) = 3320$

Kita pilih kunci public $e = 79$, karena 79 relatif prima terhadap 3320. selanjutnya kita menghitung kunci privat dengan rumus: $d = \frac{1+(k \cdot 3320)}{79}$ dengan mencoba-coba nilai k=1,2,3….(dan seterusnya) maka diperoleh nilai d yang bulat adalah 1019.

Inilah pasangan dari kunci publik yakni kunci privat, sehingga diketahui:

Kunci publik : 79

Kunci privat: 1019

Modulus: 3337

a) Pesan dengan text satu kata

Isi pesan m = Kelurahan

Nilai hash dari m adalah:

h= 6f18bf1a1fd5c7b75fb3da2be0a0f924

Nilai hash dikonversi kedalam kode ASCII menjadi:

541024956981024997491021005399559855

531029851100975098101489748102575052

Kemudian m dipecah menjadi blok yang lebih kecil:

m_1=541	m_9=005	m_{17}=975
m_2=024	m_{10}=399	m_{18}=098
m_3=956	m_{11}=559	m_{19}=101
m_4=981	m_{12}=855	m_{20}=489
m_5=024	m_{13}=531	m_{21}=748
m_6=997	m_{14}=029	m_{22}=102
m_7=491	m_{15}=851	m_{23}=575
m_8=021	m_{16}=100	m_{24}=052

Kemudian setiap blok dienkripsi menggunakan kunci privat dengan menggunakan persamaan pada *RSA.*
yakni: $c_i = m_i^e \bmod n$

$c_1 = 541^{79} \bmod 3337 = 2223$
$c_2 = 024^{79} \bmod 3337 = 3022$
$c_3 = 956^{79} \bmod 3337 = 976$
$c_4 = 981^{79} \bmod 3337 = 1768$
$c_5 = 024^{79} \bmod 3337 = 3022$
$c_6 = 997^{79} \bmod 3337 = 1436$
$c_7 = 491^{79} \bmod 3337 = 967$
$c_8 = 021^{79} \bmod 3337 = 1249$
$c_9 = 005^{79} \bmod 3337 = 270$
$c_{10} = 399^{79} \bmod 3337 = 1584$
$c_{11} = 559^{79} \bmod 3337 = 1093$
$c_{12} = 855^{79} \bmod 3337 = 2075$
$c_{13} = 531^{79} \bmod 3337 = 761$
$c_{14} = 029^{79} \bmod 3337 = 1997$
$c_{15} = 851^{79} \bmod 3337 = 1774$
$c_{16} = 100^{79} \bmod 3337 = 1287$
$c_{17} = 975^{79} \bmod 3337 = 368$
$c_{18} = 098^{79} \bmod 3337 = 617$
$c_{19} = 101^{79} \bmod 3337 = 1113$
$c_{20} = 489^{79} \bmod 3337 = 1453$
$c_{21} = 748^{79} \bmod 3337 = 3284$
$c_{22} = 102^{79} \bmod 3337 = 3230$
$c_{23} = 575^{79} \bmod 3337 = 757$
$c_{24} = 052^{79} \bmod 3337 = 3137$

Jadi cipherteks yang dihasilkan adalah:
c = 2223.3022.976.1768.3022.1436.967.1249.270.1584.1093.2075
761.1997.1774.1287.368.617.1113.1453.3284.3230.757.3137

Kemudian untuk mendekripsi pesan cipherteks dipecah menjadi blok seperti pada proses sebelumnya dan didekripsi dengan kunci public yang telah diketahui oleh pengirim dan penerima. $m_i = c_i^d \bmod n$.

$m_1 = 2223^{1019} \bmod 3337 = 541$
$m_2 = 3022^{1019} \bmod 3337 = 24$
$m_3 = 976^{1019} \bmod 3337 = 956$
$m_4 = 1768^{1019} \bmod 3337 = 981$
$m_5 = 3022^{1019} \bmod 3337 = 24$
$m_{13} = 761^{1019} \bmod 3337 = 531$
$m_{14} = 1997^{1019} \bmod 3337 = 29$
$m_{15} = 1774^{1019} \bmod 3337 = 851$
$m_{16} = 1287^{1019} \bmod 3337 = 100$
$m_{17} = 368^{1019} \bmod 3337 = 975$

$m_6=1436^{1019} \bmod 3337= 997$ $m_{18}=617^{1019} \bmod 3337= 98$

$m_7=967^{1019} \bmod 3337= 491$ $m_{19}=1113^{1019} \bmod 3337= 101$

$m_8=1249^{1019} \bmod 3337= 21$ $m_{20}=1453^{1019} \bmod 3337= 489$

$m_9=270^{1019} \bmod 3337= 5$ $m_{21}=3284^{1019} \bmod 3337=748$

$m_{10}=1584^{1019} \bmod 3337= 399$ $m_{22}=3230^{1019} \bmod 3337= 102$

$m_{11}=1093^{1019} \bmod 3337= 559$ $m_{23}=757^{1019} \bmod 3337= 575$

$m_{12}=2075^{1019} \bmod 3337= 855$ $m_{24}=3137^{1019} \bmod 3337= 52$

maka diperoleh

m'=541024956981024997491021005399559855

53102985110097509810148974810257505 2

dimana m mempunyai nilai:

h'= 6f18bf1a1fd5c7b75fb3da2be0a0f924

Tandatangan dianggap otentik karena *h=h'*

b) Pesan dengan angka

Isi pesan m = 110810

Nilai hash dari m adalah:

46421bca38842f7c1643565ea1a852d4

Kode ASCII dari nilai hash adalah:

525452504998999751565652501025

599495452515354531019749975653

5010052

m dipecah menjadi blok-blok

$m_1=525$	$m_8=652$	$m_{15}=354$	$m_{21}=501$
$m_2=452$	$m_9=501$	$m_{16}=531$	$m_{22}=005$
$m_3=504$	$m_{10}=025$	$m_{17}=019$	$m_{23}=002$
$m_4=998$	$m_{11}=599$	$m_{18}=749$	
$m_5=999$	$m_{12}=495$	$m_{19}=975$	

m_6=751 m_{13}=452 m_{20}=653

m_7=565 m_{14}=515

Kemudian setiap blok dienkripsi menggunakan kunci privat dengan menggunakan persamaan pada *RSA*

yakni: $c_i = m_i^e \bmod n$

$c_1 = 525^{79} \bmod 3337 = 2055$ $c_{13} = 452^{79} \bmod 3337 = 1809$

$c_2 = 452^{79} \bmod 3337 = 1809$ $c_{14} = 515^{79} \bmod 3337 = 574$

$c_3 = 504^{79} \bmod 3337 = 331$ $c_{15} = 354^{79} \bmod 3337 = 567$

$c_4 = 998^{79} \bmod 3337 = 2355$ $c_{16} = 531^{79} \bmod 3337 = 761$

$c_5 = 999^{79} \bmod 3337 = 3110$ $c_{17} = 019^{79} \bmod 3337 = 1265$

$c_6 = 751^{79} \bmod 3337 = 3289$ $c_{18} = 749^{79} \bmod 3337 = 1816$

$c_7 = 565^{79} \bmod 3337 = 2398$ $c_{19} = 975^{79} \bmod 3337 = 368$

$c_8 = 652^{79} \bmod 3337 = 3131$ $c_{20} = 653^{79} \bmod 3337 = 2409$

$c_9 = 501^{79} \bmod 3337 = 3207$ $c_{21} = 501^{79} \bmod 3337 = 3207$

$c_{10} = 025^{79} \bmod 3337 = 2823$ $c_{22} = 005^{79} \bmod 3337 = 270$

$c_{11} = 599^{79} \bmod 3337 = 603$ $c_{23} = 002^{79} \bmod 3337 = 3139$

$c_{12} = 495^{79} \bmod 3337 = 2541$

Jadi cipherteks yang dihasilkan adalah:

c= 2055.1809.331.23553.3110.3289.2398.3131.3207.2823.603.2541
1809.574.567.761.1265.1816.368.2409.3207.270.3139

Kemudian untuk mendekripsi pesan cipherteks dipecah menjadi blok seperti pada proses sebelumnya dan didekripsi dengan kunci public yang telah diketahui oleh pengirim dan penerima. $m_i = c_i^d \bmod n$.

$m_1 = 2055^{1019} \bmod 3337 = 525$ $m_{13} = 1809^{1019} \bmod 3337 = 452$

$m_2 = 1809^{1019} \bmod 3337 = 452$ $m_{14} = 574^{1019} \bmod 3337 = 515$

$m_3=331^{1019} \bmod 3337= 504$ $m_{15}=567^{1019} \bmod 3337= 354$

$m_4=2355^{1019} \bmod 3337= 998$ $m_{16}=761^{1019} \bmod 3337= 531$

$m_5=3110^{1019} \bmod 3337= 999$ $m_{17}=1265^{1019} \bmod 3337= 19$

$m_6=3289^{1019} \bmod 3337= 751$ $m_{18}=1816^{1019} \bmod 3337= 749$

$m_7=2398^{1019} \bmod 3337= 565$ $m_{19}=368^{1019} \bmod 3337=975$

$m_8=3131^{1019} \bmod 3337= 652$ $m_{20}=2409^{1019} \bmod 3337= 653$

$m_9=3207^{1019} \bmod 3337= 501$ $m_{21}=3207^{1019} \bmod 3337= 501$

$m_{10}=2823^{1019} \bmod 3337= 25$ $m_{22}=270^{1019} \bmod 3337= 5$

$m_{11}=603^{1019} \bmod 3337= 599$ $m_{23}=3139^{1019} \bmod 3337= 2$

$m_{12}=2541^{1019} \bmod 3337= 495$

maka diperoleh

m'= 525452504998999751565652501025

599495452515354531019749975653501005 2

dimana m mempunyai nilai

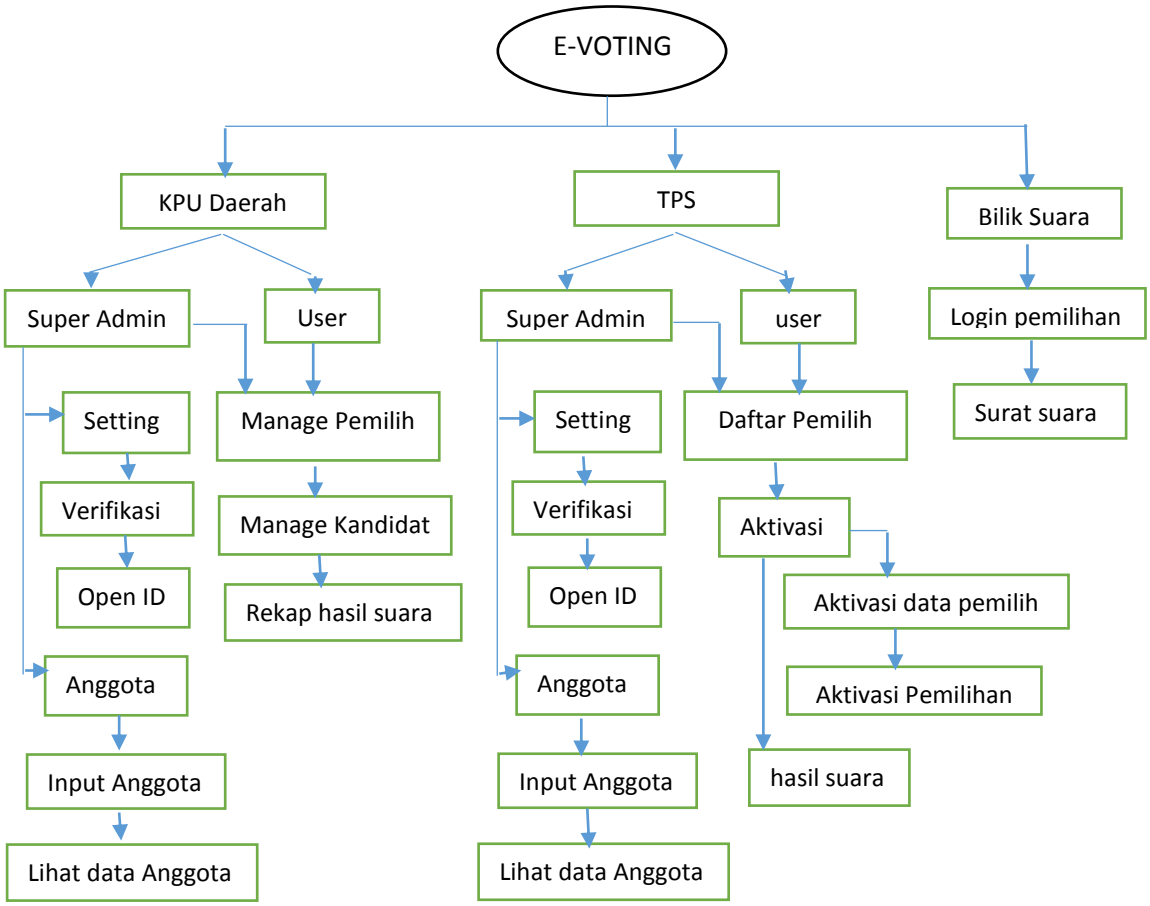
h'=46421bca38842f7c1643565ea1a852d4

tandatangan dianggap otentik karena h=h'

3.4 Perancangan Sistem

Dari sistem yang sedang berjalan, penulis mencoba menyajikan perancangan sistem e-voting pemilihan umum kepala daerah agar mempermudah dalam melakukan pemilihan umum dan perhitungan suara.

3.4.1 Bagan Kerja Sistem



Gambar 3.6 Bagan Kerja Sistem

Keterangan Bagan Sistem E-voting :

Terdiri dari 3 Halaman utama :

1. KPU Daerah
2. TPS
3. Bilik Suara

1. KPUD Daerah terdapat 2 user Yaitu :

A. Super admin

Halaman yang hanya bisa di akses oleh ketua kelompok KPU Daerah

Untuk mengoperasikan menu-menu sebagai berikut :

a. Setting signature : untuk mengetahui nilai pasangan kunci untuk kelompok yaitu, kunci public, kunci private dan modulo serta privat key untuk tiap anggota yang digunakan untuk pengiriman dan penerimaan data digital
b. Verifikasi : untuk memastikan pesan dikirim oleh pihak yang berwenang
c. Open ID : digunakan apabila suatu saat terdapat masalah yang di anggap perlu untuk mengetahui anggota kelompok yang melakukan tanda tangan pada pesan yang dikirim.
d. Anggota : Untuk mengisi dan melihat data anggota yang terlibat di sistem KPU Daerah

Super admin (ketua kelompok KPU Daerah) juga bisa mengakses menu manage pemilih, manage kandidat, Rekap hasil suara.

B. User KPU Daerah

Akses masuk menu untuk anggota KPU daerah, mengoperasikan menu-menu sebagai berikut :

a. Manage Pemilih : menu untuk mengisi data pemilih tetap yang terdaftar serta mengexport data pemilih ke tiap TPS
b. Manage Kandidat : menu untuk mengisi data pasangan calon kandidat serta mengexport data pasangan calon kandidat ke tiap TPS
c. Rekap Hasil Suara : untuk mengimport data hasil perolehan suara dari tps yang akan di dekripsikan.

2. TPS terdapat 2 user Yaitu :

A. Super admin

Halaman yang hanya bisa di akses oleh ketua kelompok TPS.

Untuk mengoperasikan menu-menu sebagai berikut :

a. Setting signature : untuk mengetahui nilai pasangan kunci untuk kelompok yaitu, kunci public, kunci private dan modulo serta privat key

untuk tiap anggota yang digunakan untuk pengiriman dan penerimaan data digital.

b. Verifikasi : untuk memastikan pesan dikirim oleh pihak yang berwenang.
c. Open ID : digunakan apabila suatu saat terdapat masalah yang di anggap perlu untuk mengetahui anggota kelompok yang melakukan tanda tangan pada pesan yang dikirim.
d. Anggota : Untuk mengisi dan melihat data anggota yang terlibat di sistem TPS.

Super admin (ketua kelompok TPS) juga bisa mengakses menu daftar pemilih, aktivasi, Rekap hasil suara.

B. User TPS

Akses masuk menu untuk anggota TPS, mengoperasikan menu-menu sebagai berikut :

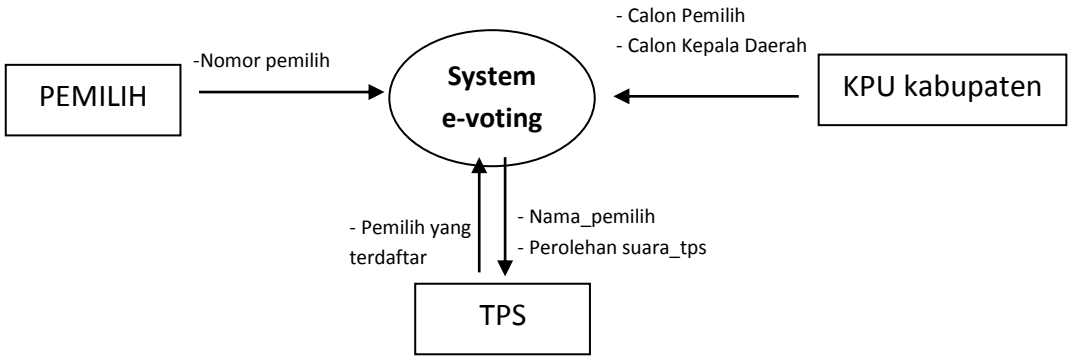
a. Daftar Pemilih : menu untuk meimport dan melihat data pemilih yang didapat dari KPU Daerah
b. Aktivasi : terdapat 2 sistem aktivasi
    1. Aktivasi pemilihan : untuk membuka sistem saat pemilihan dimulai serta menutup sistem saat pemilihan selesai.
    2. Aktivasi data pemilih : untuk pengaktifan data pemilih yang akan melaksanakan pemilihan, pemilih akan mendapat Pin setelah data pemilih sudah aktif.
c. Hasil Suara : hasil perolehan suara di TPS serta untuk mengexport data hasil perolehan suara dari tps ke Kpu daerah.

3. Bilik Suara

A. Login : Pemilih melakukan login dengan memasukkan nomer pemilih serta Pin yang telah di dapat dari petugas agar bisa melakukan pemilihan.

B. Surat Suara : halaman yang berisi tentang pilihan pasangan calon kandidat untuk dipilih.

3.4.2 Diagram Konteks

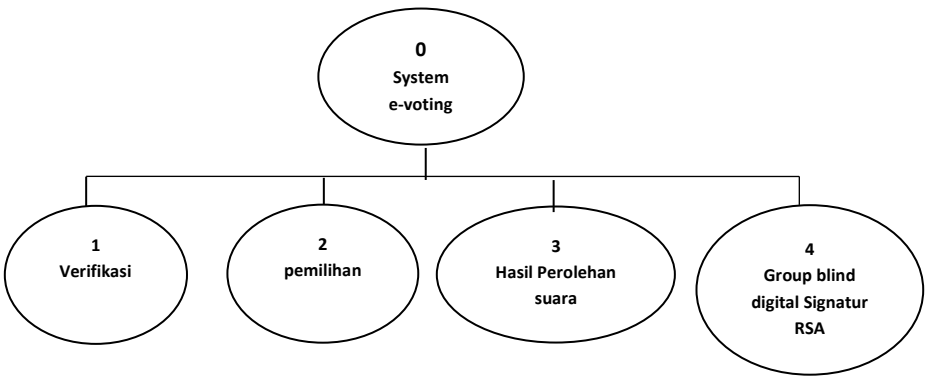


Gambar 3.7 Diagram Konteks

Adapun penjelasan dari Diagram Konteks pada gambar 3.6 diatas adalah sebagai berikut : Sistem berinteraksi dengan tiga entitas luar yaitu pemilih,Tps dan Kpu kabupaten.

1. Kpu kabupaten menginput data diri pemilih, data calon kepala daerah
2. Tps akan melakukan aktivasi data pemilih yang akan melakukan pemilihan serta menerima perolehan suara tps.
3. Pemilih melakukan pemungutan suara, pemilih memasukan nomor pendaftaran untuk login kedalam system.

3.4.3 Diagram Hirarki



Gambar 3.8 Diagram Hirarki

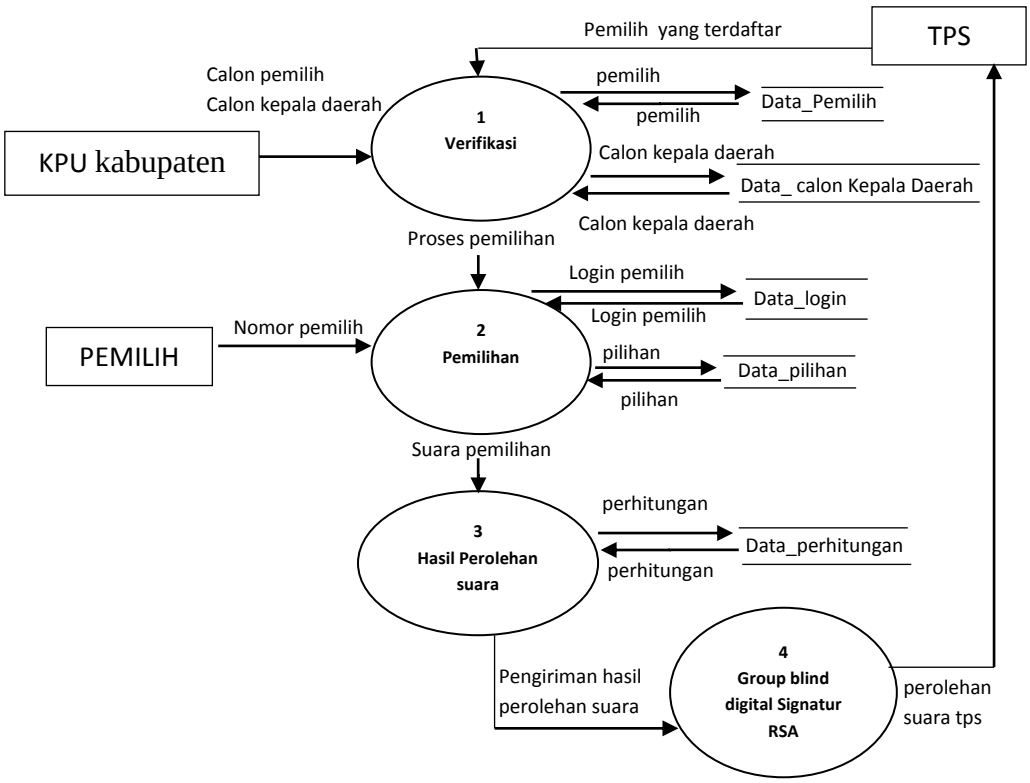
Pada gambar 3.8. dapat dijelaskan sebagai berikut:

1. Top Level : System e-voting
2. Level 1 Prose utama system E-voting :
    1. Verifikasi
    2. Pemilihan
    3. Hasil perolehan suara
    4. Group blind digital signatur RSA

3.4.4 Data Flow Diagram (DFD)

3.4.4.1 DFD Diagram Level 0

Data Flow Diagram adalah diagram yang menggambarkan proses dari diagram level 0. Data flow diagram memberikan pandangan mengenai sistem yang ditangani, menunjukkan fungsi-fungsi utama atau proses yang ada dan aliran data



Gambar 3.9 DFD Diagram Level 0

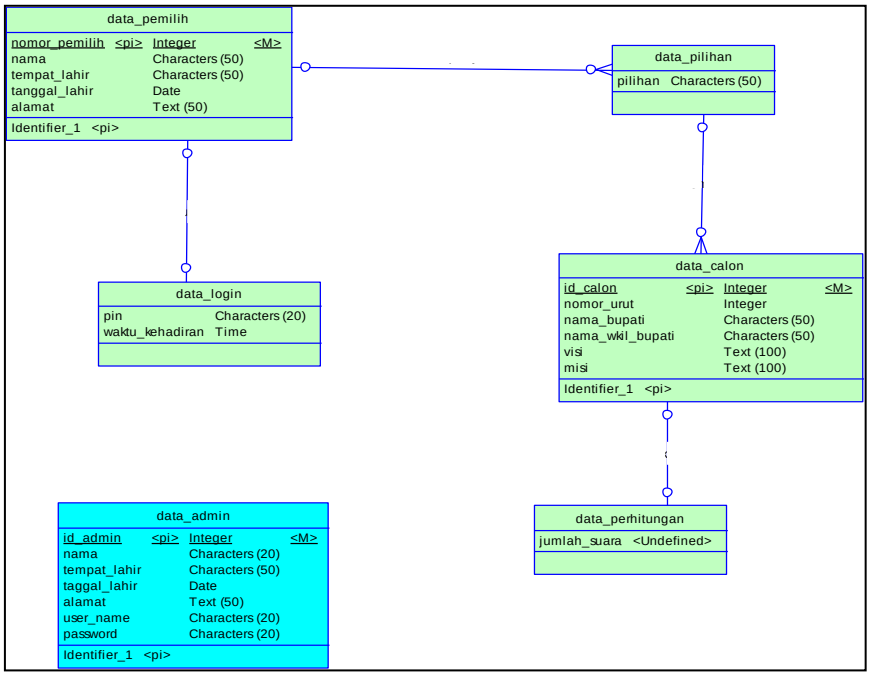
Adapun keterangan dari Gambar 3.9. adalah sebagai berikut :

Calon pemilih dan Calon Kepala daerah diinput ke dalam sistem E-voting dalam hal ini sangat berhubungan dengan terdaftarnya sebagai pemilih dan calon pasangan kepala daerah, TPS memasukkan pemilih dan calon kepala daerah yang diterima dari KPU kabupaten karena data kandidat yang ada dalam data base TPS masih kosong. data diverifikasi oleh petugas maka data akan didekripsi oleh sistem dan dimasukkan secara otomatis kedalam database TPS.Tps akan mengaktivasi data pemilih yang akan melakukan pemilihan. Pemilih dapat berinteraksi dengan sistem dalam hal pemilihan pasangan calon kepala daerah, Sistem secara otomatis menyimpan hasil perolehan suara di tingkat TPS. Tps akan melakukan penandatanganan dokumen Hasil perolehan suara dengan menggunakan group blind digital signature RSA untuk pengiriman dokumen Hasil perolehan suara.

3.4.5 Conceptual Data Model

Pada *conceptual data model* digambarkan konsep rancangan basis data yang akan digunakan oleh sistem di tingakat TPS. dalam *conceptual data model* terdapat beberapa entitas yang mempunyai keterkaitan dan saling membutuhkan untuk melengkapi data yang ada.

Pada *conceptual data model* yang ada pada gambar 3.10 entitas data pemilih memiliki hubungan *one to one* terhadap entitas data login dan data pilihan karena satu pemilih mempunyai satu data login dan satu kali pemilihan. Sedangkan entitas data calon memiliki hubungan *many to one* terhadap entitas data pemilih karena setiap calon akan memiliki banyak pemilih, sedangakan entitas data perhitungan mempunyai hubungan *one to one* dengan entitas data calon karena setiap calon mempunyai satu data perhitungan. Dalam pengiriman dokumen hasil perolehan suara menggunakan group blind digital signatur RSA dokumen di ambil dari database data_perhitungan.



Gambar 3.10 conceptual data model untuk tingkat TPS

3.5 Perancangan Basis Data

Perancangan Basis data disini dimaksudkan agar perhitungan dari hasil pemilihan umum dengan elektronik voting ini dapat di simpan dan diakumulasikan ke dalam bentuk yg lebih baik, kemudian dikonvesikan menjadi tabel dalam database Mysql, tabel yang digunakan dalam penelitian ini yaitu :

3.5.1 Struktur Tabel

Tabel master kriteria berisi data masukan beberapa kriteria yang akan menjadi patokan dalam pemilihan umum dengan elektronik voting. Struktur dari tabel master kriteria dapat dilihat dari **Tabel 3.1**

Tabel 3.1, basis data di TPS

Nama tabel	Jumlah kolom	Deskripsi
data_pemilih	8	tabel berisi daftar pemilih yang diterima dari KPU
data_calon	8	tabel berisi data pasangan calon peserta Pemilu
data_login	3	tabel yang berisi data login pemilih.

data_pilihan	5	tabel yang berisi pilihan pemilih yang di enkripsi dan terdapat pasangan kunci untuk pemilih.
tb_perhitungan	4	tabel yang berisi perolehan suara tiap pasangan calon.

Tabel 3.2, basis data di KPU Kabupaten

Nama tabel	Jumlah kolom	Deskripsi
data_pemilih	8	tabel berisi daftar pemilih yang diterima dari KPU
data_calon	8	tabel berisi data pasngan calon peserta Pemilu
data_ perhitungan	4	tabel yang berisi data perolehan suara dari tiap TPS
data_rekap	3	tabel yang berisi data file dari TPS yang telah direkap.

Rincian setiap tabel dari databse diatas dapat dilihat pada tabel berikut;

Tabel 3.3, kolom data pemilih

Nama Kolom	**Tipe Data**	**Keterangan**
nomor_pemilih	Varchar(20)	*Primary key*
Nama	Varchar(100)	
tempat_lahir	Varchar(50)	
tanggal_lahir	Date	
jenis_kelamin	Varchar(255)	
Alamat	Text	
Kecamatan	Varchar(100)	
Kelurahan	Varchar(100)	

tabel data pemilih, digunakan untuk menyimpan informasi tentang pemilih.

tabel tersebut mempunyai atribut sebagi berikut:

a. nomor pemilih, berisi nomor urut pemilih menjadi primary key yang diberikan oleh panitia penyelenggara.
b. nama, berisi nama peilih yang sesuai dengan kartu tanda penduduk.
c. tempat lahir, berisi informasi tempat pemilih tersebut dilahirkan
d. tanggal lahir, berisi informasi tanggl pemilih dilahirkan.

e. Jenis kelamin, berisi informasi jenis kelamin pemilih
f. alamat,kecamatan dan kelurahan berisi informasi pemilih tinggal dan menetap.

Tabel 3.4, kolom data calon

Nama Kolom	Tipe Data	Keterangan
id_calon	Integer	*Primary key*
nama_bupati	Varchar(20)	
nama_wakil_bupati	Varchar(20)	
partai_pendukung	Varchar(225)	
Visi	Varchar(150)	
Misi	Varchar(150)	
nomor_urut	Int(2)	
Foto	Varchar(25)	

tabel data calon, digunakan untuk menyimpan informasi tentang pasangan calon. tabel tersebut mempunyai atribut sebagai berikut:

a. id calon, berisi id pasangan calon yang kemudian menjadi primary key untuk tabel data calon.
b. nama bupati, berisi nama dari calon kepala daerah.
c. nama wakil, berisi nama calon wakil kepala daerah.
d. Partai pendukung, berisi tentang informasi partai pendukung dari calon kepala daerah dan calon wakil kepala daerah
e. visi, berisi tentang visi yang diusung oleh pasangan calon.
f. misi, berisi tentang misi yang diusung oleh pasangan calon.
g. nomor urut, berisi nomor urut pasangan yang telah ditentukan oleh panitia penyelenggara.
h. Foto, berisi tentang foto calon kepala daerah dan calon wakil kepala daerah

Tabel 3.5, kolom data login

Nama Kolom	Tipe Data	Keterangan
nomor_pemilih	Varchar(20)	*Primary key*
Pin	Varchar(20)	
waktu_hadir	Time	

tabel data login, digunakan untuk menyimpan informasi login pemilih.

tabel data login mempunyai atribut sebagai berikut:

a. nomor pemilih, berisi id pemilih yang didapat dari tabel data pemilih dan kemudian dijadikan Primary key dalam tabel ini.
b. pin, berisi kode yang digunakan pemilih untuk login
c. waktu kehadiran, berisi informasi waktu pemilih melakukan validasi kehadiran di tempat pemungutan suara.

Tabel 3.6, kolom data pilihan

Nama Kolom	Tipe Data	Keterangan
nomor_pemilih	Integer	*Primary key*
Pilihan	Text	
Privat	Text	
Public	Text	
Modulo	Text	

tabel data pilihan, berfungsi untuk menyimpan informasi kandidat yang dipilih oleh pemilih.

tabel ini memiliki atribut sebagai berikut:

a. nomor pemilih, berisi id pemilih yang didapat dari tabel data pemilih dan kemudian dijadikan prmary key dalam tabel ini.
b. pilihan, berisi tentang informasi kandidat yang dipilih oleh pemilih.

Tabel 3.7, kolom tb perhitungan di TPS

Nama Kolom	Tipe Data	Keterangan
id_perhitungan	Integer	*Primary key*
Waktu	Time	
nomor_urut	Text	
jumlah_suara	Text	

tabel data perhitungan, untuk menyimpan data perolehan suara pasangan calon di TPS.

tabel perhitungan mempunyai atribut sebagai berikut:

a. id perhitungan, berisi nomor perhitungan yang dijadikan primary key dalam tabel ini

b. Waktu, berisi tentang waktu saat pelaksanaan.
c. Nomor urut, berisi tentang no urut pasangan kandidat
d. jumlah suara, digunakan untuk menyimpan data perolehan suara yang diperoleh masing-masing pasangan kandidat.

Tabel 3.8, kolom data perhitungan di Kabupaten

Nama Kolom	Tipe Data	Keterangan
id_hitung	Integer	*Primary key*
Pasangan	Varchar(30)	
nomor_urut	Varchar(30)	
Suara	Smallint(10)	

tabel data perhitungan kabupaten, untuk menyimpan data perolehan suara pasangan calon di kabupaten.

tabel perhitungan mempunyai atribut sebagai berikut:

a. id hitung, berisi nomor perhitungan yang dijadikan primary key dalam tabel ini
b. pasangan, berisi tentang nama pasangan kandidat
c. Nomor urut, berisi tentang no urut pasangan kandidat
d. suara, digunakan untuk menyimpan data perolehan suara yang diperoleh masing-masing pasangan kandidat.

Tabel 3.9, kolom data rekap

Nama Kolom	Tipe Data	Keterangan
id_data	Integer(9)	*Primary key*
nama_file	Varchar(50)	
Ferivikasi	Varchar(3)	

Kolom data rekap, untuk rekapan hasil perolehan suara pasangan kandidat tiap keluarahan.

Kolom data rekap mempunyai atribut sebagai berikut:

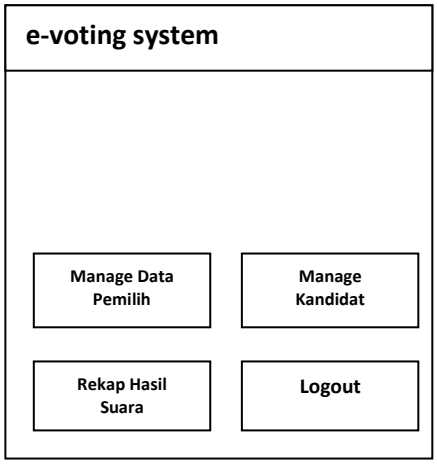
a. id data, berisi nomor data yang dijadikan primary key dalam tabel ini
b. nama file, berisi nama file perolehan suara tiap kelurahan
c. ferivikas, berisi tentang rekapan perolehan suara.

3.6 Perancangan Antarmuka

Antarmuka adalah bagian penting yang berfungsi sebagai penghubung antara sistem dan user.Antarmuka dirancang dengan seefisien mungkin untuk mempermudah user dalam memakai dan menggunakan sistem dengan baik. Dalam penelitian ini akan menggunakan layout desain seperti berikut ini:

3.6.1 Rancangan Antarmuka Form Menu Utama Admin KPU Kabupaten

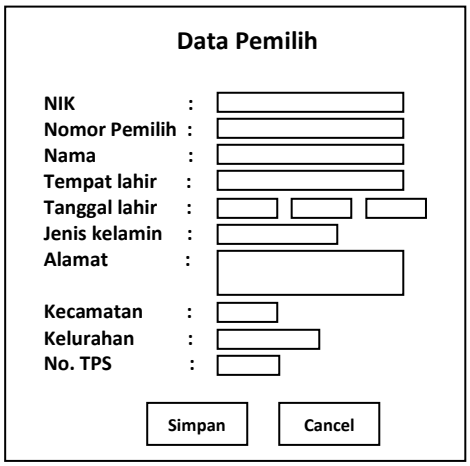
Form Menu utama untuk admin kpu kabupaten menu yang terdiri dari menu manage daftar pemilih untuk mengatur dan melihat daftar pemilih tetap, menu manage kandidat memiliki fungsi mengatur dan melihat daftar kandidat peserta pilkada, menu rekap hasil suara untuk proses rekapitulasi perolehan suara. seperti terlihat pada **gambar 3.11** berikut ini.



Gambar 3.11 Antarmuka Form Menu Utama untuk Admin KPU Kabupaten

3.6.2 Rancangan Antarmuka Form Input Data Pemilih

Form input pemilih adalah menu untuk mengisi data pemilih tetap yang terdaftar. seperti terlihat pada **gambar 3.12** berikut ini.



Gambar 3.12 Antarmuka Form Input Data Pemilih

3.6.3 Rancangan Antarmuka Form Daftar Pemilih

Form daftar pemilih adalah menu tampilan data pemilih yang terdaftar. seperti terlihat pada **gambar 3.13** berikut ini.

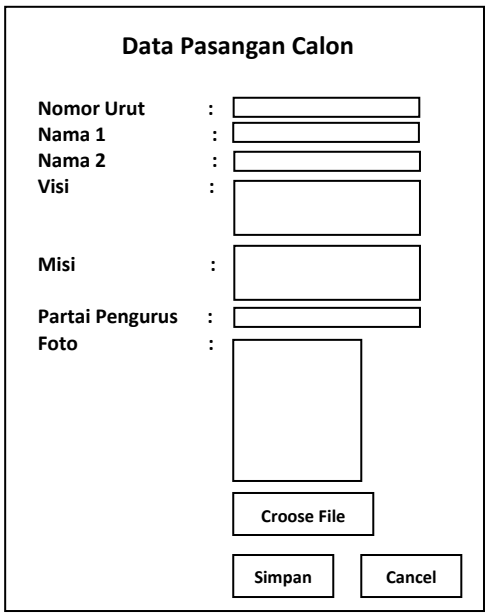
DAFTAR PEMILIH TETAP

NIK	Nomor pemilih	Nama	Tempat Lahir	Tanggal lahir	Jenis Kelamin	Alamat	Kecamatan	Kelurahan	No TPS

Gambar 3.13 Antarmuka Form Daftar Pemilih

3.6.4 Rancangan Antarmuka Form Input Data Kandidat

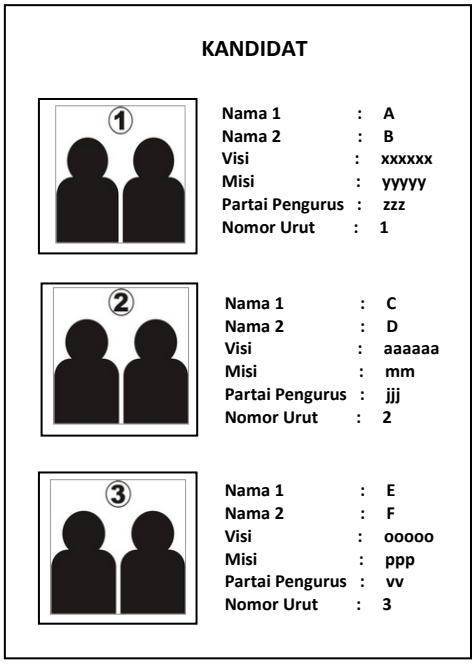
Form input data kandidat adalah menu untuk mengisi data pasangan calon kepala daerah dan calon wakil kepala daerah yang terdaftar. seperti terlihat pada **gambar 3.14** berikut ini.



Gambar 3.14 Antarmuka Form Input Data Kandidat

3.6.5 Rancangan Antarmuka Form Daftar Kandidat

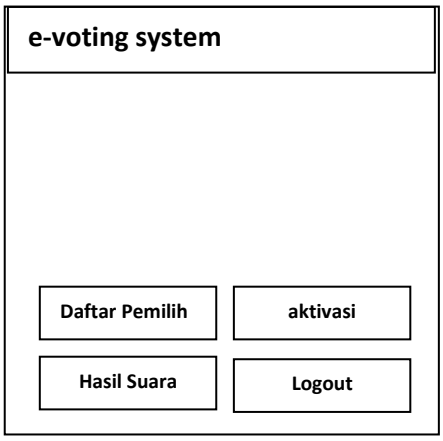
Form daftar kandidat adalah menu tampilan data pasangan calon kandidat. seperti terlihat pada **gambar 3.15** berikut ini.



Gambar 3.15 Antarmuka Form Daftar Kandidat

3.6.6 Rancangan Antarmuka Form Menu Utama Admin TPS

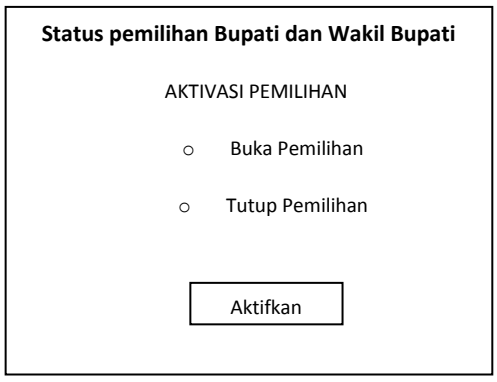
Form Menu utama untuk admin tps menu yang terdiri dari menu daftar pemilih untuk melihat daftar pemilih tetap yang berada di TPS tersebut, menu aktifasi memiliki dua fungsi yakni untuk membuka atau menutup pemilihan serta menu hasil suara tingkat tps seperti terlihat pada **gambar 3.16** berikut ini.



Gambar 3.16 Antarmuka Form Menu Utama untuk Admin TPS

3.6.7 Rancangan Antarmuka Form Aktifasi Pemilihan

Form aktifasi pemilihan ini petugas melakukan pembukaan dan penutupan terhadap pemilihan yang ada dalam tempat pemungutan suara. seperti terlihat pada **gambar 3.17** berikut ini.

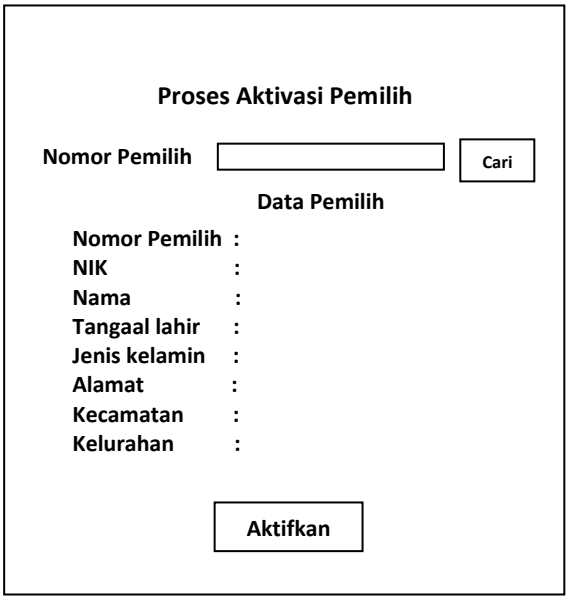


Gambar 3.17 Antarmuka Form Aktifasi Pemilihan

a. Buka pemilihan : apabila pemilihan sudah waktunya dibuka maka petugas akan melakukan buka pemilihan dan bisa melakukan pemilihan tetapi tidak bisa melihat perolehan suara
b. Tutup pemilihan : apabila pemilihan telah selesai maka petugas melakukan tutup pemilihan dan bisa melakukan perhitungan suara di Tps tersebut

3.6.8 Rancangan Antarmuka Form Aktifasi Pemilih

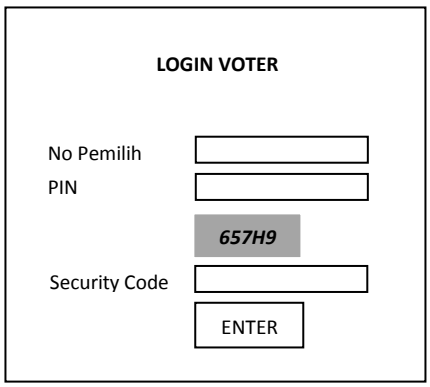
Form aktifasi pemilih digunakan untuk mengkatifkan status pemilih agar dapat melakukan pemilihan seperti terlihat pada **gambar 3.18** berikut ini.



Gambar 3.18 Antarmuka Form Aktifasi Pemilih

3.6.9 Rancangan Antarmuka Form Login Pemilih

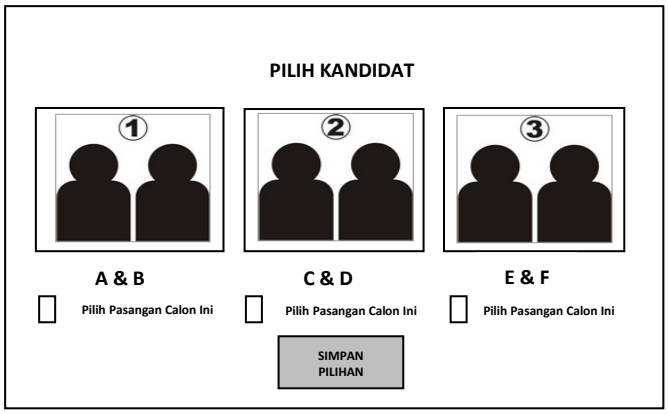
Form login untuk pemilih yang digunakan untuk melakukan pemilihan suara. seperti terlihat pada **gambar 3.19** berikut ini



Gambar 3.19 Antarmuka Form Login Pemilih

3.6.10 Rancangan Antarmuka Form Pemilihan Suara

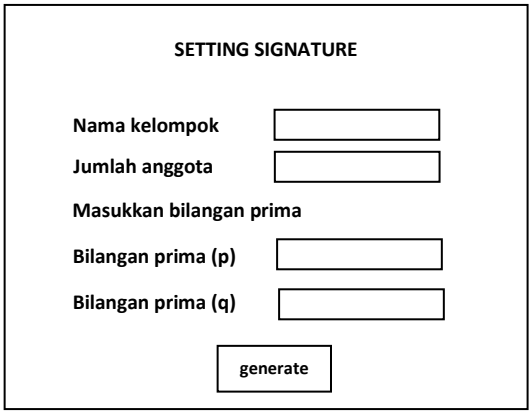
Form Pemilihan suara digunakan pemilih untuk pemilihan suara pasangan calon yang akan dipilih maka hasil pemilihan otamatis tersimpan dan terenkripsi. seperti terlihat pada **gambar 3.20** berikut ini.



Gambar 3.20 Antarmuka Form Pemilihan Suara

3.6.11 Rancangan Antarmuka Form Setting Signature

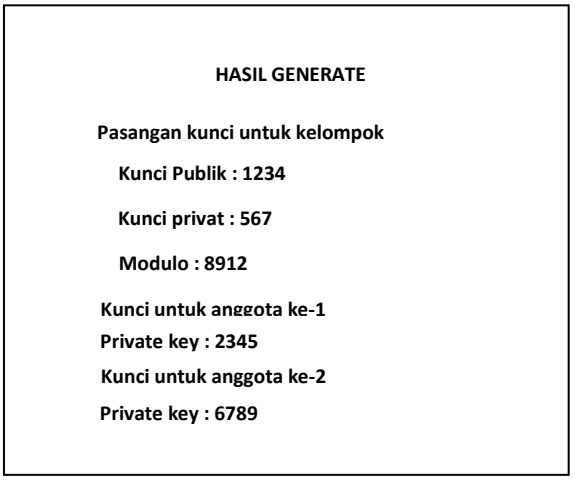
Form Setting Signature untuk mengetahui nilai pasangan kunci untuk kelompok yaitu, kunci public, kunci private dan modulo serta privat key untuk tiap anggota. seperti terlihat pada **gambar 3.21** berikut ini.



Gambar 3.21 Antarmuka Form Setting Signature

3.6.12 Rancangan Antarmuka Form Hasil Setting Signature

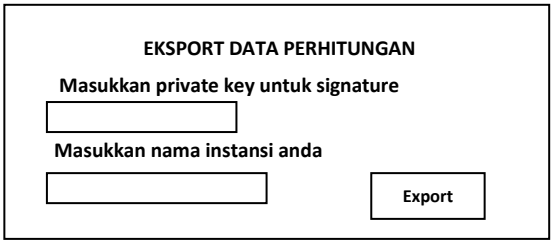
Form Hasil Setting Signature. seperti terlihat pada **gambar 3.22** berikut ini.



Gambar 3.22Antarmuka Form Hasil Setting Signature

3.6.13 Rancangan Antarmuka Form Enkripsi Data Perhitungan di TPS

Form enkripsi data perhitungan di tps untuk mengirim data perolehan suara tps. seperti terlihat pada **gambar 3.23** berikut ini.

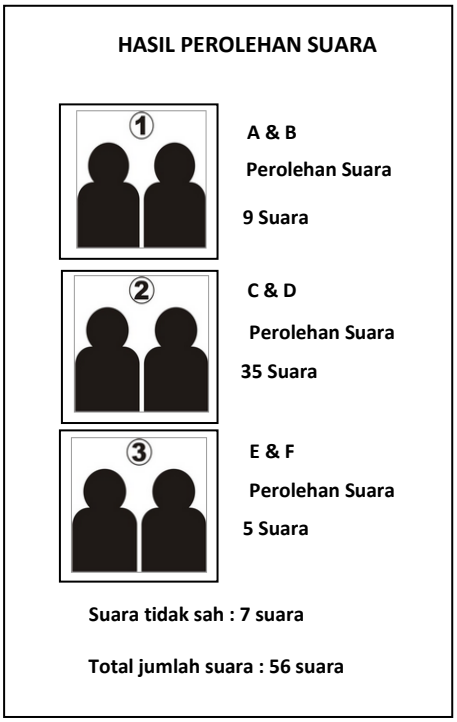


Gambar 3.23 Antarmuka Form Enkripsi Data Perhitungan di TPS

Export : yang melakukan export untuk pengiriman hasil perhitungan suara tiap tps yaitu ketua tps.

3.6.14 Rancangan Antarmuka Form Hasil Perolehan Suara di TPS

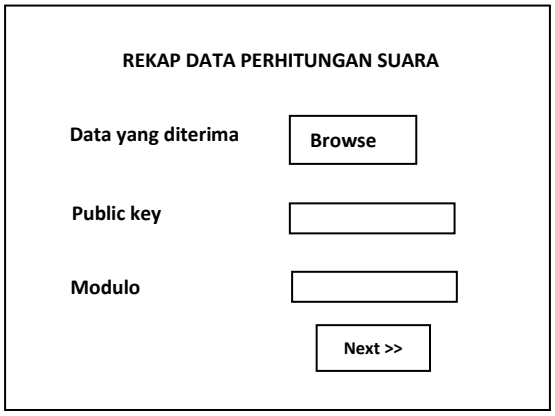
Form hasil Perolehan Suara di TPS disini akan muncul hasil dari perhitungan suara dari pemilihan yang sudah dilakukan. seperti terlihat pada **gambar 3.24** berikut ini.



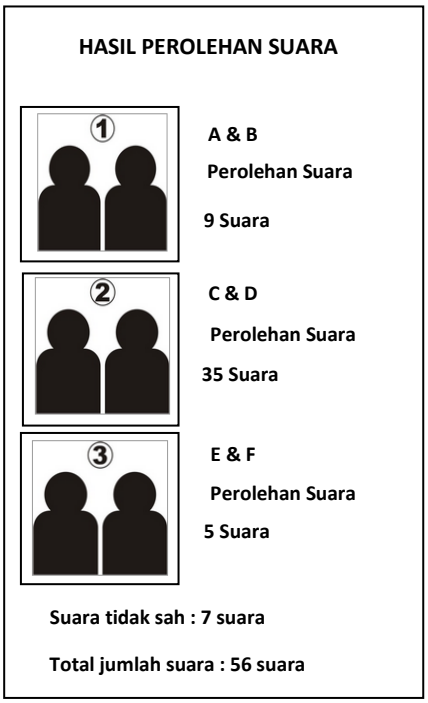
Gambar 3.24 Antarmuka Form Hasil Perolehan Suara di TPS

3.6.15 Rancangan Antarmuka Form Rekap Data Perhitungan Suara Kabupaten

Form Rekap data perhitungan suara Kabupaten akan muncul hasil pengiriman data perolehan suara dari tps yang akan di dekripsikan. seperti terlihat pada **gambar 3.25** berikut ini.



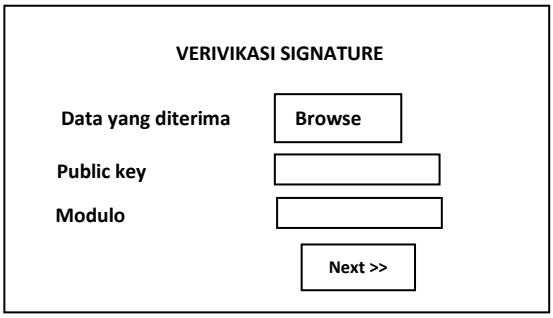
Gambar 3.25 Antarmuka Form Form Rekap Data Perhitungan Suara Kabupaten



Gambar 3.26 hasil perolehan suara setelah data dijumlahkan

3.6.16 Rancangan Antarmuka Form Verifikasi Signature

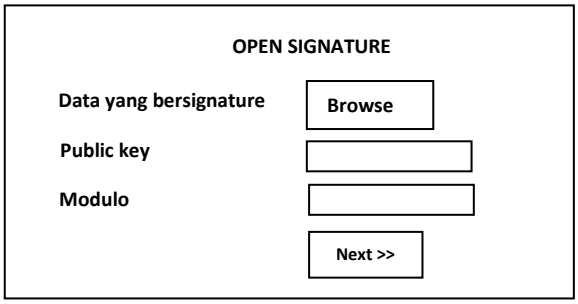
Form Verifikasi Sinature disini untuk memastikan pesan dikirim oleh pihak yang berwenang. seperti terlihat pada **gambar 3.27** berikut ini.



Gambar 3.27 Rancangan Antarmuka Form Verifikasi Signature

3.6.17 Rancangan Antarmuka Form Open Signature

Form Open Signature digunakan apabila suatu saat terdapat masalah yang di anggap perlu untuk mengetahui anggota kelompok yang melakukan tanda tangan pada pesan yang dikirim. seperti terlihat pada **gambar 3.28** berikut ini.



Gambar 3.28 Antarmuka Form Open Signature

3.7 Alur Peggunaan Sistem

Dalam penggunaan sistem dilapangan, ada beberapa alur yang harus ditempuh, alur tersebut ditempuh pada saat sebelum, sesudah dan saat pelaksanaan pemungutan suara dibuka.

1. Petugas TPS memasukkan data dari KPU yang telah diterima sebelumnya kedalam database sistem yang ada di tempat pemungutan suara dengan

mendekripsinya terlebih dahulu dan melakuakn verifikasi terhadap *signature* yang ada.

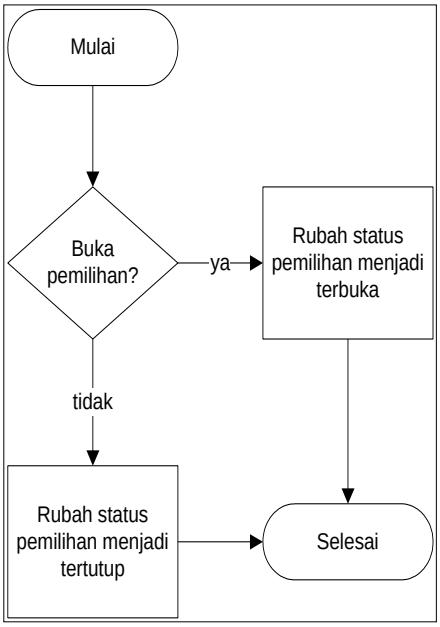
2. Setelah data sudah dimasukkan maka petugas TPS membuka pemilihan dan pemilihan sudah bisa dilaksanakan.
3. Selanjutnya Pemilih datang ke tempat pemungutan suara dan melakukan verifikasi kehadiran kepada petugas yang telah ditentukan.
4. Petugas melakukan aktifasi data pemilih dengan memeriksa nomor pemilih yang dimiliki oleh pemilih yang bersangkutan. setelah pemilih diaktifasi oleh petugas selanjutnya pemilih menerima PIN dari petugas.
5. Pemilih menuju bilik suara dan login kedalam sistem dengan memasukkan nomor pemilih dan PIN yang telah diterima sebelumnya.
6. Setelah pemilih berhasil login kedalam sistem,pemilih dipersilakn memilih kandidat yang telah ada.
7. Data kandidat yang telah dipilih oleh pemilih dienkripsi dan disimpan dalam database.
8. Setelah pemilihan selesai dengan batas waktu yang telah ditentukan maka petugas TPS menutup pemilihan di tempat pemungutan suara.
9. Setelah pemungutan suara ditutup oleh petugas maka hasil perolehan suara baru dapat ditampilkan oleh sistem, dan ditampilkan didepan umum.
10. Setelah perhitungan suara selesai, petugas TPS mengirimkan hasil perolehan suara kepada KPU untuk proses rekapitulasi. Data perolehan suara dienkripsi sebelum dikirimkan.
11. KPU menerima data perolehan suara dari setiap TPS.
12. Petugas yang berada di KPU mendekripsi data yang dari TPS kemudian dimasukkan database jika signature telah valid.
13. Hasil rekapitulasi suara dapat ditampilkan oleh sistem.

3.8 Fungsi Sistem

Dalam *Fungsi sistem* digambarkan proses penggunaan sistem secara mengalir dan berurutan.

Berikut beberapa *flow chart* yang dapat menggambarkan sistem.

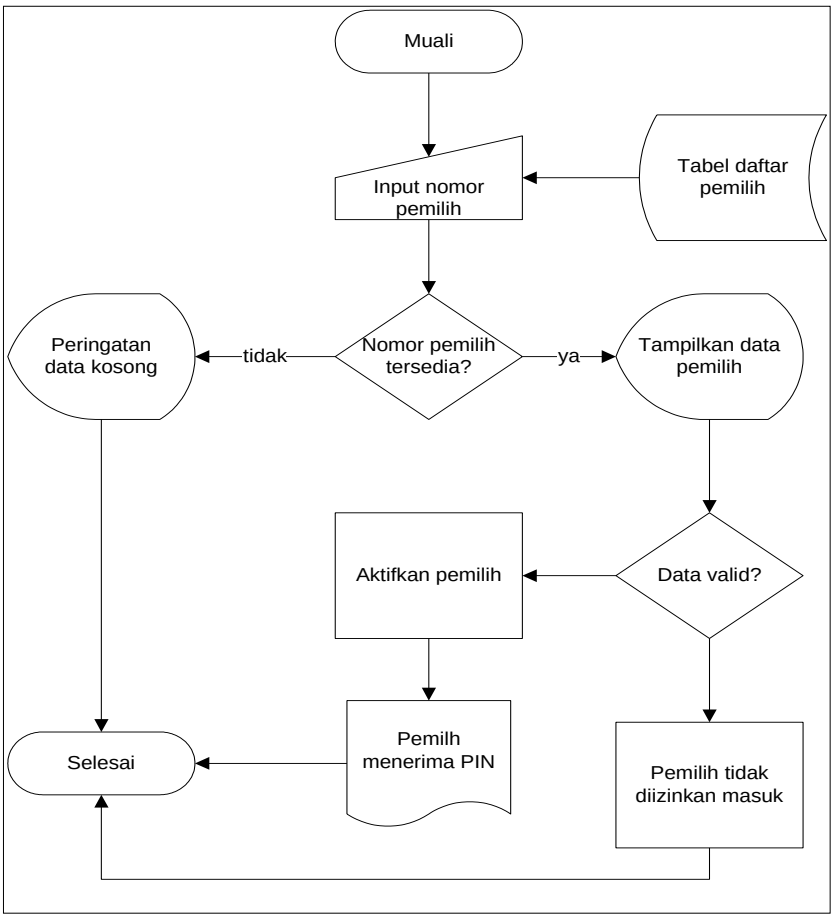
3.81 Flow chart proses aktifasi pemilihan:



Gambar 3.29 *Flow Chart* Proses aktifasi pemilihan

Proses aktifasi pemilihan digunakan petugas TPS untuk melakukan aktifasi pemilihan. apabila pemilihan sudah dibuka maka petugas akan melakukan buka pemilihan dan apabila pemilihan telah selesai maka petugas melakukan tutup pemilihan.

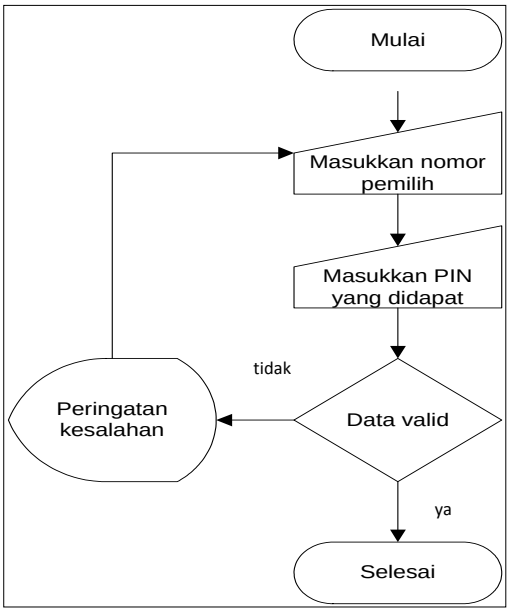
3.8.2 Flow chart proses aktifasi pemilih:



Gambar 3.30 *Flow Chart* Proses aktifasi pemilih

Proses aktifasi pemilih untuk melakukan verifikasi kehadiran para pemilih yang telah berada di TPS. Pemilih menyerahkan kartu pemilih kemudian petugas melakukan pengecekan data pemilih jika data pemilih valid maka pemilih akan mendapatkan PIN dari petugas dan pemilih telah aktif dan dapat melakukan pemilihan di bilik suara.

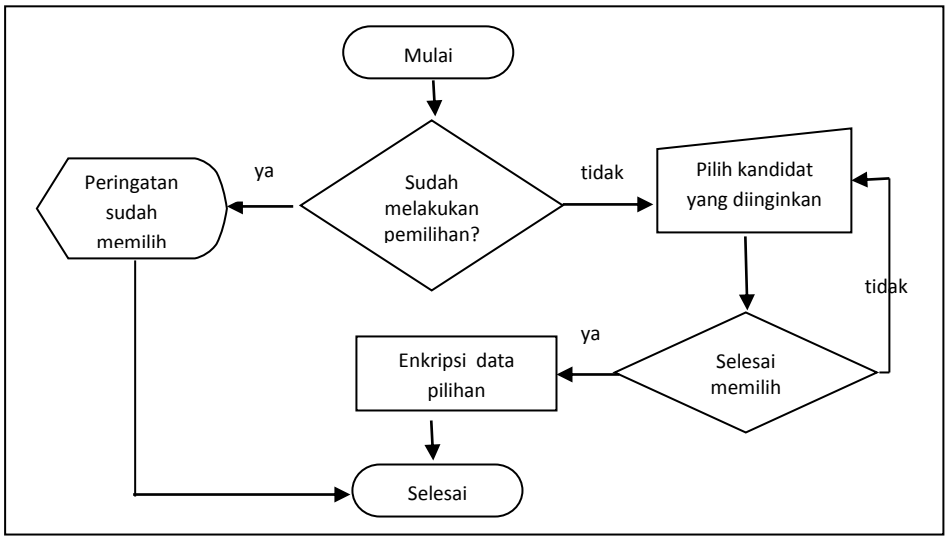
3.8.3 Flow chart proses login pemilih



Gambar 3.31 *Flow Chart* Proses Login

Proses Login digunakan pemilih untuk masuk ke dalam sistem dengan mengisikan nomor pemilih, dan PIN yang telah diberikan petugas. Setelah login, maka pemilih dapat melakukan pemilihan di system bilik suara.

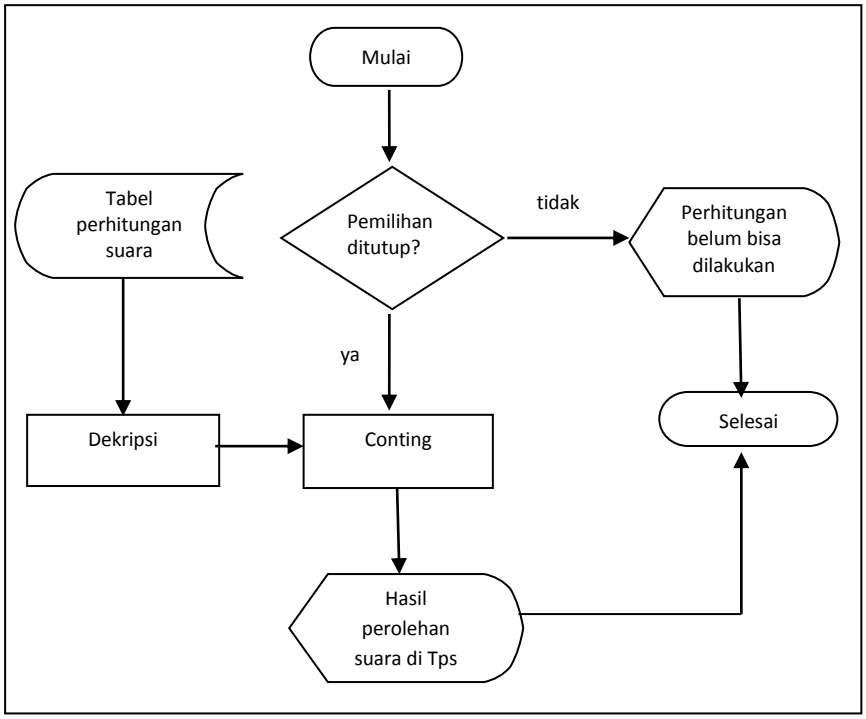
3.8.4 Flow chart proses pemilihan:



Gambar 3.32 *Flow Chart* Proses Pemilihan

Proses Pemilihan hanya bisa memberikan satu kali pilihannya dan tidak bisa mengubah pilihannya setelah melakukan pemilihan. Pemilihan hanya bisa dilakukan pada waktu yang sudah ditentukan panitia.

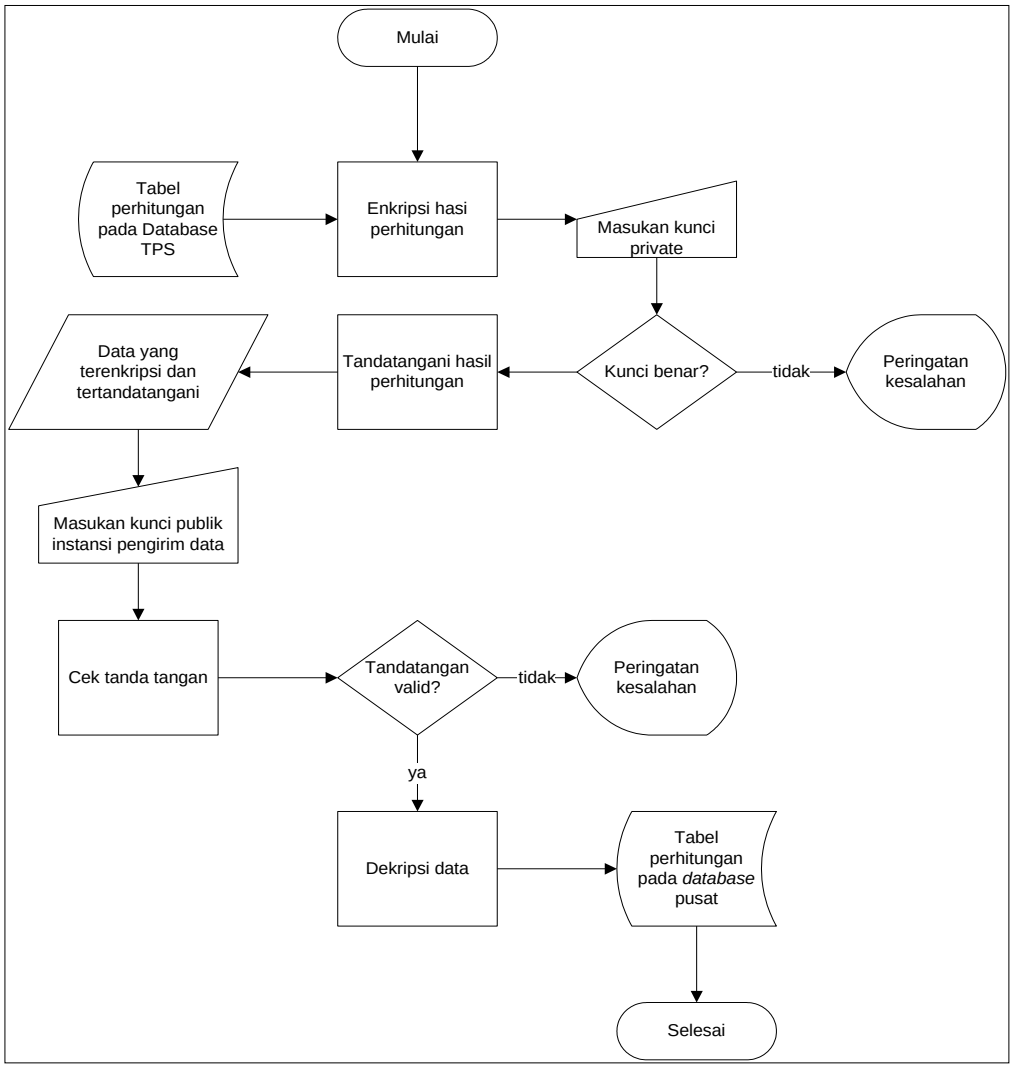
3.8.5 Flow chart penghitungan suara di TPS:



Gambar 3.33 *Flow Chart* Perhitungan Suara di TPS

3.8.6 Flowchart pengiriman hasil suara sampai di kabupaten

Perhitungan suara di TPS dapat dilaksanakan setelah pemilihan selesai dengan mengambil data perolehan suara yang ada pada *database* TPS. Kemudian data hasil perolehan suara di enkripsi dan ditandatangani secara digital kemudian dikirim ke KPU daerah



Gambar 3.34 *flow chart* pengiriman hasil suara sampai di Kabupaten

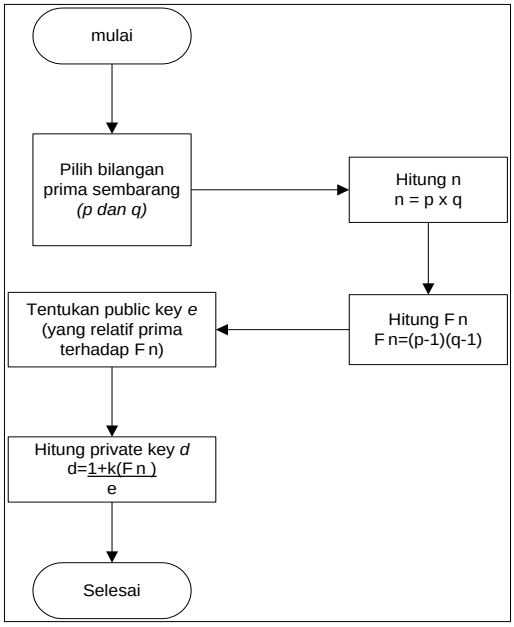
Perhitungan suara atau total merupakan hasil penjumlahan dari perhitungan suara di masing-masing TPS. Setelah perhitungan suara di TPS selesai, panitia di TPS mengirimkan hasil perhitungan suara yang sudah di enkripsi dan ditandatangani secara digital ke perhitungan pusat. Di sistem *e-voting* pusat data yang dikirimkan oleh TPS akan diverifikasi tandatangan yang ada didalamnya kemudian didekripsi lalu dijumlahkan dan diperoleh jumlah keseluruhan.

3.8.7 Flow chart algoritma pembangkit kunci RSA

Algoritma pembangkit kunci pada algoritma RSA mengggambarkan cara pembuatan kunci publik serta pembangkitan pasangan kunci yakni kunci privat.

Adapun rumus utama pembangikt pasangan kunci adalah:

$$d = \frac{1 + k\Phi(n)}{e}$$



Gambar 3.35 *Flow Chart* pembangkit kunci RSA

3.8.8 Flow chart enkripsi data

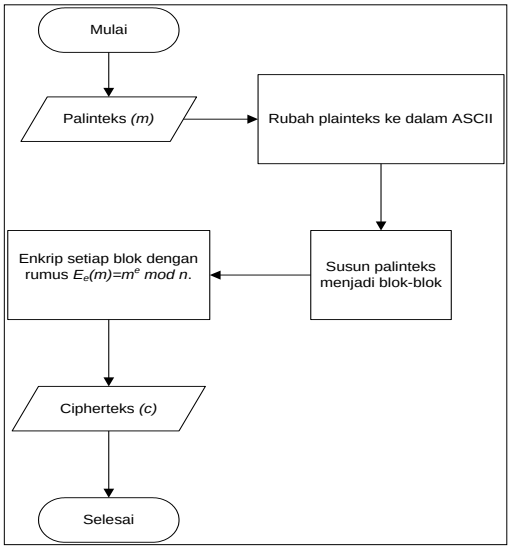
enkripsi data pada RSA menggunakan kunci public yang ditentukan oleh pengirim pesan dan tidak dirahasiakan, berikut rumus utama untuk enkripsi data menggunakan RSA.

$E_e(m)=m^e \bmod n$.

$E_e(m)$ = plainteks

e =kunci publik

n =modulo



Gambar 3.36 *Flow Chart* enkripsi pesan dengan RSA

3.8.9 Flow chart dekripsi data

dekripsi data pada RSA menggunakan kunci privat yang hanya dimiliki oleh penerima pesan dan dirahasiakan. Berikut rumus utama untuk dekripsi data menggunakan RSA.

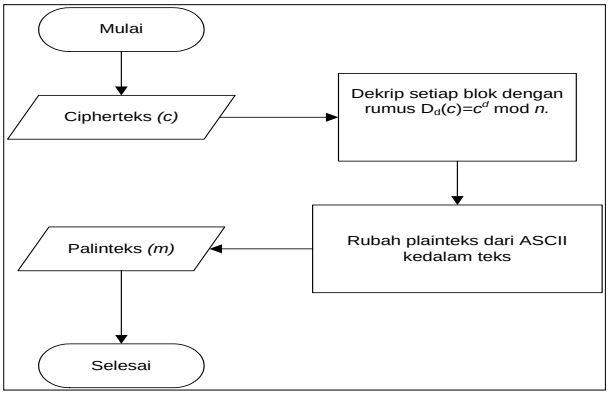
$D_d(c) = c^d \bmod n$.

dimana:

$D_d(c)$ = chiperteks

d = kunci privat

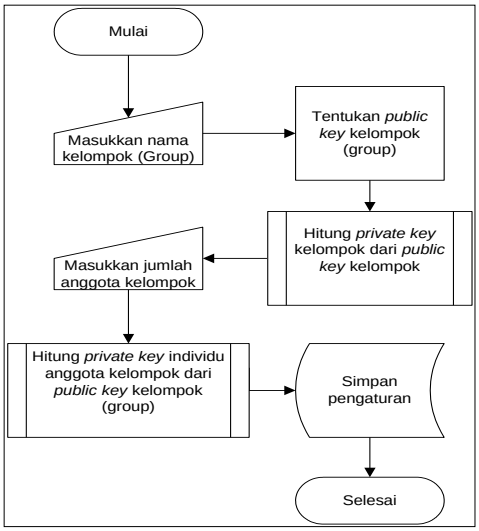
n = modulo



Gambar 3.37 *Flow Chart* dekripsi pesan dengan RSA

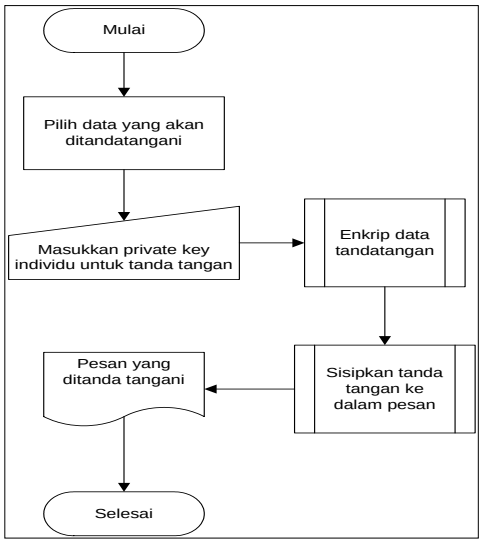
3.8.10 Flow chart skema group digital signature

Proses pengaturan tanda tangan dan penyamaran pesan yang dilakukan oleh ketua kelompok yang akan mengirimkan pesan. dalam flow chart dibawah juga terdapat pembangkitan kunci private individu.



Gambar 3.38 setup pada group blind digital signature

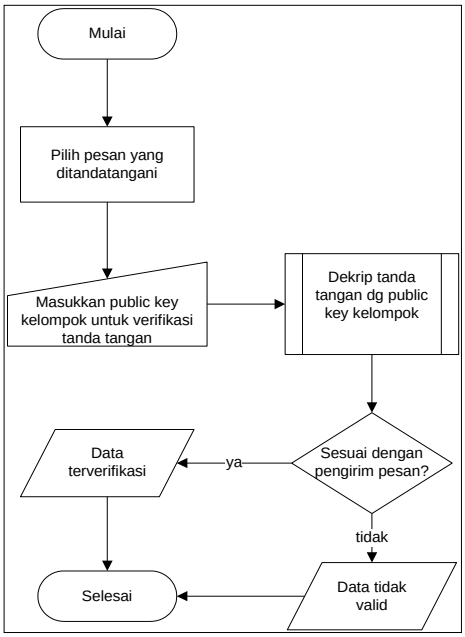
3.8.11 Flowchart sign pada pesan



Gambar 3.39 *sign* pada pesan

3.9.12 Flowchart Verifikasi pada tanda tangan pada pesan

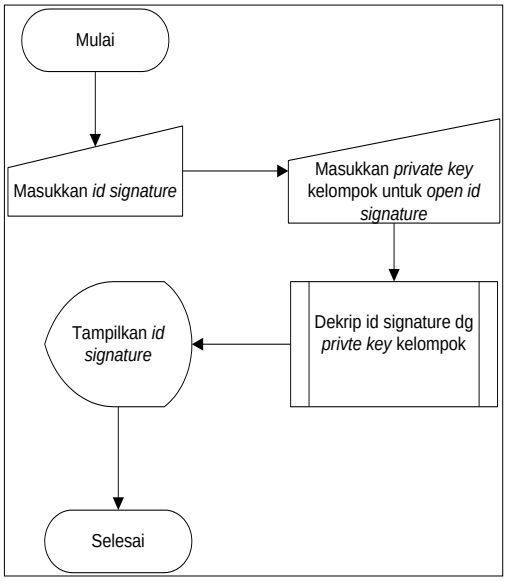
Setelah ditanda tangani pesan dikirim kepada tujuan penerima pesan, penerima pesan melakukan verifikasi terhadap tanda tangan yang ada pada pesan untuk memastikan pesan dikirim oleh pihak yang berwenang



Gambar 3.40 *Verifikasi* pada tanda tangan pada pesan

3.9.13 Flowchart open id signature pada pesan

Apabila suatu saat terdapat masalah yang di anggap perlu untuk menentukan anggota yang melakukan tanda tangan pada pesan, maka ketua kelompok melakukan *open id signature* yang dilakukan dengan mendekripsi *id signature* yang ada pada tanda tangan yang disertaka pada pesan yang dikirim. Dalam id tersebut terdapat informasi tentang anggota kelompok yang melakukan tanda tangan pada pesan.



Gambar 3.41 *open id signature* pada pesan

3.9 Skenario Pengujian

Dalam skenario pengujian sistem e-voting simulasi dilakukan dalam satu tempat pemungutan suara (TPS) yakni TPS 1 dalam satu Kecamatan dan satu Kabupaten.