BAB II
LANDASAN TEORI

2.1 Demokrasi

Demokrasi adalah bentuk pemerintahan yang semua warga negaranya memiliki hak setara dalam pengambilan keputusan yang dapat mengubah hidup mereka. Demokrasi mengizinkan warga negara berpartisipasi baik secara langsung atau melalui perwakilan dalam perumusan, pengembangan, dan pembuatan hukum. Demokrasi mencakup kondisi sosial, ekonomi, dan budaya yang memungkinkan adanya praktik kebebasan politik secara bebas dan setara.

Ada beberapa jenis demokrasi, tetapi hanya ada dua bentuk dasar. Keduanya menjelaskan cara seluruh rakyat menjalankan keinginannya. Bentuk demokrasi yang pertama adalah demokrasi langsung, yaitu semua warga negara berpartisipasi langsung dan aktif dalam pengambilan keputusan pemerintahan. Di kebanyakan negara demokrasi modern, seluruh rakyat masih merupakan satu kekuasaan berdaulat namun kekuasaan politiknya dijalankan secara tidak langsung melalui perwakilan; ini disebut demokrasi perwakilan. Konsep demokrasi perwakilan muncul dari ide-ide dan institusi yang berkembang pada Abad Pertengahan Eropa, Era Pencerahan, dan Revolusi Amerika Serikat dan Perancis.[2]

2.2 Pemilihan Umum (Pemilu)

Pemilihan Umum (Pemilu) atau dalam bahasa inggris disebut *election* adalah cara yang digunakan untuk mewujudkan partisipasi rakyat dalam pemerintahan sebagai pemegang kekuasaan tertinggi. Pemilihan umum sudah menjadi bagian yang tidak terpisahkan dari suatu negara demokrasi, hampir semua negara demokrasi melaksanakan pemilihan umum. Pemilihan umum adalah proses pemilihan wakil rakyat di parlemen dan kepala pemerintahan berdasarkan suara terbanyak. Mantan sekretaris jenderal PBB (Perserikatan Bangsa-Bangsa) atau UN (*United Nations*) pernah mengatakan bahwa pemilihan umum merupakan

elemen utama dari demokrasi sebagai sebuah cara masyarakat untuk mengambil keputusan.

Syarat pemilih dalam pemilu[3]

1. Tedaftar sebagai WNI
2. Tedaftar sebagai anggota pemilih pada suatu daerah
3. Berumur diatas 17 tahun atau sudah menikah
4. Tidak sedang terganggu jiwa/ingatannya
5. Tidak sedang dicabut hak pilihnya berdasarkan keputusan pengadilan yang telah mempunyai hukum tetap.
6. Seorang pemilih hanya dapat di daftar satu kali

2.3 Voting (Pemungutan Suara)

Pemungutan suara (voting) adalah salah satu tahap pelaksanaan pemilihan umum. Secara umum, di banyak negara, pemungutan suara dilaksanakan secara rahasia pada tempat yang khusus dipersiapkan untuk pelaksanaan pemungutan suara. Proses pemungutan suara di Indonesia masih menggunakan cara manual, yaitu menggunakan kertas suara. Berikut ini adalah urutan proses pada saat pemungutan suara di Indonesia.[4]

1. Calon pemilih datang ke TPS (Tempat Pemungutan Suara). TPS adalah tempat melakukan pemungutan suara yang disediakan oleh panitia pemilihan umum.
2. Calon pemilih memberikan kartu pemilih. Kartu pemilih ini digunakan sebagai tanda bahwa calon pemilih telah terdaftar sebagai calon pemilih.
3. Calon pemilih mengambil kertas suara (ballot) dan kemudian melakukan pencoblosan di dalam bilik suara.
4. Kertas suara dimasukkan ke dalam kotak suara (ballot box).
5. Salah satu jari pemilih diberi tanda dengan tinta sebagai penanda bahwa pemilih tersebut telah melakukan pemungutan suara.
6. Setelah waktu untuk memasukkan suara selesai, maka kemudian dilakukan perhitungan suara.

7. Kertas suara dikeluarkan dari kotak suara dan kemudian dihitung bersama-sama dengan diawasi oleh saksi dari berbagai pihak antara lain panitia dan perwakilan partai politik.
8. Hasil perhitungan tersebut kemudian dikirimkan ke kantor KPU untuk dilakukan rekapitulasi hasil pemungutan suara.

Proses pemungutan suara secara manual menggunakan kertas suara sampai saat ini masih digunakan di Indonesia dan negara-negara lain yang belum menggunakan sistem *e-voting*.

Berikut ini adalah beberapa alasan yang mungkin mendasari suatu negara tetap menggunakan sistem pemungutan suara secara manual.

1. Belum ada sistem *e-voting* yang keamanannya sudah benar-benar teruji.
2. Tingkat pendidikan masyarakat secara umum masih cukup rendah sehingga penerapan teknologi baru membutuhkan biaya dan waktu yang cukup besar untuk melakukan sosialisasi agar masyarakat mampu menggunakannya.
3. Pemerintah perlu melakukan sosialisasi sistem baru agar masyarakat mau mengadopsi sistem baru.
4. Konversi dari sistem lama (manual) ke sistem baru (*e-voting*) membutuhkan usaha yang cukup besar.

2.4 *Voting electronic*(e-voting)

Pengertian umum *e-voting* adalah penggunaan teknologi komputer dalam pelaksanaan pemungutan suara. Sebuah system *e-voting* dapat didevinisikan sebagai sebuah sistem yang memanfaatkan perangkat elektronik dan mengolah informasi digital untuk membuat surat suara, memberikan suara, menghitung perolehan suara, menayangkan perolehan suara, dan memelihara dan menghasilkan jejak audit.[5]

Seiring dengan perkembangan jaman, ada pergeseran makna terkait *e-voting*. *E-voting* saat ini lebih dikhususkan pada pemanfaatan teknologi informasi khususnya jaringan internet pada pelaksanaan pemungutan suara. Penelitian terkait *e-voting* yang memanfaatkan teknologi informasi mulai banyak

bermunculan pada tahun 1990an. Pemanfaatan *e-voting* sudah mulai dilakukan pada beberapa negara. Berikut ini adalah beberapa contoh Negara yang telah memanfaatkan teknologi *e-voting*.

1. 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, sistem *e-voting* telah digunakan pada proses pemilihan umum dengan skala yang lebih tinggi. Pada tahun 2002, lebih dari 100 juta penduduk Brazil memasukkan suara mereka menggunakan mesin *e-voting* yang berjumlah lebih dari 400.000 yang tersebar di seluruh bagian negara. Keberhasilan Brazil tersebut menunjukkan bahwa negara dengan jumlah penduduk yang sangat besar juga telah mampu memanfaatkan sistem *e-voting.*

2. 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* pada setiap TPS.

3. 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.

Selain ketiga negara di atas, sebenarnya masih banyak negara lain yang sudah mulai memanfaatkan *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 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.

E-voting menggunakan protokol-protokol pemilihan yang disebut sebagai "secure election". Protokol- protokol ini berisi aturan-aturan yang harus dipatuhi untuk mendapatkan hasil sesuai dengan yang diinginkan. Sistem e-voting menawarkan keuntungan dibandingkan dengan pemungutan suara secara konvensional yaitu pemungutan suara lebih sederhana, penghematan pencetakan surat suara, penghitungan suara mudah dan cepat dan begitu pula penghitungan ulang.

Dalam teknologi e-voting, pemungutan suara dapat dilakukan dengan dua cara. Pertama, sistem pemindaian optik memungkinkan pemilih untuk memberikan tanda pada surat suara dan kemudian surat suara tersebut direkam secara elektronik. Dengan sistem ini, rekaman kertas tersedia untuk dapat digunakan dalam perhitungan ulang, dan untuk memelihara konsistensi antara suara suara yang dipungut pada Tempat Pemungutan Suara (TPS) dan yang tidak hadir di TPS (*absentee*). Namun, pencetakan surat suara yang dapat dipindai dengan optik membutuhkan rancangan yang rumit dan biaya mahal. Selain daripada itu, tanda yang melewati batas kotak marka suara dapat menyebabkan kesalahan penghitungan oleh mesin pemindai.

Kedua, sistem *direct recording electronic* (DRE) menyediakan surat suara yang dapat dipilih dengan menggunakan perangkat elektronik atau komputer yang dilengkapi dengan layar sentuh, mengolah data dengan perangkat lunak, dan menyimpan perolehan suara dan surat suara di dalam memori. Sistem DRE pada komputer dapat diprogram untuk menampilkan surat suara sesuai dengan pemilihan umum yang diselenggarakan. Setelah pemungutan suara selesai, sistem

DRE melakukan penghitungan suara, mencetak dan menayangkan perolehan suara di TPS. Rekaman pemungutan suara disimpan secara teramankan di dalam media penyimpanan seperti flash disk dan dikirim ke pusat penghitungan suara melalui jaringan komunikasi data atau dengan mengirimkan media penyimpanan secara langsung. Sistem ini dapat memastikan seorang pemilih memilih hanya satu kali meskipun antar TPS tidak terhubung oleh jaringan komunikasi data.

Penelitian terkait *e-voting* masih terus dilakukan sampai sekarang. Ada bermacam-macam teknologi yang digunakan dalam mengembangkan *e-voting* tersebut. Berikut ini beberapa persyaratan yang harus dipenuhi dalam suatu sistem *e-voting*.

1. *Accuracy* (akurasi) yaitu ketepatan hasil perhitungan suara. Ketepatan ini meliputi tidak ada satupun pihak yang diperbolehkan mengubah suara yang telah masuk, semua suara yang valid dihitung dengan tepat, dan suara yang tidak valid tidak boleh dihitung.
2. *Democracy* (demokrasi) yaitu hanya calon pemilih yang memenuhi syarat berhak untuk memilih dan setiap pemilih hanya berhak untuk memasukkan suaranya satu kali.
3. *Privacy* (privasi) yaitu tidak seorang pun yang dapat menghubungkan seseorang dengan hasil pilihannya.
4. *Robustness* yaitu tidak ada gangguan yang menghalangi pelaksanaan pemungutan suara. Jadi aspek ini berkaitan erat dengan aspek *security* (keamanan).
5. *Verifiability* yaitu setiap orang dapat membuktikan bahwa tidak ada manipulasi terhadap hasil perhitungan.
6. *Uncoercibility* yaitu tidak adanya paksaan kepada pemilih dalam menentukan pilihannya. Agar tidak terjadi maka pemilih harus tidak dapat membuktikan hasil pilihannya kepada orang lain (*receipt freeness*).
7. *Fairness* yaitu setiap orang tidak dapat mengetahui hasil pemilihan sebelum proses pemilihan selesai dan dilakukan perhitungan suara.
8. *Verifiable participation* yaitu mampu membuktikan apakah seseorang telah melakukan pemungutan suara atau belum.

Pada sub bab berikut akan dijelaskan mengenai beberapa contoh penelitian terkait dengan sistem *e-voting*.[6]

2.4.1 E Vox

E-Vox adalah sebuah sistem *e-voting* yang dikembangkan oleh Mark A. Herschberg pada tesis yang *berjudul Secure Electronic Voting Over the World Wide Web* tahun 1997. Sistem E-Vox mempunyai kelebihan dalam kemudahan akses oleh pemilih. Pemilih hanya membutuhkan *username* (identitas pemilih) dan *password* untuk dapat mengakses system tersebut. Pemilih tidak perlu menggunakan otentikasi lainnya. Penanganan keamanan sistem ditangani secara internal dan tidak menyulitkan calon pemilih dalam mengoperasikan sistem tersebut.

2.4.2 E Vote

Sistem e-VOTE adalah sebuah sistem *voting* berbasis internet. e-VOTE adalah sebuah proyek yang dilakukan oleh konsursium terdiri dari universitas-universitas dan perusahaan-perusahaan IT di Eropa pada tahun 2000. e-VOTE mempunyai tujuan untuk membuat desain, mengembangkan, dan melakukan validasi sebuah sistem *e-voting* berbasis internet. Sistem ini meliputi registrasi pemilih, validasi pemilih, mengumpulkan suara, dan melakukan perhitungan hasil suara.

2.4.3 MarkPledge

MarkPledge adalah sistem *e-voting* yang dikembangkan oleh Andrew Neff sekitar tahun 2000. Pada sistem MarkPledge, penanganan faktor keamanan dan kerahasiaan data secara khusus tidak tampak dalam arsitekturnya. Sistem MarkPledge lebih menekankan pada verifikasi terhadap hasil perhitungan suara. Pada sistem tersebut, verifikasi perhitungan suara dilakukan dengan dua macam cara yaitu *universal verifiability* dan *ballot casting assurance*. *Universal verifiability* adalah verifikasi yang dapat dilakukan oleh semua pihak yang berkepentingan terhadap hasil suara sedangkan ballot casting assurance adalah verifikasi hasil perhitungan suara yang dilakukan oleh pemilih (setiap pemilih hanya dapat melakukan verifikasi terhadap surat suaranya masing-masing).

2.4.4 Sistem *E-Voting* Terpusat

Sistem *E-Voting* Terpusat adalah sistem yang dikembangkan oleh Philip Anderson Hutapea pada tahun 2009 sebagai bagian dari tugas akhir program studi Informatika, Sekolah Teknik Elektro dan Informatika, Institut Teknologi Bandung. Sistem yang dikembangkan tersebut membahas lebih mendalam mengenai cara menangani factor keamanan data khususnya terkait masalah kerahasiaan data. Metode yang digunakan untuk mengatasi faktor tersebut adalah dengan melakukan kriptografi. Sistem ini menggunakan kartu pemilihan, yaitu sebuah kartu kecil yang mempunyai *chip memory* dan digunakan sebagai media penyimpanan suara yang dapat digunakan untuk perhitungan suara secara manual.

2.5 Kriptografi

Kriptografi merupakan Teknik untuk mengacak suatu pesan agar tidak dapat diketahui maknanya disebut enkripsi, dan membentuk suatu bidang keilmuan yang disebut Kriptografi. Prinsip dasarnya adalah menyembunyikan informasi sedemikian rupa agar orang yang berhak saja yang dapat mengetahui isi dari informasi yang tersembunyi tersebut. Teknik ini sudah ada sejak jaman dahulu, bahkan sejak jaman sebelum Masehi pada masa perang yang digunakan untuk mengirim pesan rahasia antar sesama kawan agar apabila pesan terbaca oleh musuh ditengah jalan, isi dari pesan tersebut tidak dapat terbaca. Seiring dengan kemajuan teknik yang digunakan untuk mengenkripsi maka didalamnya terkandung unsur matematis yang membuat isi dari informasi itu semakin sulit untuk dibongkar.[7]

Ada empat tujuan mendasar dari ilmu kriptografi ini yang juga merupakan aspek keamanan informasi yaitu:

a. Kerahasiaan, adalah layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka/ mengupas informasi yang telah disandi.
b. Integritas data, adalah berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak

berhak, antara lain penyisipan, penghapusan, dan pensubsitusian data lain ke dalam data yang sebenarnya.

c. Autentikasi, adalah berhubungan dengan identifikasi/pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan melalui kanal harus diautentikasi keaslian, isi datanya, waktu pengiriman, dan lain-lain.
d. Non-repudiasi adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman/terciptanya suatu informasi oleh yang mengirimkan/membuat.

2.6 Kegunaan Kriptografi Dalam Electronic Voting

Para peneliti di bidang electronic voting menyepakati empat properti yang harus dimiliki oleh sistem *electronic voting.*antara lain adalah rahasia. Suatu sistem electronic voting dikatakan rahasia apabila tidak ada pihak berwenang ataupun pihak lainnya yang dapat memastikan siapa pemilih dari suatu surat suara dan tidak ada pemilih yang dapat membuktikan bahwa dia sudah memilih suatu kandidat tertentu.

Faktor kerahasiaan yang kedua dinilai penting untuk mencegah pembelian suara. Untuk menjaga kerahasiaan dalam sistem sebagai sala satu property yang harus dimiliki oleh system electronic voting maka diperluakan sebuah metode atau ilmu yang mempelajari tentang penjagaan keamanan pesan atau data.

Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasisaan, integrita data, serta otentifikasi.[7] Kriptografi sebagai ilmu dan seni mengamankan pesan mampu menawarkan solusi pada permasalahan electronic voting dalam hal ini terkait permasalahan keamanan dan kerahasiaan data.[9]

Adaya banyak jenis kripptografi yang telah digunakan dalam berbagai applikasi termasuk dalam pembuatan e-voting, adapun metode-metode atau algoritma yang bisaa digunakan dalam e-voting antara lain algoritma RSA, blind digital signature, group blind digital signature.

2.7 Digital Signature

Fungsi tanda tangan pada dokumen kertas juga diterapkan untuk otentifikasi pada data digital seperti pesan yang dikirim melelui saluran jaringan komunikasi yang berupa data digital.

Tanda tangan dijital (*Digital Signature*) merupakan tanda tangan untuk data dijital. Tanda tangan dijital bukanlah tulisan tanda tangan yang di-digitisasi (di-scan), melainkan suatu nilai kriptografis yang bergantung pada isi pesan dan kunci.[8] selain digunakan untuk menjamin integritas data, tanda tangan dijital juga dapat digunakan untuk membuktikan asal pesan (keabsahan pengirim), dan nirpenyangkalan.

Menandatangani pesan dapat dilakukan dengan salah satu dari dua cara berikut:[7]

1. Enkripsi data

Mengenkripsi pesan dengan sendirinya juga menyediakan ukuran otentifikasi. Pesan yang telah terenkripsi sudah menyatakan bahwa pesan tersebut telah ditandatangani.

2. Tanda tangan digital dengan fungsi hash

Tanda tangan digital dibangkitkan dari hash terhadap pesan. Nilai hash adalah kode ringkas dari pesan. Tanda tangan digital berlaku seperti tanda tangan pada dokumen kertas. Tanda tangan digital ditambahkan pada pesan .

Pemberian tanda tangan dengan menenkripsi pesan dapat dilakuakn dengan algoritma kunci publik, salahasatu algoritma kunci publik yang banyak digunakan adalah algoritma RSA.

Adapun langkah pemberian tanda tangan digital dengan algoritma RSA adalah sebagai berikut:[7]

1. Pengirim menghitung nilai hash dari pesan M yang akan dikirim, misalkan nilai hash dari pesan M adalah h.
2. Pengirim mengenkripsi h dengan kunci privatnya menggunakan persamaan enkripsi RSA, yaitu:

$S = h^{SK} \bmod n$

dalam hal ini SK adalah kunci privat pengirim dan n adalah modulus (n=pq, p dan q adalah dua buah bilangan prima).

3. Pengirim mengirim M + S ke penerima.

Langkah-langkah pemverifikasian tanda tangan dijital dengan algoritma RSA adalah sebagai berikut:[7]

1. Penerima menghitung nilai hash dari pesan M yang dikirim, misalkan nilai hash dari M adalah h'.
2. Penerima melakukan dekripsi terhadap tanda tangan S dengan kunci publik si pengirim menggunakan persamaan dekripsi RSA, yaitu:

   $h = S^{PK} \bmod n$

   dalam hal ini PK adalah kunci publik pengirim dan n adalah modulus (n=pq, p dan q adalah dua buah bilangan prima).
3. Penerima membandingkan h dengan h'. Jika h=h' maka tanda tangan dijital adalah otentik. Jika tidak sama, maka tanda tangan dijital tidak otentik sehingga pesan dianggap tidak asli lagi atau pengirimnya bukanlah orang yang sebenarnya.

2.8 Group Digital Signature

Group digital signature adalah metode yang membuat seorang anggota sebuah grup untuk menanda-tangani sebuah pesan sebagai wakil dari grup. Konsep ini pertama kali diperkenalkan oleh David Chaum dan Eugene van Heyst pada 1991.[11]

Pada skema *group digital signature*, anggota dari suatu kelompok dapat melakukan tanda tangan dijital pada suatu dokumen atas nama seluruh anggota kelompok. Tanda tangan tersebut dapat diverifikasi dengan menggunakan kunci publik kelompok (*group public key*). Selanjutnya, group signature ini harus didesain sehingga tidak ada seorang anggota kelompok pun yang dapat memalsukan tanda tangan anggota kelompok lainnya. Jadi, pada group digital

signature, terdapat satu kunci publik kelompok dan lebih dari satu kunci privat anggota kelompok.[12]

Hanya ketua kelompok yang dapat mengetahui siapa anggota kelompok yang telah menanda tangani dokumen yang ada, dalam *group digital signature* tanda tangan tidak dapat dipalsukan oleh anggota lain dalam satu kelompok.

Kebutuhan dasar yang harus dipenuhi untuk keamanan *group digital signature* adalah sebagai berikut:

a. *Soundness and Completeness*: tanda tangan yang valid akan selalu benar saat diverifikasi, dan tanda tangan yang tidak valid akan selalu tidak dapat melewati proses verifikasi.
b. *Unforgeable*: Hanya anggota grup yang dapat membuat tanda tangan kelomok yang valid.
c. *Signer ambiguous*: Apabila diberikan pesan beserta tanda tangannya, identitas dari individu pemberi tanda tangan tidak dapat ditentukan tanpa kunci rahasia manager.
d. *Unlinkability*: Antara satu anggota dengan anggota yang lain berbeda.
e. *No Framing*: Tidak ada anggota kelompok termasuk ketua kelompok yang dapat membuat tanda tangan untuk pihak yang tidak berpartisipasi dalam kelompok.
f. *Unforgeable tracing verification*: ketua kelompok tidak dapat salah menyatakan bahwa individu tersebutlah yang memberi tanda tangan padahal sebenarnya tidak.

Adapun skema *group digital signature* terdapat lima prosedur sebagai berikut:

1. *Setup*

   dalam proses ini dilakukan pembangkitan kunci publik kelompok dan sebuah kunci rahasia administrasi yang dilakukan oleh ketuakelompok.
2. *Join*

   pembangiktan kunci individu(*private key*) untuk setiap anggota kelompok dilakukan oleh ketua kelompok.

3. *Sign*

   proses penanda tanganan oleh anggota kelompok menggunakan kunci private yang telah diberikan kepada anggota yang bersangkutan.

4. *Verify*

   proses verifikasi tanda tangan yang ada pada dokumen yang diterima dari pengirim pesan, verifikasi dilakukan menggunakan kunci publik yang dimiliki kelompok pengirim pesan. proses ini dilakukan oleh penerima pesan.

5. *Open*

   proses ini ditujukan untuk mengetahui anggota yang telah melakukan tanda tangan, proses ini hanya bisa dilakukan oleh ketua kelompok yang megirim pesan beserta tanda tangan dengan menggunakan kunci private yang dimiliki kelompok yang bersangkutan.

2.9 Group Blind Digital Signature

Group digital signature pertama kali dikemukakan oleh Lysyanskaya dan Ramzan. *Group blind digital signature* mengkombinasikan properti dari *grup signature* dan *blind signature*.[11]

Kebutuhan keamanan dari *Group Blind Digital Signature* sangat mirip dengan yang dimiliki *Group Digital Signature*. Penambahan yang ada kita membutuhkan properti penyamaran dalam pesan. Berikut kebutuhan-kebutuhan dari *group blind digital signature*:[11]

a. *Blindness of Signature*: pemberi tanda tangan harus tidak dapat melihat isi dari pesan yang ia beri tanda tangan, walaupun penerima dapat memverifikasi bahwa tanda tangan tersebut valid.

b. *Soundness and Completeness*: tanda tangan yang valid akan selalu benar saat diverifikasi, dan tanda tangan yang tidak valid akan selalu tidak dapat melewati proses verifikasi.

c. *Unforgeable*: Hanya anggota grup yang dapat membuat tanda tangan kelomok yang valid.

d. *Signer ambiguous*: Apabila diberikan pesan beserta tanda tangannya, identitas dari individu pemberi tanda tangan tidak dapat ditentukan tanpa kunci rahasia manager.
e. *Unlinkability*: Antara satu anggota dengan anggota yang lain berbeda.
f. *No Framing*: Tidak ada anggota kelompok termasuk ketua kelompok yang dapat membuat tanda tangan untuk pihak yang tidak berpartisipasi dalam kelompok.
g. *Unforgeable tracing verification*: ketua kelompok tidak dapat salah menyatakan bahwa individu tersebutlah yang memberi tanda tangan padahal sebenarnya tidak.
h. *Undeniable Signer Identity*: Ketua dari kelompok selalu dapat member tahu siapa yang memberika tanda tangan yang valid
i. *Coalition Resistance*: Hanya ketua kelompok yang dapat membuat melakukan *setup group signature* yang valid.

Seperti halnya syarat keamanan pada *group digital signature*, protokol atau prosedur pada *group blind digital signature* pun sama persis seperti protokol pada *group digital signature.* Protokol-protokol tersebut yaitu: *setup, join, sign, verify,* dan *open*.

Beberapa kelebihan dari *group blind digital signature* yang juga merupakan bagian dari *digital signature* antara lain adalah dalam hal autentifikasi data yang dikirim, karena pemberian tandatangan hanya dapat dilakukan dengan menggunakan kunci privat yang dimiliki anggota kelompok, maka pada saat ferivikasi tanda tangan yang ada dalam pesan valid maka pihak penerima dapat memastikan bahwa data dikirim dari kelompok yang dimaksud.

Telah dilakukan enkripsi terhadap pesan data yang dikirim yang membuat pesan tidak dapat terbaca oleh pihak lain selain penerima dan pengirim pesan. hal ini yang dapat menjaga integritas data yang dikirim.

Dalam penggunaan *group blind digital signature* seseorang yang telah melakukan tandatangan tidak dapat menyangkal bahwasanya bukan dirinya yang melakukan tandantangan terhadap pesan yang dikirim, karena dalam *group blind*

digital signature data seseorang yang melakukan tandatangan dapat dibuktikan dengan menggunakan kuci privat yang dimiliki oleh meneger atau ketua kelompok.[9]

2.10 Captcha

CAPTCHA adalah suatu bentuk uji tantangan-tanggapan *(challange-response test*) yang digunakan dalam perkomputeran untuk memastikan bahwa jawaban tidak dihasilkan oleh suatu komputer. Proses ini biasanya melibatkan suatu komputer (server) yang meminta seorang pengguna untuk menyelesaikan suatu uji sederhana yang dapat dihasilkan dan dinilai oleh komputer tersebut. Karena komputer lain tidak dapat memecahkan **CAPTCHA**, pengguna manapun yang dapat memberikan jawaban yang benar akan dianggap sebagai manusia.[10]

2.11 Algoritma RSA

Algoitma RSA dibuat oleh 3 orang peneliti dari Massachussets Institute of technology (MIT) pada tahun 1976,yaitu Ron Riivest,Adi Shamir, dan Leronard Adleman. Keamana algoritma RSA terletak pada sulitnya memfaktorkan bilangan menjadi factor-faktor prima. Pemfaktoran dilakukan untuk memperoleh kunci prifat. Selama pemfaktoran bilangan besar menjadi factor-faktor prima belum ditemukan algoritma yang mangkus, maka selama itu pula keamanan lagoritma RSA tetap terjaga.[10]

Algoritma RSA didasarkan pada teorema euler yang menyatakan bahwa :

$a^{\phi(n)} \equiv 1 \pmod{n}$.....(3.1)

Pada RSA masalah pemfaktoran berbunyi: faktor *n* menjadi dua faktor primanya, *p* dan *q*, sedemikian sehingga $n = p.q$. Sekali *n* behasil difaktorkan mejadi *p* dan *q*, maka $\phi(n) = (p-1)(q-1)$ dapat dihitumg. Selanjutnya, karena kunci enkripsi e diumumkan (tidak rahasia), maka kunci dekripsi d dapat dihitung dengan persamaan $e.d = 1 \pmod{\phi(n}$. [10]

Secara umum dapat disimpulkan bahwa RSA hanya aman jika n cukup besar. Jika panjang n hanya 256 bit atau kurang maka ia dapat difaktorkan dalam beberapa jam saja dengan sebuah computer dan program yang tersedia secara

bebas. Jika panjang n 512 bit atau kurang maka ia dapat difaktor dengan beberapa ratus computer.[10]

Algoritma pembangkit kunci pada RSA adalah sebagi berikut:

1. Pilih dua bilangan prima sembarang,*p* dan *q*.
2. Hitung $n=p \cdot q$ (sebaiknya $p \neq q$).
3. Hitung $\Phi(n)= (p - 1) (q - 1)$.
4. Pilih kunci Publik e yang relative prima terhadap $\Phi(n)$.
5. Bangkitkan kunci prifat dengan persamaan berikut:

$$d = \frac{1 + k\Phi(n)}{e} \quad \text{.....(3.2)}$$

sedangkan untuk enkripsi dan dekripsi digunakan rumus sebagai berikut:

Untuk mengenkripsi dgunakan persamaan:

$$E_e(m)=m^e \bmod n. \quad \text{.....(3.3)}$$

Untuk mendekripsi digunakan rumus senbagi berikut:

$$D_d(c)=c^d \bmod n. \quad \text{.....(3.4)}$$

RSA lebih lambat daripada algoritam kunci-munci seperti DES dan AES. Oleh karena itu, di dalam praktek penggunaannya pesan tetap dienkripsi dengan menggunakan salah satu algoritma kriptografi kunci simetri dan kunci rahasia, sedangkan RSA digunakan untuk mengenkripsi kunci rahasia. Pesan dan kunci rahasia yang sudah di enkripsi dapat dikirim bersama-sama. Penerima pesan mula-mula mendekripsi kunci rahasia dengan kunci privatnya kemudian menggunakan kunci rahasia tersebut untuk mendekripsi pesan.[7]

Contoh Kasus Pembuatan Kunci dengan bilangan yang kecil (*hanya sebagai ilustrasi cara kerja alghoritma*).

1. Pilih 2 bilangan prima yang berbeda untuk p dan q. Misalnya:
   p=61 dan q=53
2. Hitung n=pq
   61*53 = 3233
3. Hitung pq=(p-1) * (q-1);
   (61-1)*(53-1) = 3120;

4. Pilih bilangan e dengan syarat (1 < e < 3120) dan gcd(e,3120)=1, kita ambil e=17, dimana
   17 memenuhi syarat: (1 < 17 < 3120) dan (gcd(17,3120)=1).
5. Pilih nilai d, dimana (d*e) mod pq = 1. Kita ambil d=2753 dimana:
   (2753*17) mod 3120 = 1
   46801 mod 3120 = 1

Dengan perhitungan tersebut Kita telah mendapatkan Private dan Public Key, dimana Private Key adalah (n=3233 dan d=2753) dan Public Key adalah (n=3233 dan e=17).

Proses Enkripsi

Berikut adalah ilustrasi enkripsi dengan menggunakan RSA:[13]
Ahmad mengirimkan public key (n,e) nya untuk Idik, dan menyimpan secara rahasia private key-nya. Idik ingin mengirimkan pesan "M" pada Ahmad. Idik kemudian merubah M menjadi kode ascii (berupa integer) dan menghitung ciphertext "c" (nilai yang telah terenkripsi) dengan menggunakan public key yang dikirimkan oleh Ahmad kepadanya, kemudian Idik mengirimkan nilai c kepada Ahmad untuk di-decrypt dengan menggunakan private-key miliknya.

Ada beberapa syarat dalam enkripsi di RSA, dimana nilai M harus lebih besar dari 0, dan harus lebih kecil dari nilai n (dari public key).
Kode Ascii untuk M adalah 77. Bila Public Key adalah (n=3233 dan e=17) maka nilai M ini memenuhi syarat0 < 77 < 3233; dan dapat langsung dilakukan kalkulasi.
Proses enkripsi sangat mudah, hanya dengan melakukan kalkulasi

```
1. c = (M pangkat e) mod n
```

Bila **M=77**, dan public Key adalah **n=3233** dan **e=17** maka:

```
1. c = (77 pangkat 17) mod 3233
2. c = 11758240203309717474913682878759 7 mod 3233
3. c = 3123
```

Untuk lebih efisien, Kita dapat menggunakan fungsi powmod (dalam bcmath dapat menggunakan**bcpowmod**, dalam GMP dapat menggunakan **gmp_powm**). Atau membuat fungsi powmod yang efisien seperti pada logika kode berikut:

```
1. function AmarullzPowMod(a,b,c){
2.      r=a;
3.      for (i=1;i<b;i++){
4.          r=(a*r) % c;
5.      }
6.      return r;
7. }
8.
9. cipher = AmarullzPowMod(77,17,3233);
```

Proses Dekripsi

Operasi Dekripsi/decrypt tidak berbeda jauh dengan operasi encrypt, yang berbeda adalah nilai yang dimasukkan kedalam fungsi powmod itu. Dalam operasi decrypt, nilai M diganti dengan nilai c dari ciphertext (*hasil enkripsi*) dan nilai e dari public key diganti dengan nilai d dari private key, sedangkan nilai n dari public key selalu sama dengan nilai n dari private key.[13]

Dari penjelasan sebelumnya Kita sudah mendapatkan data-data sebagai berikut:

```
1. Private Key = (n=3233 dan d=2753)
2. c = 3123
```

Dengan menggunakan private key, Kita ingin melakukan decrypt dari c menjadi M kembali, caranya adalah:

```
1. M2 = (c pangkat d) mod n
2. M2 = (3123 pangkat 2753) mod 3233
3. M2 = 7+E8301 mod 3233
4. M2 = 77
```

Kita coba menghitungnya dengan fungsi bcpowmod, gmp_powm atau AmarullzPowMod di atas:

```
1. M2 = AmarullzPowMod(3123,2753,3233);
2. M2 akan bernilai 77
```

Dengan perhitungan tersebut, kita sudah dapat mengimplementasikan Private dan Public Key sebagai sarana untuk melakukan enkripsi dengan menggunakan alghoritma RSA, dimana Idik melakukan enkripsi data M=77 dengan public key dan mendapatkan nilai c=3123, kemudian mengirimkannya kepada Ahmad untuk di dekripsi dengan menggunakan private key dan mendapatkan data yang sama dengan yang dimaksudkan oleh Idik, yaitu M2=77.

2.12 Digital Signature dengan RSA

Langkah-langkah penandatangan digital dengan *RSA* telah dijelaskan diatas, berikut contoh pesan dengan *RSA* yang akan digunakan untuk *digital signature.*

Pada awalnya kita tentukan kunci privat, kuci publik, dan modulus dengan menggunakan algoritma pembangkit kunci yang telah dijelaskan sebelumnya.[14]

misalkan kita memilih p= 73 dan q=67 selanjutnya kita menghitung

n = 73 x 67 = 4891

φ= (73 - 1) x (67 - 1) = 4752

kita pilih kunci public e = 7, dan Memilih 679 sebagai bilangan d karena memenuhi syarat de ≡ 1 mod φ , *Private key* nya adalah 679 dan *public key*nya adalah 7. Selanjutnya langkah – langkah yang dilakukan dalam mengirim data adalah :

Pemberian signature

Untuk huruf T, ST = 124679 mod 4891 = 1669

Untuk huruf E, SE = 105679 mod 4891 = 2048

Untuk huruf S, Ss = 123679 mod 4891 = 2713

kemudian mengirimkan data berisi 1669-2048-2713-1669

untuk membuka data dan memverifikasinya akan melakukan :

Verifikasi signature

Untuk m1 = 16697 mod 4891 = 124

Untuk m2 = 20487 mod 4891 = 105

Untuk m3 = 27137 mod 4891 = 123

2.13 Riset Sebelumnya

Penelitian mengenai *e-voting* telah banyak dilakukan, ada beberapa penelitian yang dijadikan acuan dalam tugas akhir ini antara lain:

1. Penelitaina ini dilakuakn oleh Muhammad Fikri Isnaini, Mahasiswa Departemen Ilmu Komputer Fakultas Matematika Dan Ilmu Pengetahuan Alama Institut Pertanian Bogor Bogor dengan judul Analisis Dan Implementasi *e-voting system* Pada Pemilihan Kepala Daerah , Pada penelitian ini dirancang protokol dan simulasi sistem *e-voting* pada pemilihan kepala daerah. Fungsi-fungsi pada sistem ini memenuhi beberapa kriteria, yaitu *Eligibility, Unreusability, Anonymity, Accuracy, Fairness, Vote and Go, dan Public Verifiability.*

Dalam penelitian ini adalah untuk sistem pendaftaran pemilih, validasi dan pengaktifan pemilih, sistem pemilihan, dan sistem perhitungan suara. Untuk menjaga keamanan dan kerahasiaan data, system *e-voting* ini menggunakan algoritme kunci publik dan algoritme kunci simetri.

Hasil dari penelitian sistem *e-voting* berbasis web yang berjalan memenuhi kriteria dari skema *e-voting*. Hasil penelitian menunjukkan bahwa *e-voting* dapat mempercepat proses perhitungan suara dan menghilangkan kesalahan perhitungan yang dapat terjadi jika dilakukan secara manual oleh manusia.[6]

2. Penelitian ini dilakukan oleh Muhammad Shalahuddin Mahasiswa Program Magister Informatika Institut Teknologi Bandung dengan judul Pembuatan Model *E-Voting* Berbasis Web (Studi Kasus Pemilu Legislatif Dan Presiden Indonesia), Pembuatan model *e-voting* pada tesis ini difokuskan pada teknologi berbasis web karena teknologi tersebut mudah dalam pengaksesannya. Model yang dihasilkan pada tesis ini diberi nama Web-Vote. Model yang dihasilkan tersebut untuk pemilihan umum di Indonesia. Hasil pengujian membuktikan bahwa model yang dihasilkan mampu memenuhi persyaratan *e-voting* yang baik. [4]