SISTEM KEAMANAN *E-VOTING* MENGGUNAKAN FUNGSI HASH DAN ALGORITMA *ONE TIME PAD*

SKRIPSI

diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana Pendidikan Program Studi Pendidikan Teknik Informatika dan Komputer

Oleh

Nurul Istiqamah

5302410189

JURUSAN TEKNIK ELEKTRO

FAKULTAS TEKNIK

UNIVERSITAS NEGERI SEMARANG

2016

PERSETUJUAN PEMBIMBING

Nama	:	Nurul Istiqamah
NIM	:	5302410189
Program Studi	:	Pendidikan Teknik Informatika dan Komputer, S1
Judul Skripsi	:	Sistem Keamanan *Evoting* Menggunakan Fungsi Hash dan Algoritma *One Time Pad*

Skripsi ini telah disetujui oleh pembimbing untuk diajukan ke sidang panitia sebagai ujian skripsi Program Studi S-1 Pendidikan Teknik Informatika dan Komputer.

Semarang, Juni 2016
Dosen Pembimbing Utama,

Dr. Subiyanto, S.T., M.T.
NIP. 197008091975031003

UNNES
UNIVERSITAS NEGERI SEMARANG

PERNYATAAN

Dengan ini saya menyatakan bahwa skripsi ini benar-benar hasil karya saya sendiri, bukan plagiat dari karya tulis orang lain baik sebagian atau seluruhnya. Pendapat atau temuan orang lain yang terdapat dalam skripsi ini dikutip untuk dirujuk berdasarkan kode etik ilmiah dan disebutkan di dalam daftar pustaka. Apabila dikemudian hari ditemukan plagiat dalam karya ini, maka saya bersedia menerima sanksi sesuai ketentuan peraturan perundang-undangan.

Semarang, Juni 2016

METERAI TEMPEL 1576DADF663150889 6000 ENAM RIBU RUPIAH

Nurul Istiqamah
NIM. 5302410189

UNNES
UNIVERSITAS NEGERI SEMARANG

PENGESAHAN

Skripsi dengan judul "Sistem Keamanan *Evoting* Menggunakan Fungsi Hash dan Algoritma *One Time Pad*" ini telah dipertahankan di depan sidang Panitia Ujian Skripsi Fakultas Teknik UNNES pada:

Hari, tanggal : Jum'at, 1 Juli 2016

Panitia Ujian

Ketua	Sekretaris
Dr. Ing. Dhidik P., S.T., M.T. NIP. 197805312005011002	Ir. Ulfah Mediaty, M.T. NIP. 196605051998022001

Penguji I	Penguji II
Dr. H. Noor Hudallah, M.T. NIP. 196410161989011001	Anggraini Mulwinda, S.T., M.Eng. NIP. 197812262005012002

Penguji III

Dr. Subiyanto, S.T., M.T.
NIP. 197008091975031003

Mengetahui,
Dekan Fakultas Teknik UNNES

Dr. Nur Qudus, M.T.
196911301994031001

UNNES
UNIVERSITAS NEGERI SEMARANG

MOTTO

Pikiran yang baik, perasaan yang indah dan semangat yang kuat adalah pembentuk keajaiban

Sejauh apapun kita pergi, kemanapun kita berlari. Keluarga selalu menjadi rumah untuk kembali

Setiap niat baik akan selalu diberi jalan dan kemudahan

UNNES
UNIVERSITAS NEGERI SEMARANG

PERSEMBAHAN

Untuk orangtua terhebat, Ibunda Safiah dan Ayahanda Drs. Anwar Idris yang selalu setia mendampingi dalam segala do'a dan upaya. Terimakasih untuk motivasi tanpa henti, untuk kesabaran juga keihkalasan

Saudara-saudaraku Anik Nurfitri Safiansah, Umara' Nurrahmi dan Rabi'unnisa Sulaimah juga tiga orang keponakan yang selalu menjadi pengingat dan penyemangat

Keluarga besar Al-Idris yang tak henti memberi dukungan

Muhammad Akbar, thank you for caring and sharing

Almamaterku...

UNNES
UNIVERSITAS NEGERI SEMARANG

ABSTRAK

Istiqamah, Nurul. 2016. *Sistem Keamanan Evoting Menggunakan Fungsi* Hash *dan Algoritma One Time Pad*. Skripsi, Jurusan Teknik Elektro, Fakultas Teknik, Universitas Negeri Semarang. Pembimbing Utama Dr. Subiyanto, S.T., M.T.

Pada umumnya, pelaksanaan pemilu hingga saat ini masih dilakukan secara konvensional. Dimana dalam penyelenggaraannya masih ditemukan beberapa kelemahan seperti besarnya anggaran yang dikeluarkan, adanya indikasi kecurangan seperti penggelembungan suara, pencoblosan ganda, kurangnya transparansi, dan masih tingginya jumlah surat suara tidak sah. Penelitian ini bertujuan mengembangkan sistem *evoting* sebagai alternatif pengganti pemilu konvensional guna mengurangi beberapa kelemahan yang ada. Pengembangan sistem *evoting* juga harus memperhatikan aspek-aspek keamanan informasi yang meliputi: aspek kerahasiaan, aspek otentifikasi, aspek integritas data, aspek ketersediaan dan aspek nir-penyangkalan. Pemenuhan aspek keamanan dapat dilakukan dengan melakukan enkripsi menggunakan beberapa jenis kriptografi.

Penelitian ini menerapkan fungsi hash kriptografis dan algoritma *one time pad* (OTP) untuk merancang sistem keamanan *evoting* dengan melakukan enkripsi terhadap hasil pemungutan suara yang diinisialisasi sebagai *plaintext*. Proses enkripsi dibagi dalam dua tahapan, tahap pertama yaitu membangkitkan nilai *hash* dengan mengenkripsi *plaintext* menggunakan algoritma SHA-256. Tahap kedua, proses enkripsi menggunakan algoritma OTP. Proses enkripsi OTP dilakukan dengan mengoperasikan logika XOR pada bit *plaintext* dengan bit kunci berupa bilangan acak yang dibangkitkan menggunakan fungsi PRNG (*Pseudo Random Number Generator*). Setibanya di server, hasil *ciphertext* dari algoritma OTP kemudian di dekripsi kembali dengan kunci yang sama, kemudian nilai *plaintext* awal di *hash* menggunakan algoritma SHA-256. Nilai *hash* pada tahap pertama dan kedua kemudian dibandingkan, jika bernilai sama maka surat suara dianggap sah lalu disimpan dalam basisdata untuk selanjutnya dilakukan perhitungan perolehan suara masing-masing kandidat capres dan cawapres. Presentase perolehan suara kemudian ditampilkan secara *realtime* pada halaman utama sistem *evoting*.

Pengembangan sistem *evoting* dalam penelitian ini dibuat dalam bentuk simulasi komputer yang dibangun menggunakan bahasa pemrograman PHP dan dijalankan melalui *web browser*. Berdasarkan hasil penelitian yang diperoleh, sistem *evoting* yang dikembangkan mampu mengatasi beberapa kelemahan pada pemilu konvensional dan telah memenuhi aspek keamanan sistem *evoting*. Pemenuhan aspek keamanan diterapkan pada proses sistem pendaftaran, validasi pemilih, sistem *login*, validasi waktu, sistem pemilihan dan sistem perhitungan suara.

Kata kunci : pemilu, *evoting*, kriptografi, fungsi hash, algoritma *one time pad*

KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Allah SWT, yang memberikan rahmat dan hidayah-Nya. Shalawat serta salam penulis haturkan kepada Nabi Muhammad SAW dan keluarganya serta kepada para sahabatnya. Penulis sangat bersyukur karena dengan rahmat dan hidayah-Nya serta partisipasi dari berbagai pihak yang telah banyak membantu baik moril maupun materil sehingga penulis dapat menyelesaikan penyusunan skripsi yang berjudul ”Sistem Keamanan *Evoting* Menggunakan Fungsi Hash dan Algoritma *One Time Pad*”. Oleh karena itu dengan kerendahan hati penulis menyampaikan ucapan terimakasih kepada:

1. Prof. Dr. Fathur Rokman, M. Hum., Rektor Universitas Negeri Semarang yang telah memberikan kesempatan kepada penulis untuk menyelesaikan studi di Jurusan Teknik Elektro Universitas Negeri Semarang.
2. Dr. Nur Qudus, M.T., Dekan Fakultas Teknik Universitas Negeri Semarang yang telah memberikan ijin penelitian dalam memperlancar penyelesaian skripsi ini.
3. Dr. Ing. Dhidik P., M.T., Ketua Jurusan Teknik Elektro Fakultas Teknik Universitas Negeri Semarang yang telah memberikan kemudahan administrasi kepada penulis dalam penyusunan skripsi ini.
4. Ir. Ulfah Mediaty, M.T., Ketua Program Studi Pendidikan Teknik Informatika dan Komputer.
5. Dr. Subiyanto, S.T., M.T., Dosen Pembimbing Utama yang telah memberikan waktu, ilmu, motivasi, bimbingan, dan petunjuk dalam menyelesaikan skripsi ini.

6. Dr. Djuniadi, M.T., Dosen Wali yang telah memberikan motivasi dan semangat hingga terselesaikannya skripsi ini.
7. Feddy Setio Pribadi, S.T., M.T., yang dengan tangan terbuka memberikan masukan dan semangat hingga proses penyelesaian skripsi ini.
8. Semua pihak yang telah membantu sehingga terselesaikannya skripsi ini.

Penulis juga menyadari bahwa dalam skripsi ini masih terdapat banyak kekurangan, oleh karena itu dengan segala kerendahan hati penulis mengharapkan kritik dan saran yang membangun dalam perbaikan skripsi ini. Semoga Allah SWT memberikan pahala berlipat ganda atas bantuan dan kebaikannya. Aamiin.

Semarang, Juni 2016
Nurul Istiqamah

UNNES
UNIVERSITAS NEGERI SEMARANG

DAFTAR ISI

HALAMAN JUDUL ..... **i**

HALAMAN PERSETUJUAN PEMBIMBING ..... **ii**

HALAMAN PERNYATAAN..... **iii**

HALAMAN PENGESAHAN..... **iv**

MOTTO ..... **v**

PERSEMBAHAN..... **vi**

ABSTRAK. ..... **vii**

KATA PENGANTAR..... **viii**

DAFTAR ISI..... **x**

DAFTAR TABEL. ..... **xiv**

DAFTAR GAMBAR..... **xv**

DAFTAR LAMPIRAN. ..... **xvii**

BAB I PENDAHULUAN..... **1**

1.1. Latar Belakang. 1

1.2. Identifikasi Masalah 8

1.3. Pembatasan Masalah. 10

1.4. Perumusan Masalah 10

1.5. Tujuan Penelitian 11

1.6. Manfaat Penelitian 11

1.7. Penegasan Istilah..... 12

BAB II PUSTAKA DAN LANDASAN TEORI **14**

2.1. Tinjauan Pustaka 14

UNNES
UNIVERSITAS NEGERI SEMARANG

2.2. Landasan Teori 17

2.2.1. Pemilihan Umum 17

2.2.1.1. Pelaksanaan Pemilu di Indonesia 20

2.2.1.2. Pemungutan Suara..... 23

2.2.2. Kartu Tanda Penduduk..... 25

2.2.2.1. Aturan Penomoran NIK KTP 26

2.2.2.2. Kartu Tanda Penduduk Elektronik (KTP-el) 26

2.2.3. *Evoting* 28

2.2.3.1. Persyaratan Sistem *Evoting* 29

2.3.3.2. Kelebihan dan Kelemahan *Evoting*. 31

2.2.4. Keamanan Sistem *Evoting* 32

2.2.5. Kriptografi. 34

2.2.6. Algoritma *One Time Pad* 41

2.2.7. Algoritma SHA 256 44

2.3. Kerangka Berpikir 46

BAB III PERANCANGAN SISTEM *EVOTING*. 49

3.1. Analisis Kebutuhan 50

3.1.1. Identifikasi Kebutuhan 50

3.1.1.1. Kebutuhan Fungsional 50

3.1.1.2. Kebutuhan Non-fungsional 51

3.1.2. Identifikasi Aktor 52

3.1.3. Analisis Desain Basisdata 53

3.1.3.1. *Class Diagram* 53

UNNES
UNIVERSITAS NEGERI SEMARANG

3.2. Perancangan Sistem *Evoting* 54

3.2.1. Rancangan Alur Sistem *Evoting* 54

3.2.2. Rancangan *Usecase Diagram* 56

3.2.3. Rancangan Tampilan Antarmuka 56

3.2.3.1. Halaman Pengguna/Pemilih 57

3.2.3.2. Halaman Administrator 58

3.3. Rancangan Sistem Keamanan *Evoting* 59

3.3.1. Rancangan Keamanan Aspek Kerahasiaan 59

3.3.2. Rancangan Keamanan Aspek Otentifikasi 60

3.3.3. Rancangan Keamanan Aspek Integritas Data 60

3.3.4. Rancangan Keamanan Aspek Ketersediaan 63

3.3.5. Rancangan Keamanan Aspek Nir-penyangkalan 63

3.4. Rancangan Pengujian Sistem *Evoting* 64

BAB IV IMPLEMENTASI DAN PENGUJIAN SISTEM *EVOTING* 66

4.1. Impelementasi Sistem *Evoting* 66

4.1.1. Implementasi Antarmuka Sistem *Evoting* 66

4.2. Implementasi Keamanan Sistem *Evoting* Menggunakan Fungsi Hash dan Algoritma *One Time Pad* 73

4.2.1. Implementasi Enkripsi Fungsi Hash 73

4.2.2. Implementasi Algoritma OTP 74

4.3. Pengujian Sistem *Evoting* 75

4.3.1. Pemenuhan Kebutuhan Dasar *Evoting* 75

4.3.2. Pengujian *Prototype* 77

UNNES
UNIVERSITAS NEGERI SEMARANG

4.3.3. Pengujian Model 80

BAB V HASIL DAN PEMBAHASAN 81

5.1. Hasil Kemanan Sistem *Evoting* 81

5.1.1. Hasil Keamanan Aspek Kerahasiaan 81

5.1.2. Hasil Keamanan Aspek Otentifikasi 82

5.1.3. Hasil Keamanan Aspek Integritas Data 83

5.1.4. Hasil Kemanan Aspek Ketersediaan 84

5.1.5. Hasil Keamanan Aspek Nir-penyangkalan 85

5.2. Hasil Pengujian Sistem *Evoting* 86

5.2.1. Hasil Pemenuhan Kebutuhan Dasar *Evoting* 86

5.2.2. Hasil Pengujian *Prototype* 87

5.2.3. Hasil Pengujian Model 90

5.3. Pembahasan 94

BAB VI PENUTUP 97

5.1. Simpulan 97

5.2. Saran 97

DAFTAR PUSTAKA 99

LAMPIRAN

UNNES
UNIVERSITAS NEGERI SEMARANG

DAFTAR TABEL

Tabel 2.1. Aturan Penomoran NIK. 26

Tabel 2.2. Kelebihan dan Kelemahan *Evoting*..... 31

Tabel 2.3. Kode Biner *Plaintext* OTP 43

Tabel 2.4. Kode Biner Kunci OTP..... 43

Tabel 2.5. Daftar Informasi Algoritma Fungsi Hash 46

Tabel 3.1. Identifikasi Aktor 53

Tabel 4.1. Pemenuhan Kebutuhan Dasar *Evoting*..... 76

Tabel 4.2. Pengujian *Prototype*..... 77

Tabel 5.1. Validasi Pemenuhan Kebutuhan Dasar *Evoting* 86

Tabel 5.2. Hasil Pengujian *Prototype* 87

UNNES
UNIVERSITAS NEGERI SEMARANG

DAFTAR GAMBAR

Gambar 2.1. Pihak-pihak yang Terkait Pemilu 21

Gambar 2.2. Alur Pemungutan Suara di TPS. 24

Gambar 2.3. Skema Enkripsi dan Dekripsi 36

Gambar 2.4. Kriptografi Kunci Simetris 37

Gambar 2.5. Kriptografi Kunci Asimetris 38

Gambar 2.6. Fungsi Hash Satu Arah 39

Gambar 2.7. Fungsi Hash SHA 256 45

Gambar 2.8. Diagram Kerangka Berpikir 47

Gambar 3.1. *Class Diagram* Sistem *Evoting* 53

Gambar 3.2. Rancangan Alur Pemilihan Kandidat Sistem *Evoting* 55

Gambar 3.3. *Usecase Diagram* Sistem *Evoting* 56

Gambar 3.4. Rancangan Antarmuka Halaman Awal 57

Gambar 3.5. Rancangan Antarmuka *Login* Voter 57

Gambar 3.6. Rancangan Antarmuka Pilih Kandidat 58

Gambar 3.7. Rancangan Antarmuka *Login* Admin 58

Gambar 3.8. Rancangan Antarmuka Halaman Admin 59

Gambar 3.9. Tahap Enkripsi Pertama 61

Gambar 3.10. Tahap Enkripsi Kedua 62

Gambar 3.11. Proses Perbandingan Nilai Hash 63

Gambar 4.1. Tampilan Awal Antarmuka Sistem *Evoting* 66

Gambar 4.2. Tampilan Antarnuka *Login* User 67

Gambar 4.3. Tampilan Antarmuka Reset Password 67

Gambar 4.4. Tampilan Antarmuka Pilih Kandidat 68

Gambar 4.5. Tampilan Antarmuka *Login* Admin 68

Gambar 4.6. Tampilan Antarmuka Daftar Pemilh 69

Gambar 4.7. Tampilan Antarmuka Tambah Pemilih 70

Gambar 4.8. Tampilan Antarmuka Data Kandidat 70

Gambar 4.9. Tampilan Antarmuka Tambah Data Kandidat 71

Gambar 4.10. Tampilan Halaman Edit Data Kandidat 71

Gambar 4.11. Tampilan Antarmuka Pengaturan Batasan Waktu Pemilihan ... 72

Gambar 4.12. Tampilan Antarmuka Antarmuka Set Home..... 72

Gambar 4.13. Implementasi Enkripsi Fungsi Hash 73

Gambar 4.14. Fungsi PRNG (Pembangkitan Bilangan Acak)..... 74

Gambar 4.15. Implementasi Enkripsi Algoritma OTP..... 75

Gambar 5.1. Kotak Dialog Peringatan Tidak Memiliki Hak Pilih..... 81

Gambar 5.2. Kotak Dialog Peringatan Otentifikasi 82

Gambar 5.3. Otentifikasi Waktu Pemungutan Suara Belum Dimulai 82

Gambar 5.4. Otentifikasi Waktu Pemungutan Suara Telah Berakhir 83

Gambar 5.5. Perolehan Suara Kandidat Capres & Cawapres 83

Gambar 5.6. Diagram Batang Hasil Perhitungan Suara *Realtime* 84

Gambar 5.7. Informasi Status Pemilihan Pemilih..... 84

Gambar 5.8. Informasi Presentasedan Jumlah Surat Suara Tidak Sah 85

Gambar 5.9. Kotak Dialog Peringatan Nir-pengyangkalan 85

UNNES
UNIVERSITAS NEGERI SEMARANG

DAFTAR LAMPIRAN

Lampiran 1 *Syntax* Cetak Halaman *Live Result*

Lampiran 2 Hasil Cetak Halaman *Home*

Lampiran 3 *Syntax* Cetak Data Pemilih

Lampiran 4 Hasil Cetak Data Pemilih

Lampiran 5 Kalibrasi Nilai Hash Hasil Enkripsi Sistem *Evoting* dengan Aplikasi SHA256 Hash Generator

Lampiran 6 Kalibrasi Nilai Hash Hasil Enkripsi Sistem *Evoting* dengan Kalkulator Hash 256 secara *Online*

Lampiran 7 Tabel ASCII (*American Standard Code for Information Interchange*)

UNNES
UNIVERSITAS NEGERI SEMARANG

BAB I

PENDAHULUAN

1.1. Latar Belakang

Pemilihan umum yang berlangsung di Indonesia sejak dimulainya era reformasi menunjukkan perkembangan ke arah yang lebih baik. Tetapi tidak dapat dipungkiri bahwasanya masih terdapat banyak kekurangan dalam proses penyelenggaraannya. Sebagai negara demokrasi, berdasarkan peraturan perundang-undangan, Indonesia melaksanakan pemilu setiap lima tahun sekali. Dimana dalam pelaksanaannya hingga saat ini pada umumnya masih dilakukan secara konvensional yaitu dengan mencoblos kertas suara pada bilik yang telah disediakan di masing-masing TPS. Proses ini masih memiliki beberapa kelemahan, diantaranya yaitu: lamanya proses perhitungan suara, kurang akurat dalam hasil perhitungan suara (faktor *human error*), tidak ada salinan kertas suara, sulitnya perhitungan kembali dan besarnya anggaran yang dikeluarkan, (Rokhman: 2011).

Besarnya anggaran pemilu di Indonesia tersebut sejalan dengan data terakhir dari Komisi Pemilihan Umum, dimana pemerintah telah menyetujui anggaran pemilu di Indonesia mencapai Rp 10,4 triliun untuk pelaksanaan pemilu tahun 2009 sampai dengan tahun 2014. Anggaran yang sangat besar tersebut digunakan untuk proses pencetakan kertas suara, distribusi kertas suara, gaji panitia pengawas, dll, (Shalahuddin: 2007).

Masalah lain yang muncul pada pelaksanaan pemilu presiden pada tahun 2014 lalu adalah adanya indikasi kecurangan yang dilakukan oleh beberapa oknum dalam hal penggelembungan DPT, DPTb, DPK dan DPKTb. Di beberapa daerah di Indonesia ditemukan penggunaan DPT yang tidak wajar, karena jumlahnya melebihi 2% dari jumlah penduduk di daerah tersebut. Sehingga muncul dugaan bahwa satu orang memilih lebih dari satu kali. Tindak kecurangan ini tidak dapat dibuktikan begitu saja. Sehingga dibutuhkan solusi alternatif untuk menekan tingkat kecurangan yang terjadi terkait dengan penyalahggunaan DPT, DPTb, DPK dan DPKTb. Beberapa pakar politik di Indonesia mengungkapkan penggunaan DPTb, DPK dan DPKTb sebaiknya tidak lagi digunakan pada pemilihan umum selanjutnya, baik pada pemilihan kepala daerah dan pemilihan presiden di masa yang akan datang. Beberapa pakar ini berpendapat bahwa warga negara yang berhak terdaftar dalam DPT (Daftar Pemilih Tetap) adalah mereka yang telah memiliki KTP-el.

Pemerintah ke depannya diharapkan mulai menyiapkan strategi untuk memperbaiki kelemahan yang masih ada dalam proses penyelenggaraan pemilu. Salah satu upaya yang dapat dilakukan ialah dengan memanfaatkan perkembangan teknologi modern saat ini. Pemanfaatan teknologi yang dimaksud ialah dengan menggunakan internet sebagai media *online* untuk melakukan pemilihan umum atau lebih dikenal dengan *evoting*.

Teknologi *evoting* sendiri telah diterapkan dibeberapa negara di dunia, diantaranya adalah: Australia, Italia, Brazil, Estonia, Jepang, India, Prancis, Amerika Serikat, Filipina, (Rokhman: 2011). Salah satu negara yang berhasil

UNNES
UNIVERSITAS NEGERI SEMARANG

melaksanakan *evoting* adalah India. India, pada tahun 2003 telah melaksanakan pemilu di negara bagian menggunakan *Electronic Voting Machine* (EVMs). Alat ini juga telah digunakan pada pemilu nasional untuk memilih anggota parlemen India pada tahun 2004 dan 2009. Menurut data statistik yang bersumber dari media massa utama di India, lebih dari 400 juta pemilih (60% dari pemilih yang terdaftar) telah menggunakan hak mereka melalui EVMs pada pemilu tahun 2009.

Yang menarik, ternyata penggunaan *evoting* di Indonesia telah dilakukan dalam rentang waktu Nopember–Desember 2009 pada 31 kepala dusun (banjar) yang ada di 18 desa/kelurahan di Jembrana – Bali. Penggunaan *evoting* ini sesuai dengan putusan Mahkamah Konstitusi pada 30 Maret 2010 yang telah mengijinkan penggunaan layar sentuh atau *touch screen* atau *evoting* dalam pemilukada. Hal ini secara tidak langsung memberikan pencerahan terhadap pelaksanaan pemilu di semua jenjang, baik tingkat II, tingkat I ataupun pusat yaitu pemilu legislatif dan pemilu presiden, (Priyono: 2010).

Indonesia saat ini melalui BPPT (Badan Pengkajian dan Penerapan Teknologi) telah mengembangkan perangkat *evoting* berbasis *Direct Electronic Recording* (DRE). Perangkat ini diaktivasi melalui *smart card*, dengan *power supply* AC 220 V/DC 12 Volt, dilengkapi dengan layar LCD Display 5.7 inci. BPPT telah melakukan simulasi *evoting* di beberapa daerah di Indonesia dan hasilnya merekomendasikan agar penenarapan teknologi *evoting* dilakukan secara nasional. Beberapa daerah tersebut antara lain Pandeglang, Banda Aceh, Tegal, Gorontalo dan Pasuruan, (Laporan Pelaksanaan Tugas Tahun 2011 KPU Kabupaten Klaten: 2012).

UNNES
UNIVERSITAS NEGERI SEMARANG

Sejalan dengan hasil rekomendasi simulasi *evoting* tersebut, SETARA *Institute* sebagai salah satu lembaga survei di Indonesia pada tahun 2013 telah melakukan survei terhadap 200 Ahli Tata Negara, dimana hasil survei tersebut melaporkan tentang penguatan demokrasi elektoral sebagai berikut:

> *Dalam permohonan pengujian UU No 22 Tahun 2004 tentang UU Pemda, MK menyatakan dibolehkannya pemberian suara dengan cara evoting. Dalam perkara No. 147/PUU-VII/2009 ini Pasal 88 UU dinyatakan konstitusional bersyarat (conditionally constitutional). Hal ini menyebabkan kata 'mencoblos' diartikan pula menggunakan metode evoting dengan beberapa syarat kumulatif di antaranya tidak melanggar asas Luber (Langsung, Umum, Bebas dan Rahasia) dan Jurdil (Jujur dan Adil). Tak hanya itu, daerah yang menerapkan metode evoting sudah siap dari sisi teknologi, pembiayaan, sumber daya manusia maupun perangkat lunaknya, kesiapan masyarakat didaerah yang bersangkutan, serta persyaratan lain yang diperlukan. Jika tata cara pemberian suara hanya mencoblos maka tidak sejalan dengan Pasal 28C ayat (1) dan ayat (2) UUD 1945. Hal ini karena para Pemohon terhalang haknya memperoleh manfaat ilmu pengetahuan dan teknologi, demi meningkatkan kualitas hidupnya dan memajukan dirinya dalam memperjuangkan haknya secara kolektif untuk membangun masyarakat, bangsa, dan negaranya. Cara mencentang tidak bertentangan dengan asas-asas Pemilu yang Luber dan Jurdil tidak juga mengurangi keabsahan Pemilu karena masih dalam batas-batas yang wajar, termasuk evoting.*

UNNES
UNIVERSITAS NEGERI SEMARANG

Sesuai dengan hasil survei SETARA *Institute* tersebut, penggunaan *evoting* tidak boleh melanggar asas luber (langsung, umum, bebas, rahasia) dan jurdil (jujur dan adil), maka pengembangan *evoting* harus sesuai dengan enam asas pemilu di Indonesia yaitu:

1. Langsung, rakyat pemilih mempunyai hak untuk secara langsung memberikan suaranya sesuai dengan kehendak hati nuraninya, tanpa perantara.
2. Umum, pada dasarnya semua warga Negara yang memenuhi persyaratan minimal dalam usia yang berumur 17 tahun berhak ikut memilih dalam pemilihan umum.
3. Bebas, setiap warga Negara yang berhak memilih bebas menentukan pilihannya tanpa ada tekanan dan paksaan dari siapapun.
4. Rahasia, dalam memberikan suaranya, pemilih dijamin bahwa pilihannya tidak akan diketahui oleh pihak manapun dan dengan jalan apapun.
5. Jujur, dalam menyelenggarakan pemilihan umum, semua pihak yang terlibat harus bersikap jujur dan tidak melakukan kecurangan.
6. Adil berarti dalam menyelenggarakan pemilu, setiap pemilih mendapat perlakuan yang sama tanpa membedakan suku, agama dan ras.

Pengembangan sistem *evoting* memiliki ranah yang sangat luas untuk dikaji, penelitian ini hanya berfokus pada aspek keamanan sistem *evoting*. Untuk menjamin keamanan informasi, ada 5 aspek yang harus dipenuhi oleh semua sistem/organisasi yaitu:

1. Aspek kerahasiaan (*confidentiality*) yaitu aspek pencegahan penyingkapan informasi kepada pihak yang tidak memiliki hak terhadap informasi tersebut

UNNES
UNIVERSITAS NEGERI SEMARANG

2. Aspek keutuhan data (*data integrity*) yaitu aspek pencegahan perubahan informasi oleh pihak yang tidak memiliki otoritas untuk merubah informasi tersebut
3. Aspek ketersediaan (*availability*) yaitu aspek dimana informasi harus tersedia ketika dibutuhkan
4. Aspek otentifikasi (*authentication*) yaitu aspek yang menjamin informasi tersebut adalah asli juga untuk menjamin keabsahan orang-orang yang terlibat dalam pertukaran informasi
5. Aspek nir-penyangkalan (*non repudiation*) yaitu aspek yang menjamin agar pihak-pihak yang terlibat tidak dapat menyangkal dikemudian hari.

Salah satu cara yang dapat dilakukan untuk menjaga keamanan informasi sistem *evoting* ialah dengan menerapkan ilmu kriptografi. Kriptografi memiliki definisi yang luas, secara umum kriptogradi adalah ilmu dan seni untuk menjaga kerahasiaan berita. Pada kriptografi modern terdapat berbagai macam algoritma, secara umum kriptografi modern dikelompokkan menjadi tiga jenis yaitu: algoritma simetris, algortima asimetris, dan fungsi hash kriptografis. Penelitian ini menerapkan algoritma simetris dan fungsi hash kriptografis untuk memberi keamanan informasi pada sistem *evoting* yang dikembangkan. Algoritma simetris yang digunakan adalah algoritma *one time pad* dan fungsi hash yang digunakan adalah algoritma SHA-256.

Fungsi hash adalah fungsi yang menerima masukan string yang panjangnya sembarang kemudian mentransformasikannya menjadi string keluaran yang panjangnya tetap (nilai *hash*). Fungsi hash berisi fungsi matematika yang

menggabungkan operasi logika untuk biner, teori bilangan dan komposisi fungsi. Fungsi hash kriptografis adalah fungsi hash yang memiliki beberapa sifat keamanan tambahan sehingga dapat dipakai untuk tujuan keamanan data. Umumnya digunakan untuk keperluan autentikasi dan integritas data. Hal ini sesuai dengan kebutuhan keamanan informasi untuk otentifikasi dan integritas data sistem *evoting*. Algoritma SHA-256 sebagai algoritma SHA generasi kedua digunakan dalam penelitian ini sebab pada algoritma SHA generasi pertama masih ditemukan adanya bentrokan (*collision*) nilai *hash* dari masukan string yang berbeda.

Sementara algoritma OTP merupakan algoritma berjenis kunci simetris, artinya bahwa kunci yang digunakan untuk melakukan enkripsi dan dekripsi merupakan kunci yang sama. Dalam proses enkripsi, algoritma ini menggunakan cara *stream cipher* dimana *ciphertext* berasal dari hasil XOR antara bit *plaintext* dan bit kunci. Sebagai tambahan, algoritma ini sering digunakan dalam proses enkripsi *cookie* (termasuk pemrosesan transaksi *online* menggunakan kartu kredit) karena prosesnya yang relatif mudah. Operasi XOR dilakukan dengan terlebih dahulu mengubah karakter *plaintext* dan kunci ke dalam bentuk biner. Kekuatan algoritma OTP terletak pada penggunaan kunci yang sepenuhnya acak, dalam penelitian ini pembangkitan kunci bilangan acak menggunakan algoritma PRNG (*Pseudo Random Number Generator*) dan masing-masing pemilih memiliki kunci OTP yang berbeda-beda. Sehingga satu kunci hanya digunakan untuk satu orang pemilih.

UNNES
UNIVERSITAS NEGERI SEMARANG

Hingga saat ini algoritma OTP merupakan salah satu algoritma kriptografi yang tidak dapat dipecahkan, dengan syarat beberapa kondisi: proses enkripsi menggunakan operasi XOR (sifat sama dengan operasi modulo), kunci yang digunakan merupakan bilangan yang sepenuhnya acak, *plaintext* dan kunci memiliki panjang yang sama, setiap kunci hanya digunakan sekali kemudian dimusnahkan setelah dipakai, (Rijmenants: 2014).

Untuk mengetahui apakah sistem yang dikembangkan telah memenuhi kebutuhan-kebutuhan *evoting*, dilakukan proses pengujian sistem dalam tiga tahapan yakni: pemenuhan kebutuhan dasar sistem *evoting*, pengujian *prototype* dan pengujian model. Pengujian *prototype* dilakukan untuk mengetahui apakah sistem yang dikembangkan telah sesuai dengan hasil yang diharapkan dengan melihat hasil eksekusi program melalui *test case* (kasus uji) yang dibuat. Sementara pengujian model dilakukan untuk mengetahui apakah sistem telah memenuhi kebutuhan fungsional dan non-fungsional sistem *evoting*.

Melalui berbagai permasalahan dan rancangan metode yang dikembangkan dalam penelitian ini, maka penulis memilih mengadakan penelitian dengan judul, "Sistem Keamanan *Evoting* Menggunakan Fungsi Hash dan Algoritma *One Time Pad*" sebagai penerapan kriptografi untuk keamanan sistem *evoting*.

1.2. Identifikasi Masalah

Identifikasi masalah atau ruang lingkup dari penelitian ini adalah sebagai berikut:

1. Model *evoting* yang dihasilkan adalah *evoting* berbasis web dan spesifik untuk pemilihan umum di Indonesia
2. Program *evoting* yang dirancang menggunakan studi kasus pemilihan umum presiden dan wakil presiden
3. Beberapa kelemahan pemilu konvensional yang ingin diatasi dalam penelitian ini antara lain:
   a. Kurang akuratnya hasil perhitungan suara yang disebabkan oleh faktor *human error*
   b. Sulitnya perhitungan kembali jika terjadi ketidak percayaan terhadap hasil perhitungan suara
   c. Potensi tindak kecurangan, seperti: penggelumbangan suara, pencoblosan ganda dan kurangnya transparansi
   d. Tingginya jumlah surat suara tidak sah
   e. Besarnya anggaran yang dikeluarkan untuk melakukan proses pemungutan suara
4. Sistem *evoting* yang dikembangkan dimulai dari tahap pemungutan suara sampai dengan perhitungan suara.
5. Fokus utama dalam penelitian ini adalah pengembangan sistem keamanan *evoting* yang diterapkan untuk menjaga proses pemungutan suara hingga proses perhitungan suara secara *realtime*
6. Sistem keamanan yang dikembangkan menggunakan fungsi hash kriptografis dengan algoritma SHA-256 dan kriptografi kunci simetris dengan algoritma *one time pad*

UNNES
UNIVERSITAS NEGERI SEMARANG

1.3. Pembatasan Masalah

Berdasarkan identifikasi masalah yang diuraikan, maka berikut dibuat beberapa batasan masalah:

1. Keamanan sistem *evoting* dalam penelitian ini terkait lima aspek, diantaranya: aspek integritas, aspek otentifikasi, aspek ketersediaan, aspek kerahasiaan, aspek nir-penyangkalan
2. Aspek integritas data dalam penelitian ini hanya berfokus pada keamanan hasil pemungutan suara
3. Penelitian ini bertujuan untuk mengembangkan sistem *evoting* pada pemilihan presiden dan wakil presiden yang diterapkan melalui simulai pada lingkungan terbatas
4. Pengujian sistem dilakukan dengan cara pemenuhan kebutuhan *evoting* yang telah diidentifikasi terlebih dahulu

1.4. Perumusan Masalah

Berdasarkan latar belakang yang dipaparkan di atas rumusan masalah dari penelitian ini adalah:

1. Mampukah sistem *evoting* membantu mengurangi kelemahan pelaksanaan pemilu konvensional di Indonesia?
2. Apakah implementasi kriptografi fungsi hash dan algoritma *one time pad* dapat digunakan untuk pengembangan sistem keamanan *evoting* yang sesuai dengan enam asas pemilu di Indonesia?

UNNES
UNIVERSITAS NEGERI SEMARANG

3. Apakah hasil pengujian sistem *evoting* yang dikembangkan telah memenuhi kebutuhan dan aspek keamanan sistem *evoting*?

1.5. Tujuan Penelitian

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

1. Merancang sistem *evoting* guna mengurangi beberapa kelemahan pelaksanaan pemilu konvensional.
2. Merancang sistem keamanan *evoting* menggunakan kriptografi fungsi hash dan algoritma *one time pad* dengan tetap berlandaskan pada enam asas pemilu di Indonesia.
3. Merancang pengujian sistem *evoting* untuk mengetahui bahwa sistem yang dikembangkan telah memenuhi kebutuhan dan aspek keamanan sistem *evoting*.

1.6. Manfaat Penelitian

Manfaat dari penelitian ini adalah sebagai berikut:

1. Bagi Penulis:
   a. Menerapakan ilmu yang telah diperoleh
   b. Mendapatkan pemahaman tentang sistem *evoting*
   c. Mendapatkan pemahanan tentang kriptografi
2. Bagi pengguna, melalui penelitian ini diharapkan dapat menjadi salah satu referensi dalam pengembangan sistem keamanan *evoting* di Indonesia.

UNNES
UNIVERSITAS NEGERI SEMARANG

1.7. Penegasan Istilah

Penegasan istilah diperlukan untuk memberikan gambaran yang lebih jelas untuk menyatukan pengertian berdasarkan beberapa istilah yang terdapat dalam penulisan dengan judul "Sistem Keamanan *Evoting* Menggunakan Fungsi Hash dan Algoritma *One Time Pad*".

a. *Evoting*, suatu sistem pemilihan dimana data dicatat, disimpan, dan diproses dalam bentuk informasi digital. *Evoting* pada hakekatnya adalah pelaksanaan pemungutan suara yang dilakukan secara elektronik (digital) mulai dari proses pendaftaran pemilih, pelaksanaan pemilihan, penghitungan suara, dan pengiriman hasil suara, (Rokhman: 2011).

b. KTP-el adalah KTP yang memiliki spesifikasi dan format KTP nasional dengan sistem pengamanan khusus yg berlaku sebagai identitas resmi yang diterbitkan oleh Dinas Kependudukan dan Pencatatan Sipil Kab/Kota.

c. Kriptografi, secara umum adalah ilmu dan seni untuk menjaga kerahasiaan berita. Pengertian lainnya, kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data dan autentikasi data.

d. Enkripsi, teknik untuk mengacak suatu pesan agar tidak dapat diketahui maknanya.

e. *Database*, atau basisdata adalah kumpulan data yang disimpan secara sistematis di dalam komputer yang dapat diolah atau dimanipulasi menggunakan perangkat lunak (program aplikasi) untuk menghasilkan informasi. Pendefinisian basis data meliputi spesifikasi berupa tipe data,

UNNES
UNIVERSITAS NEGERI SEMARANG

struktur data dan juga batasan-batasan data yang akan disimpan. Basis data merupakan aspek yang sangat penting dalam sistem informasi dimana basis data merupakan gudang penyimpanan data yang akan diolah lebih lanjut.

f. Fungsi hash, yang juga sering disebut fungsi hash satu arah (*One-Way Function*), *message digest*, *fingerprint*, fungsi kompresi, dan *Message Authentication Code* (MAC), merupakan fungsi matematika yang mengambil masukan panjang variabel dan mengubahnya ke dalam urutan biner dengan panjang yang tetap.

g. Fungsi hash kriptografis, fungsi hash yang memiliki beberapa sifat keamanan tambahan sehingga dapat dipakai untuk tujuan keamanan data.

h. Algortima *One Time Pad* (OTP), merupakan salah satu jenis kriptografi kunci simetris dengan metode *stream cipher*. Artinya, kunci yang digunakan untuk proses enkripsi-dekripsi adalah kunci yang sama. Dimana proses enkripsi-dekripsi dilakukan dengan operator logika XOR (*Exlusive OR*).

UNNES
UNIVERSITAS NEGERI SEMARANG

BAB II

PUSTAKA DAN LANDASAN TEORI

2.1. Tinjauan Pustaka

Berdasarkan studi literatur yang telah dilakukan, penulis memperoleh beberapa literatur terkait penelitian sebelumnya yang telah merancang berbagai sistem dengan penerapan kriptografi di dalamnya untuk keamanan data pada sistem yang mereka kembangkan.

Shalahuddin pada tahun 2009 telah merancang sebuah sistem *evoting* dengan studi kasus pemilu legislatif dan presiden di Indosesia dengan harapan bahwa model *evoting* berbasis web yang dibuatnya mampu memenuhi syarat untuk menggantikan pemilihan umum secara konvensional yang selama ini digunakan di Indonesia. Untuk menjaga keamanan identitas pemilih dalam *evoting*, Shalahuddin menggunankan modul *anonymizer* untuk menyamarkan identitas pemilih. Modul *anonymizer* ini akan memberikan nomor acak dan unik sebagai bukti bahwa seseorang telah melakukan pemilihan dan kemudian nomor tersebut yang akan disimpan ke dalam basis data.

Abdulhamid dkk, pada April 2013 telah membuat rancangan sistem *evoting* berbasis web untuk penyelenggaraan pemilu di Nigeria. Program-program yang digunakan untuk membangun sistem ini antara lain PHP, MySQL, Java Query, CSS dan HTML. Tujuan pembuatan sistem *evoting* ini sebagai salah satu alternatif pengganti pemilu yang masih dilakukan secara konvensional di Nigeria yang dianggap memiliki banyak kelemahan. Dalam sistem ini mereka yang dapat

melakukan pemilihan adalah mereka yang telah memiliki *Voter's Card* sebagai bukti telah melakukan registrasi sebelumnya. Keamanan identitas pemilih dilakukan dengan enkripsi data menggunakan fungsi hash kriptografis algoritma SHA-1.

Olaniye dkk, pada November 2013 telah merancang sebuah sistem *evoting* berbasis web yang bisa di akses melalui komputer dan ponsel untuk pelaksanaan pemilu di Nigeria. Sistem *evoting* yang dibangun bertujuan untuk meningkatkan keamanan hasil perhitungan suara agar tidak di *hack* selama proses pengiriman sebelum sampai ke database server. Suara hasil pemilihan di enkripsi menjadi dua bagian. Enkripsi pertama segera di hash dengan algoritma SHA256. Sementara enkripsi kedua menggunakan algortima RSA dengan nilai *private key* tertentu. Ketika enkripsi kedua telah sampai ke server, hasil suara ini lalu di dekripsi ke nilai awal dan selanjutnya di enkripsi kembali dengan algoritma SHA 256. Perhitungan suara akan otomatis dilakukan oleh sistem jika enkripsi pertama dan enkripsi kedua bernilai persis sama. Jika ternyata hasil perbandingan keduanya tidak sama, berarti telah terjadi kemungkinan bahwa suara berhasil di *hack* ketika proses pengiriman suara berlangsung. Dan tidak akan dilakukan perhitungan untuk suara ini karena suara dianggap tidak sah.

UNNES
UNIVERSITAS NEGERI SEMARANG

Lukas, penelitian yang dikembangkannya pada tahun 2007 dengan judul Analisis Waktu Enkripsi-Dekripsi File Text Meggunakan Metode *One Time Pad* dan Rivest, Shamir, Adleman (RSA) bertujuan untuk mengetahui perbandingan kecepatan waktu enkripsi-dekripsi pada metode OTP dan RSA. Hasil penelitian yang diperoleh membuktikan bahwa proses enkripsi-dekripsi pada metode OTP

untuk file berukuran kecil membutuhkan waktu yang relatif lebih cepat dibandingkan dengan metode RSA.

Neyman dkk pada tahun 2013 merancang sebuah penelitian yang berjudul Penerapan Sistem *Evoting* pada Pemilihan Kepala Daerah di Indonesia. Pada sistem *evoting* yang mereka kembangkan penggunaan kriptografi yang diterapkan untuk menjaga keamanan sistem *evoting* ialah menggunakan kriptografi kunci asimetris yaitu algoritma RSA dan kriptografi kunci simetris yaitu algoritma *twofish*. RSA dipilih dalam penelitian ini karena algoritma tersebut banyak digunakan untuk aplikasi yang membutuhkan keamanan data digital. Algoritma *twofish* dipergunakan dalam sistem ini untuk enkripsi kunci privat. Penelitian ini bertujuan untuk mengembangkan sistem *evoting* pada pemilihan kepala daerah di Indonesia dengan melakukan simulasi pada lingkungan terbatas. Pada penelitian ini simulasi sistem dibatasi pada pembuatan sistem berbasis *desktop*, dan belum melakukan keamanan pada kerahasiaan isi basisdata sistem.

Dyah Ayu Marhaeningtyas Galuh Wisnu dalam penelitiannya yang berjudul Rancang Bangun Sistem *Evoting* Dengan Menerapkan Hash dan Digital *Signature* Untuk Verifikasi Data Hasil Voting menjelaskan bahwa untuk membangun suatu sistem *evoting* yang aman diperlukan untuk memenuhi semua aspek keamanan komputer yang meliputi: *privacy*, *integrity*, *authentication*, dan *availability*. Dalam penelitiannya hanya berfokus pada aspek *integrity*. Sehingga pada pengerjaannya hanya memfokuskan bagaimana mengimplementasikan suatu sistem yang dapat menjaga integritas data. Pada kasus *evoting*, integritas data

UNNES
UNIVERSITAS NEGERI SEMARANG

dibutuhkan ketika melakukan pengiriman hasil voting dari tempat pemungutan suara ke pusat pemungutan suara. Untuk mengatasinya diselesaikan dengan adanya proses *hashing* dan *digital signature*. Proses *hashing* akan membantu untuk mendeteksi ada atau tidaknya perubahan yang dilakukan pada file yang terkirim. Sedangkan *digital signature* akan digunakan untuk mengetahui apakah file yang terkirim berasal dari pengirim yang bersangkutan atau tidak.

2.2. Landasan Teori

2.2.1 Pemilihan Umum

Pemilihan umum, selanjutnya disebut pemilu, adalah sarana pelaksanaan kedaulatan rakyat yang dilaksanakan secara langsung, umum, bebas, rahasia, jujur, dan adil dalam Negara Kesatuan Republik Indonesia berdasarkan Pancasila dan Undang-Undang Dasar Negara Republik Indonesia, (Peraturan KPU No 10 Tahun 2012 Tentang Pemantau dan Tata Cara Pemantauan Pemilu Anggota DPR, DPD, dan DPRD Tahun 2014).

Sementara, Pemilihan Umum Presiden dan Wakil Presiden, selanjutnya disebut Pemilu Presiden dan Wakil Presiden, adalah pemilihan umum untuk memilih Presiden dan Wakil Presiden dalam Negara Kesatuan Republik Indonesia berdasarkan Pancasila dan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, (Undang-Undang Republik Indonesia Nomor 42 Tahun 2008 Tentang Pemilihan Umum Presiden Dan Wakil Presiden).

Pemilu Presiden dan Wakil Presiden dilaksanakan secara efektif dan efisien berdasarkan asas langsung, umum, bebas, rahasia, jujur, dan adil, (Pasal 2

Bab 11 UU No. 42 Tahun 2008). Pemilu Presiden dan Wakil Presiden dilaksanakan setiap 5 (lima) tahun sekali. Pemilu Presiden dan Wakil Presiden dilaksanakan di seluruh wilayah Negara Kesatuan Republik Indonesia sebagai satu kesatuan daerah pemilihan. Pemungutan suara dilaksanakan secara serentak pada hari libur atau hari yang diliburkan, (Pasal 3 Bab III UU No. 42 Tahun 2008).

Sebagaimana pula telah diatur dalam Undang-Undang bahwa tugas penyelenggara pemilu diberikan kepada Komisi Pemilihan Umum dengan tugas dan wewenang yang telah ditetapkan. Pelaksanaan pemilu secara langsung di Indonesia dimulai sejak jaman reformasi yakni pada tahun 1998. Hingga sampai saat ini Indonesia terhitung telah melakukan 5 kali pemilu secara langsung dimana proses pemilihannya dilakukan melalui pencoblosan kertas suara.

Proses pemilu di Indonesia dibagi dalam beberapa tahapan yakni dimulai dari proses pendaftaran pemilih, pelaksanaan pemilihan, penghitungan suara dan pengiriman hasil perhitungan suara. Warga yang berhak melakukan pemilihan umum adalah mereka yang telah terdaftar dalam Daftar Pemilih Tetap, Daftar Pemilih Tambahan, Daftar Pemilih Khusus dan Daftar Pemilih Khusus Tambahan. Secara berurutan dijelaskan mengenai keempat jenis daftar pemilih tersebut dalam Peraturan Komisi Pemilihan Umum No. 26 Tahun 2013 pada Bab I Pasal 1 ayat 22, 23, 24 dan ayat 25. Berikut penjelasan mengenai DPT, DPTb, DPK dan DPKTb:

1. Ayat 22: Daftar Pemilih Tetap, selanjutnya disingkat DPT, adalah susunan nama penduduk Warga Negara Indonesia yang telah memenuhi syarat

sebagai Pemilih berdasarkan undang-undang dan berhak menggunakan haknya untuk memberikan suara di TPS dalam Pemilu Anggota DPR, DPD, DPRD Provinsi/DPRA/DPRP/DPRPB dan DPRD Kabupaten/Kota/DPRK.

2. Ayat 23: Daftar Pemilih Tambahan selanjutnya disingkat DPTb, adalah susunan nama penduduk Warga Negara Indonesia yang telah memenuhi syarat sebagai Pemilih berdasarkan Undang-Undang dan telah terdaftar dalam DPT tetapi karena keadaan tertentu tidak dapat menggunakan hak pilihnya untuk memberikan suara di TPS tempat Pemilih yang bersangkutan terdaftar dalam DPT dan memberikan suara di TPS lain.
3. Ayat 24: Daftar Pemilih Khusus selanjutnya disingkat DPK, adalah susunan nama penduduk Warga Negara Indonesia yang telah memenuhi syarat sebagai Pemilih berdasarkan Undang-Undang tetapi tidak memiliki identitas kependudukan dan/atau memiliki identitas kependudukan tetapi tidak terdaftar dalam Daftar Pemilih Sementara (DPS), Daftar Pemilih Sementara Hasil Perbaikan (DPSHP), Daftar Pemilih Tetap (DPT), atau Daftar Pemilih Tambahan (DPTb).
4. Ayat 25: Daftar Pemilih Khusus Tambahan selanjutnya disingkat DPKTb, adalah susunan nama penduduk Warga Negara Indonesia yang telah memenuhi syarat sebagai Pemilih berdasarkan undang-undang dan memiliki kartu tanda penduduk atau Identitas Lain atau Paspor tetapi tidak terdaftar dalam DPT, DPTb atau DPK, dan memberikan suara di TPS pada Hari dan tanggal pemungutan suara menggunakan Kartu Tanda Penduduk dan Kartu Keluarga atau Paspor atau Identitas lain.

UNNES
UNIVERSITAS NEGERI SEMARANG

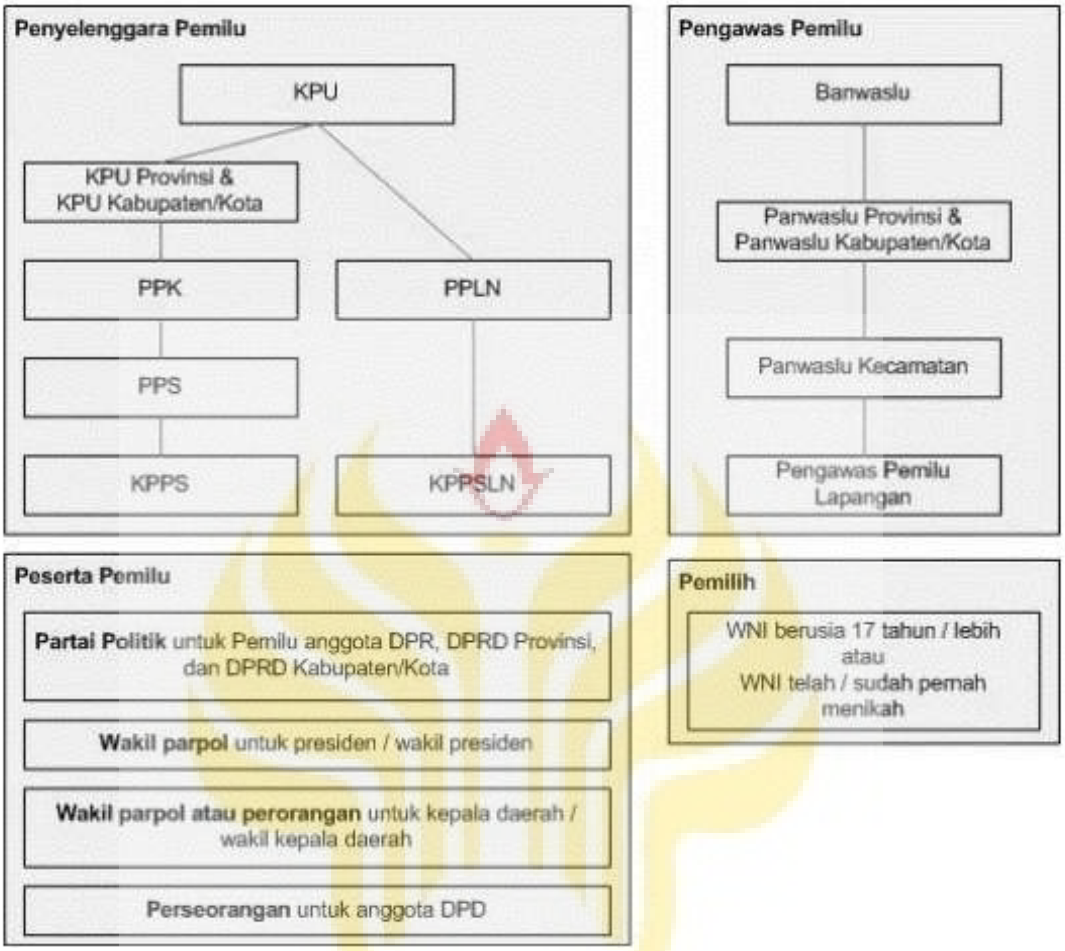
2.2.1.1. Pelaksanaan Pemilu di Indonesia

Pelaksanaan pemilu di Indonesia diselenggarakan dalam beberapa tahapan sebagai berikut:

1. Pemutakhiran data pemilih dan penyusunan daftar pemilih
2. Pendaftaran peserta pemilu
3. Penetapan peserta pemilu
4. Penetapan jumlah kursi dan penetapan daerah pemilihan
5. Pencalonan Presiden dan Wakil Presiden
6. Masa kampanye
7. Masa tenang
8. Pemungutan dan penghitungan suara
9. Penetapan hasil pemilu
10. Pengucapan sumpah/janji calon presiden dan wakil presiden terpilih

Pelaksanaan pemilu di Indonesia melibatkan beberapa pihak. Gambar 2.1. berikut menunjukkan pihak-pihak yang terkait dengan pelaksanaan pemilu sesuai dengan Undang-Undang Nomor 22 Tahun 2007 Tentang Penyelenggaraan Pemilihan Umum.

UNNES
UNIVERSITAS NEGERI SEMARANG



Gambar 2.1. Pihak-pihak yang terkait Pemilu

Berikut ini adalah penjelasan setiap bagian pada Gambar 2.1. mengenai pihak-pihak yang terkait pemilu:

1. Komisi Pemilihan Umum (KPU) adalah lembaga penyelenggara Pemilu yang bersifat nasional, tetap dan mandiri.
2. KPU Provinsi dan KPU Kabuoaten/Kota adalah penyelenggara Pemilu di tingkat provinsi dan kabupaten/kota.
3. Panitia Pemilihan Kecamatan (PPK) adalah panitia yang dibentuk oleh KPU Kabupaten/Kota untuk menyelenggarakan Pemilu di tingkat kecamatan.

4. Panitia Pemungutan Suara (PPS) adalah panitia yang dibentuk oleh KPU Kabupaten/Kota untuk menyelenggarakan Pemilu di tingkat desa/kelurahan.
5. Panitia Pemilihan Luas Negeri (PPLN) adalah panitia yang dibentuk oleh KPU untuk menyelenggarakan Pemilu di luar negeri.
6. Kelompok Penyelenggara Pemungutan Suara (KPPS) adalah kelompok yang dibentuk oleh PPS untuk menyelenggarakan pemungutan suara di tempat pemungutan suara.
7. Kelompok Penyelenggara Pemungutan Suara Luar Negeri (KPPSLN) adalah kelompok yang di bentuk oleh PPLN untuk menyelenggarakan pemungutan suara di tempat pemungutan suara di luar negeri.
8. Badan Pengawas Pemilu (Banwaslu) adalah badan yang bertugas mengawasi penyelenggaraan Pemilu di seluruh Indonesia.
9. Panitia Pengawas Pemilu (Panwaslu) Provinsi dan Panwaslu Kabupaten/Kota bertugas untuk mengasawasi penyelenggaraan Pemilu di tingkat provinsi dan kabupaten/kota.
10. Panwaslu Kecamatan adalah panitia yang dibentuk oleh Panwaslu Kabupaten/Kota untuk mengawasi penyelenggaraan Pemilu di desa/kelurahan.
11. Pengawas Pemilu Lapangan adalah petugas yang dibentuk oleh Panwaslu Kecamatan untuk mengawasi penyelenggaraan Pemilu di desa/kelurahan.
12. Pemilih adalah warga negara Indonesia yang telah berusia 17 tahun atau lebih atau sudah pernah menikah dan tidak sedang dicabut hak pilihnya.
13. Peserta Pemilu ada beberapa macam.

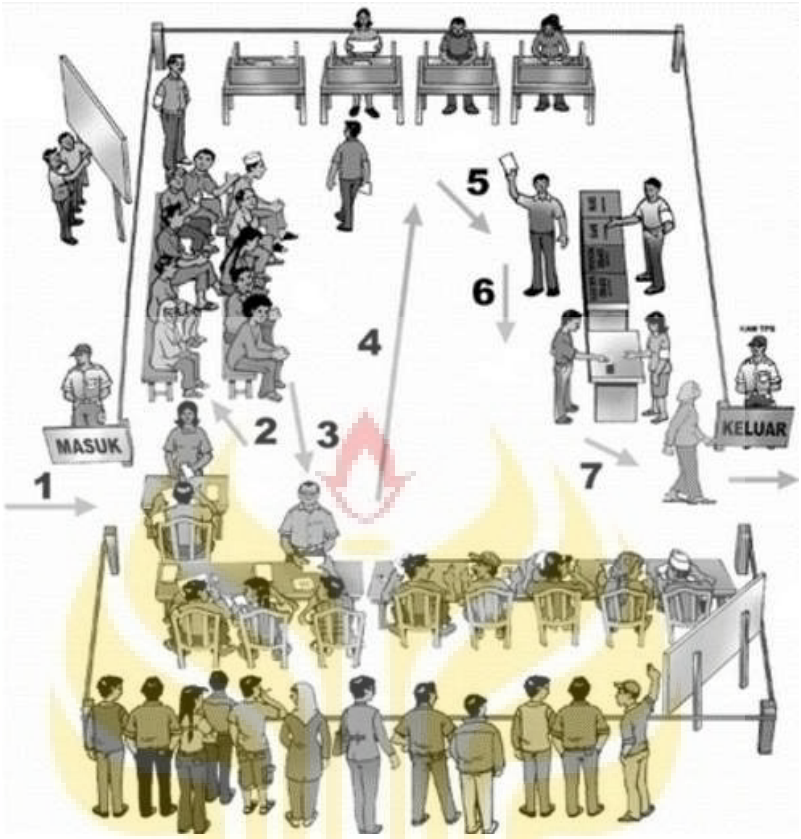
UNNES
UNIVERSITAS NEGERI SEMARANG

a. Pada pemilihan anggota DPR, DPRD tingkat 1 dan DPRD tingkat 2 peserta Pemilu adalah partai politik
b. Pada Pemilu anggotan DPD, peserta Pemilu adalah perorangan.
c. Pada Pemilu presiden/wakil presiden, peserta Pemilu adalah wakil partai politik
d. Sedangkan pada pemilihan kepala daerah/wakil kepala daerah, peserta Pemilu adalah wakil partai politik atau perorangan.

2.2.1.2. Pemungutan Suara

Pemungutan suara (*voting*) adalah salah satu tahapan 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. Untuk mempermudah pemahaman mengenai alur pemungutan suara berikut disajikan pada ilustrasi Gambar 2.2.

UNNES
UNIVERSITAS NEGERI SEMARANG



Gambar 2.2. Alur Pemungutan Suara di TPS

Berikut uraian alur pemungutan suara sebagaimana dimaksud:

1. Pemilih yang telah menerima pemberitahuan (undangan), maupun pemilih dengan identitas datang ke TPS dan kemudian mendaftarkan diri kepada petugas KPPS;
2. Setelah didaftarkan, pemilih dipersilakan untuk menunggu antrian;
3. KPPS akan memanggil pemilih (sesuai dengan antrian) untuk menerima surat suara. Jika pemilih menerima surat suara dalam kondisi rusak maka pemilih berhak mendapatkan penggantian surat suara;

UNNES
UNIVERSITAS NEGERI SEMARANG

4. Pemilih yang telah mendapatkan surat suata, kemudian menuju bilik suara untuk melakukan pemilihan dengan cara mencoblos pilihannya pada surat suara;
5. Setelah selesai memberikan suara, kemudian pemilih menuju bilik suara untuk melakukan pemilihan dengan cara mencoblos pilihannya pada suat suara yang telah diterima;
6. Pemilih menuju pemberian tanda dalam bentuk tinta, sebagai penanda bahwa pemilih yang bersangkutan telah melaksanakan pemungutan suara; dan
7. Pemilih yang telah selesai melaukan seluruh proses pemungutan suara dipersilakan untuk meninggalkan area Tempat Pemungutan Suara (TPS).

2.2.2 Kartu Tanda Penduduk

Berdasarkan Undang-Undang Republik Indonesia Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan, Kartu Tanda Penduduk yang selanjutnya disingkat KTP adalah identitas resmi Penduduk sebagai bukti diri yang diterbitkan oleh Instansi Pelaksana yang berlaku di seluruh wilayah Negara Kesatuan Republik Indonesia. Identitas yang terdapat pada KTP antara lain ialah Nomor Induk Kependudukan, Nama, Tempat/Tanggal Lahir, Jenis Kelamin, Alamat (RT/RW, Kel/Desa, Kecamatan), Agama, Status Perkawinan, Pekerjaan, Kewarganegaraan dan Tanggal Kadaluarsa KTP.

Nomor Induk Kependudukan bersifat unik, khas, tunggal, dan melekat selamanya yang diberikan oleh Pemerintah dan diterbitkan oleh Instansi Pelaksana kepada setiap Penduduk setelah dilakukan pencatatan biodata. Nomor Induk Kependudukan ini dijadikan dasar penerbitan paspor, suart izin

mengemudi, nomor pokok wajib pajak, polis asuransi, sertifikat hak atas tanah, dan penerbitan dokumen identitas lainnya.

2.2.2.1 Aturan Penomoran NIK Kartu Tanda Penduduk

Angka-ankga yang tertera pada Nomor Induk Kependudukan yang melekat pada Kartu Tanda Penduduk maupun pada Akta Kelahiran memiliki fungsinya masing-masing. Nomor induk kependudukan ini bersifat unik, khas, tunggal, dan melekat selamanya, yang diberikan negara kepada penduduk. Nomor Induk Kependudukan terdiri dari 16 digit angka, aturan penomoran NIK disajikan pada Tabel 2.1. di bawah ini:

Tabel 2.1. Aturan Penomoran Nomor Induk Kependudukan

AA (1-2)	Kode provinsi dimana NIK diterbitkan
BB (3-4)	Kode kabupaten/kota dimana NIK diterbitkan. Angka lebih dari 70 menandakan kota
CC (5-6)	Kode kecamatan dimana NIK diterbitkan
DD (7-8)	Tanggal lahir. Jika perempuan, maka tanggal lahir ditambah 40
EE (9-10)	Bulan lahir
FF (11-12)	Dua angka terakhir tahun lahir
GGGG (13-16)	Nomor urut penduduk mulai dari 0001-9999. Berurut sesuai dengan 12 angka sebelumnya

2.2.2.2 Kartu Tanda Penduduk Elektronik (KTP-el)

Berdasarkan Peraturan Presiden Tentang Perubahan Kedua Atas Peraturan Presiden Nomor 112 Tahun 2013 Tentang Perubahan Keempat Atas Peraturan Presiden Nomor 26 Tahun 2009 Tentang Penerapan Kartu Tanda Penduduk Berbasis Nomor Induk Kependudukan Secara Nasional, KTP

elektronik yang selanjutnya disingkat KTP-el adalah Kartu Tanda Penduduk yang dilengkapi cip yang merupakan identitas resmi penduduk sebagai bukti diri yang diterbitkan oleh Instansi Pelaksana.

Selanjutnya pada Pasal 10 A dijelaskan lebih lanjut bahwa KTP elektronik merupakan KTP yang dilengkapi dengan cip berisi rekaman elektronik dan berlaku secara nasional di seluruh wilayah Negara Kesatuan Republik Indonesia. Lebih rinci pada Pasal 10B dijelaskan bahwa:

(1) KTP elektronik sebagaimana dimaksud dalam Pasal 10A merupakan:

1. Identitas resmi bukti domisili penduduk;
2. Bukti diri penduduk untuk pengurusan kenpentingan yang berkaitan dengan administrasi pemerintahan;
3. Bukti diri penduduk untuk pengurusan kepentingan pelayanan publik di Instansi Pemerintah, Pemerintah Daerah, Lembaga Perbankan, dan Swasta yang berkaitan dengan dan tidak terbatas pada Perizinan, Usaha, Perdagangan, Jasa Perbankan, Asuransi, Perpajakan dan Pertanahan.

Manfaat KTP elektronik atau KTP-el dibagi menjadi dua, yaitu:

1. Manfaat bagi negara, untuk perencanaan pembangunan, akses pelayanan publik, data dan statistik kependudukan, keamanan negara, demokrasi (pemilu dan pilkada), dan mencegah penyalah gunaan dokumen kependudukan, tindak terorisme dan pekerja ilegal; dan
2. Manfaat bagi penduduk, sebagai dasar penerbitan dokumen lain seperti; Paspor, SIM, NPWP, Polis Asuransi, Sertifikat Hak Atas Tanah, Dokumen Identitas lainnya.

UNNES
UNIVERSITAS NEGERI SEMARANG

2.2.3 *Evoting*

Pesatnya perkembangan teknologi mulai diaplikasikan pada proses demokrasi di berbagai belahan negara di dunia. Pemilu konvensional yang umumnya digunakan dalam pemungutan suara baik untuk pemilihan kepala daerah maupun kepala negara mulai ditinggalkan oleh beberapa negara. Dengan alasan beberapa kelemahan yang dimiliki pemilu konvensional seperti yang telah dipaparkan sebelumnya. Proses pemilihan umum dewasa ini mulai memanfaatkan kemajuan iptek terutama pemanfaatan jaringan internet untuk proses pemungutan suara secara *online*, selanjutnya sistem ini biasa dikenal dengan beberapa istilah seperti *online voting* dan *electronic voting* atau disingkat *evoting*.

Evoting adalah suatu sistem pemilihan dimana data dicatat, disimpan, dan diproses dalam bentuk informasi digital. Sementara menurut International IDEA (2011) *evoting* adalah sistem pencatatan, pemberian suara atau pemilihan suara dalam pemilu politik dan referendumnya yang melibatkan teknologi informasi dan komunikasi. *Evoting* pada hakekatnya adalah pelaksanaan pemungutan suara yang dilakukan secara elektronik (digital) mulai dari proses pendaftaran pemilih, pelaksanaan pemilihan, penghitungan suara, dan pengiriman hasil suara, (Rokhman: 2011).

Menurut International IDEA (2011), pelaksanaan *evoting* secara umum dikategorikan ke dalam empat tipe sebagai berikut:

1. Mesin pemungutan suara dengan pencatatan elektronik langsung (DRE). DRE bisa disertai atau tidak disertai jejak data dokumen (jejak data dokumen

audit pemilih yang dapat diverifikasi/VVPAT). VVPAT ditunjukan untuk menyediakan bukti fisik dari suara yang diberikan.

2. Sistem OMR yang didasarkan pada mesin pemindai dapat mengenali pilihan pemilih di surat suara yang dapat dibaca oleh mesin khusus. Sistem OMR digunakan sebagai pusat sistem penghitungan (tempat surat suara dipindai dan dihitung di pusat penghitungan khusus) atau sistem pemindaian optik perhitungan terbatas (PCOS, saat pemindaian dan penghitungan dilaksanakan di TPS, secara langsung segera setelah pemilih memasukkan surat suara mereka ke mesin penghitungan suara).
3. Mesin pencetak surat suara (EBP), perangkat yang serupa dengan mesin DRE yang menghasilkan kertas yang dapat dibaca mesin atau koin elektronik yang berisikan pilihan pemilih. Koin ini dimasukkan ke pemindai surat suara terpisah yang melakukan penghitungan suara otomatis.
4. Sistem pemilihan melalui internet yaitu saat suara diberikan melalui internet ke server pusat penghitungan. Suara dapat diberikan baik melalui komputer umum ataupun dari bilik pemungutan suara di TPS atau—yang lebih umum—dari komputer mana pun yang terkoneksi internet yang dapat diakses pemilih.

UNNES
UNIVERSITAS NEGERI SEMARANG

2.2.3.1 Persyaratan Sistem *Evoting*

Penelitian terkait *evoting* masih terus dilakukan hingga sekarang. Terdapat berbagai macam teknologi yang digunakan dalam mengembangkan *evoting* tersebut. Setiap sistem *evoting* yang dikembangkan harus memenuhi beberapa persyaratan berikut ini:

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.

UNNES
UNIVERSITAS NEGERI SEMARANG

2.2.3.2 Kelebihan dan Kelemahan *Evoting*

Selain memiliki kelebihan-kelebihan tidak dapat dipungkiri bahwa terdapat pula kelemahan pada *evoting*. Berikut disajikan dalam Tabel 2.2. kelebihan dan kelemahan pada sistem *evoting*.

Tabel 2.2. Kelebihan dan Kelemahan *Evoting*

No.	Kelebihan	Kelemahan
1.	Penghitungan dan tabulasi suara lebih cepat	Kurangnya transparansi
2.	Hasil lebih akurat karena kesalahan manusia diabaikan	Terbatasnya keterbukaan dan pemahaman sistem bagi yang bukan ahlinya
3.	Penanganan yang efisien dari formula sistem pemilu yang rumit yang memerlukan prosedur perhitungan yang melelahkan	Kurangnya standar yang disepakati untuk sistem *evoting*
4.	Meningkatkan kenyamanan bagi para pemilih	Resiko manipulasi oleh orang dalam sengan akses istimewa ke sistem atau oleh peretas dari pihak luar
5.	Berpotensi meningkatkan partisipasi dan jumlah suara, khususnya pemilihan melalui internet	Kemungkinan kecurangan dengan manipulasi besar-besaran oleh sekelompok kecil orang dalam
6.	Lebih selaras dengan kebutuhan masyarakat yang mobilitasnya semakin tinggi	Meningkatnya persyaratan infrastruktur dan lingkungan, contohnya berkaitan dengan pasokan listrik dan teknologi komunikasi
7.	Pencegahan kecurangan di TPS dan selama pengiriman dan tabulasi hasil dengan mengurangi campur tangan manusia	Meningkatnya persyaratan keamanan untuk melindungi sistem
8.	Kemungkinan menggunakan layar multibahasa yang dapat melayani para pemilih multibahasa dengan lebih baik dibandingkan dengan surat suara	Kemungkinan perhitungan ulang terbatas
9.	Berpotensi menghemat biaya	Kebutuhan untuk kampanye

	dalam jangka panjang melalui penghematan waktu pekerja pemungutan suara dan mengurangi biaya untuk produksi dan distribusi surat suara	tambahan bagi pendidikan pemilih
10.	Penghematan biaya melalui pemilihan dengan internet: jangkauan global dengan pengeluaran logistik yang sangat sedikit. Tidak ada biaya pengiriman, tidak ada keterlambatan saat pengiriman materi dan menerimanya kembali.	Berpotensi kurangnya kepercayaan publik pada pemilihan berdasarkan *evoting* sebagai hasil dari kelemaha-kelemahan di atas.
11.	Jika dibandingkan dengan pemilihan melalui pos, maka pemilihan melalui internet dapat mengurangi insiden penjualan suara	Kurangnya tingkat kendali oleh penyelenggara karena tingginya tingkat ketergantungan terhadap vendor dan/atau teknologi

2.2.4 Keamanan Sistem *Evoting*

Aspek keamanan menjadi salah satu syarat yang harus dipenuhi dalam pengembangan sistem *evoting*. Hal ini penting karena sistem *evoting* berbasis web akan rawan mengalami banyak serangan dan gangguan baik dari dalam sistem itu sendiri maupun dari luar sistem. Hal ini sejalan dengan asas pemilu di Indonesia yaitu langsung, umum, bebas, rahasia, jujur dan adil. Asas kerahasiaan inilah yang harus tetap dijaga dengan memberikan keamanan pada sistem *evoting* yang dikembangkan.

Beberapa persyaratan keamanan yang harus dipenuhi dalam suatu sistem *evoting* menurut *A Survey of Modern Electronic Voting Technologies* antara lain:

1. *Eligibility and authentication*, pemilih hanya diperbolehkan melakukan proses vote setelah proses otentifikasi

2. *Uniqueness*, pemilih hanya memilik kesempatan memilih satu kali
3. *Accuracy*, hasil *vote* dicatat dan disimpan dengan benar
4. *Integrity*, hasil *vote* tidak dapat dirubah dan dihapus
5. *Verifiability* dan *accountability*, sistem memiliki fasilitas untuk memverifikasi hasil *vote* dihitung dengan benar
6. *Reliability*, sistem pemilihan harus daat bekerja dengan baik dalam menghadapi beberapa masalah seperti kehlangan hasil *vote*, kegagalan mesin *voting* dan kerugian komunikasi internet
7. *Secrecy* dan *non-coerbility*, pilihan yang dilakukan oleh pemilih harus rahasia, tidak ada yang mengetahui pilihan yang dipilih oleh pemilih dan pemilih tidak memiliki catatan pilihannya
8. *Flexibility*, sistem dapat digunakan oleh berbagai jenis pemilih
9. *Convenience*, pemilih mendapatkan kenyamanan pada saat melakukan proses *voting*
10. *Certifiability*, sistem *evoting* yang akan digunakan harus diuji oleh petugas pemilu terlebuh dahulu
11. *Transparency*, pemilih harus mampu memahami sistem secara umum
12. *Cost*, sistem yang digunakan tidak boleh terlalu mahal

Untuk menjamin keamanan informasi pada sistem *evoting*, ada 5 aspek yang harus dipenuhi dalam sistem/organisasi apapun yaitu: (1) Aspek kerahasiaan (*confidentiality*) yaitu aspek pencegahan penyingkapan informasi kepada pihak yang tidak memiliki hak terhadap informasi tersebut, (2) Aspek keutuhan data (*data integrity*) yaitu aspek pencegahan perubahan informasi oleh pihak yang

UNNES
UNIVERSITAS NEGERI SEMARANG

tidak memiliki otoritas untuk merubah informasi tersebut, (3) Aspek ketersediaan (*availability*) yaitu aspek dimana informasi harus tersedia ketika dibutuhkan, (4) Aspek otentifikasi (*authentication*) yaitu aspek yang menjamin informasi tersebut adalah asli juga untuk menjamin keabsahan orang-orang yang terlibat dalam pertukaran informasi, dan (5) Aspek nir-penyangkalan (*non repudiation*) yaitu aspek yang menjamin agar pihak-pihak yang terlibat tidak dapat menyangkal dikemudian hari.

2.2.5 Kriptografi

Kriptografi berasal dari bahasa Yunani yang terdiri dari dua suku kata yaitu *cryptos* (rahasia) dani *graphein* (tulisan), maka kriptografi dapat diartikan sebagai tulisan rahasia. Kriptografi, secara umum adalah ilmu dan seni untuk menjaga kerahasiaan berita. Pengertian lainnya, kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data dan otentifikasi data.

Ilmu kriptografi ini sebenarnya sudah mulai dipelajari manusia sejak jaman sebelum Masehi tepatnya sejak tahun 400 SM yaitu pada zaman Yunani Kuno. Pada perkembangan selanjutnya penggunaan kriptografi kemudian dimanfaatkan oleh Julius Caesar pada zaman Romawi Kuno sebagai salah satu strategi perang yang dinamakan *Caesar Cipher*. Prinsip perhitungan *Caesar Cipher* ialah menggunakan penyandian transposisi yaitu setiap huruf digantikan dengan huruf yang berada tiga posisi berikutnya dalam urutan alfabet. Sebagai

UNNES
UNIVERSITAS NEGERI SEMARANG

contoh huruf “a” digantikan dengan huruf “D” huruf “b” digantikan dengan huruf “E” dan seterusnya. Transformasi yang digunakan adalah:

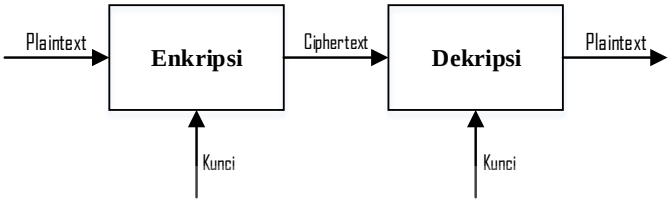
plain	:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
cipher	:	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Sebuah sistem kriptografi dikatakan sudah terpenuhi jika sudah memenuhi kondisi dari lima tuple (*five-tuple*) berikut, yaitu **P, C, K, E, D**:

1. **P** adalah himpunan berhingga dari *plaintext*
2. **C** adalah himpunan berhingga dari *ciphertext*
3. **K** adalah himpunan berhingga dari kunci
4. Untuk setiap k Є **K,** terdapat aturan enkripsi e_k Є **E** dan berkorespondensi dengan aturan dekripsi d_k Є **D.** Setiap $e_k : P \rightarrow C$ dan $d_k : C \rightarrow P$ adalah fungsi sedemikian hingga $d_k(e_k(x)) = x$ untuk setiap x Є P.

Beberapa istilah yang umum digunakan dalam kriptografi adalah pesan, *plaintext*, dan *ciphertext*. Pesan (*message*) atau yang juga disebut dengan *plaintext* merupakan data atau informasi yang dapat dimengerti maknanya. Pesan dapat berupa citra (*image*), suara (*audio*), dan video, atau berkas biner lainnya. Sedangkan *ciphertext* adalah hasil dari pesan yang sudah disandikan. Sementara enkripsi adalah teknik untuk mengacak suatu pesan atau *plaintext* dengan kunci tertentu sehingga pesan tersebut berubah menjadi *ciphertext* yang tidak dapat diketahui maknanya oleh pihak-pihak yang tidak memiliki kepentingan. Sedangkan proses kebalikannya disebut dekripsi. Seiring dengan kemajuan teknik yang digunakan untuk melakukan enkripsi maka didalamnya terkandung unsur matematis yang membuat isi dari informasi itu

semakin sulit untuk dipecahkan. Berikut disajikan skema enkripsi dan dekripsi pada Gambar 2.3. dibawah ini.



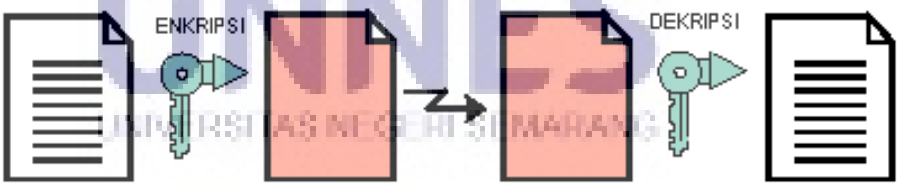
Gambar 2.3. Skema Enkripsi dan Dekripsi

Prinsip-prinsip yang mendasari kriptografi yakni:

1. Kerahasiaan (*confidentiality*), layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka/ mengupas informasi yang telah disandi.
2. Integritas data (*data integrity*), 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 kedalam data yang sebenarnya.
3. Autentikasi (*authenticity*), berhubungan dengan jaminan atas identitas dan keabsahan pihak-pihak yang melakukan transaksi dilakukan dengan menggunakan password atau sertifikat digital. Begitu pula dengan informasi yang dikirim/diterima harus diautentikasi keaslian, isi datanya, waktu pengiriman, dan lain-lain.
4. Non-repudiasi (*non-repudiation*), transaksi dapat dijadikan barang bukti yang tidak bisa disangkal oleh pihak-pihak yang melakukan transaksi.

Pada kriptografi modern terdapat berbagai macam algoritma, secara umum kriptografi modern dikelompokkan menjadi tiga jenis yaitu:

1. Algoritma simetris merupakan jenis kriptografi yang paling umum digunakan. Algoritma simetris menggunakan kunci yang sama untuk melakukan enkripsi dan dekripsi. Kunci yang digunakan untuk proses enkripsi dan dekripsi pada prinsipnya identik, tetapi satu buah kunci dapat pula diturunkan dari kunci yang lainnya. Kunci-kunci ini harus dirahasiakan. Oleh karena itulah sistem ini sering disebut sebagai *secret-key ciphersystem*. Karena pembuat pesan dan penerimanya harus memiliki kunci yang sama persis, siapapun yang memiliki kunci tersebut – termasuk pihak-pihak yang tidak diinginkan – dapat membuat dan membongkar rahasia *ciphertext*. Problem yang paling jelas disini terkadang bukanlah masalah pengiriman *ciphertext*-nya, melainkan masalah bagaimana menyampaikan kunci simetris tersebut kepada pihak yang diinginkan. Skema kriptografi kunci simetris disajikan pada Gambar 2.4. berikut ini.



Gambar 2.4. Kriptografi Kunci Simetris

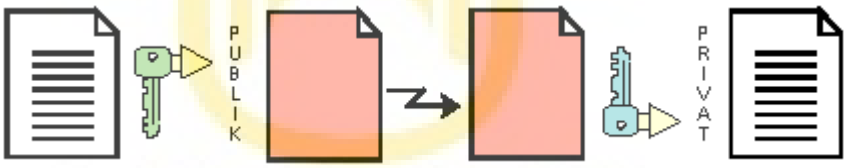
Aplikasi dari algoritma simetris digunakan oleh beberapa algoritma:

a. *Block Cipher*, yaitu proses penyandiannya berorientasi pada sekumpulan bit atau *byte* data (per blok). Contoh algoritma block *cipher* yaitu: *Data*

Encryption Standard (DES), *Advance Encryption Standard* (AES), *International Data Encryption Algoritma* (IDEA).

b. *Stream Cipher*, yaitu proses penyandiannya berorientasi pada satu bit atau satu *byte* data. Contoh algoritma stream cipher yaitu: A5, RC4, *One Time Pad* (OTP).

2. Algoritma asimetris adalah pasangan kunci kriptografi yang salah satunya digunakan untuk proses enkripsi dan yang satu lagi digunakan untuk proses dekripsi. Semua orang yang mendapatkan kunci publik dapat menggunakannya untuk mengenkripsikan suatu pesan, sedangkan hanya satu orang saja yang memiliki rahasia tertentu – dalam hal ini kunci privat – untuk melakukan pembongkaran terhadap sandi yang dikirim untuknya. Skema kriptografi kunci asimetris disajikan dalam Gambar 2.5. berikut ini.



Gambar 2.5. Kriptografi Kunci Asimetris

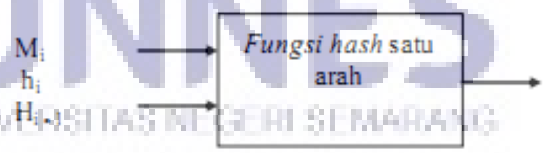
Beberapa contoh algoritma yang menerapkan kunci asimetris diantaranya: *Digital Signature Algorithm* (DSA), RSA (*Rivest-Shamir-Adleman*), *Diffie-Hellman* (DH), *Elliptic Curve Cryptiography* (ECC), Kripto Quantum.

3. Fungsi *hash* yang juga sering disebut fungsi *hash* satu arah (*One-Way Function*), *message digest*, *fingerprint*, fungsi kompresi, dan *message authentication code (MAC)*, merupakan suatu fungsi matematika yang mengambil masukan panjang variabel dan mengubahnya ke dalam urutan

biner dengan panjang yang tetap. Disebut fungsi hash satu arah karena pesan yang dienkrispi dengan metode ini tidak dapat dikembalikan ke pesan semula. Pesan (yang besarnya dapat bervariasi) yang akan di *hash* disebut *pre-image*, sedangkan outputnya yang memiliki ukuran yang tetap, disebut *hash value* (nilai *hash*). Fungsi *hash* biasanya diperlukan untuk membuat sidik jari dari suatu pesan. Sidik jari pada pesan merupakan suatu tanda untuk memastikan bahwa pesan tersebut benar-benar berasal dari orang-orang yang diinginkan. Jaminan dari keamanan sidik jari berangkat dari kenyataan bahwa hampir tidak ada dua *pre-image* yang memiliki nilai *hash* yang sama. Inilah yang disebut dengan sifat *collision free* dari suatu fungsi *hash* yang baik. Selain itu, sangat sulit untuk membuat suatu *pre-image* jika hanya diketahui nilai *hash*nya saja. Masukan fungsi *hash* adalah blok pesan (M) dan keluaran dari *hashing* blok pesan sebelumnya,

$$h_i = H\ (M_i, h_i - 1)$$

Skema fungsi *hash* satu arah ditunjukkan pada Gambar 2.6. di bawah ini



Gambar 2.6. Fungsi *Hash* Satu Arah

Sifat-sifat fungsi *hash* satu arah adalah sebagai berikut:

1. Fungsi H dapat diterapkan pada blok data berukuran variatif
2. H menghasilkan nilai (h) dengan panjang tetap (*fixed-length output*)
3. H(x) mudah dihitung untuk setiap nilai x yang diberikan

4. Untuk setiap h yang dihasilkan, tidak mungkin dikembalikan sedemikian hingga H(x) = h. Itulah sebabnya fungsi H dikatakan fungsi *hash* satu-arah (*one-way function output*)
5. Tidak mungkin mencari pasangan x dan y sedemikian sehingga: H(x) = H(y)

Aplikasi fungsi *hash* satu arah bertujuan untuk:

1. Menjaga integritas data
   a. Fungsi hash sangat peka terhadap perubahan 1 bit pesan
   b. Pesan berubah 1 bit, nilai hash berubah sangat signifikan
   c. Bandingkan nilai *hash* baru dengan nilai hash lama. Jika sama pesan masih asli. Jika tidak pesan sudah dimodifikasi
2. Menghemat waktu pengiriman
   a. Untuk memverifikasi sebuah file salinan arsip dengan arsip asli
   b. Salinan dokumen berada di tempat jauh dari basisdata arsip asli
   c. Untuk lebih menghemat waktu dalam melakukan verifikasi salinan arsip dengan arsip aslinya cukup dengan membandingkan *message digest*-nya.
   d. Jika nilai *message digest* salinan arsip sama dengan *message digest* arsip asli berarti salinan arsip tersebut sama dengan arsip master.
3. Menormalkan panjang data yang beraneka ragam
   a. Misalkan *password* panjangnya bebas (minimal 8 karakter)
   b. *Password* disimpan di komputer *host* (server) untuk keperluan otentifikasi pemakai komputer

UNNES
UNIVERSITAS NEGERI SEMARANG

c. *Password* disimpan dalam basisdata

d. Untuk menyeragamkan panjang *field password* di dalam basisdata, *password* disimpan dalam bentuk hash.

Beberapa contoh algoritma yang menerapkan kriptografi fungsi *hash* diantaranya: MD5 (*Message digest 5*), SHA 1 (*Secure* Hash *Algorithm 1*), SHA 256 (*Secure* Hash *Algorithm 256*).

Dari beberapa algoritma yang dijelaskan di atas, penulis menggunakan fungsi *hash* dengan algortima SHA-256 dan algoritma simetris *stream cipher* dengan algoritma *one time pad* dalam merancang keamanan sistem *evoting*.

2.2.6 Algoritma *One Time Pad*

One Time Pad (OTP) atau yang sering disebut sebagai Vernam cipher karena ditemukan oleh Mayor J. Maugborne dan G. Vernam ditahun 1917 pada perang dunia kedua. Metode ini telah diklaim sebagai satu-satunya algoritma kriptografi sempurna yang tidak dapat dipecahkan. Suatu algoritma dikatakan aman apabila tidak ada cara untuk menemukan *plaintext*-nya. Hingga saat ini, hanya algoritma OTP yang dinyatakan tidak dapat dipecahkan meskipun diberikan sumber daya yang tidak terbatas.

UNNES
UNIVERSITAS NEGERI SEMARANG

OTP memiliki keunggulan dalam melakukan proses enkripsi dan dekripsi yaitu setiap karakter dalam kunci digunakan untuk mengenkripsi dan mendekripsi setiap karakter dalam *plaintext*. Hal ini membuat kriptanalis kesulitan dalam menemukan *plaintext* asli jika kunci yang digunakan adalah kunci yang acak. Sisi yang lain, OTP memiliki kelemahan dalam penggunaannya untuk melakukan enkripsi dan dekripsi yaitu OTP hanya cocok digunakan

untuk melakukan enkripsi dan dekripsi pesan yang berukuran kecil atau pesan singkat saja. Hal ini dikarenakan panjang kunci yang digunakan harus sama dengan panjang pesan, sehingga semakin besar panjang pesan akan berakibat semakin besar pula panjang kunci yang dibutuhkan. Penelitian terdahulu juga telah membuktikan bahwa waktu yang dibutuhkan metode OTP untuk melakukan enkripsi-dekripsi pada data kecil lebih singkat dibandingkan metode lainnya.

Hal ini sesuai dengan kebutuhan sistem yang dikembangkan. Karena dalam proses perancangan sistem keamanan *evoting* ini data *plaintext* yang digunakan adalah data id kandidat capres dan cawapres yang hanya berukuran 8 karakter. Sehingga algoritma OTP sangat cocok digunakan untuk enkripsi data pada sistem yang dikembangkan, karena proses enkripsi-dekripsi membutuhkan waktu yang relatif cepat.

Proses enkripsi metode ini ialah dengan melakukan operasi XOR (*Exlusive OR*) pada *plaintext* dan kuncinya, dimana deretan karakter-karakter kunci yang digunakan dibangkitkan secara acak. Operasi XOR menghasilkan nilai 1 jika dan hanya jika memiliki inputan nilai yang berbeda yaitu 0 dan 1. Dan bernilai 0 jika inputan nilai bernilai sama. Metode OTP merupakan metode yang sempurna (*perfect methods*), karena: (1) tidak mungkin bisa dipecahkan dengan melakukan perhitungan matematis, dan (2) tidak mungkin ada dua buah pesan yang berbeda menjadi 1 buah pesan *ciphertext* yang sama. Sementara sifat OTP, antara lain ialah:

1. Kunci yang digunakan hanya diketahui oleh pengirim dan penerima pesan

UNNES
UNIVERSITAS NEGERI SEMARANG

2. Pembangkitan kunci dilakukan dengan menggunakan PRNG (*Pseudo Random Number Generator*)
3. Panjang kunci sama dengan panjang pesan
4. Kunci digunakan hanya untuk satu kali proses enkripsi (*session key*)

Berikut disajikan langkah sederhana mengenai proses perhitungan algoritma OTP:

1. Menentukan *plaintext* terlebih dahulu, dalam hal ini misalnya ditentukan kunci sepanjang 5 karakter yaitu RUSDI
2. Menentukan *key* atau kunci dengan panjang yang sama dengan *plaintext*, dalam hal ini misalnya ditentukan kunci yaitu CRASH
3. Mengubah *plaintext* ke bentuk biner, berikut disajikan dalam Tabel 2.3. di bawah ini

Tabel 2.3. Kode Biner *Plaintext* OTP

Karakter	ASCII	Kode Biner
R	82	0101 0010
U	85	0101 0101
S	83	0101 0011
D	68	0100 0100
I	73	0100 1001

4. Langkah yang sama juga dilakukan untuk kunci, yaitu mengubahnya ke dalam bentuk biner. Berikut disajikan dalam Tabel 2.4. di bawah ini

Tabel 2.4. Kode Biner Kunci OTP

Karakter	ASCII	Kode Biner
C	67	0100 0011
R	82	0101 0010
A	65	0100 0001
S	83	0101 0011
H	72	0100 1000

5. Untuk memperoleh *ciphertext* langkah selanjutnya ialah melakukan operasi XOR pada masing-masing karakter *plaintext* dengan kunci, maka diperoleh hasil sebagai berikut:

RUSDI	= 0101 0010	0101 0101	0101 0011	0100 0100	0100 1001	
CRASH	= 0100 0011	0101 0010	0100 0001	0101 0011	0100 1000	XOR
Ciphertext	= 0001 0001	0000 0111	0001 0010	0001 0111	0000 0001	
ASCII	= Ctrl-Q	Ctrl-G	Ctrl-R	Ctrl-W	Ctrl-A	

6. Proses dekripsi untuk memperoleh kembali *plaintext* menggunakan metode yang sama yaitu dengan melakukan operasi XOR antara *ciphertext* dan kunci. Sehingga diperoleh hasil sebagai berikut:

Ciphertext	= 0001 0001	0000 0111	0001 0010	0001 0111	0000 0001	
CRASH	= 0100 0011	0101 0010	0100 0001	0101 0011	0100 1000	XOR
Plaintext	= 0101 0010	0101 0101	0101 0011	0100 0100	0100 1001	
ASCII	= R	U	S	D	I	

2.2.7 Algoritma SHA 256

Hingga saat ini ada lima algoritma SHA yaitu SHA-0, SHA-1, SHA-224, SHA-256, SHA-384, dan SHA-512. Varian SHA-0 dikenal dengan SHA-0 pada tahun 1993, Varian SHA-1 dikenal dengan SHA-1 pada tahun 1995, varian SHA-224, SHA-256, SHA-384, dan SHA-512 dikenal dengan SHA-2 pada tahun 2002. SHA adalah fungsi hash (*message digest*) satu arah yang dibuat oleh NIST, dirancang oleh NSA (*National Security Agency*) dan digunakan bersama DSS (*Digital Signature Standard*). Oleh NSA, SHA dinyatakan sebagai standard fungsi hash satu arah. SHA-1 dikembangkan dalam beberapa aplikasi keamanan dan

protokol digunakan secara luas, mencakup TLS dan SSL, PGP, SSH, S/MIME, dan IPsec. SHA-1 dianggap sebagai turunan dari MD5, dikenal lebih awal dari MD5, fungsi hash digunakan secara luas. Proses *hashing* dengan algoritma SHA-256 disajikan dalam Gambar 2.7. di bawah ini.

Gambar. 2.7. Fungsi Hash SHA-256

Algoritma SHA-256 dapat digunakan untuk menghitung nilai *message digest* dari sebuah pesan, dimana pesan tersebut memiliki panjang maksimum 264 bit. Algoritma ini menggunakan sebuah *message schedule* yang terdiri dari 64 elemen 32-bit word, delapan buah variabel 32-bit, dan variabel penyimpan nilai *hash* 8 buah word 32-bit. Hasil akhir dari algoritma SHA-256 adalah sebuah *message digest* sepanjang 256-bit. *Preprocessing* dilakukan dengan menambahkan bit pengganjal, membagi-bagi pesan dalam *block* berukuran 512-bit, dan terakhir menginisiasi nilai *hash* awal. Misalkan panjang pesan M adalah l bit. Proses penambahan bit pengganjal adalah pertama tambahkan bit “1” pada akhir pesan, diikuti dengan bit “0” sejumlah k, dimana k adalah solusi dari persamaan: l+0+k=448mod512.

Kemudian tambahkan 64-bit *block* yang menyatakan panjang pesan semula (*l*) dalam representasi biner. Dalam proses komputasinya, SHA-256 menggunakan enam fungsi logika, dimana setiap fungsi beroperasi menggunakan tiga buah word 32-bit (x, y, dan z), dan keluarannya berupa sebuah word 32-bit. Dengan menggunakan perbandingan dibawah ini sekiranya dapat menyimpulkan

dalam pemilihan algoritma *hash* untuk kedepannya. Dengan tujuan memperbaiki algoritma yang kurang memenuhi standar keamanan dalam hal ini sebagai fungsi hash. Tabel 2.5. di bawah ini menyajikan daftar informasi mengenai beberapa jenis algoritma fungsi hash.

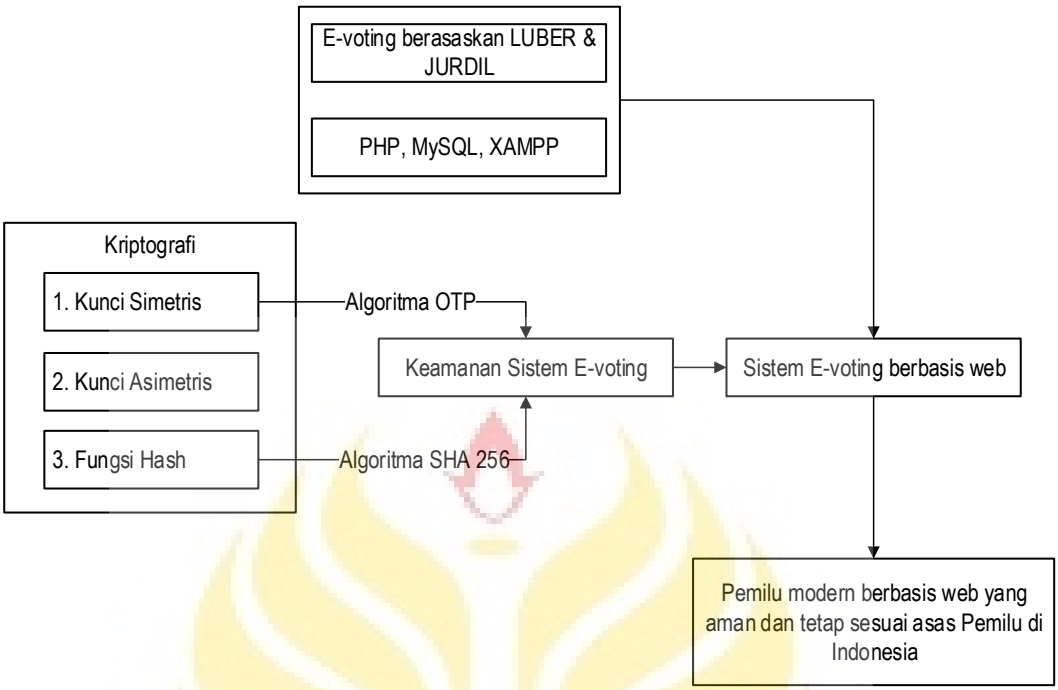
Tabel 2.5. Daftar Informasi Algoritma Fungsi Hash

Algoritma	Output Size	Internal	Block	Length	Word	Collision
HAVAL	256/224/192/128	256	1024	64	32	Yes
MD2	128	384	128	No	8	Almost
MD4	128	128	512	64	32	Yes
MD5	128	128	512	64	32	Yes
PANAMA	256	8736	256	No	32	With flaws
RIPEMD	128	128	512	64	32	Yes
SHA-0	160	512	512	64	32	No
SHA-1	160	512	512	64	32	No
SHA-256/224	256/224	512	512	64	32	Yes
SHA-512/384	512/384	1024	1024	128	64	No
Tiger(2)	192/160/128	512	512	64	64	No
VEST-4/8	160/256	176/304	8	80	1	No
VEST-16	320/512	424/680	8	88	1	No
WHIRLPOOL	512	512	512	256	8	No

Penjelasan di atas menggambarkan beberapa algoritma beserta *output size*, *internal*, *block*, *length*, *word* dan *collision*. Algoritma tersebut memiliki kelebihan masing-masing dan terdapat kekurangan pada algoritma tertentu karena terjadi tabrakan/bentrok (*collision*).

2.3. Kerangka Berpikir

Berdasarkan latar belakang masalah dan hasil kajian pustaka yang dilakukan, untuk mempermudah pemahaman tentang penelitian "Sistem Keamanan *Evoting* Menggunakan Fungsi Hash dan Algoritma *One Time Pad*" ini berikut disajikan diagram kerangka berpikir dalam Gambar 2.8. di bawah ini.



Gambar 2.8. Diagram Kerangka Berpikir

Penelitian ini di rancang berdasarkan penemuan masalah tentang kelemahan pemilu konvensional yang hingga saat ini masih digunakan dalam pemilihan kepala daerah maupun kepala negara di Indonesia. Dengan harapan dapat membantu mengurangi kelemahan-kelemahan tersebut peneliti melakukan studi literatur tentang rancang bangun sistem *evoting* yang telah dilakukan oleh peneliti terdahulu. Sistem *evoting* yang dikembangkan dalam penelitian ini disesuaikan dengan asas pemilu di Indonesia yaitu langsung, umum, bebas, rahasia, jujur dan adil.

Untuk membangun sistem *evoting* berbasis web, digunakan program-program seperti XAMPP, MySQL, PHP dan HTML. Sistem *evoting* yang dikembangkan harus menjamin keamanan identitas pemilih dan hasil pemungutan suara. Sehingga setiap data harus dijaga keamanannya dengan merubah bentuknya

menjadi pesan lain (*encrypted data*) yang tidak dapat diketahui oleh pihak-pihak yang tidak berwenang.

Dalam penelitian ini penulis menggunakan dua teknik enkripsi yang diterapkan secara bersamaan dalam proses penyandian data yaitu menggunakan algoritma fungsi *hash* SHA-256 dan algoritma kunci simetris *one time pad*. Fungsi *hash* digunakan untuk menjamin integritas data melalui fungsi satu arahnya. Sementara algoritma *one time pad* digunakan karena sesuai dengan peruntukannya yang lebih baik digunakan pada data dengan ukuran kecil. Dua metode enkripsi ini diharapkan dapat memberi keamanan pada sistem *evoting* yang dikembangkan.

UNNES
UNIVERSITAS NEGERI SEMARANG

BAB VI

SIMPULAN DAN SARAN

6.1. Simpulan

Berdasarkan hasil penelitian dan pembahasan yang dilakukan, dapat diambil simpulan sebagai berikut:

1. Rancangan sistem *evoting* yang dikembangkan dalam penelitian ini mampu mengatasi beberapa kelemahan yang terdapat dalam pelaksanaan pemilu konvensional dan tetap sesuai dengan enam asas pemilu di Indonesia yaitu langsung, umum, bebas, rahasia, jujur dan adil.
2. Penerapan fungsi *hash* kriptografis dan algoritma *one time pad* dapat digunakan untuk pengembangan sistem keamanan *evoting*. Pemenuhan keamanan *evoting* dalam penelitian ini diterapkan pada proses registrasi pemilih, validasi waktu, sistem *login*, validasi pemilih, sistem pemilihan dan sistem perhitungan suara secara *realtime*.
3. Hasil pengujian sistem *evoting* menunjukkan bahwa sistem yang dikembangkan telah memenuhi sebagian besar kebutuhan-kebutuhan *evoting*, baik kebutuhan dasar, kebutuhan fungsional dan kebutuhan non-fungsional.

6.2. Saran

Saran yang diberikan untuk pengembangan penelitian selanjutnya ialah:

1. Fitur keamanan yang digunakan dalam sistem *evoting* yang dikembangkan dalam penelitian ini menggunakan metode kriptografi yang mungkin masih ditemui kelemahannya. Sehingga pada penelitian selanjutnya dapat menggunakan kriptografi dengan algoritma yang berbeda.
2. Penambahan fitur-fitur lain yang berguna untuk sistem *evoting* sehingga pengguna/pemilih tidak hanya dapat melakukan pemungutan suara.
3. Pengembangan keamanan pada aspek integritas data hanya terfokus pada hasil pemungutan suara, penelitian selanjutnya dapat melakukan keamanan integritas data pada aspek yang berbeda.
4. Otentifikasi menggunakan *username* dan *password* masih memiliki kelemahan, penelitian selanjutnya dapat mengembangkan sistem otentifikasi yang diperkuat dengan kontrol fisik seperti: sensor sidik jari, sensor retina, tanda tangan digital, dsb.
5. Proses tabulasi suara dalam penelitian ini dilakukan secara langsung, penelitian selanjutnya diharapkan melakukan tabulasi awal pada masing-masing TPS terlebih dahulu untuk mencegah terjadinya *overload* pada basisdata server.

UNNES
UNIVERSITAS NEGERI SEMARANG

DAFTAR PUSTAKA

Abdulhamid, Shafi'i Muhammad, dkk. 2013. The Design and Development of Real-Time *Evoting* System in Nigeria with Emphasis on Security and Result Veracity. *I.J. Computer Network and Information Security* 5: 9-18.

Arief, M Rudyanto. 2011. *Pemrograman Web Dinamis Menggunakan PHP & MySQL*. Yogyakarta: Penerbit Andi.

Agustina, Esti Rahmawati., Kurniati, Agus. 2009. Pemanfataan Kriptografi Dalam Mewujudkan Keamanan Informasi Pada *Evoting* di Indonesia. *Seminar Nasional Informatika 2009 (semnasIF 2009) 23 Mei 2009.* UPN Veteran Yogyakarta.

Chandrakar, Sagar. 2014. An Innovative Approach for Implementation of One-Time Pads. *International Journal of Computer Applications* 89 (13): 35-37.

Evecek, Hakan. 2007. *Online Evoting System Software Requirements Specification*. UCCS Computer Science Department.

Gritzalis, D. 2002. *Secure Electronic Voting; New Trends New Threats*. Athens: Dept. of Informatics Athens University of Economics & Business and Data Protection Commission of Greece.

Gritzalis, Dimitris A. 2002. Principles and Requirements for A Secure *Evoting* System. *Elsevier Advanced Technology Computers and Security* 21 (6): 539-556.

Komisi Pemilihan Umum. 2012. *Laporan Pelaksanaan Tugas Tahun 2011*. KPU Kabupaten Klaten. Klaten.

Laporan Survei. 2013. *Persepsi 200 Ahli Tata Negara terhadap Kinerja Mahkamah Konstitusi RI.* SETARA Institute. Jakarta.

Lukas, Samuel., dan Artati , NP Sri. 2007. Analisis Waktu Enkripsi-Dekripsi File Text Menggunakan Metode One-Time Pad (OTP) dan Rivest, Shamir, Adleman (RSA). *Seminar Nasional Sistem dan Informatika Bali.* 16 November 2007: 50-55.

Mulyono, Hengky., Rodiah. 2013. Implementasi Algoritma One Time Pad Pada Penyimpanan Data Berbasis Web. *Seminar Nasional Teknologi Informasi dan Multimedia, 19 Januari 2013.* STMIK AMIKOM Yogyakarta.

UNNES
UNIVERSITAS NEGERI SEMARANG

Nagaraj, Nithin. 2012. One-Time Pad as A Nonlinear Dynamical System. *Elsevier Advanced Technology Computers and Security* 17: 4029–4036.

Neyman, Shelvie Nidya. 2013. Penerapan Sistem *Evoting* pada Pemilihan Kepala Daerah di Indonesia. *Jurnal Sains Terapan Edisi III Vol-3*: 45-61.

Nugoroho, Bunafit. 2004. *PHP dan MySQL dengan Editor Dreamweaver MX*. Yogyakarta: Penerbit Andi.

Olaniye, Olayemi Mikail., Arulogun, Oladiran Tayo., Omidiora, Elijah Olusayo., and Oludotun, Adeoye. 2013. Design of Secure Electronic Voting System Using Multifactor Authentication and Cryptographic Hash Functions. *International Journal of Computer and Information Technology* 2(6): 1122-1130.

Peraturan Komisi Pemilihan Umum No. 10 Tahun 2012 Pemantau dan Tata Cara Pemantauan Pemilihan Umum Anggota Dewan Perwakilan Rakyat, Dewan Perwakilan Daerah dan Dewan Perwakilan Rakyat Daerah Tahun 2014. 13 Agustus 2012. Jakarta.

Peraturan Komisi Pemilihan Umum No. 26 Tahun 2013 Pemungutan dan Penghitungan Suara Dalam Pemilihan Umum Anggota Dewan Perwakilan Rakyat, Dewan Perwakilan Daerah, Dewan Perwakilan Rakyat Daerah Provinsi, Dewan Perwakilan Rakyat Daerah Kabupaten/Kota. 31 Desember 2013. Jakarta.

Peraturan Presiden Tentang Perubahan Kedua Atas Peraturan Presiden Nomor 26 Tahun 2009 Tentang Penerapan Kartu Tanda Penduduk Berbasis Nomor Induk Kependudukan Secara Nasional. 27 September 2011. Jakarta.

Policy Paper. 2011. Introducing Elctronic Voting Essential Considerations. International IDEA. Stockholm.

Priyono, Edi. 2010. *Evoting*: Urgensi Transparansi Dan Akuntabilitas. *Seminar Nasional Informatika 2010 (semnasIF 2010) UPN "Veteran" Yogyakarta*. 22 Mei 2010: 55-62.

Pressman, Roger S. 2002. *Rekayasa Perangkat Lunak; Pendekatan Praktisi (Buku I).* Yogyakarta: Penerbit Andi.

Rijmenants, Dirk. 2014. The Complete Guide To Secure Communications With The One Time Pad Cipher. *Cipher Machines and Cryptology* 6(2):1-27.

Rokhman, A. 2011. Prospek dan Tantangan Penerapan *Evoting* di Indonesia. *Seminar Nasional Peran Negara dan Masyarakat dalam Pembangunan*

Demokrasi dan Masyarakat Madani di Indonesia, 7 Juli 2011. Jakarta: Universitas Terbuka.

Shalahuddin, M. 2009. Pembuatan Model *Evoting* Berbasis Web (Studi Kasus Pemilu Legislatif dan Presiden Indonesia). *Tesis*. Program Pasca Sarjana Institut Teknologi Bandung. Bandung.

Sutarman. 2007. *Membangun Aplikasi Web dengan PHP dan MySQL*. Yogyakarta: Graha Ilmu.

Undang-Undang Republik Indonesia No. 42 Tahun 2008 Pemilihan Umum Presiden dan Wakil Presiden. 13 November 2008. Jakarta.

Undang-Undang Republik Indonesia Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan. 29 Desember 2006. Jakarta.

Winaryo, Febryan Christy. 2014. Implementasi Modifikasi Kriptografi *One Time Pad* (OTP) untuk Pengamanan Data *File*. *Artikel Ilmiah*. Program Studi Teknik Informatika Universitas Kristen Satya Wacana. Salatiga.

Zissis, Dimitrios. 2011. Methodologies and Technologies for Designing Secure Electronic Voting Information Systems. *Dissertation.* University of The Aegean. Syros.

UNNES
UNIVERSITAS NEGERI SEMARANG