IMPLEMENTASI ALGORITMA BLOWFISH UNTUK PRIVACY DATA E-VOTING

Edy Waly Rumaf
STMIK Tidore Mandiri
edy.waly.rumaf@stmik-tm.ac.id

ABSTRAK

Salah satu bagian terpenting dalam merancang suatu aplikasi e-voting ditinjau dari segi keamanan data adalah, memiliki kemampuan merahasiakan dan menjaga informasi pemilihan yang tersimpan dalam database. Penelitian ini bertujuan untuk membuat aplikasi prototipe e-voting khususnya pada sisi keamanan privacy (kerahasiaan) yang dapat melakukan proses enkripsi dan dekripsi menggunakan algoritma kriptografi blowfish. Proses enkripsi dan dekripsi merupakan salah satu metode yang digunakan dalam melakukan pengacakan data menjadi sesuatu yang sulit dipahami oleh manusia dan dapat dikembalikan ke bentuk semula. Implementasi algoritma blowfish untuk proses enkripsi dilakukan saat pemilih memilih kandidat, sedangkan proses dekripsinya dilakukan saat proses perhitungan jumlah suara. Metode yang digunakan dalam penelitian ini adalah metode deskriptif analitis, yaitu mengumpulkan data-data yang sebenarnya kemudian disusun, diolah dan dianalisis untuk mendapatkan gambaran dan kejelasan persoalan yang akan diselesaikan. Hasil penelitian menunjukkan bahwa aplikasi sudah berjalan dengan baik dan mampu melakukan proses enkripsi-dekripsi data. Hal itu ditunjukkan dengan perubahan data nomor urut kandidat dalam database yang sudah berbentuk data acak (chipertext), dan keberhasilan dalam melakukan perhitungan jumlah suara yang mana terlebih dahulu dilakukan proses dekripsi untuk mengembalikan data ke bentuk asli (plaintext).

Kata kunci: Algoritma, Blowfish, Privacy, E-Voting

I. PENDAHULUAN

Pemilihan Umum (Pemilu) merupakan salah satu contoh bentuk kegiatan demokrasi yang bertujuan untuk memilih pemimpin. Kegiatan Pemilu di Indonesia sampai saat ini hampir sebagian besar masih dilakukan secara manual. Hal ini menyebabkan pelaksanaan Pemilu memakan waktu yang lama dan penghitungan suara yang kurang akurat. Berdasarkan hal tersebut maka pelaksanaan Pemilu perlu ditingkatkan kualitasnya dengan mengedepankan peran teknologi informasi di dalamnya. Salah satu penerapan peran teknologi informasi yaitu proses pengiriman data Pemilu dari KPU daerah ke KPU pusat menjadi lebih cepat, mempercepat proses penghitungan suara. Selain itu efisiensi biaya penyelenggaraan Pemilu seperti penyediaan surat suara (Harahap dkk., 2012).

Teknologi informasi dan komunikasi dalam proses Pemilihan Umum (Pemilu) dapat didefinisikan sebagai teknologi yang digunakan dalam memperoleh, memanipulasi, menyajikan dan dalam pemanfaatan data. Dengan kemajuan teknologi informasi dan komunikasi yang ada sekarang ini, maka permasalahan-permasalahan umum yang terjadi selama ini terutama Daftar Pemilih Tetap (DPT) bisa diminimalkan dengan rancangan sistem yang dapat mendeteksi secara otomatis (Sallu, 2014).

Pemanfaatan teknologi informasi dan komunikasi yang dimaksud adalah menyelenggarakan pemilihan secara elektronik (e-voting). Teknologi e-voting pada saat ini menjadi pilihan yang sangat penting dalam melaksanakan salah satu pilar demokrasi yang paling utama, yaitu Pemilu. Teknologi e-voting ini bisa menjadi pilihan dalam pelaksanaan Pilkada. Terutama setelah dalam beberapa tahun sebelumnya cara-cara konvensional telah terbukti 'kurang berhasil' menjawab tuntutan masyarakat terhadap mekanisme Pemilu yang berasaskan luber dan jurdil.

E-voting adalah suatu sistem pemilihan dimana data dicatat, disimpan, dan diproses dalam bentuk informasi digital. Dengan kata lain e-voting merupakan pelaksanaan pemungutan suara yang dilakukan secara elektronik (digital), dimulai dari proses pendaftaran pemilih, pelaksanaan pemilihan, penghitungan suara sampai dengan pengiriman hasil perolehan suara (Rokhman, 2011).

Salah satu faktor yang sangat penting dalam e-voting adalah keamanan data. Hal tersebut sesuai dengan Peraturan Pemerintah nomor 82 tahun 2012 tentang pelaksanaan Undang-Undang nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, asas Pemilu yakni Langsung, Umum, Bebas, Rahasia, Jujur dan Adil (Luber Jurdil).

Berdasarkan hal tersebut maka diperlukan suatu metode agar e-voting mendapat kepercayaan dan diterima oleh masyarakat umum dalam pelaksanaan Pemilu. Salah satu metode yang dapat digunakan terkait dengan keamanan data e-voting adalah dengan memanfaatkan algoritma kriptografi.

II. TINJAUAN PUSTAKA

A. Electronic Voting

E-Voting (Electronic voting) adalah proses pemilihan umum yang memungkinkan pemilih untuk mencatatkan pilihannya yang bersifat rahasia secara elektronik yang teramankan. Pengertian lain e-voting adalah pemungutan suara yang dilakukan secara elektronik (digital) mulai dari proses pendaftaran pemilih, pelaksanaan pemilihan, penghitungan suara dan pengiriman hasil suara (Hutagulung, 2012).

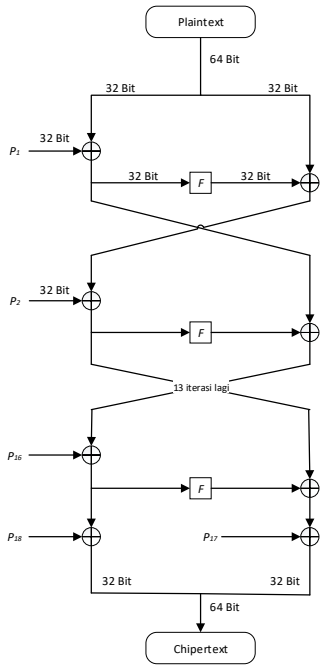
B. Algoritma Blowfish

Algoritma kriptografi blowfish adalah salah satu algoritma kunci simetri blok kode yang dirancang pada tahun 1993 oleh Bruce Schneier untuk mengganti algoritma DES. Dimana pada saat itu banyak sekali rancangan algoritma yang ditawarkan, namun hampir semua terhalang oleh paten atau kerahasiaan pemerintah Amerika. Keberhasilan blowfish dalam menembus pasar terbukti dengan diadopsinya blowfish sebagai Open Cryptography Interface (OCI) pada kernel Linux versi 2.5 ke atas. Dengan diadopsinya blowfish berarti dunia open source menganggap blowfish adalah salah satu algoritma terbaik (Ariyus, 2008).

Blowfish adalah algoritma kriptografi kunci simetri blok kode dengan panjang blok tetap 64 bit (8 byte). Blowfish menerapkan teknik kunci berukuran sembarang. Dimana ukursn kunci yang dapat diterima oleh blowfish adalah antara 32 bit (4 byte) hingga 448 bit (56 byte), dengan ukuran default sebesar 128 bit (16 byte). Blowfish memanfaatkan teknik pemanipulasian bit dan teknik pemutaran ulang dan pergiliran kunci yang dilakukan sebanyak 16 kali. Algoritma utama dari blowfish terbagi menjadi 2 sub algoritma utama yaitu, bagian ekspansi kunci dan bagian enskripsi-dekripsi data. Pengekspansian kunci dilakukan pada saat awal dengan masukan sebuah kunci dengan panjang 32 bit hingga 448 bit dan keluaran adalah sebuah larik upa-kunci dengan total 4168 byte. Bagian enkripsi-dekripsi data terjadi dengan memanfaatkan perulangan 16 kali

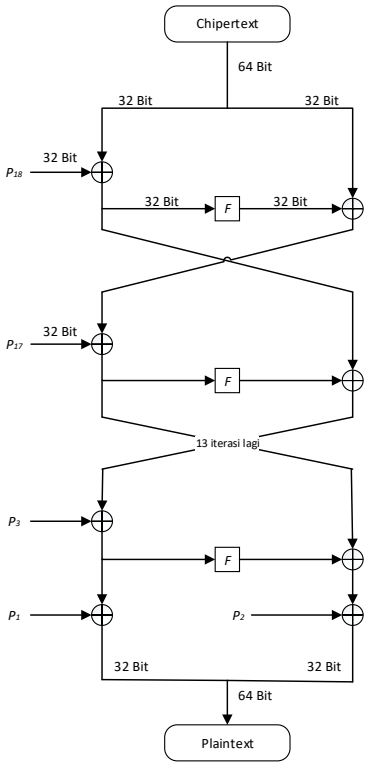
terhadap jaringan feitsel. Setiap perulangan terdiri dari permutasi dengan masukan kunci dan subtitusi data. Semua operasi dilakukan dengan memanfaatkan operator XOR dan operator penambahan. Penambahan dilakukan terhadap 4 larik lookup yang dilakukan setiap putarannya.
Algoritma blowfish memanfaatkan subkunci yang besar. Kunci tersebut harus dihitung terlebih dahulu sebelum proses enkripsi atau dekripsi dilakukan. Selain itu, algoritma blowfish adalah algoritma yang menerapkan jaringan Feistel yang terdiri dari 16 putaran dengan inputan 64 bit. Adapun alur dari algoritma enkripsi dengan blowfish adalah sebagai berikut.

a. Inisialisasi P-array sebanyak 18 buah (P1,P2, ….. P18) masing-masing bernilai 32 bit subkunci.
   P1 , P2 , ……. , P18
b. Bentuk S-box sebanyak 4 buah masing-masing bernilai 32 bit yang masing-masing memiliki masukan 256.
   $S_{1,0}$, $S_{1,1}$, ……. , $S_{1,255}$
   $S_{2,0}$, $S_{2,1}$, ……. , $S_{2,255}$
   $S_{3,0}$, $S_{3,1}$, ……. , $S_{3,255}$
   $S_{4,0}$, $S_{4,1}$, ……. , $S_{4,255}$
c. Plainteks yang akan dienkripsi diasumsikan sebagai masukan yang diambil sebanyak 64 bit dan apabila kurang dari 64 bit maka ditambahkan bit-nya sehinga dalam operasi nanti sesuai dengan datanya.
d. Bagi masukan menjadi 2 buah bagian sama besar yakni XL sepanjang 32 bit dan XR sepanjang 32 bit.
e. Selanjutnya lakukan operasi XL = XL xor Pi dan XR = F(XL) xor XR.
f. Hasil dari operasi tersebut kemudian ditukar, XL menjadi XR dan XR menjadi XL.
g. Lakukan perulangan sebanyak 16 kali kemudian lakukan lagi proses penukaran XL dan XR.
h. Pada proses ke 17 lakukan operasi untuk XR = XR xor P17 dan XL = XL xor P18.
i. Langkah terakhir yaitu satukan kembali XL dan XR sehingga menjadi 64 bit kembali.



Gambar 1. Proses enkripsi pada algoritma Blowfish

Untuk proses dekripsi dengan algoritma blowfish sama persis dengan proses enkripsi, hanya saja pada P-array (P1, P2, ….. , P18) digunakan dengan urutan terbalik.



Gambar 1. Proses dekripsi pada algoritma Blowfish

III. METODE PENELITIAN

Adapun metode penelitian yang digunakan adalah metode pengembangan aplikasi *waterfall* yang terdiri dari tahap analisis, desain, implementasi dan evaluasi.

A. Waktu dan Lokasi Penelitian

Waktu pelaksanaan penelitian ini dilakukan mulai dari bulan Oktober sampai dengan bulan Desember 2018 dan berlokasi di Lab. Komputer STMIK Tidore Mandiri.

B. Jenis Penelitian

Jenis penelitian yang digunakan dalam penelitian ini adalah penelitian deskriptif analitis, yaitu mengumpulkan data-data sebenarnya kemudian disusun, diolah dan dianalisis untuk mendapatkan gambaran dan kejelasan persoalan yang akan diselesaikan.

C. Instrumen Penelitian

Instrumen atau alat yang digunakan dalam penelitian ini terdiri dari perangkat keras komputer yaitu *laptop* dan untuk pembuatan aplikasi menggunakan perangkat lunak yang terdiri dari bahasa pemrograman Visual Basic dan aplikasi manajemen database MySQL. Sedangkan untuk mengolah data dan pembuatan laporan menggunakan aplikasi Microsoft Office.

D. Tahapan Penelitian

Secara garis besarnya, tahapan-tahapan penelitian yang dilakukan dalam perancangan dan pembuatan aplikasi sistem informasi ini adalah sebagai berikut.

1. Analisis Kebutuhan Sistem.
2. Rancangan Model Sistem.
3. Rancangan Sistem Aplikasi.
4. Implementasi Aplikasi.
5. Evaluasi Hasil Implementasi Aplikasi.

IV. HASIL DAN PEMBAHASAN

Hasil dari penelitian ini adalah berupa sebuah aplikasi prototipe e-voting yang terdiri dari halaman untuk memilih kandidat dan database hasil pilihan pemilih yang sudah dalam keadaan terenkripsi saat pengguna melakukan pemilihan.

A. Aplikasi untuk Memilih Kandidat

Aplikasi untuk memilih kandidat digunakan untuk memilih kandidat yang sudah disediakan dalam aplikasi tersebut. Tampilan memilih kandidat dapat dilihat pada gambar berikut ini.

Gambar 2. Tampilan Memilih Kandidat

B. Implementasi Algoritma Blowfish Dalam Aplikasi

Penggunaan algoritma kriptografi simetri blowfish dalam aplikasi e-voting adalah melakukan enkripsi saat pemilih memilih pasangan kandidat dan untuk dekripsinya dilakukan saat penghitungan perolehan suara pasangan kandidat. Proses enkrpsi dilakukan saat pemilih memilih kandidat dengan cara mengklik salah satu foto pasangan kandidat yang kemudian data pemilihan seperti nomor urut pasangan kandidat akan disimpan ke dalam database. Namun sebelum nomor urut tersebut disimpan, sistem akan melakukan proses enkripsi terlebih dahulu

dengan algoritma kriptografi blowfish terhadap nomor urut kandidat tersebut. Untuk menghindari chipertext yang sama berulang-ulang maka dilakukan pengacakan plaintext yang penulis namakan dengan manipulasi string. Adapun metode manipulasi string yang dimaksud cukup sederhana, yakni plaintext dalam hal ini nomor urut kandidat sebelum dilakukan pengacakan akan ditambahkan dengan Nomor Urut Kependudukan (NIK) yang memilih nomor urut kandidat tersebut. Sedangkan untuk proses dekripsinya dilakukan pengurangan plaintext setelah didekripsi sehingga data yang tersimpan tersisa nomor urut saja.

Gambar 8. Proses Enkripsi dan Dekripsi Nomor Urut Kandidat

Objects | tblpemilihan @dbevoting (Kon...

Begin Transaction | Memo | Filter | Sort | Import

id	id_nik	no_urut	tanggal	status_pilih
1	00001	A832FFBCAB0F481D	2015-10-22 11:32:58	Sudah
2	00002	3471C10FD1CFD6F9	2015-10-22 12:50:34	Sudah
3	00003	E921DA8E9F1E6B57	2015-10-22 14:17:38	Sudah
4	00004	4BE4A5C067A3A576	2015-10-22 19:44:23	Sudah

Gambar 9. Nomor Urut Pasangan Kandidat Berbentuk Chipertext

V. Kesimpulan

Berdasarkan pada pembahasan dan hasil penelitian dapat disimpulkan bahwa implementasi algoritma blowfish pada aplikasi e-voting dalam penelitian ini telah berjalan dengan baik dan sudah sesuai dengan yang diharapkan. Selain itu untuk melihat kinerja dan keakuratan enkripsi dan dekripsi dengan menggunakan algoritma blowfish, telah dilakukan uji coba dengan

membandingkan hasil proses klasifikasi dan rekapitulasi aplikasi e-voting dengan aplikasi Ms. Excel. Dari hasil perbandingan tersebut menunjukkan bahwa keluaran nilai antara keduanya adalah sama. Untuk itu maka bisa dikatakan bahwa prototipe aplikasi e-voting dengan menggunakan algoritma kriptografi blowfish telah berjalan dan berfungsi dengan baik.

REFERENSI:

1. Ariyus D, 2008. **Pengantar Ilmu Kriptografi (Teori Analisis dan Implementasi)**. Yogyakarta: Penerbit Andi.
2. Harahap R.N., Arifin S.P., & Syarif D. 2012. **Rancang Bangun Infrastruktur Teknologi Informasi dan Prototipe E-Voting Untuk Pilkada Di Pekanbaru**. Jurnal Sistem Informasi Volume 1.
3. Harahap R.N., Arifin S.P., & Syarif D. 2012. **Rancang Bangun Infrastruktur Teknologi Informasi dan Prototipe E-Voting Untuk Pilkada Di Pekanbaru**. Jurnal Sistem Informasi Volume 1.
4. Neyman S.N., Isnaini M.F., & Nurdiati S. 2013. **Penerapan Sistem E-Voting pada Pemilihan Kepala Daerah di Indonesia**. Jurnal Sains Terapan, Edisi III, Volume 3, Nomor 1, 45-61.
5. Rokhman A. 2011. **Prospek dan Tantangan Penerapan e-Voting di Indonesia**. Seminar Nasional Demokrasi dan Masyarakat Madani, Universitas Terbuka, Jakarta.
6. Sallu S. 2014. **Rancangan Sistem Informasi Pemilihan Umum Yang Real Time Menggunakan E-KTP Menuju Pemilu 2019**. Seminar Nasional Inovasi dan Teknologi Informasi (SNITI).
7. Sitinjak S., Yuli F., & Juwairiah. 2010. **Aplikasi Kriptografi File Menggunakan Algoritma Blowfish**. Seminar Nasional Informatika, UPN Veteran, Yogyakarta.
8. Sutardi. (2015**). Implementasi Algoritma Blowfish Untuk Keamanan Data Suara**. DINAMIKA Jurnal Ilmiah Teknik Mesin, Volume 6, Nomor 2.
9. Tetuko P.N., & Qoiriah A. (2013**). Rancang Bangun Aplikasi Enkripsi Database MySQL dengan Algoritma Blowfish**. Jurnal Manajemen Informatika, Volume 2, Nomor 1, 39-44.
10. Utami E., Erikawaty S., & Tambunan A. (2010). **Penerapan Algoritma Blowfish untuk Membuat Sebuah Model Kriptosistem Algoritma dan Menganalisis Kinerja Algoritma Blowfish dengan Simulasi Data Terbatas**. Open Journal System Jurnal DASI, Volume 11, Nomor 2.
11. Wibowo S., & Suprayogi. (2014). **Aplikasi Enkripsi Email dengan Menggunakan Metode Blowfish Berbasis J2SE**. Jurnal Tekonologi Informasi Techno.COM, Volume 13, Nomor 2, 75-83.