Teknik Pengamanan Data pada Sistem Proses Surat dengan Metode Blowfish di Badan Kepegawaian Daerah Provinsi Jawa Tengah

Agustinus Aditya Eka – A11.2009.05008
Program Studi Teknik Informatika – Fakultas Ilmu Komputer
Universitas Dian Nuswantoro – Semarang

ABSTRAK

Inovasi kemajuan jaringan komputer semakin lama semakin canggih dalam keamanan informasi data didalam dunia maya. Keamanan data merupakan kebutuhan penting dari perkembangan teknologi informasi karena tidak lepas dalam kehidupan sehari-hari, semisal penggunaan sosial media, file sharing, dan transaksi online. Dengan ilmu pengetahuan keamanan data sebuah teks dari informasi data dapat di enkripsi dan dideskripsi agar data tersebut tidak dapat diakses ataupun dilihat oleh pihak yang tidak memiliki kewenangan dalam mengakses informasi tertentu ilmu tersebut biasa dikenal dengan Kriptografi. Salah satu Algoritma Blowfish adalah metode teknik pengamananan data yang paling sulit untuk diretas. Algoritma Blowfish merupakan algoritma yang berjalan pada mode cipher blok dengan operasi yang sangat sederhana. Blowfish menggunakan operasi penambahan, ekslusif OR (XOR) dan penelusuran tabel. Teknik pengamanan data dengan Algoritma Blowfish dapat menjadi salah satu alternatif keamanan sistem didalam jaringan komputer. Penggunaan Algoritma blowfish ini bertujuan memperkenalkan metode baru untuk mengamankan informasi data login pada sistem proses surat di Badan Kepegawaian Daerah Provinsi Jawa Tengah.

Kata kunci : Kriptografi, Algoritma Blowfish, Enkripsi, Deskripsi, Sistem

1. Pendahuluan

Perkembangan *Information and Comunication Techology* (ICT) atau Teknologi Informasi dan Komunikasi (TIK) dari waktu ke waktu kian meningkat. Perkembangan teknologi meningkat dengan sangat pesat dan memiliki fungsi yang berbeda-beda sesuai dengan kebutuhan. Kebutuhan manusia akan perangkat informasi dan komunikasi tidak dapat dilepaskan dalam kehidupan sehari-hari, serta dapat membantu pekerjaan manusia lebih cepat dalam menyelesaikan tugas dengan tepat waktu dan menghemat biaya. Setiap hari inovasi akan perkembangan dalam bidang ini kian berkembang. Salah satunya adalah komunikasi data sebagai inovasi yang terus berkembang dalam jaringan komputer.

Jaringan komputer pada awalnya digunakan untuk bertukar informasi terhadap orang yang dipercayai sehingga dapat terbentuk interaksi atau hubungan dalam komunikasi, dan pada awal mulanya interaksi hanya terbatas antara dua orang yang saling bertukar informasi. Namun seiring berjalannya waktu dan berkembangnya ilmu pengetahuan di bidang Teknologi Informasi dan Komunikasi yang dapat berinteraksi langsung dengan, ada salah satu aspek pendukung yang sangat diperlukan, yaitu masalah keamanan data.

Dibalik kemudahan dan efisiensi biaya dalam hal berkomunikasi, berbagai jenis komunikasi data yang ada belum tentu aman untuk digunakan, karena belum tentu adanya standar keamanan yang digunakan untuk masing-masing perangkat komunikasi data tersebut. Yang membuat komunikasi menjadi salah satu ancaman akan adanya penyadapan ataupun pencurian data yang tidak diinginkan. Sebagai contoh telah banyak data-data penting dunia yang bocor, dan yang pernah terjadi yaitu situs web pemerintahan dan kepresidenan pernah diambil alih oleh hacker. Serta informasi pribadi yang kita miliki dapat bocor ataupun diambil oleh pihak yang tidak berwenang dan tidak berhak. Hal ini semakin membuktikan bahwa keamanan data (pada contoh ini adalah data tulisan dan berita) sangat dibutuhkan. Apalagi jika informasi yang

dibocorkan itu bersifat rahasia dan diterapkan dalam lingkup kenegaraan.

Solusi yang dapat diterapkan adalah mengenkripsi data (teks, visual atau suara). Teknik ini memiliki tingkat keamanan yang tinggi. Enkripsi dilakukan sebelum data itu dikirimkan, sehingga data yang dikirimkan tersebut tidak dapat dipahami oleh pihak yang tidak berhak meskipun data tersebut telah berhasil didapatkan atau diperoleh. Proses selanjutnya adalah proses deskripsi, yaitu kebalikan dari enkripsi. Mengubah data yang terenkripsi menjadi data semula. Deskripsi hanya dapat dilakukan oleh pihak yang berhak.

Sistem proses surat di Badan Kepegawaian Daerah (BKD) menjadi perhatian penulis untuk melakukan penelitian terhadap keamanan databasenya. Karena BKD sendiri merupakan intansi pemerintah yang bergerak di bagian Pegawai Negeri Sipil (PNS), yang memiliki kewenangan untuk mengeluarkan keputusan ataupun nota dinas untuk proses mutasi, pensiun, ataupun kenaikan pangkat terhadap PNS. Maka dari itu data yang ada di dalam BKD merupakan suatu rahasia negara.

Setelah penulis melakukan penelitian di BKD, banyak data-data yang tersimpan tidak menggunakan keamanan sistem, sehingga membuat data-data tersebut rentan untuk diambil ataupun diakses oleh karyawan atau orang lain yang tidak mempunyai kewenangan terhadap sistem tersebut. Karena jika ada pihak luar yang dapat mengakses sistem tersebut, maka dapat juga terjadi penggantian data tanpa melakukan prosedur yang benar.

Dengan ini tujuan dari penulis melakukan penelitian adalah untuk mengamankan data dalam sistem proses surat yang terdapat di BKD, karena data yang terdapat di BKD merupakan data yang bersifat rahasia. Dan sistem ini digunakan juga sebagai pengarsipan terhadap data yang telah di proses di BKD tersebut, sehingga dapat juga untuk mengamankan data arsip proses surat tersebut. Serta memberi batasan terhadap hak akses terhadap sistem tersebut.

Enkripsi dan deskripsi merupakan bagian dari kinerja sebuah algoritma kriptografi. Algoritma yang akan digunakan dalam tugas akhir ini adalah algoritma *Blowfish* sebagai salah satu jenis metode yang dapat diterapkan dalam pengamanan data.

2. Algoritma Blowfish

Blowfish adalah sebuah algoritma kriptografi yang beroperasi pada mode blok. Algoritma *Blowfish* merupakan algoritma yang diciptakan oleh seorang *cryptanalyst* bernama Bruce Schneier pada tahun 1993. Algoritma *Blowfish* termasuk ke dalam kriptografi kunci simetrik (S*ymmetric Cryptosystem*), dan metoda enkripsinya serupa dengan DES (*Data Encryption Standard-Like Cipher*). Algoritma ini ditujukan untuk mikroprosessor besar (32 bit ke atas dengan *cache* data yang besar). Algoritma *Blowfish* terdiri dari dua bagian yaitu ekspansi kunci dan enkripsi data. Ekspansi kunci mengubah sebuah kunci dengan panjang maksimal 448 bit kepada beberapa *array* subkunci dengan ukuran total 4168 *byte*. Secara umum, algoritma *Blowfish* dikembangkan untuk memenuhi kriteria sebagai berikut :

a. Cepat, pada implementasi yang optimal *Blowfish* dapat mencapai kecepatan 26 *clock cycle per byte*

b. Ringan, *Blowfish* dapat berjalan pada memori kurang dari 5KB

c. Sederhana, *Blowfish* hanya menggunakan operasi yang sederhana, yakni : penambahan (*addition*), XOR (Ekslusif OR), dan penelusuran tabel (*table lookup*) pada bilangan yang di operasikan (*operand*) 32-bit

d. Tingkat keamanan yang variatif, panjang kunci *Blowfish* dapat bervariasi (minimum 32 bit, maksimum 448 bit, *multiple* (kelipatan) 8 bit, *default* 128 bit).

Algoritma *Blowfish* merupakan algoritma yang kuat, dan sampai saat ini belum

ditemukan kelemahan yang berarti. Algoritma *Blowfish* pun dapat digabungkan dengan algoritma-algoritma enkripsi lainnya dalam mengenkripsi sebuah informasi/pesan untuk lebih menjamin isi dari pesan tersebut. Enkripsi data terdiri dari sebuah fungsi sederhana yang mengalami putaran atau iterasi sebanyak 16 kali. Setiap putaran terdiri dari sebuah permutasi yang bergantung pada kunci dan substitusi yang bergantung pada kunci dan data. Seluruh operasi berupa penambahan dan XOR (⊕) dengan kata sepanjang 32 bit. Operasi tambahan yang digunakan hanya berupa *data look-up* terhadap *array* dengan empat indeks yang dilakukan setiap putaran. *Blowfish* menggunakan sejumlah besar subkunci. Kunci-kunci tersebut harus dibangkitkan terlebih dahulu sebelum proses enkripsi dan dekripsi data dilakukan. Menurut Sukmawan (2000), alur proses enkripsi algoritma *Blowfish* dapat dijelaskan sebagai berikut:

1. *P-array* terdiri dari 18 buah subkunci dengan ukuran 32 bit:

   P1, P2, ..., P18
2. Empat buah Kotak-S dengan ukuran 32 bit mempunyai masukan sebanyak 256 buah. Kotak-kotak tersebut adalah:

   S1,0, S1,1, ..., S1,255
   S2,0, S2,1, ..., S2,255
   S3,0, S3,1, ..., S3,255
   S4,0, S4,1, ..., S4,255

   Subkunci dibangkitkan dengan menggunakan algoritma *Blowfish.*
3. Masukan terhadap jaringan *Feistel* ini adalah *X*, yang merupakan elemen data (plainteks) dengan ukuran 64-bit. Bila kurang dari 64-bit, maka akan dilakukan proses *padding* (penambahan bit).
4. Bagi *X* menjadi setengah bagian, yaitu dengan ukuran 32-bit. 32-bit pertama disebut *X*L, 32-bit yang kedua disebut *X*R.
5. Lakukan langkah-langkah berikut dalam 16 putaran (*iterasi*)

   $$XL = XL \oplus Pi$$

   $$XR = F(XL) \oplus XR$$

   Kemudian tukar *X*L dengan *X*R.

   Keterangan:

   i = 1, 2, …, 16 (menunjukkan nomor putaran/iterasi)
6. Setelah melakukan perulangan yang ke-16, lakukan lagi proses penukaran *X*L dengan *X*R.
7. Lakukan operasi XOR (⊕), yaitu :

   $$XR = XR \oplus P17$$
8. Lakukan operasi XOR (⊕), yaitu :

   $$XL = XL \oplus P18$$
9. Gabungkan kembali *X*L dan *X*R, yaitu :

   $$X = XR + XL$$

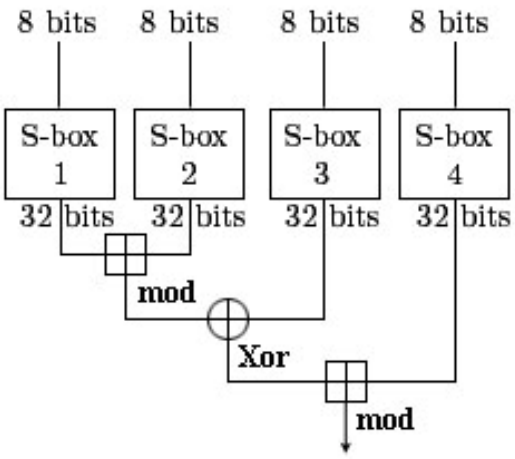
Fungsi F yang terdapat pada jaringan *Feistel* didefinisikan sebagai berikut:

1. Bagi *X*L menjadi empat bagian yang berukuran 8 bit. Keempat bagian yang dihasilkan adalah *a*, *b*, *c*, dan *d*.

2. Fungsi F(*X*L) didefinisikan sebagai berikut:

$F(XL) = ((S1,a + S2,b \bmod 2^{32}) \oplus S3,c) + S4,d \bmod 2^{32}$

Proses dekripsi dilakukan dengan langkah yang sama dengan proses enkripsi, kecuali *P1, P2, ..., P18* digunakan dengan urutan terbalik dari proses enkripsi.



Skema S-box

Implementasi algoritma *Blowfish* yang memerlukan waktu cepat harus mengurangi jumlah putaran dan memastikan bahwa semua subkunci tersimpan dalam *cache* (penyimpanan sementara).

3. Metode Pengembang Sistem

Metode pengembangan adalah menyusun suatu system yang baru untuk menggantikan system yang lama secara keseluruhan atau memperbaiki system yang telah berjalan.

Metode yang dipakai adalah *Prototyping*, karena metode ini memiliki perkembangan siklus yang cepat dan pengujian terhadap model kerja (prototipe) dari aplikasi baru melalui proses interaksi dan berulang-ulang yang biasa digunakan ahli sistem informasi dan ahli bisnis. *Prototyping* disebut juga desain aplikasi cepat (rapid application design/RAD) karena menyederhanakan dan mempercepat desain sistem.

Sering kali seorang user dapat mendefinisikan serangkaian sasaran umum perangkat lunak, tetapi tidak melakukan identifikasi kebutuhan output, pemrosesanm ataupun input detail. Pada kasus lain , pengembang mungkin tidak memiliki data mengenai kepastian terhadapa efisiensi algoritma, kemampuan penyseuaian dari sebuah sistem operasi, atau bentuk – bentuk yang harus dilakukan oleh interaksi manusia dengan komputer. Dalam hal ini banyak pula situasi situasi yang lain dalam kehidupan, sehingga paradigm *prototyping* mungkin menawarkan pendekatan yang lebih baik.

Prototyping paradigm dimulai dengan mengumpulkan kebutuhan. Perancang dan pemakai sistem bertemu, dan mendefinisikan obyektif keseluruhan dari perangkat lunak yang akan dibuat, mengidentifikasi segala kebutuhan yang diketahui dan area garis besar dimana definisi lebih jauh merupakan keharusan kemudian dilakukan perancangan kilat. Perancangan kilat berfokus pada penyajian dari aspek – aspek perangkat lunak tersebut yang akan nampak bagi user. Perancangan kilat membawa konstruksi sebuah *prototyping*. *Prototyping* tersebut kemudian dievaluasi oleh user dan dipakai untuk menyaring kebutuhan pengembangan perangkat lunak. Iterasi terjadi pada saat *prototyping* kemudian di set untuk memenuhi kebutuhan dalam keamanan data. Kemudian di saat yang bersamaan pengembang melakukan pengamatan sehingga pengembang lebih mengerti tentang keamanan data dengan algoritma blowfish.

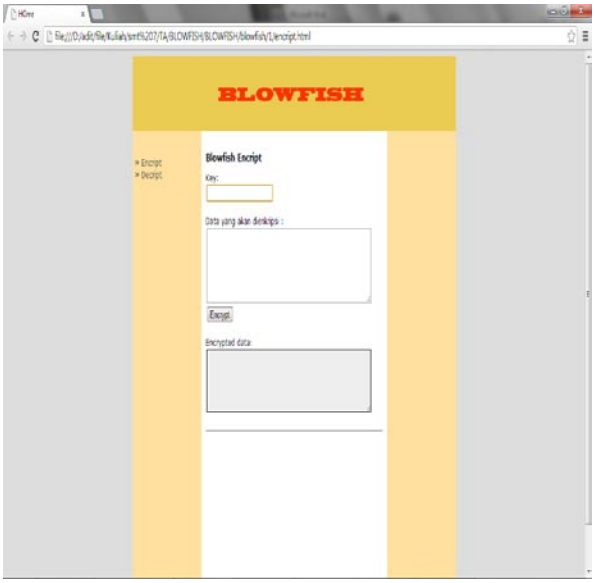
4. Perancangan Sistem

Kematangan dan terealisasinya sebuah pekerjaan pembangunan perangkat lunak didasarkan pada bagian perancangan dan analisa kebutuhan. Pada tahap ini, ditentukan persyaratan secara teknis secara terperinci. Sehingga dengan analisa, sistem dapat mampu membuktikan perancangan keamanan sistem dengan menggunakan algoritma blowfish yang dapat melakukan enkripsi dan deskripsi sebagai pembuktian atas perancangan sistem ini. Serta dapat diterapkan untuk mengamankan login pada sistem proses surat di Badan Kepegawaian Daerah Provinsi Jawa Tengah.

4.1 **Perancangan form Enkripsi dan Deskripsi**

Program enkripsi adalah form masukan teks yang akan diproses untuk dienkripsi. Ada dua jenis data masukan, yaitu data plainteks dan kunci. Program deskripsi adalah form masukan teks untuk membuktikan hasil dari

enkripsi yang telah menjadi chiperteks untuk menjadi plainteks kembali. Di dalam program deskripsi ada dua data masukan, yaitu hasil chiperteks dari hasil enkripsi dan kunci yang sama dengan kunci pada program enkripsi.



Gambar Rancangan form sistem enkripsi

Gambar Rancangan Form Sistem Deskripsi

4.2 **Validasi Data Masukan**

Ketika user memasukkan data sebagai data masukan, dimungkinkan terjadinya kesalahan-kesalahan, yaitu: kunci kosong (*blank password*), plainteks bukan dalam standar ASCII (Sebagai contoh: huruf katakana dan hiragana). Oleh karena itu, untuk menghindari terjadinya hal tersebut, diperlukan beberapa langkah validasi.

Ketentuan-ketentuan yang digunakan dalam validasi data masukan adalah :

1. tidak diperbolehkan tidak mengisi kata kunci (kunci kosong),
2. tidak diperbolehkan memasukkan karakter lain selain standar ASCII

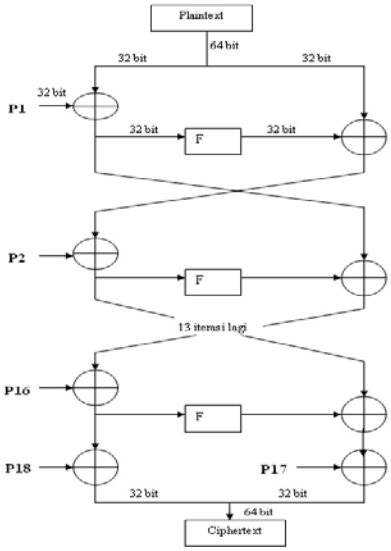
4.3 **Struktur Algoritma Blowfish**

Blowfish adalah algoritma kunci simetri, yang berarti menggunakan kunci yang sama untuk melakukan enkripsi dan dekripsi berkas. Blowfish juga merupakan cipher blok, yang berarti selama proses enkripsi dan dekripsi, Blowfish akan membagi pesan menjadi blok-blok dengan ukuran yang sama panjang. Panjang blok untuk algoritma Blowfish adalah 64-bit, yang merupakan *multiple* (kelipatan) dari 8-bit. Jika bukan merupakan kelipatan dari 8-bit, maka akan ditambahkan bit-bit tambahan (*padding*) sehingga ukuran untuk tiap blok sama.

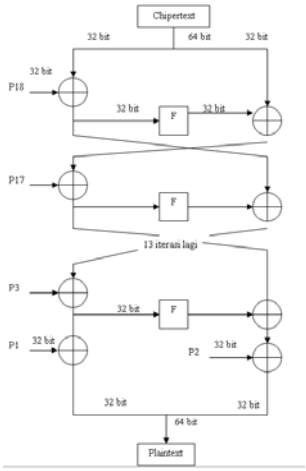
Proses blowfish dalam enkripsi dibagi menjadi dua dengan besaran yang sama yaitu XL dan XR dengan panjang 32-bit. Didalam XL kunci pada plainteks ditambahkan yang kemudian digabungkan bersama XR yang mempunyai proses array dalam kunci blowfish dengan s-box, yang terdiri dari s-box[0], s-box[1], s-box[3] dan s-box[4].

Algoritma dalam Blowfish terbagi menjadi dua bagian, yaitu ekspansi kunci (*key expansion*) dan enkripsi data (*data encryption*). Proses ekspansi kunci akan melakukan konversi sebuah kunci mulai dari 56-byte (448-bit) sampai beberapa beberapa *array* sub kunci dengan total mencapai 4168-byte.

Sedangkan proses enkripsi data terjadi pada jaringan Feistel, yang mengandung fungsi pengulangan (iterasi) sebanyak enam belas kali. Blowfish menggunakan jaringan *Feistel* yang terdiri dari 16 buah putaran. Skema jaringan *Feistel* pada algoritma Blowfish dapat dilihat pada Gambar



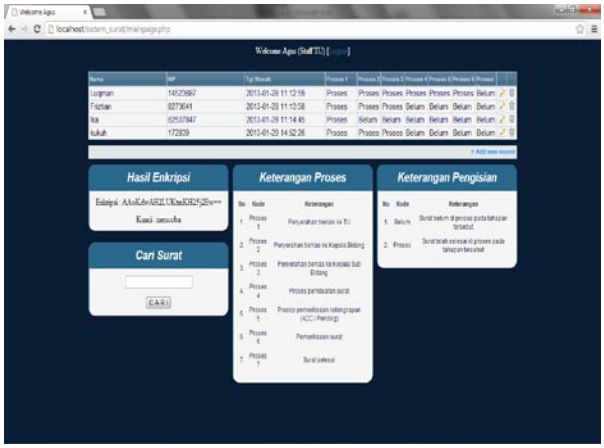
Gambar Skema Jaringan Feistel pada Algoritma Enkripsi Blowfish



Gambar Skema Jaringan Feistel pada Algoritma Deskripsi Blowfish

4.4 Sistem Login pada Proses Surat

Gambar Halaman Login pada Sistem Proses Surat



Gambar Halaman Isi pada Sistem Proses Surat

5. Kesimpulan

Berdasarkan pembahasan dapat diambil kesimpulan sebagai berikut:

a. Telah dibuat sistem pengamanan data dengan menggunakan algoritma Blowfish, khususnya data teks.

b. Blowfish merupakan salah satu solusi yang baik untuk mengatasi masalah keamanan dan kerahasiaan data yang pada umumnya diterapkan dalam saluran komunikasi dan berkas.

c. Algoritma Blowfish merupakan algoritma dengan operasi yang sederhana dan menggunakan jaringan *Feistel*

d. Tingkat keamanan algoritma Blowfish ditentukan oleh jumlah iterasi dan panjang kunci yang digunakan.

e. Algoritma Blowfish merupakan algoritma yang kuat, yang belum ditemukan titik lemahnya.

f. Menerapkan Algoritma Blowfish ke dalam Sistem Proses Surat di Badan Kepegawaian Daerah Provinsi Jawa Tengah.

6. Daftar Pustaka

Ratih. "STUDI DAN IMPLEMENTASI ALGORITMA BLOWFISH UNTUK APLIKSI ENKRIPSI DAN DEKRIPSI FILE" http://www.informatika.org/~rinaldi/Kriptografi/2006-2007/Jurnal/Jurnal1-077.pdf

Pratiwi, Aprianti. "IMPLEMENTASI ENKRIPSI DATA DENGAN ALGORITMA BLOWFISH MENGGUNAKAN JAVA PADA APLIKASI EMAIL" http://opencourseware.politekniktelkom.ac.id

Purwanto, Anggi. "Implementasi Sistem Keamanan File Menggunakan Algoritma Blowfish pada Jaringan LAN" http://openstorage.gunadarma.ac.id/~mwiryana/KOMMIT/per-artikel/03-02-008-Implementasi[Ledya].pdf

Susanto, Hery. "Pembangunan Com Add In Microsoft Outlock Dengan Memanfaatkan Algoritma Blowfish" www.mercubuana.ac.id/file/JURNAL%20hery%20susanto.pdf

Sitinjak, Suriski. "APLIKASI KRIPTOGRAFI FILE MENGGUNAKAN ALGORITMA BLOWFISH" http://repository.upnyk.ac.id/395/1/C12_APLIKASI_KRIPTOGRAFI_FILE_MENGGUNAKAN_ALGORITMA_BLOWFISH.pdf

Kurniawan J., Ir. , M.T (2004)., Kriptografi, Keamanan Internet dan Jaringan Komunikasi, Penerbit Informatika Bandung.

Aryus, Doni. (2008). Pengantar Ilmu Kriptografi. Yogyakarta: Andi

Howard, Jhon D.(1997). An Analysis Of Security Incidents On The Internet.

Munir, Rinaldi. (2006). *Kriptografi*. Penerbit Informatika Bandung.

Schneier, Bruce (1996). *Applied Cryptography 2nd.* Penerbit John Willey & Sons

Sukmawan, Budi (2000). *Metoda Enkripsi Blowfish. http://bdg.centrin.net.id/~budskman/artikel.htm*