Implementasi Algoritma *Twofish* Untuk Sekuriti Dan RSA Untuk Otentikasi Pada *Website* Lowongan Pekerjaan

James Filipus / 13507087
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
if17087@students.if.itb.ac.id, james_filipus_12@hotmail.com

***Abstrak*—Pengangguran merupakan salah satu masalah utama yang dihadapi oleh bangsa Indonesia dan berdampak negatif pada tingkat perekonomian rakyat. Akan tetapi sebenarnya letak permasalahan bukan pada tidak tersedianya lowongan pekerjaan, akan tetapi karena informasi mengenai lowongan pekerjaan tersebut kurang terdistribusi. Di lain pihak masalah dalam sekuriti dan otentikasi pada *website* di jaringan internet juga perlu diperhatikan karena penyadapan dan manipulasi data semakin marak.**

Dengan memanfaatkan media internet, maka penyebaran informasi lowongan pekerjaan dapat menjadi lebih mudah dan efisien. Akan tetapi masih ada masalah mengenai sekuriti dan otentikasi di media internet, untuk mencegah terjadinya masalah ini kebanyakan *website* menggunakan HTTPS agar dapat melakukan transfer data dengan aman. Akan tetapi untuk menggunakan HTTPS diperlukan biaya tambahan yang tidak sedikit oleh karena itu pada Tugas Akhir ini digunakan alternatif lain yaitu dengan mengimplementasikan algoritma *Twofish* dan RSA pada *website* lowongan pekerjaan. Algoritma *Twofish* merupakan algoritma kriptografi simetris yang merupakan salah satu finalis dalam kompetisi AES, kekuatan dan kecepatan algoritma *Twofish* dapat diandalkan untuk sekuriti pada *website*. Sedangkan untuk otentikasi *website* dapat menggunakan fungsi hash SHA-1 dan algoritma RSA untuk membubuhi tanda tangan digital pada *email* yang dikirim dari *server*.

Implemetasi dalam Tugas Akhir ini berupa sebuah *website* lowongan pekerjaan bernama "Job And Friends" dengan implementasi algoritma *Twofish* untuk sekuritinya dan implementasi algoritma RSA untuk otentikasinya. *Website* dibangun menggunakan kakas Microsoft Visual Studio 2010 dengan bahasa C# dan berjalan dalam sistem operasi Windows. Algoritma *Twofish* diimplementasikan menggunakan bahasa C# pada *server* dan bahasa *javascript* pada *client.* Sedangkan algoritma RSA hanya diimplementasikan dalam bahasa C# pada *server*.

Dengan implementasi algoritma *Twofish* untuk transfer data dan basis data pada *website* "Job And Friends" maka setiap data yang ditransfer dan tersimpan dalam basis data sudah berbentuk cipherteks sehingga dapat mencegah terjadinya penyadapan. Untuk setiap *email* yang dikirim dari *website* sudah dibubuhi tanda tangan digital dan dapat divalidasi melalui halaman yang tersedia pada *website* sehingga dapat mencegah terjadinya manipulasi informasi.

***Kata kunci*— pengangguran, internet, distribusi lowongan kerja, sekuriti *website*, otentikasi *email*, Job And Friends, *Twofish*, SHA-1, RSA.**

I. PENDAHULUAN

Pengangguran merupakan salah satu masalah utama yang banyak terjadi di Indonesia. Sebenarnya yang menjadi penyebab utama masalah pengangguran ini bukan karena kurangnya lapangan pekerjaan yang tersedia, tetapi karena kurang terdistribusinya lapangan pekerjaan yang ada sehingga sulit diketahui informasi tentang lowongan pekerjaan dan informasi mengenai cara melamar pekerjaannya. Internet merupakan sebuah media yang sangat efektif untuk menyebarkan informasi, dalam hal ini yaitu menyebarkan informasi mengenai lowongan pekerjaan. Pada umumnya informasi yang di simpan di internet dapat berupa *website*, dimana para pengunjung *website* dapat mengeksplorasinya untuk mendapatkan informasi yang sesuai dengan kebutuhan pengunjung. Selain itu *website* di internet dapat diakses dengan mudah oleh semua orang yang memiliki akses internet dan juga internet bersifat global sehingga dapat diakses dari mana pun.

Akan tetapi ada kelemahan dari internet yaitu dari sisi keamanannya. Keamanan dari sebuah *website* semakin menjadi faktor yang penting dan perlu perhatian khusus karena di jaman sekarang yang semakin maju, semakin banyak pula penyadapan dan penyalah gunaan informasi pada *website* yang ada di internet untuk keuntungan pribadi ataupun untuk tujuan-tujuan yang tidak baik. Untuk itu diperlukan suatu bentuk sekuriti agar keamanan dari *website* terjamin beserta informasi dan data yang tersimpan di dalamnya sehingga tidak disalahgunakan oleh pihak yang tidak diinginkan. Salah satu cara yang dapat digunakan untuk sekuriti *website* adalah dengan menggunakan kriptografi.

Dengan memanfaatkan kriptografi khusunya pengenkripsian dan pendekripsian pesan maka data dan informasi yang disimpan maupun dikirimkan di internet dapat semakin terjamin keamannya. Dalam pelaksanaan Tugas Akhir ini algoritma Twofish dimanfaatkan untuk mengenkripsi data dan informasi yang akan dikirimkan

antar *client* dan *server*, serta untuk mengenkripsi data yang disimpan di *server website*. Algoritma Twofish merupakan salah satu dari lima pemenang AES (Advanced Encryption Standard), dimana AES merupakan standar enkripsi dengan kunci simetris yang diadopsi oleh pemeritah Amerika Serikat, oleh karena itu algoritma ini tidak diragukan lagi dari segi kekuatan, performansi dan kecepatan enkripsinya (Federal Information Processing Standards Publication 197, 2001).

Keamanan dari *website* juga mencakup otentikasi dan orisinalitas data dan informasi yang diperoleh pengunjung *website* dari *website* tersebut. Seiring dengan berkembangnya teknologi dan dunia informasi maka tingkat pemalsuan atau modifikasi informasi yang ditujukan untuk kepentingan pribadi atau penipuan semakin meningkat pula. Untuk itu diperlukan suatu bentuk otentikasi dalam memeriksa keaslian dari setiap informasi yang diterima. Hal ini dapat dilakukan dengan membubuhkan tanda tangan digital pada *email* yang akan dikirimkan oleh *website* yang dibangun dalam pelaksanaan Tugas Akhir ini. Dalam mengimplementasikan tanda tangan digital menggunakan fungsi hash SHA-1 dan RSA (Rives Shamir Adleman) yang merupakan algoritma enkripsi yang populer digunakan oleh perusahaan sekuriti jaringan di Amerika Serikat. Dengan memanfaatkan kedua algoritma ini setiap *email* yang dikirim oleh *website* akan ditanda tangan digital sehingga penerima dapat mengotentikasi keaslian dari *email* tersebut.

Sebenarnya peluang ini sudah dilihat oleh beberapa pihak baik dalam dan luar negri serta sudah diimplementasikan yaitu dalam bentuk *website* yang memuat informasi mengenai lowongan pekerjaan dan cara melamar pekerjaan tersebut (seperti www.jobstreet.com dan www.bursalowonganpekerjaan.com). Secara garis besar *website* ini bertujuan untuk mendistribusikan dan mempermudah akses serta proses pelamaran pekerjaan, akan tetapi untuk sekuriti dari proses transfer data, *website* tersebut kebanyakan menggunakan HTTPS untuk transfer data aman sehingga perlu biaya tambahan yang tidak sedikit. Maka dari itu, dengan implementasi algoritma Twofish khususnya untuk sekuriti transfer data pada *website* lowongan pekerjaan, maka data yang ditransfer akan tetap aman dan terbebas dari penyadapan meskipun tanpa menggunakan HTTPS. Penghematan biaya ini menjadi suatu kelebihan dari *website* yang dibangun dari *website* lowongan pekerjaan lain yang menggunakan HTTPS. Selain itu keaslian *email* yang dikirim dari *website* pun dapat dijamin karena *email* dibubuhi tanda tangan digital menggunakan SHA-1 dan RSA.

II. TEORI YANG DIGUNAKAN

A. Kriptografi

Menurut Rinaldi Munir (2005), kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematis yang berhubungan dengan aspek keamanan informasi seperti : keabsahan, integritas data, serta autentifikasi data.

Prosesnya pada dasarnya sangat sederhana. Sebuah plaintext (m) akan dilewatkan pada proses enkripsi (E) sehingga menghasilkan suatu ciphertext (c). Kemudian untuk memperoleh kembali plaintext, maka ciphertext (c) melalui proses dekripsi (D) yang akan menghasilkan kembali plaintext (m).

Berdasarkan jenis kunci yang digunakan dalam proses enkripsi dan dekripsi, kriptografi dapat dibedakan menjadi dua jenis, yaitu kriptografi simetrik dan kriptografi asimetrik. Kriptografi simetrik sangat menekankan pada kerahasiaan kunci yang digunakan untuk proses enkripsi dan dekripsi. Oleh karena itulah kriptografi ini dinamakan pula sebagai kriptografi kunci rahasia. Kriptografi asimetrik adalah algoritma kriptografi yang menggunakan kunci yang ber beda untuk proses enkripsi dan dekripsinya. Skema ini disebut juga sebagai sistem kriptografi kunci publik karena kunci untuk enkripsi dibuat secara umum (public-key) atau dapat diketahui oleh siapa saja, tetapi untuk proses dekripsinya yang dibuat satu saja, yakini hanya oleh yang berwenang untuk mendekripsinya (disebut private-key).

B. Algoritma Twofish

Twofish menggunakan sebuah Struktur Feistel-like 16-round dengan tambahan whitening pada masukan dan keluaran. Satu-satunya unsur non-Feistel adalah 1-bit rotasi. Perputaran dapat dipindah ke dalam fungsi F untuk membuat suatu struktur Feistel murni, tapi memerlukan suatu tambahan perputaran kata-kata yang tepat sebelum langkah keluaran whitening (Horatio Paul Stancu, 2004).

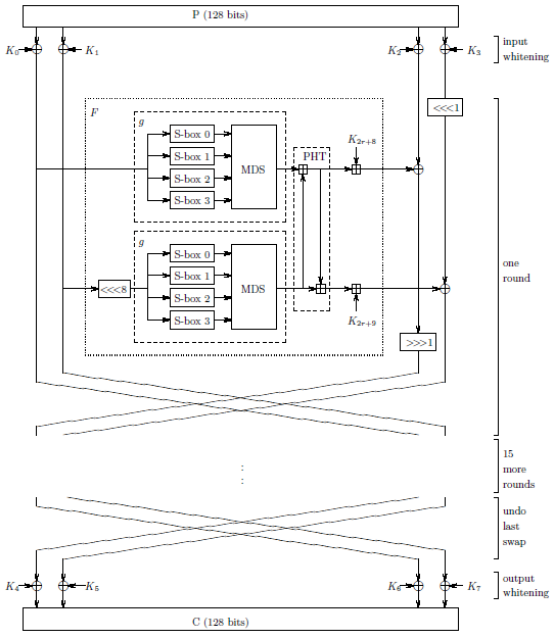
Plaintext dipecah menjadi empat kata 32-bit. Pada langkah whitening masukan terdapat xored dengan empat kata kunci. Ini diikuti oleh enam belas putaran. Pada setiap putaran, dua kata-kata pada sisi kiri digunakan sebagai masukan kepada fungsi g (Salah satu darinya diputar pada 8 bit pertama). Fungsi g terdiri dari empat byte-wide S-Box key-dependent, yang diikuti oleh suatu langkah pencampuran linier berdasar pada suatu matriks MDS. Hasil kedua fungsi g dikombinasikan menggunakan suatu Pseudo Hadamard Transform (PHT), dan ditambahkan dua kata kunci. Kedua hasil ini kemudian di-XOR ke dalam kata-kata pada sisi kanan (salah satunya diputar ke kanan 1 bit pertama, yang lainnya diputar ke kanan setelahnya). Yang kiri dan kanan dibelah dua kemudian ditukar untuk putaran yang berikutnya, pertukaran yang terakhir adalah dibalik, dan yang empat kata di-XOR dengan lebih dari empat kata kunci untuk menghasilkan ciphertext. Secara formal, 16 byte plaintext p0,… p15 yang yang pertama dipecah menjadi 4 kata P0,…P3 dari 32 bit masing-masing menggunakan konvensi little-endian.

$$P_i = \sum_{j=0}^{3} P(4i+j).2^{8j} \qquad i=0,\ldots,3$$

Di dalam langkah whitening, kata-kata ini di-XOR dengan 4 kata dari kunci yang diperluas.

$$R_{0,i} = P \oplus K_i \qquad i=0,\ldots,3$$

Gambar 1 memperlihatkan struktur dari blok-cipher Twofish.



Gambar 1. Skema enkripsi dan dekripsi algoritma Twofish (Bruce Schneier, 1998)

Pada setiap 16 putaran, dua kata pertama digunakan sebagai masukan kepada fungsi F, yang juga mengambil angka bulat itu sebagai masukan. Kata yang ketiga di-XOR dengan keluaran pertama F dan kemudian diputar ke kanan satu bit. Kata keempat diputar ke kiri satu bit kemudian di-XOR dengan kata keluaran F Yang kedua . Akhirnya, keduanya saling ditukar menghasilkan persamaan :

$$\begin{aligned} (Fr,0,Fr,1) &= F(Fr,0,Fr,1,r) \\ Rr+1,0 &= ROR(Rr,2) \oplus Fr,0,1) \\ Rr+1,1 &= ROL(Rr,3,1) \oplus Fr,1 \\ Rr+1,2 &= Rr,0 \\ Rr+1,3 &= Rr,1 \end{aligned}$$

untuk r= 0,…,15 di mana ROR dan ROL adalah berfungsi memutar argumentasi pertama (32-bit kata) ke kanan dengan angka bit-bit diindikasikan dengan argumentasi keduanya. Langkah whitening keluaran membatalkan `pertukaran' putaran terakhir dan meng XOR kata-kata dengan 4 kata dari kunci yang diperluas.

$$Ci = R16,(i+2) \bmod 4 \oplus Ki+4 \qquad I = 0,\ldots,3$$

Eempat kata dari ciphertext kemudian menulis seperti 16 byte c0,…,c15 sama seperti menggunakan konversi little-endian untuk plaintext.

$$ci = \left\lfloor \frac{C\lfloor i/4 \rfloor}{2^{8(i \bmod 4)}} \right\rfloor \bmod 28 \qquad i = 0,\ldots,15$$

C. HTTPS

HTTPS adalah HTTP melalui SSL. Oleh karena itu untuk memahami HTTPS diperlukan pengertian yang lebih dalam terlebih dahulu mengenai HTTP atau Hyper Text Transfer Protocol, dimana HTTP adalah protokol atau bahasa yang digunakan oleh semua web browser saat berkomunikasi atau behubungan dengan web *server*. Sedangkan SSL atau Secure Sockets Layer adalah protocol yang menyediakan jalan yang aman bagi web browser dan web *server* untuk saling berkomunikasi. (Thomas Boutell, 2011)

Ketika web browser dan web *server* saling berkomunikasi melalui HTTPS, keduanya perlu melakukan verifikasi mengenai identitas masing-masing dan juga metode enkripsi yang hendak digunakan. Enkripsi digunakan untuk mengenkripsi kunci yang dikirim, data utama dan juga HTTPS memanfaatkan fungsi hash untuk mengirimkan message digest dari komunikasi yang terlaksana antara web browser dan web *server*. Penentuan algoritma enkripsi dan juga fungsi hash yang diguanakan dilakukan melalui sertifikat SSL, dan untuk memperoleh sertifikat SSL ini diperlukan biaya sesuai dengan spesifikasi dan waktu berlaku dari sertifikat SSL tersebut. Metode enkripsi yang digunakan pun ditentukan berdasarkan sertifikat SSL. Pada proses komunikasi melalui HTTPS, koneksi terlaksana pada TCP/IP dengan port nomor 443. Sedangkan komunikasi yang melalui HTTP menggunakan koneksi TCP/IP pada port 80.

D. Fungsi SHA-1

Hash atau kadang disebut dengan digest adalah semacam tanda tangan untuk sebuah teks atau file data. Sebagai contoh SHA-1 menghasilkan 160 bit tanda tangan untuk sebuah teks. Untuk *digital signatures*, dilakukan dengan cara mengenkrip nilai hash sebuah dokumen dengan menggunakan *private key*, sehingga menghasilkan tanda tangan digital untuk dokumen tersebut. Orang lain dapat memeriksa otentikasi dokumen tersebut dengan cara mendekrip tanda tangan tersebut menggunakan *public key* untuk mendapatkan nilai hash yang asli dan membandingkannya dengan nilai hash dari teks.

E. RSA

RSA merupakan salah satu algoritma kunci publik yang paling terkenal. Algoritma RSA ini dibuat oleh Ron Rivest, Adi Shamir dan Leonard Adleman yang merupakan tiga orang peneliti dari MIT. Berikut adalah besaran besaran yang digunakan pada algoritma RSA menurut Rinaldi Munir (2005):

1. p dan q bilangan prima (rahasia)
2. n = p . q (tidak rahasia)
3. ∅(n) =(p -1)(q – 1) (rahasia)
4. e (kunci enkripsi) (tidak rahasia)
5. d (kunci dekripsi) (rahasia)
6. m (plainteks) (rahasia)
7. c (cipherteks) (tidak rahasia)

Algoritma RSA memiliki dua bagian yaitu algoritma pembangkit pasangan kunci untuk proses enkripsi dan dekripsi dan algoritma enkripsi dan dekripsi itu sendiri.

Enkripsi

1. Ambil kunci publik peneriman pesan, e, dan modulus n
2. Nyatakan plainteks m menjadi blok-blok $m_1, m_2, ...$, sedemikian sehingga setiap blok merepresentasikan nilai di dalam selang $[0, n-1]$
3. Setiap blok m_i dienkripsi menjadi blok c_i dengan rumus

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

Dekripsi

1. Setiap blok cipherteks c_i didekripsi kembali menjadi blok m_i dengan rumus

$$m_i = c_i^d \bmod n$$

F. Pembangkit Pasangan Kunci

Dalam algoritma RSA diperlukan pasangan kunci yaitu kunci privat dan kunci publik untuk mengenkripsi dan mendekripsi pesan rahasia. Antara kunci privat dan kunci publik terdapat suatu keterikatan matematik, oleh karena itu algoritma pembangkit pasangan kunci digunakan dalam lagoritma RSA. Langkah-langkah untuk membangkitkan pasangan kunci yaitu sebagai berikut :

1. Pilih dua buah bilangan prima sembarang, p dan q.
2. Hitung $n = p \cdot q$ (sebaiknya $p \neq q$, sebab jika $p = q$ maka $n = p^2$ sehingga p dapat diperoleh dengan menarik akar pangkat dua dari n
3. Hitung $\emptyset(n) = (p-1)(q-1)$
4. Pilih kunci publik, e, yang relative prima terhadap $\emptyset(n)$
5. Bangkitkan kunci privat dengan menggunakan persamaan

Karena $e \cdot d \equiv 1 \pmod{\emptyset(n)} e \cdot d \equiv 1 \pmod{\emptyset(n)}$ ekivalen dengan $e \cdot d = 1 + k\emptyset(n)$, maka ddapat dihitung dengan

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

Akan terdapat bilangan bulat k yang memberikan bilangan bulat d. Maka hasil dari proses pembangkitan pasangan kunci di atas:

- Kunci publik (e, n)
- Kunci privat (d, n)
-

Dimana n tidak bersifat rahasia karena kan diperluakn dalam perhitungan enkripsi dan dekripsi (Rinaldi Munir, 2005).

III. ANALISIS

A. Analisis Masalah

Masalah yang diangkat sebagai fokus dan topik utama dari Tugas Akhir ini yaitu tingginya tingkat pengangguran di Indonesia dan juga rentannya sekuritas di dunia maya khususnya dalam hal sekuriti *website* dan otentikasi.

Sebenarnya yang menjadi penyebab utama masalah pengangguran ini bukan karena kurangnya lapangan pekerjaan yang tersedia, tetapi karena kurang terdistribusinya lapangan pekerjaan yang ada sehingga para pencari sulit diketahui informasi tentang lowongan pekerjaan. Faktor lain yang menyebabkan banyak orang mengangur yaitu jumlah yang sedikit untuk sarana yang memadai, aman, mudah, murah dan dapat dipercaya untuk menyalurkan informasi mengenai lowongan pekerjaan dari pihak penyedia kerja langsung ke para pencari kerja.

Kurang terdistribusinya informasi mengenai lapangan pekerjaan yang tersedia akan menjadi topik bahasan dan permasalahan yang dibahas serta akan dicoba diatasi melalui Tugas Akhir ini. Informasi mengenai lowongan pekerjaan tidak terdistribusi dengan baik dapat mengakibatkan informasi tersebut sampai ke calon pekerja yang kurang tepat atau tidak sesuai dengan kriteria yang diinginkan perusahaan ataupun pekerjaan yang tidak sesuai dengan yang diinginkan oleh seorang calon pekerja.

Pemilihan media publikasi lowongan pekerjaan yang kurang tepat pun dapat mengakibatkan informasi tidak sampai pada para calon pekerja yang potensial yang diinginkan oleh perusahaan. Media internet dipilih sebagai media yang akan digunakan untuk mendistribusikan lowongan pekerjaan karena dianggap paling efektif.

Akan tetapi di balik semua kenyamanan dan kemudahan yang diperoleh dari media internet, ada pula kelemahan yang terkadang terlupakan atau bahkan tidak diketahui oleh pengguna internet yaitu bahwa arus informasi yang lalu lalang di jaringan internet itu dapat disadap oleh pihak lain. Sehingga informasi yang bersifat rahasia dan tidak boleh diketahui orang lain dapat disadap dan diketahui oleh pihak lain. Hal ini menyebabkan

internet menjadi media yang kurang aman karena mudahnya menyadap informasi dikirimkan melalui internet. Baik informasi tersebut berupa *email* maupun berupa paket-paket data yang dikirimkan antara *client* dan *server* dari sebuah *website*.

Oleh karena itu banyak upaya yang dilakukan untuk menjaga agar jaringan internet tetap aman dan dapat digunakan dengan bebas tanpa takut adanya penyadapan. Yaitu dengan membuat saluran yang aman untuk transfer data, sebagai contoh yaitu mengirimkan data melalui HTTPS dimana data yang dikirimkan menggunakan SSL. Dengan HTTPS maka data yang dikirim antar *client* dan *server* sudah dienkripsi sehingga walaupun disadap oleh pihak lain, infromasi yang ada di dalam nya tidak akan dapat diketahui karena berupa cipherteks. Akan tetapi untuk menggunakan HTTPS ini diperlukan biaya tambahan, yaitu biaya untuk membeli sertifikat SSL dari penyedia layanan HTTPS dan biaya yang dibutuhkan tidaklah sedikit dan biasanya hanya berlaku untuk setahun.

Tidak hanya penyadapan saja yang marak terjadi di dunia maya, manipulasi data pun menjadi semakin banyak terjadi. Manipulasi data yang dilakukan biasanya didasari motif untuk keuntungan pribadi. Dalam Tugas Akhir ini yang menjadi fokus bahasan dari manipulasi data adalah manipulasi *email*.

B. Analisis Solusi

Seperti yang telah dibahas pada sub bab Analisis Masalah, salah satu penyebab utama tingginya tingkat pengangguran di Indonesia yaitu kurang terdistribusinya informasi lowongan pekerjaan yang tersedia dan informasi lowongan pekerjaan yang tidak sampai pada target yang tepat. Maka solusi yang dibangun pada Tugas Akhir ini adalah "Job And Friends", sebuah *website* lowongan pekerjaan dimana pada *website* ini seorang wakil dari perusahaan dapat mendaftarkan perusahaannya dengan mengisi data perusahaannya dan menyimpannya pada *website* ini. Setelah perusahaan didaftarkan maka seorang wakil perusahaan dapat mendaftarkan lowongan pekerjaan dari perusahaan yang bersangkutan. Di lain pihak seorang calon pelamar pekerjaan dapat mendaftarkan dirinya dengan mengisi data diri dan menyimpannya pada *website* ini. Setelah terdaftar calon pelamar pekerjaan dapat melihat-lihat pekerjaan yang tersedia dari berbagai perusahaan yang terdaftar pada *website*.

Dengan "Job And Friends" ini pihak calon pelamar dapat mencari pekerjaan yang sesuai dengan yang diinginkannnya dan juga calon pelamar dapat melihat profil perusahaan yang menawarkan lowongan pekerjaan tersebut. Agar dapat menjadi produktif seorang pekerja perlu mengenal tempatnya bekerja. Selain itu calon pelamar akan memperoleh informasi mengenai pekerjaan yang diinginkannya beserta perusahaannya langsung pada *email* pribadi sang calon pelamar pekerjaan. Bagi pihak perusahaan "Job And Friends" menjadi alternatif publikasi lowongan pekerjaan yang murah, praktis dan efektif karena pihak perusahaan dapat menyimpan data perusahaan sekaligus data mengenai lowongan pekerjaan yang ditawarkannya secara gratis.

Penyadapan data dan informasi sangat perlu ditanggulangi dalam "Job And Friends" karena informasi yang disimpan dalam basis data dan juga yang dikirimkan antara *client* dan *server* merupakan data pribadi seseorang dan juga data perusahaan. Oleh karena itu alangkah baiknya apabila kerahasiaan dan keamanan dari informasi yang disimpan pada "Job And Friends" ini terjamin. Seperti yang sudah dijelaskan pada analisis masalah, yaitu keamanan transfer data dapat terjamin apabila sebuah *website* menggunakan HTTPS, akan tetapi diperlukan biaya tambahan untuk menggunakan HTTPS. Maka dari itu, masalah mengenai penyadapan informasi ini diatasi dalam "Job And Friends" dengan menggunakan algoritma enkripsi Twofish yang sudah terintegrasi dengan *website* "Job And Friends".

Twofish digunakan untuk mengenkripsi data yang dikirimkan dari *client* ke *server*, data bisa berupa data pribadi calon pelamar, data mengenai profil perusahaan maupun data rincian lowongan pekerjaan. Untuk itu, data tersebut perlu dienkripsi sebelum dikirimkan ke *server*, maka Twofish diimplementasikan dalam bahasa Javascript sehingga dapat digunakan di *client* dan data yang dikirimkan ke *server* sudah berupa cipherteks, di *server* cipherteks tersebut akan langsung disimpan ke basis data, dengan demikian data yang ada pada basis data pun berupa cipherteks. Apabila data pada basis data hendak ditampilkan atau diedit maka data akan didekripsi lalu ditampilkan pada *client*. Dalam penggunaannya Twofish dikombinasikan dengan string Base64 sehingga karakter cipherteks dapat diterima oleh *server* dan basis data.

Dengan memanfaatkan Twofish mengenkripsi data yang akan ditansfer antar *client* dan *server* serta data yang disimpan dalam basis data maka masalah penyadapan dapat teratasi, baik penyadapan saat transfer data maupun pembobolan basis data karena data berupa cipherteks dan tidak memiliki arti apapun bila tidak didekripsi dengan kunci yang sesuai. Dengan demikian tidak diperlukan biaya tambahan untuk menggunakan HTTPS karena data yang dikirim sudah dienkripsi menggunakan Twofish, sehingga meskipun tidak melalui protokol SSL melainkan melalui HTTPS biasa akan tetapi keamanan transfer data antara *client* dan *server* "Job And Friends" dapat berlangsung dengan aman.

Otentikasi untuk setiap *email* yang dikirim oleh "Job And Friends" juga sangatlah penting karena di dalamnya berisi data lowongan pekerjaan, data perusahaan dan juga data pribadi setiap calon pelamar pekerjaan. Oleh karena itu untuk menjamin agar infomasi yang sampai pada *email* tujuan tidaklah salah dan tidak dimanipulasi maka tanda tangan digital diimplentasikan pada setiap *email* yang dikirim oleh "Job And Friends", sehingga apabila isi dari *email* tersebut diubah maka ketika diotentikasi

hasilnya akan menunjukkan bahwa *email* tersebut sudah tidak orisinil lagi.

Implementasi tanda tangan digital ini menggunakan fungsi hash SHA-1 untuk membuat message digest dari *email* yang akan dikirim, lalu message digest ini dienkripsi dengan menggunakan algoritma kriptografi asimetrik yaitu RSA. Kemudian cipherteks hasil enkripsi ini disertakan pada *email* sebagai tanda tangan digital dari *email* tersebut. Di lain pihak, sang penerima *email* dapat melakukan valiidasi terhadap *email* yang diterimanya dari "Job And Friends" yaitu dengan membuka halaman validasi *email* pada *website* "Job And Friends". Pada halaman validasi *email*, sang penerima dapat menyertakan isi dari *email* yang diteimanya dan juga tanda tangan digital *email* yang bersangkutan lalu "Job And Friends" akan memeriksa orisinalitas dari isi *email* tersebut dengan mencocokkan hasil enkripsi message digest isi *email* yang disertakan dengan tanda tangan digital yang disertakan pula. Apabila sama maka *email* tersebut masih orisinil dan isinya benar benar dari "Job And Friends", akan tetapi bila hasilnya berbeda maka mungkin ada pihak lain yang merubah isi dari *email* tersebut ataupun tanda tangan digitalnya.

IV. PERANCANGAN

Perangkat lunak yang dibangun yaitu sebuah *website* lowongan pekerjaan "Job And Friends" dimana *website* ini dibangun karena dapat menjadi solusi bagi permsalahan yang diangkat menjadi fokus pada Tugas Akhir ini. Karena "Job And Friends" merupakan sebuah *website* yang terdapat di jaringan internet maka untuk mengaksesnya memerlukan sebuah PC atau laptop yang memiliki koneksi internet minimal 128 Kbps dan juga bekerja pada sistem operasi Windows XP / Vista / 7. Browser seperti Google Chrome atau Mozilla Firefox yang dapat menjalankan fungsi Javascript diperlukan untuk menjalankan *website* ini dengan sempurna.

Pada dasarnya "Job And Friends" merupakan sebuah *website* lowongan pekerjaan yang dapat menyimpan data perusahaaan, lowongan pekerjaan dan juga data diri calon pelamar pekerjaan. Data perusahaan dan lowongan pekerjaan yang sudah disimpan pada basis data "Job And Friends" dapat diubah dan dihapus oleh orang yang bersangkutan yakni yang mendaftarkannya, apabila terjadi akses untuk mengubah atau menghapus baik secara sengaja maupun tidak maka akses akan ditolak. Sedangkan untuk data diri pelamar, orang yang mendaftarkan diri sebagai pelamar hanya bisa mengubah data dirinnya saja dan tidak bisa menghapusnya.

Dengan "Job And Friends" ini diharapkan dapat membawa kemudahan bagi kedua belah pihak yang terlibat sebagai user, yaitu pihak perusahaan dan pihak calon pelamar pekerjaan. Bagi pihak perusahaan diharapkan dapat mempublikasikan lowongan pekerjaannya dengan mudah, murah dan praktis, serta dapat mengenal para pelamar pekerjaan secara lebih dekat dengan mengetahui data diri mereka terlebih dahulu sehingga diharapkan pula para pelamar pekerjaan sesuai dengan kriteria yang diinginkan perusahaan untuk lowongan pekerjaannya. Bagi pihak calon pelamar pekerjaan diharapkan dapat memperoleh informasi yang benar dan akurat mengenai lowonga pekerjaan yang diinginkannya.

"Job And Friends" juga dilengkapi dengan sistem keamanan yaitu penggunaan algoritma Twofish pada basis data dan juga pada data yang ditensfer antar *client* dan *server*. Selain itu ada juga sistem penjaga orisinalitas dari *email* yang dikirim ke pihak perusahaan maupun kepada calon pelamar pekerjaan, yaitu dengan membubuhkann tanda tangan digital pada *email* tersebut menggunakan fungsi hash SHA-1 dan algoritma RSA. Skema umum mengenai cara kerja "Job And Friends" dan juga implementasi sistem pengamanan oleh Twofish dan RSA dapat dilihat pada Gambar 2.

Gambar 2. Skema Umum Perangkat Lunak

Kebutuhan perangkat lunak dibagi dalam dua bagian yaitu kebutuhan fungsional dan nonfungsional.

A. Kebutuhan Fungsional

1. Menerima masukan berupa data perusahaan, lowongan pekerjaan maupun data diri calon pelamar pekerjaan.
2. Mengenkripsi data yang akan dikirim dari *client* ke *server* menggunakan algoritma *Twofish* dalam bahasa *Javascript*.
3. Menyimpan data perusahaan, lowongan pekerjaan dan data diri calon pelamar pekerjaan dengan bentuk cipherteks pada basis data "Job And Friends".
4. Memungkinkan *user* yang mempunyai otoritas yang bersesuaian untuk mengubah data perusahaan, lowongan kerja dan data dirinya.
5. Menampilkan daftar lowongan pekerjaan yang tersedia.
6. Menampilkan daftar perusahaan yang terdaftar dan menyediakan lowongan pekerjaan.
7. Mengirimkan *email* berisi detil informasi mengenai lowongan pekerjaan yang diminati dan perusahaannya.
8. Mengirimkan daftar pelamar pekerjaan yang mendaftar menjadi pelamar pekerjaan pada sebuah lowongan pekerjaan.

9. Membubuhi tanda tangan digital pada setiap *email* yang dikirim,
10. Melakukan validasi teradap *email* yang dikirim.

B. Kebutuhan Nonfungsional

1. Antarmuka yang simpel dan menarik sehingga memudahkan *user* untuk memahami dan bereksplorasi dengan "Job And Friends" secara nyaman.
2. Proses yang ringan dan cepat memungkinkan *user* untuk bereksplorasi dengan lancar.
3. Lebih dekat dengan *user* karena informasi dapat langsung dikirim pada *email* pribadi *user*.
4. Keamanana dan otentikasi data yang baik dapat mencegah terjadinya manipulasi data dan penyadapan informasi.

V. IMPLEMENTASI

A. Lingkungan Implementasi

Ada dua macam lingkungan pengembangan implementasi untuk perangkat lunak yang dibangun, yaitu lingkungan perangkat lunak dan lingkungan perangkat keras. Perangkat lunak yang digunakan untuk implementasi ini yaitu:

1. Sistem Operasi : Microsoft Windows 7
2. DBMS : SQL *Server* Basis data
3. Kakas : Microsoft Visual Studio 2010
4. Framework : Model View Controller (MVC)

Selain itu, perangkat keras yang digunakan dalam pembangunan perangkat lunak ini yaitu:

1. *Processor Inter® Core™2 Duo*
2. RAM 2.00GB
3. Monitor dengan resolusi 1280 x 800

Sedangkan untuk implementasi *website* pada *server*, berikut adalah spesifikasi implementasinya :

1. Sistem Operasi : Microsoft Windows 2003
2. DBMS : SQL *Server* 2005
3. *Server* : *Server* IIX PT. INDONESIA ONLINE
4. Hosting : Paket *hosting* B-500
5. Nama domain : www.jobandfriends.com

B. Batasan Implementasi

Implementasi perangkat lunak inventory management dengan peramalan dua metode ini dilakukan sesuai dengan analisis yang sudah dilakukan pada bab sebelumnya. Fitur yang disediakan terbatas pada:

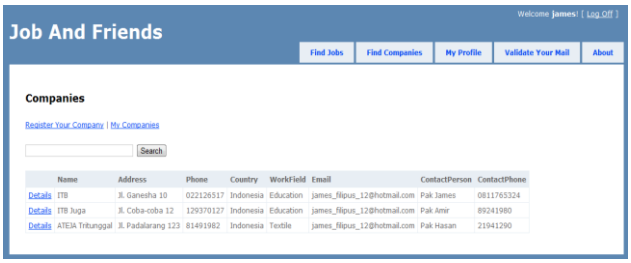
1. *Website* tidak dibuat dalam versi *mobile*
2. *Website* akan di-*hosting* dengan nama domain www.jobandfriends.com akan tetapi hanya selama 3 bulan saja, dimulai pada tanggal 25 Mei 2011
3. Fitur-fitur utama yang diimplementasikan yaitu :
   a. Registrasi dan edit data diri pencari kerja, perusahaan dan lowongan pekerjaan
   b. Penghapusan data perusahaan dan lowongan kerja
   c. Pencari kerja dapat mendaftar sebagai pelamar untuk suatu lowongan kerja dan dapat menghapus lamaran tersebut
   d. Data yang akan dienkripsi hanya data yang akan dikirim dari *client* ke *server* dan disimpan dalam basis data, sedangkan data yang dikirim dari *server* ke *client* sudah berbentuk plainteks karena sudah didekripsi di *server* sebelum dikirimkan ke *client*. Data yang dienkripsi adalah data diri pencari kerja, data perusahaan dan data lowongan kerja, semua data itu dienkripsi saat pengiriman data untuk registrasi dan edit dari *client* ke *server*.
   e. *Email* yang dikirim dari *server* akan dibubuhi tanda tangan digital yang dapat divalidasi pada halaman *website*.

C. Implementasi Antarmuka

Implementasi antarmuka *website* "Job And Friends" terdiri dari beberapa halaman web yang mencakup halaman registrasi, edit dan hapus untuk data perusahaan, lowongan kerja, data diri dan juga data lamaran. Serta ada juga halaman validasi *email* dan halaman yang menampilkan daftar perusahaan, lowongan kerja dan lamaran. Gambar 3 merupakan gambar halaman utama *website* "Job And Friends".

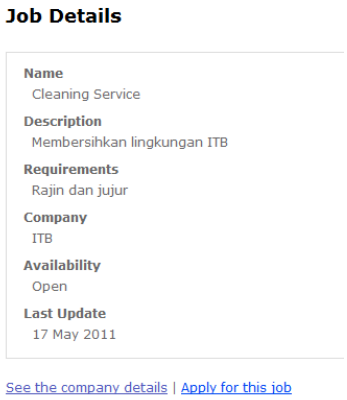
Gambar 3. Halaman Home

Gambar 4 merupakan gambar halaman index yang menampilkan daftar lowongan kerja, perusahaan dan lamaran pada website "Job And Friends".



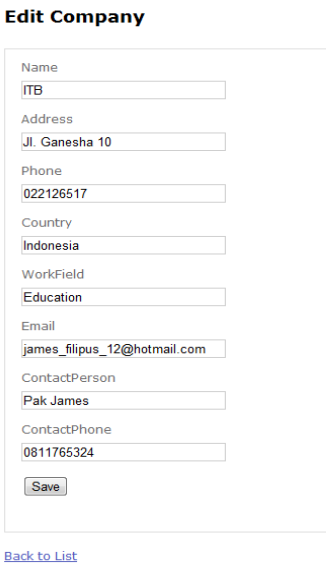
Gambar 4. Halaman Index

Gambar 5 merupakan gambar halaman *details* yang menampilkan detil lowongan kerja dan perusahaan pada website "Job And Friends".



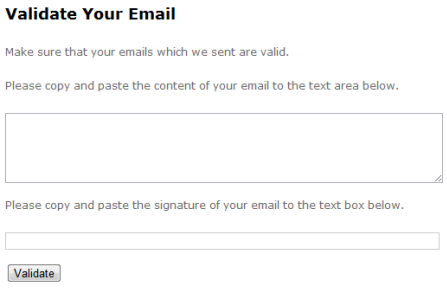
Gambar 5. Halaman Details

Gambar 6 merupakan gambar halaman edit yang digunakan untuk mengubah data perusahaan, lowongan pekerjaan dan data diri. Desain untuk halaman create pun sama dengan halaman edit.



Gambar 6. Halaman Edit

Gambar 4 merupakan gambar halaman validasi yang digunakan untuk melakukan validasi terhadap *email* yang dikirim dari *server* "Job And Friends".



Gambar 7. Halaman Validasi

VI. PENGUJIAN

Tujuan pengujian pada aplikasi yang dibangun adalah sebagai berikut:

1. Memastikan bahwa data perusahaan, lowongan kerja dan data diri pencari kerja yang dikirim dari *client* ke *server* sudah berupa cipherteks dalam format string base64.
2. Memastikan bahwa data perusahaan, lowongan kerja dan data diri pencari kerja yang disimpan di dalam basis data sudah berupa cipherteks dan dapat didekripsi kembali sesuai dengan plainteks awalnya.
3. Memastikan bahwa *email* yang dikirim dari *server* sudah dibubuhi tanda tangan digital dan fungsi validasi dapat digunakan untuk menjamin keaslian *email*.
4. Memastikan bahwa algoritma *Twofish* dan RSA yang diimplementasikan berfungsi dengan baik dan benar.

Dalam melakukan pengujian ini ada beberapa kasus uji yang harus dilakukan untuk mendapatkan tujuan dari pengujian ini. Beberapa kasus uji yang akan dilakukan adalah sebagai berikut:

1. Melakukan pengujian algoritma *Twofish* dan RSA
2. Menambah dan mengubah data perusahaan, lowongan pekerjaan dan data diri pencari kerja.
3. Melihat data yang ditambahkan dan disimpan dalam basis data.
4. Melakukan validasi terhadap *email* yang diterima dari *server*.

Pengujian dilakukan pada lingkungan yang sama dengan lingkungan pengembangan perangkat lunak, akan tetapi dengan tambahan beberapa kakas yaitu :

1. Web Browser : Google Chrome 11.0.672.2 dengan *javascript*
2. Pemeriksa paket : Wireshark & Google Chrome Developer Tools
3. Mail *Client* : Hotmail dan jobandfriends mail *client*
4. Pemeriksa Basis data : SQL *Server* Management Studio Express

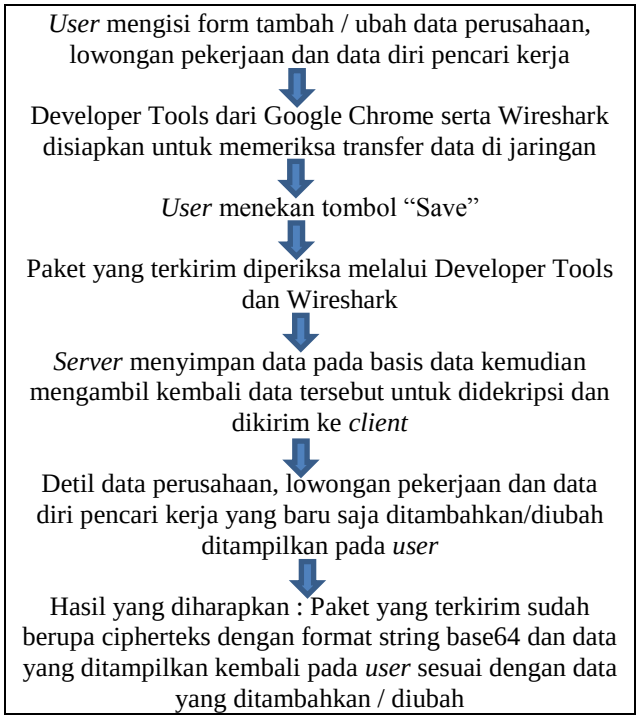
Untuk menguji algoritma *Twofish* dan RSA, dibangun sebuah program tersendiri untuk masing-masing algoritma. Program penguji algoritma *Twofish* digunakan untuk mengenkripsi sebuah teks dengan kunci tertentu dan kemudian didekripsi kembali. Hasil dari pengujian ini yaitu semua cipherteks dapat didekripsi kembali menjadi plainteks semula dengan benar. Sedangkan untuk RSA, program digunkana untuk memberi tanda tangan digital pada sebuah teks yang kemudian divalidasi. Hasilnya yaitu program akan memberikan peringatan bahwa teks tidak valid bila teks atau tanda tangan dimanipulasi, dan sebaliknya, bila teks masi asli maka akan muncul pesan bahwa teks masi asli.

Pengujian untuk sekuriti *website* dilakukan dengan menambah dan mengubah data perusahaan, lowongan pekerjaan dan data diri. Kemudian data yang sudah disimpan pada basis data ditampilkan kembali pada *user*.

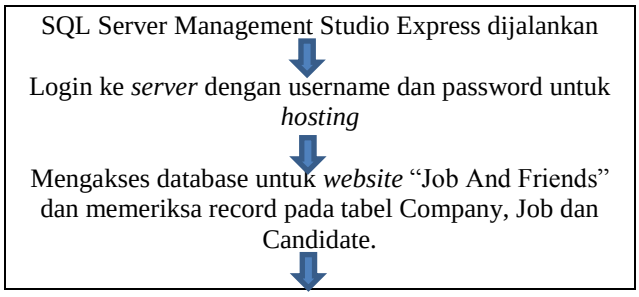
Hasil dari pengujian ini yaitu semua data yang tersimpan pada basis data sudah berupa cipherteks dan ketika ditampilkan kembali pada *user* dapat dikembalikan menjadi plainteks yang benar. Proses lengkap pengujian sekuriti *website* dapat dilihat pada bagan di Gambar 8.

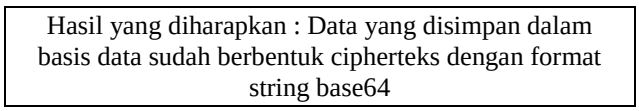
Selanjutnya untuk memastikan data tersimpan dengan aman pada basis data maka perlu dilakukan pengujian. Pengujian dilaksanakan dengan memeriksa basis data "Job And Friends" pada server. Gambar 9 menampilkan langkah-langkah pengujian yang dilakukan.

Otentikasi pada *website* diuji dengan melakukan pendaftaran untuk suatu lowongan kerja dan melihat daftar pelamar pekerjaan, sehingga *server* akan mengirimkan email yang sudah diberi tanda tangan digital ke *email user* (Gambar 10). Kemudian *email* tersebut divalidasi pada halaman validasi yang sudah disediakan pada *website*. Hasil dari pengujian ini yaitu *email* yang diterima sudah diberi tanda tangan digital. Selain itu apabila *email* yang belum dimanipulasi divalidasi maka *website* menampilkan pesan bahwa *email* sudah diubah, dan begitu pula sebaliknya, *website* menampilkan pesan bahwa *email* masih asli bila dilakukan validasi terhadap *email* yang tidak dimanipulasi (Gambar 11).



Gambar 8. Pelaksanaan pengujian sekuriti transfer data

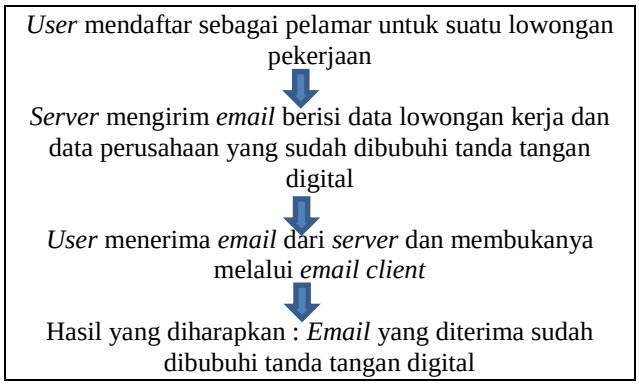




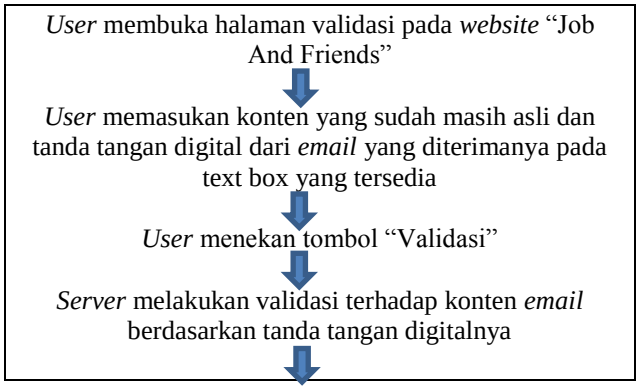
Gambar 9. Pelaksanaan pengujian sekuriti basis data

VII. KESIMPULAN

1. Dengan *website* lowongan pekerjaan "Job And Friends" yang telah dibangun pada Tugas Akhir ini, distribusi lowongan pekerjaan dapat dilakukan dengan lebih mudah dan juga dengan biaya yang lebih sedikit karena tidak perlu menggunakan HTTPS. Dengan implementasi algoritma *Twofish*, transfer data dapat dilakukan dengan aman dan keamanan data yang tersimpan pada database juga terjamin. Otentikasi *email* dapatt dilakukan dengan implementasi algoritma RSA sehingga keaslian informasi yang dikirim terjamin.
2. Fitur keamanan yang disertakan pada *website* "Job And Friends" yaitu enkripsi menggunakan algoritma *Twofish* berjalan dengan baik dan benar. Setiap data yang dienkripsi dapat didekripsi kembali menjadi plainteks yang sama seperti semula.
3. Setiap *email* yang dikirim dari *server* "Job And Friends" kepada *user* sudah diberi tanda tangan digital. Validasi terhadap *email* yang sudah diberi tanda tangan digital dapat dilaksanakan dengan benar, sehingga dapat mengidentifikasi adanya manipulasi data sekecil apapun pada *email*.



Gambar 10. Pelaksanaan pengujian otentikasi



Hasil yang diharapkan : *Server* menampilkan pesan bahwa *email* otentik

Gambar 11. Pelaksanaan pengujian validasi email

REFERENSI

Anonim. *Implementasi Pengamanan Basis Data dengan Teknik Enkripsi.* Sekolah Tinggi Teknik Harapan

Baran, Paul. 1964. *Distributed Communications, Volume XI*

Boutell, Thomas. 2011. *What is HTTPS?* URL: http://www.boutell.com/newfaq/definitions/https.html Waktu Akses : 17 Mei 2011

Budiharjo, Akhmad. 2003. *Otentikasi Pada Aplikasi Berbasis Web*. Institut Teknologi Bandung.

C13-09.2009. *2010, Pengangguran di Indonesia masih 10 persen.* Kompas, Kamis, 12 November 2009 URL:http://bisniskeuangan.kompas.com/read/2009/11/12/14145447/2010..Pengangguran.di.Indonesia.Masih.10.Persen Waktu Akses : 29 November 2010

Widyantoro, Dwi Hendratmo. 2009. *Sistem Cerdas untuk Perangkat Lunak Layanan Bursa Kerja.* URL: http://www.omrc-drn.or.id/kegiatan-riset.html?rid=18944&cid1=&cid= 1455 Waktu Akses : 19 Juni 2011

earif. 2007. *SHA – Algoritma Kriptografi HASH.* Insight URL : http://earief.wordpress.com/2007/06/13/sha-%E2%80%93-algoritma-kriptografi-hash/ Waktu Akses : 30 November 2010

Federal In*form*ation Processing Standards Publication 197.2001. *Announcing The Advanced Encryption Standard (AES).*

Mudeng, Denny. 2003. *Kriptografi Twofish.* Magister Teknologi In*form*asi. Institut Teknologi Bandung.

Munir, Rinaldi. 2005. *Diktat Kuliah Kritografi.* Institut Teknologi Bandung.

Review Stream. 2010. URL:http://www.reviewstream.com/reviews/?p=38502 Waktu Akses : 29 November 2010

Schneier, Bruce, John Kelsey, Doug Whitin, David Wagner, Chris Hall, Niels Ferguson. 1998. *Twofish : A 128-Bit Block Cipher.*

Stancu , Horatio Paul. 2004. *Twofish Encryption Algorithm.*

Wibowo, Fendi Arie. 2005. *Sistem Keamanan Email.* Sekolah Tinggi Manajemen In*form*atika : Program Studi Sistem In*form*asi.

Widiantoro, Fajar. 2010. *10 Fakta Penting Tentang Keamanan Internet.* Detikinet. URL:http://www.detikinet.com/read/2010/03/08/151215/1313697/323/10-fakta-penting-tentang-keamanan-internet Waktu Akses : 29 November 2010