PERANCANGAN FORMULIR ELEKTRONIK DI*ENKRIPSI* DENGAN METODE *BLOWFISH* PADA SISTEM PENDAFTARAN *ONLINE* (STUDI KASUS : SELEKSI MANDIRI UNIVERSITAS TANJUNGPURA)

Ferry Kurniawan

Program Studi Teknik Informatika
Jurusan Teknik Elektro Fakultas Teknik Universitas Tanjungpura
fherrhye@gmail.com

Abstract- **Seleksi Mandiri Tanjungpura University is one of the entrance method to the college, especially in the TanjungpuraUniversity. Registration of Seleksi Mandiri Tanjungpura University done directly by the candidates of the student. This existing method takes quite a long time. The number of applicants is not proportional to the number of committees that serve and verify the administrative requirements of participants, so this resulted in a queue ofstudent candidates. Online system that used as a service in the registration system have been widely applied in daily life. It proved to minimize the problems that previously occurred. Long lines of queue and paper used as a medium of registration can be reduced and prevented with the online service systems. Electronic form is an application that designed for Seleksi Mandiri Tanjungpura Tanjungpura University registration system. Application form fulfillment will be possible to conduct in conditions of a computer connected or not connected to the Internet. However it can be done at offline. One method to protect data from unwanted party is to randomize the data sent, so if the data is received by the other party, they do not understand the purpose of the data. Blowfish algorithm is an algorithm which is quite good and applicable. Blowfish have varying levels of security, the key length used by Blowfish may vary by the system. The application uses data snap technology by applying service application so it becomes more secure because of the indirect communications with the back end. The results show that the design and testing of these applications can be used for the registration process. Prospective participants will receive a registration receipt cards used to take exams.**

Keywords- Seleksi Mandiri, electronic forms, offline, blowfish, service application..

1. Pendahuluan

Seleksi Mandiri Universitas Tanjungpura adalah kegiatan seleksi calon mahasiswa masuk Universitas Tanjungpura dengan pola ujian tulis. Seleksi Mandiri diselenggarakan setelah proses SNMPTN berlangsung. Hal ini bertujuan untuk memberikan kesempatan yang seluas-luasnya bagi masyarakat sehingga dapat masuk pada perguruan tinggi negeri khususnya di Universitas Tanjungpura.

Penyelenggaraan Seleksi Mandiri Universitas Tanjungpura dilakukan secara *offline.* Cara ini memakan waktu yang cukup lama. Banyaknya pendaftar tidak sebanding dengan banyaknya panitia yang bertugas untuk memeriksa kelengkapan administrasi peserta, sehingga hal ini mengakibatkan antrian dari para calon mahasiswa. Biaya yang cukup besar untuk datang langsung ke Universitas Tanjungpura melakukan proses pendaftaran.

Salah satu faktor penting untuk layanan *online* adalah adanya layanan *internet.* Pengisian formulir pendaftaran mewajibkan calon mahasiswa untuk mengisi data-data secara *online*. Merujuk pada sistem yang telah diterapkan yaitu sistem pendaftaran SNMPTN *online*, banyaknya permasalahan yang sering terjadi seperti *Loss Connection, Server Not Responding, Server Time Out, Server Down* karena diakses secara bersamaan dan masih banyak lagi permasalahan yang sering kali terjadi ketika kita men-*submit* data yang akan kita proses. Tidak hanya masalah teknis tersebut, faktor non teknis yang terjadi dilapangan ternyata para calon mahasiswa yang berasal dari daerah tidak dapat mendiskusikan secara langsung kepada orang tua mereka, mengenai jurusan apa yang sebaiknya dipilih.

Formulir elektronik merupakan sebuah aplikasi yang dirancang untuk sistem pendaftaran *online* seleksi mandiri Universitas Tanjungpura. Pengisian formulir yang ada dalam aplikasi tidak hanya dapat dilakukan dalam kondisi komputer tersambung dengan *internet.* Namun dapat dilakukan pada saat *offline.* Artinya calon mahasiswa tidak harus datang ke lokasi pendaftaran, tetapi calon mahasiswa cukup men-*download* aplikasi tersebut untuk kemudian melakukan pengisian data yang tersedia pada aplikasi tersebut. Hal ini diharapkan dapat membantu para calon mahasiswa dari daerah-daerah dan masih belum terjangkau atau jauh dari jangkauan *internet*.

Data yang diisikan bersifat rahasia, artinya tidak boleh diketahui oleh orang lain selain pengirim (peserta) dan penerima data (panitia lokal). Salah satu cara untuk melindungi data dari pihak yang tidak diinginkan adalah dengan mengacak data yang dikirim tersebut. Algoritma *blowfish* merupakan algoritma kriptografi yang cukup baik dan aplikatif. Blowfish memiliki tingkat keamanan

yang bervariasi, panjang kunci yang digunakan oleh *Blowfish* dapat bervariasi dan bisa sampai sepanjang 448 bit. Program aplikasi yang akan dirancang nantinya adalah dengan menggunakan algoritma *blowfish.*

2. Teori Dasar

2.1 Formulir

Formulir, dari bahasa Belanda, *formulier*, adalah sebuah kertas yang berisi banyak pertanyaan yang harus diisi. Menurut Kamus Lengkap Bahasa Indonesia, formulir adalah lembar isian; surat isian: -- yang telah diisi harus diserahkan kepada bagian pendaftaran. (EM Zul Fajri & Ratu AS, 2008) [1].

Formulir merupakan sehelai kertas tercetak yang menyediakan ruangan untuk dimuat catatan-catatan, informasi atau instruksi – instruksi yang akan diteruskan kepada individu – individu, atau organisasi lain. Formulir merupakan alat penting untuk menciptakan dokumen karena formulir menentukan informasi apa yang akan di kumpulkan dan disimpan.

2.1.1 Formulir Elektronik

Dengan meluasnya pemakaian komputer, maka pemakaian formulir elektronik juga semakin banyak. Dalam hal ini, formulir dapat diartikan sebagai ruang yang ditayangkan dalam layar komputer yang digunakan untuk menampung data yang akan diolah dalam pengolahan data elektronik. (Gunawan Wibisono, UGM)[2].

Formulir elektronik terdiri dari dua kata, yaitu formulir dan elektronik. Seperti telah dijelaskan sebelumnya, formulir adalah lembar isian sedangkan elektronik dapat diartikan sebagai sebuah alat yang bekerja atas dasar elektronika. Dari dua pengertian tersebut dapat ditarik kesimpulan bahwa formulir elektronik merupakan ruang yang ditayangkan dalam layar komputer yang digunakan untuk menangkap data yang akan diolah dalam pengolahan data elektronik. Dengan penggunaan formulir elektronik, perancangan, pengelolaan, dan pengisian setiap formulir dapat dilakukan melalui sistem yang terintegrasi. Sistem komputer dapat menyimpan dan menyediakan data beberapa kali suatu formulir telah digunakan, bagaimana bentuk formulir setelah revisi yang terakhir, dan berapa lama suatu formulir telah digunakan sejak revisi terakhir.

2.2 Kriptografi

Kriptografi dalam sejarahnya tercatat dipergunakan secara terbatas oleh bangsa Mesir 4000 tahun lalu. Kriptografi (*Cryptography*) berasal dari dua kata yaitu "*Crypto & graphy*" yang dalam sudut bahasa "*Crypto*" dapat diartikan rahasia (*secret*) dan "graphy" dapat diartikan tulisan (*writing*) jadi Kriptografi (*Cryptography*) dapat diartikan sebagai suatu ilmu atau seni untuk mengamankan pesan agar aman dan dilakukan oleh *"Cryptographer"*. (Jack Febrian, 2004) [3]

Menurut Anjar Syafari (2007), enkripsi dan deskrisi secara matematis diterangkan sebagai berikut :

EK (M) = C (Proses Enkripsi)

DK (C) = M (Proses Deskripsi)

Keterangan :
EK : *Enkripsi.*
DK : *Deskripsi.*
M : *Message* (Pesan sebelum dienkripsi).
C : *Cipher* (Pesan setelah dienkripsi).

2.2.1 Pengenalan *Blowfish*

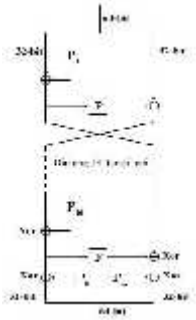
Blowfish alias "*OpenPGP.Cipher.4*" merupakan enkripsi yang termasuk dalam golongan *Symmetric Cryptosystem* , metoda enkripsinya mirip dengan DES (DES-like Cipher) diciptakan oleh seorang *Cryptanalyst* bernama Bruce Schneier. Dibuat untuk digunakan pada komputer yang mempunyai *microposesor* besar . *Blowfish* merupakan algoritma yang tidak dipatenkan dan *license free*, dan tersedia secara gratis untuk berbagai macam kegunaan. (Anjar Syafari, 2007) [4].

Pada saat *Blowfish* dirancang, diharapkan mempunyai criteria perancangan sebagai berikut (Schneier,1996) [5]:

1. Cepat, *Blowfish* melakukan enkripsi data pada *microprocessors* 32-bit dengan rate 26 *clock cycles per byte*.
2. Compact (ringan), *Blowfish* dapat dijalankan ada memori kurang dari 5K.
3. Sederhana, *Blowfish* hanya menggunakan operasi-operasi sederhana: penambahan, XOR, dan lookuptabel pada operan 32-bit.
4. Memiliki tingkat keamanan yang bervariasi, panjang kunci yang digunakan oleh *Blowfish* dapat bervariasi dan bisa sampai sepanjang 448 bit.

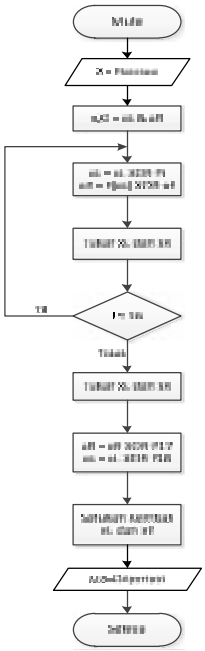
Blowfish termasuk dalam *enkripsi block Cipher* 64-bit dangan panjang kunci yang bervariasi antara 32-bit sampai 448-bit. Algoritma *Blowfish* terdiri atas dua bagian :

1. Key-Expansion
   Berfungsi merubah kunci (Minimum 32-bit, Maksimum 448-bit) menjadi beberapa array subkunci (subkey) dengan total 4168 byte.
2. Enkripsi Data
   Terdiri dari iterasi fungsi sederhana (*Feistel Network*) sebanyak 16 kali putaran. Setiap putaran terdiri dari permutasi kunci-*dependent* dan substitusi kunci- dan data-*dependent*.Semua operasi adalah penambahan (*addition*) dan XOR pada variabel 32-bit.Operasi tambahan lainnya hanyalah empat penelusuran tabel (*table lookup*) array berindeks untuk setiap putaran.



Gambar 1 Algoritma *Blowfish*

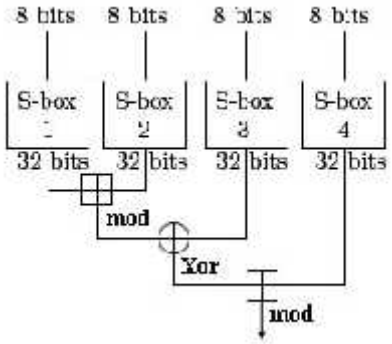
1. Bentuk inisial P-array sebanyak 18 buah (P1,P2,.....P18) masing-msing bernilai 32-bit.
   Array P terdiri dari delapan belas kunci 32-bit subkunci :
   $P_1,P_2,.....,P_{18}$
2. Bentuk S-box sebanyak 4 buah masing-masing bernilai 32-bit yang memiliki masukan 256.
   Empat 32-bit S-box masing-masing mempunyai 256 entri :
   $S_{1,0},S_{1,1},.....,S_{1,255}$
   $S_{2,0},S_{2,1},.....,S_{2,255}$
   $S_{3,0},S_{3,1},.....,S_{3,255}$
   $S_{4,0},S_{4,1},.....,S_{4,255}$
3. Plaintext yang akan dienkripsi diasumsikan sebagai masukan, Plaintext tersebut diambil sebanyak 64-bit, dan apabila kurang dari 64-bit maka kita tambahkan bitnya, supaya dalam operasi nanti sesuai dengan datanya.
4. Hasil pengambilan tadi dibagi 2, 32-bit pertama disebut XL, 32-bit yang kedua disebut XR.
5. Selanjutnya lakukan operasi XL = XL xor Pi dan XR = F(XL) xor XR
6. Hasil dari operasi diatas ditukar XL menjadi XR dan XR menjadi XL.
7. Lakukan sebanyak 16 kali, perulangan yang ke-16 lakukan lagi proses penukaran XL dan XR.
8. Pada proses ke-17 lakukan operasi untuk XR = XR xor P17 dan XL = XL xor P18.
9. Proses terakhir satukan kembali XL dan XR sehingga menjadi 64-bit kembali.



Gambar 2 *Flowchart Blowfish*

Subkunci dihitung menggunakan algoritma *Blowfish*, metodanya adalah sebagai berikut :

1. Pertama-tama inilialisasi P-array dan kemudian empat S-box secara berurutan dengan string yang tetap. String ini terdiri atas digit hexadesimal dari Pi.
2. XOR P1 dengan 32-bit pertama kunci, XOR P2 dengan 32-bit kedua dari kunci dan seterusnya untuk setiap bit dari kunci (sampai P18). Ulangi terhadap bit kunci sampai seluruh P-array di XOR dengan bit kunci.
3. Enkrip semua string nol dengan algoritma *Blowfish* dengan menggunakan subkunci seperti dijelaskan pada langkah (1) dan (2).
4. Ganti P1 dan P2 dengan keluaran dari langkah (3).
5. Enkrip keluaran dari langkah (3) dengan algoritma *Blowfish* dengan subkunci yang sudah dimodifikasi.
6. Ganti P3 dan P4 dengan keluaran dari langkah (5).
7. Lanjutkan proses tersebut, ganti seluruh elemen dari P-array, kemudian seluruh keempat S-box berurutan, dengan keluaran yang berubah secara kontiyu dari algoritma *Blowfish*.



Gambar 3 fungsi F dalam *Blowfish*

Total yang diperlukan adalah 521 iterasi untuk menghasilkan semua subkunci yang dibutuhkan. Aplikasi kemudian dapat menyimpan subkunci ini dan tidak membutuhkan langkah-langkah proses penurunan berulang kali, kecuali kunci yang digunakan berubah.

2.2.2 Keamanan *Blowfish*

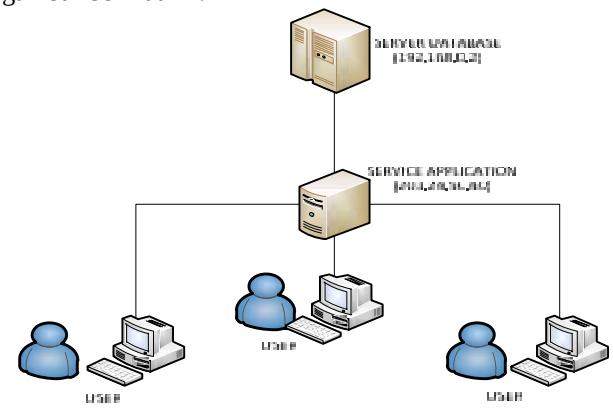
Sampai saat ini algoritma *Blowfish* belum ditemukan kelemahan yang berarti hanya adanya *weak key* dimana dua entri dari S-box mempunyai nilai yang sama. Belum ada cara untuk mengecek *weak key* sebelum melakukan *key expansion*, tetapi hal ini tidak berpengaruh terhadap hasil *enkripsi.*

3. Hasil Eksperimen

Sistem yang dibangun terdiri dari aplikasi *desktop* yang berfungsi sebagai *client* dan *web* yang berfungsi sebagai form registrasi awal untuk mendapat kode akses pendaftaran. Pendaftar *(user)* melakukan pengisian data melalui aplikasi *desktop*, dan kemudian akan dikirimkan ke *server*.

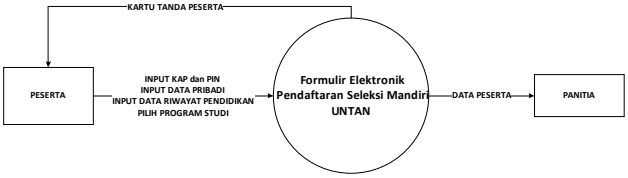
Aplikasi mengirimkan data isian ke server melalui *service*. Untuk menghubungkan aplikasi tersebut ke *server* menggukanan teknologi *data snap.* File yang dikirimkan dari *client*, akan diproses di sisi *service. Service* akan memproses satu persatu file yang berhasil masuk ke *server*. *Service* akan mendekripsi file *.xml tersebut dan kemudian melakukan penginputan data kedalam *database*. Setelah proses tersebut berhasil, maka *user* akan mendapatkan respon berupa nomor peserta dan

kartu tanda peserta yang akan digunakan pada saat ujian berlangsung. Desain arsitektur sistem dapat dilihat pada gambar berikut ini.



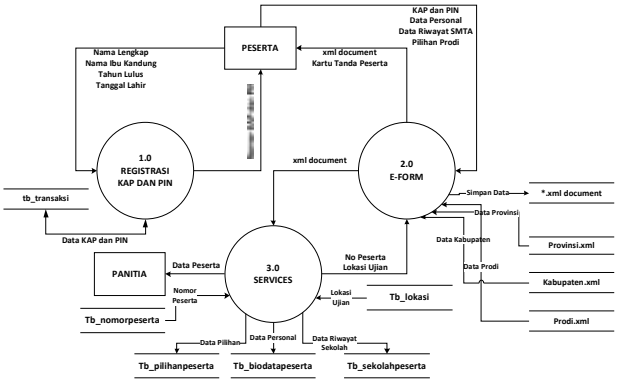
Gambar 4. Desain Arsitektur Sistem

Secara garis besar, alur kerja aplikasi seperti ditunjukan pada diagram konteks berikut :



Gambar 5. Diagram konteks

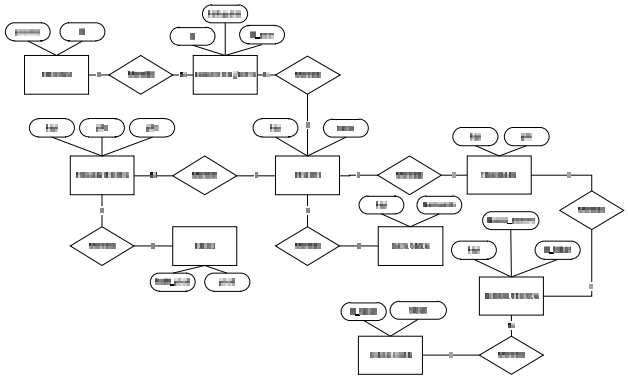
Sistem yang dibangun memiliki 3 buah sub sistem. Proses *registrasi* dibangun berbasis *web*, sedangkan *e-form* dan *services* dibangun menggunakan *desktop.*



Gambar 6. Diagram overview sistem

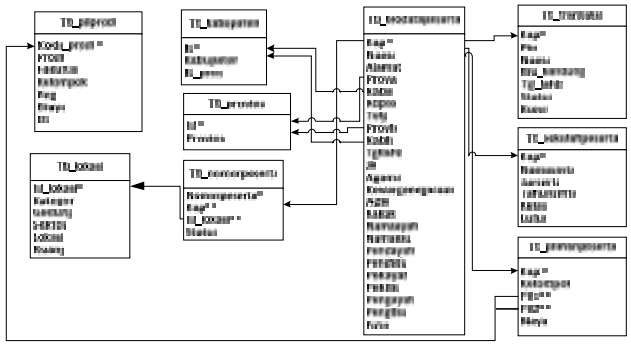
Entity Relational Diagram (ERD) merupakan gambaran hubungan antar-entitas yang dipergunakan dalam sistem. Perancangan ERD meliputi tahap penentuan entitas, penentuan relasi antar-entitas, tingkat relasi yang terjadi, dan konektivitas antar-entitas. Entitas-entitas yang ada adalah sebagai berikut:

1. Provinsi, yaitu data-data provinsi yang ada di Indonesia.
2. Kabupaten / Kota, yaitu data-data kabupaten / kota di Indonesia.
3. Prodi, yaitu data-data program studi yang tersedia pada jalur seleksi mandiri.
4. Lokasi, yaitu lokasi tempat ujian calon peserta.
5. Nomor Peserta, yaitu data-data nomor peserta pada Seleksi Mandiri
6. Biodata Peserta, yaitu data calon peserta yang telah mendaftar.
7. Sekolah peserta, yaitu data tempat dimana calon peserta bersekolah
8. Pilihan Peserta, yaitu pilihan prodi yang dipilih oleh calon peserta.
9. Transaksi, yaitu data nomor KAP dan PIN



Gambar 7. Diagram ER

Physical design merupakan tahap akhir dari pembuatan pendaftaran *online* seleksi mandiri Universitas Tanjungpura yang dalam hal ini merupakan gambaran nyata dari database yang akan dibuat. Berikut merupakan *physical design* dari pendaftaran *online* seleksi mandiri Universitas Tanjungpura.



Gambar 8. Hubungan antar tabel

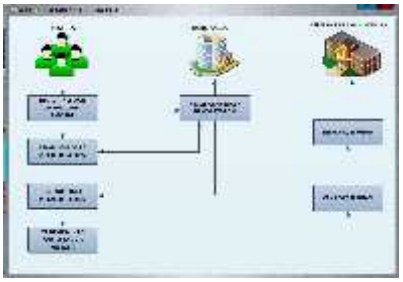
Berikut adalah tampilan hasil perancangan antarmuka aplikasi.

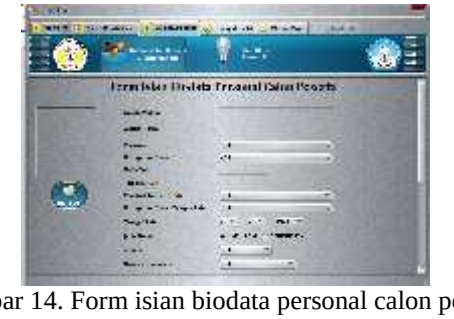
Gambar 9. Halaman *registrasi* awal

Gambar 10 Splash screen E-Form

Gambar 11. Aktivitas utama e-form

Gambar 12. Halaman cek kartu peserta


Gambar 13. Halaman alur pendaftaran


Gambar 14. Form isian biodata personal calon peserta

Gambar 15. Form penyesuaian foto

Gambar 16. Halaman pengisian informasi pendidikan calon peserta

Gambar 17. Halaman pengisian pilihan program studi

Gambar 18. Halaman konfirmasi pengisian data

Gambar 19. File hasil enkripsi

Gambar 20. Antarmuka aplikasi *services*

3.1 Pengujian Aplikasi

Pengujian sistem yang dilakukan meliputi dua tahapan, yaitu pengujian *Alpha* dan *Betha*. Pengujian *Alpha* merupakan pengujian fungsional yang digunakan untuk menguji sistem yang telah dibuat dengan metode pengujian *black box* yaitu *input* berupa suatu set data untuk menguji validitas dari integrasi dan konsistensi sistem. Pengujian *betha* merupakan pengujian sistem berdasarkan objek penelitian langsung yaitu pengguna aplikasi, yang mengacu dari hasil kuisioner. Pengujian juga dilakukan pada proses pengiriman data serta proses enkripsi dan dekripsi apakah *chipertext* yang dihasilkan akan sama ketika di *dekripsi* pada sisi *server*. Pengujian tersebut dilakukan untuk mengevaluasi hasil sistem yang dibuat.

3.2 Analisis Hasil Pengujian

1. Calon peserta melakukan *registrasi* awal melalui website 203.24.50.40/seleksimandiri. Calon peserta akan mendapatkan nomor KAP dan PIN yang digunakan untuk proses pendaftaran melalui formulir elektronik.
2. Formulir elektronik ini dapat didistribusikan langsung. Namun, calon peserta harus melakukan registrasi untuk memiliki KAP dan PIN.
3. Nomor KAP dan PIN tersebut harus divalidasi dengan cara melakukan pembayaran pada Bank KALBAR.
4. Aplikasi menyimpan data dalam bentuk file pmb_untan_ecbl.xml yang di*enkripsi* menggunakan metode *blowfish.*
5. Aplikasi menggunakan teknologi data snap dengan menerapkan *service application.*
6. Hasil perancangan dan pengujian menunjukan bahwa aplikasi ini dapat digunakan untuk proses pendaftaran. Calon peserta akan mendapatkan kartu tanda bukti pendaftaran yang digunakan untuk mengikuti ujian.
7. Berdasarkan hasil kuesioner, dapat disimpulkan bahwa perangkat lunak yang dirancang dinilai cukup berhasil.

4. Kesimpulan

Setelah melalui beberapa analisis dan pengujian terhadap aplikasi, dapat disimpulkan bahwa:

1. Calon peserta melakukan *registrasi* awal dan mendapatkan nomor KAP dan PIN yang digunakan untuk proses pendaftaran melalui formulir elektronik.
2. Aplikasi dapat mengenkripsi data isian yang menghasilkan file pmb_untan_ecbl.xml sebagai media penyimpanan data yang telah di*enkripsi* menggunakan metode *blowfish.* sehingga dapat digunakan sebagai media pengisian formulir pendaftaran *online* pada Seleksi Mandiri Universitas Tanjungpura
3. Hasil perancangan dan pengujian menunjukan bahwa aplikasi ini dapat digunakan untuk proses pendaftaran. Calon peserta akan mendapatkan kartu tanda bukti pendaftaran yang digunakan untuk mengikuti ujian.
4. Berdasarkan hasil kuesioner dan diukur dengan skala *Likert's Summated Rating* (LSR) nilai yang didapat adalah 1766 dari nilai maksimum 2480, dapat disimpulkan bahwa perangkat lunak yang dirancang dinilai cukup berhasil.

Referensi

[1] Em Zul Fajri, Ratu Aprilia Senja. 2008. *Kamus Lengkap Bahasa Indonesia.* (cetakan ketiga). Difa Publisher.

[2] Wibisono, Gunawan. *Formulir.* Universitas Gajah Mada. www.fileden.com/files/2007/11/24/1604922/bab3.pdf. Tanggal Akses : 16 Juni 2012

[3] Febrian, Jack. 2004. *Pengetahuan Komputer dan Teknologi Informasi*. Bandung: Informatika.

[4] Syafari, Anjar 2007. *Sekilas Tentang Enkripsi Blowfish.http://ilmukomputer.com/2007/07/21/sekilas-tentang-enkripsi-blowfis* Tanggal akses: 4 Januari 2012

[5] Schneier, Bruce, 1996, *Applied Cryptography*, Second Edition, John Wiley & Son, New York.

Biography

Ferry Kurniawan lahir di Karangan, Kalimantan Barat, tanggal 04 Maret 1990. Memperoleh gelar Sarjana Teknik dari Universitas Tanjungpura, Pontianak, Indonesia, 2013.