Vol.3 No.1 Januari-Juni 2017
JESIK
JURNAL ELEKRONIK SISTEM INFORMASI DAN KOMPUTER
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER (STMIK) BINA MULIA

ANALISA DAN IMPLEMENTASI KRIPTOGRAFI PADA PESAN RAHASIA MENGGUNAKAN ALGORITMA *CIPHER TRANSPOSITION*

Arif Prayitno
Nurdin Nurdin
Email: nnurdin69@gmail.com

ABSTRAK

Dalam era teknologi informasi, pengiriman informasi selalu terjadi sehingga unsur keamanan menjadi sangat penting. Hal ini karena seringkali dalam proses pengiriman terjadi penyadapan atau pencurian informasi oleh pihak yang tidak berhak. Untuk itu sangat diperlukan suatu sistem keamanan untuk menjaga kerahasiaan informasi dan salah satu cara yang dapat digunakan adalah kriptografi karena tujuan kriptografi adalah kerahasiaan, integritas, otentikasi, dan pembuktian tak tersangkal. Kriptografi memiliki banyak teknik dalam mengenkripsi data, diantaranya adalah Algoritma *Transposition Cipher*, yaitu teknik pengenkripsian pesan dengan cara mengubah urutan huruf-huruf didalam pesan menjadi pesan acak agar isi dari pesan tersebut tidak dapat dipahami kecuali oleh orang-orang tertentu. Karena itu penelitian ini akan membangun suatu sistem keamanan menggunakan Algoritma *Transposition Cipher* untuk menjamin keamanan pesan/data yang mencegah pihak yang tidak berwenang untuk menggunakan/mengubah pesan/data tersebut. Penelitian ini merupakan penelitian deskriptif dengan pendekatan rekayasa perangkat lunak. Dengan menggunakan metode *prototype*, penelitian ini merancang aplikasi kriptografi Algoritma *Cipher Transposition* yang dapat menjamin keamanan suatu pesan/data. Hasil penelitian ini menyimpulkan Algoritma *Cipher Transposition* dapat menjadi salah satu alternatif dalam pengamanan data yang penting atau rahasia dan penggunaan kunci adalah hal yang sangat penting sehingga dibutuhkan suatu kerahasiaan dalam pemakaiannya. Penelitian kedepan perlu menambahkan beberapa *tools* yang dapat mengembangkan aplikasi ini.

Kata Kunci: Kriptografi, Kerahasiaan, *Cipher Transposition*.

1. Latar Belakang

Dalam era teknologi informasi saat ini, pengiriman informasi selalu terjadi sehingga unsur keamanan informasi menjadi sangat penting. Hal ini karena seringkali dalam proses pengiriman terjadi penyadapan atau pencurian informasi oleh pihak yang tidak berhak. Karena itu dalam pengiriman/penerimaan informasi, pengguna membutuhkan suatu jaminan yang dapat meyakinkan mereka bahwa yang diperoleh adalah informasi yang aman dan benar.

Untuk itu sangat diperlukan suatu sistem keamanan untuk menjaga kerahasiaan informasi. Salah satu cara yang digunakan untuk tujuan tersebut adalah kriptografi dengan mengenkripsi informasi yang dikirim karena tujuan kriptografi adalah kerahasiaan, integritas, otentikasi, dan pembuktian tak tersangkal.

Kriptografi adalah bidang pengetahuan yang menggunakan persamaan matematis untuk melakukan proses enkripsi dan dekripsi. Teknik ini untuk mengkonversi data ke bentuk kode-kode tertentu agar informasi tidak dapat terbaca oleh siapapun kecuali pihak yang berhak. Salah satu metode kriptografi yang biasa digunakan adalah algoritma simetris yang menggunakan kunci yang sama saat melakukan enkripsi dan dekripsi sehingga informasi sulit dipahami maknanya.

Kriptografi memiliki banyak teknik dalam mengenkripsi data, diantaranya adalah Algoritma Cipher Transposisi, yaitu teknik pengenkripsian pesan dengan cara mengubah urutan huruf-huruf didalam pesan menjadi pesan yang acak dengan cara tertentu agar isi dari pesan tersebut tidak dapat dipahami kecuali oleh orang-orang tertentu.

Dengan dasar pemikiran tersebut maka penelitian ini akan membangun suatu rancangan keamanan informasi dengan menggunakan Algoritma *Transposition Cipher***.**

2. Tinjauan Pustaka

2.1 Analisis

Analisis diartikan sebagai penguraian suatu pokok atas berbagai penelahan bagian itu sendiri, serta hubungan antar bagian untuk memperoleh pengertian yang tepat dan pemahaman arti keseluruhan [1]. Analisis adalah suatu kegiatan berpikir untuk menguraikan suatu keseluruhan menjadi komponen sehingga dapat mengenali tanda-tanda komponen, serta hubungannya satu sama lain dan fungsi masing-masing dalam satu keseluruhan yang terpadu [2].

Dengan demikian dapat disimpulkan bahwa analisis merupakan suatu kegiatan berpikir menguraikan suatu pokok hal atau permasalahan menjadi bagian-bagian atau komponen tertentu sehingga diketahui ciri atau tanda setiap bagian, dan hubungan suatu bagian dengan bagian lain serta fungsi setiap bagian secara keseluruhan. Sedangkan implementasi merupakan kegiatan penerapan teknologi untuk dapat digunakan dalam suatu organisasi (Nurdin, Stockdale, & Scheepers, 2012). Dengan demikian faktor keamanan menjadi sangat penting agar dapat digunakan dalam sebuah organisasi.

2.2 Perancangan

Perancangan didefinisikan sebagai suatu tugas yang berfokus pada spesifikasi solusi detail berbasis komputer. Terdapat beberapa strategi dalam perancangan dasain suatu sistem, yaitu [3]:

a. Desain stuktur modern.
b. Teknik informasi.
c. *Prototyping*.
d. *Join Application Development* (JAD).
e. *Rapid Application Development* (RAD).
f. Desain berorientasi objek.

Terkadang teknik perancangan tersebut dianggap teknik yang saling bersaing, tetapi seringkali untuk jenis proyek tertentu diperlukan kombinasi dari beberapa diantaranya sehingga dapat saling melengkapi satu sama lainnya.

2.3 Keamanan Data

Secara umum data dikategorikan menjadi data yang bersifat rahasia dan data tidak bersifat rahasia. Data tidak bersifat rahasia biasanya tidak terlalu penting. Data yang penting adalah data yang bersifat rahasia, dimana setiap informasi yang ada didalamnya sangat berharga bagi pihak yang membutuhkan karena data tersebut dapat dengan mudah digandakan. Untuk mendapatkan informasi didalamnya, biasa dilakukan berbagai cara yang tidak sah sehingga dibutuhkan suatu sistem yang dapat menjamin keamanan data.

Keamanan suatu data terkait dengan hal-hal sebagai berikut [4]:

a. Fisik. Dalam hal ini pihak yang tidak berwenang terhadap data berusaha untuk mendapatkan data dengan melakukan sabotase atau penghancuran tempat penyimpanan data.
b. Organisasi. Dalam hal ini pihak yang tidak berwenang terhadap data berusaha untuk mendapatkan data melalui kelalaian atau kebocoran anggota yang menangani data.
c. Ancaman dari luar. Dalam hal ini pihak yang tidak berwenang terhadap data berusaha untuk mendapatkan data melalui media komunikasi dan melakukan pencurian data yang tersimpan didalam komputer.

Adapun fungsi keamanan dalam komputer adalah menjaga tiga karakteristik, yaitu [4]:

a. *Secrecy*, adalah isi program komputer yang hanya dapat diakses oleh orang yang berhak. Termasuk *reading, viewing, printing*, atau mengetahui keberadaan sebuah objek.
b. *Integrity*, adalah isi komputer yang dapat dimodifikasi oleh orang yang berhak. Termasuk *writing, changing status, deleting*, dan *creating*.
c. *Availability*, adalah isi komputer yang tersedia untuk beberapa kelompok yang diberi hak.

2.4 Algoritma

Ditinjau dari asal usul katanya, algoritma mempunyai sejarah yang aneh. Para ahli hanya menemukan kata *algorism* yang berarti proses menghitung dengan angka arab dan seseorang dikatakan *algorist* jika menggunakannya. Para ahli bahasa berusaha menemukan asal kata ini namun hasilnya kurang memuaskan. Akhirnya para ahli sejarah matematika menemukan bahwa kata ini berasal dari seorang penulis buku Arab terkenal, yaitu Abu Ja'far Muhammad Ibnu Musa Al-Khuwarizmi (770-840M). Ia menulis buku berjudul Kitab Aljabar Walmuqabala yang artinya Buku Pemugaran dan Pengurangan (*The Book off Restoration and Reduction*). Dari judul buku itu memperoleh akar kata Aljabar (*Algebro*).

Karena kata *algorism* sering dikelirukan dengan *arithmetic* maka dilakukan perubahan kata *algorism* menjadi kata *algorithm*, dimana akhiran "*sm*" menjadi "*thm*". Adapun perhitungan dengan angka arab telah menjadi hal biasa, sehingga kata *algorithm* berangsur-angsur digunakan sebagai metode perhitungan (komputasi) sehingga kehilangan makna kata aslinya. Dalam bahasa Indonesia, *algorithm* diserap menjadi algoritma.

Jadi, algoritma adalah langkah-langkah penyelesaian masalah yang tersusun secara sistematik dan logis [5]. Kata logis adalah kata kunci dalam algoritma karena langkah-langkah dalam algoritma harus logis dan harus dapat ditentukan apakah bernilai salah atau benar.

2.5 Kriptografi

Kriptografi telah menjadi bagian penting dalam dunia teknologi informasi, terutama dalam bidang komputer. Hampir semua penerapan teknologi informasi menggunakan kriptografi sebagai alat untuk menjamin keamanan dan kerahasiaan data atau informasi. Karena itu kriptografi menjadi suatu ilmu yang berkembang pesat dan dalam waktu singkat banyak muncul algoritma-algoritma baru yang dianggap lebih unggul daripada algoritma pendahulunya.

2.5.1 Definisi Kriptografi

Kriptografi (*cryptography*) berasal dari bahasa Yunani yang terdiri dari dua suku kata, yaitu *cryptós* yang berarti rahasia dan *gráphein* yang berarti kata tulisan. Karena itu secara umum kriptografi diartikan sebagai tulisan rahasia.

Terdapat beberapa definisi kriptografi dalam berbagai literatur. Definisi pada tahun 80-an

menyatakan kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan. Kata seni dalam definisi ini berasal dari fakta sejarah bahwa pada awal sejarah kriptografi, setiap orang mempunyai cara yang unik untuk merahasiakan pesan.

Sedangkan definisi dalam buku-buku terbaru menyatakan kriptografi merupakan ilmu mengenai metode untuk mengirimkan pesan secara rahasia sehingga hanya penerima yang dimaksud yang dapat menghapus dan membaca pesan tersebut atau memahaminya [6]. Pengertian lain kriptografi yaitu ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi. Kata *graphy* dalam kata *cryptography* itu sendiri sudah menyiratkan sebuah seni [5].

Jadi, kriptografi adalah suatu ilmu sekaligus seni yang bertujuan untuk menjaga keamanan suatu pesan (*cryptography is the art and science of keeping messages secure*). Secara umum, kriptografi adalah teknik pengamanan informasi dimana informasi diubah dengan kunci tertentu melalui enkripsi sehingga menjadi informasi baru yang tidak dapat dimengerti oleh orang yang tidak berhak menerimanya, dan informasi tersebut hanya dapat diubah kembali oleh orang yang berhak menerimanya melalui dekripsi.

2.5.2 Sejarah Kriptografi

Kriptografi dimulai pertama sekali dengan metode pertukaran posisi untuk mengenkripsi suatu pesan tertentu. Dalam perkembangannya, dikatakan bahwa Julius Caesar dalam mengirim pesan selalu mengacak pesan sebelum diberikan kepada para kurir. Karena itu ada pendapat bahwa yang dilakukan Julius Caesar dianggap sebagai awal mula dari penggunaan kriptografi. Namun sesungguhnya kriptografi telah digunakan untuk pertama kalinya oleh bangsa Mesir pada 4000 tahun lalu dan masih digunakan hingga kini.

Saat ini kriptografi masih diperbincangkan secara luas karena kriptografi dapat digunakan sebagai suatu alat untuk melindungi kerahasiaan dan strategi negara. Sejarah kriptografi sebagian besar merupakan kriptografi klasik, yaitu metode enkripsi yang menggunakan kertas dan pensil atau dengan bantuan alat mekanik sederhana.

Secara umum algoritma kriptografi klasik dikelompokkan dalam dua kategori, yaitu *transposition cipher* dan *substitution cipher*. *Transposition cipher* mengubah susunan huruf-huruf yang ada dalam pesan, sedangkan *substitution cipher* mengganti setiap huruf atau kelompok huruf yang ada dalam pesan dengan huruf atau kelompok huruf lain.

Kriptografi klasik mencatat penggunaan algoritma *transposition cipher* oleh tentara Sparta di Yunani pada awal tahun 400 SM saat mereka menggunakan suatu alat bernama *scytale* yang terdiri dari sebuah kertas panjang dari daun *papyrus* yang dililitkan pada sebuah selinder berdiameter tertentu yang menyatakan kunci penyandian pesan. Pesan kemudian ditulis secara horizontal, baris per baris. Bila pita dilepaskan, huruf-huruf yang ada didalamnya telah tersusun secara acak membentuk pesan rahasia. Untuk membaca pesan, penerima pesan harus melilitkan kembali kertas tersebut pada selinder berdiameter sama dengan diameter selinder pengirim.

Sedangkan penggunaan *substitution cipher* yang paling awal dan paling sederhana adalah *Caesar Cipher* yang digunakan raja Yunani kuno, yaitu Julius Caesar. Caranya dengan mengganti setiap karakter dalam alphabet dengan karakter yang terletak pada tiga posisi berikutnya dalam susunan alphabet yang digunakan.

Pada masa awal agama Kristen, kalangan gereja juga menggunakan kriptografi untuk menjaga tulisan religius yang ada dari gangguan otoritas politik atau budaya yang dominan berkuasa pada saat itu. Metode yang terkenal pada saat itu adalah Angka si Buruk Rupa (*Number of the beast*) yang ada dalam Kitab Perjanjian Baru, yaitu angka "666". Angka ini menyatakan cara kriptografi untuk menyembunyikan pesan yang dipandang berbahaya. Para ahli percaya bahwa pesan ini mengacu pada Kerajaan Romawi [5].

Di India kriptografi digunakan oleh para pecinta untuk berkomunikasi tanpa diketahui orang lain. Metode ini kebanyakan digunakan oleh masyarakat yang terbukti dengan ditemukan kriptografi dalam buku Kama Sutra yang merekomendasikan agar kaum wanita seharusnya mempelajari seni dengan memahami *cipher*. Adapun pada abad ke-17, Ratu Skotlandia (Queen Mary) merupakan salah seorang korban hukuman mati pancung. Hukuman ini ditetapkan setelah ditemukan surat rahasia milik Ratu di balik penjara yang berhasil dipecahkan oleh seorang pemecah kode. Surat rahasia tersebut merupakan surat terenkripsi yang berisi rencana pembunuhan terhadap Ratu Elizabeth I.

Pada abad ke-15 Leon Battista Alberti menemukan Kode Roda (*Wheel Cipher*) yang terdiri dari dua potong silendris, yaitu silendris dalam dan silendris luar, yang disebut *cipher disk*. Masing-masing silendris memiliki seluruh label alfabet dengan susunan yang tidak harus terurut dan sama. Silendris luar merupakan alfabet untuk teks-kode dengan metode *monoalphabetic substitution cipher alphabet,* yaitu metode enkripsi yang satu karakter di teks asli diganti dengan satu karakter bersesuaian atau fungsi satu ke satu. Metode ini terus dikembangkan menjadi alat enkripsi dan dekripsi hingga saat ini.

Awalnya metode ini dikembangkan oleh Thomas Jefferson sehingga dinamakan Roda Kode Jefferson. Selanjutnya dikembangkan oleh Bazeries dan dinamakan Silinder Bazerries. Metode ini lebih fleksibel dari metode lama karena dapat dikembangkan secara terus menerus untuk menghindari *code breaking*. Namun metode ini dapat dipecahkan oleh Deviaris pada tahun 1893 tetapi metode ini tetap dikembangkan dan dianggap aman untuk kasus-kasus tertentu.

Pada abad ke-20 kriptografi lebih banyak digunakan kalangan militer. Pada perang dunia II, Nazi Jerman membuat mesin enkripsi bernama *enigma* yang menggunakan beberapa *rotor* (roda berputar) dan melakukan enkripsi yang sangat rumit. Nazi Jerman percaya bahwa pesan yang dikirim melalui *enigma* tidak terpecahkan. Tetapi anggapan ini salah karena setelah bertahun-tahun mempelajari mesin *enigma*, pihak Sekutu berhasil memecahkannya. Saat Nazi Jerman mengetahui kode mereka telah terpecahkan, mereka membuat beberapa kali perubahan pada mesin *enigma*.

Mesin *enigma* yang digunakan Nazi Jerman dapat mengenkripsi satu pesan dengan 15 milyar kemungkinan. *Enigma* termasuk dalam kriptografi berbasis *rotor* yang dibangun dan dipatenkan oleh beberapa orang Penemu dari beberapa negara yang berbeda sejak tahun 1917 hingga 1921, yaitu Edward Hug Hebern (Amerika), Arthur Scherbius (Jerman), Alexander Koch (Belanda), dan Arvid Gerhard Damm (Swedia). Mesin Koch kemudian dikembangkan untuk versi militer oleh Arthur Scherbius yang dipatenkan dengan nama *Enigma*. Diperkirakan mesin *enigma* yang digunakan pada tahun 1935-1945 berjumlah 100.000 mesin.

Perkembangan paling pesat dan berpengaruh dalam sejarah kriptografi adalah pada tahun 1976 dimana Whitfield Diffie dan Martin Hellman mempublikasikan tesis berjudul *New Direction in Cryptography* yang memperkenalkan konsep kunci publik kriptografi yang revolusioner dan metode baru dalam pertukaran kunci, yaitu keamanan berdasarkan algoritma diskrit.

Selanjutnya pada tahun 1978 Rivest, Shamir, dan Adleman menemukan enkripsi kunci publik pertama yang dikenal sebagai RSA (*Rivest, Shamir, and Adleman*). Skema RSA didasarkan permasalahan matematika rumit yang terdiri dari pemfaktoran bilangan-bilangan bernilai besar. Salah satu sumbangan penting dari kriptografi kunci publik ini adalah tanda tangan digital. Pada tahun 1991, standar internasional pertama untuk tanda tangan digital yang dipergunakan adalah berdasarkan pada skema kunci publik RSA.

2.5.3 Tujuan Kriptografi

Terdapat empat tujuan yang mendasari kriptografi, yaitu [5]:

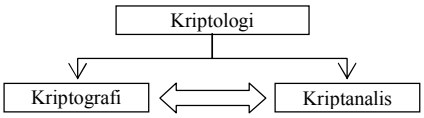
a. Kerahasiaan. Memberikan kerahasiaan pesan dan menyimpan data dengan menyembunyikan data/informasi dengan teknik enkripsi.
b. Integritas data. Memberikan jaminan bahwa dari setiap bagian dalam informasi tidak mengalami perubahan dari saat dibuat/dikirim hingga saat informasi tersebut dibuka.
c. Penyangkalan. Memberikan cara untuk membuktikan bahwa suatu dokumen datang dari seseorang bila ia mencoba menyangkal telah memiliki dokumen tersebut.
d. Autentikasi. Memberikan dua bentuk layanan, pertama adalah mengidentifikasi keaslian suatu pesan dan memberikan jaminan keotentikannya, dan kedua adalah untuk menguji identitas seseorang bila ia akan memasuki sebuah sistem.

2.5.4 Istilah dan Konsep Dalam Kriptografi

Dalam kriptografi terdapat beberapa istilah atau terminologi penting sebagai berikut [6]:

a. *Plainteks* dan *Cipherteks*.
   Plainteks (pesan) merupakan data/informasi yang dipahami maknanya. Pesan dapat dikirim atau disimpan dalam media penyimpanan. Agar pesan tidak dapat dipahami oleh pihak yang tidak berkepentingan, pesan perlu disandikan kedalam bentuk yang tidak dapat dipahami yang disebut *ciphertext*.
b. Peserta Komunikasi.
   Komunikasi data melibatkan pertukaran pesan diantara paling kurang dua entitas. Entitas pertama adalah pengirim yang mengirim pesan kepada entitas lainnya. Entitas kedua adalah penerima yang menerima pesan tersebut. Entitas-entitas ini dapat berupa orang, mesin (komputer), kartu kredit, dan lain sebagainya.
c. Enkripsi dan Dekripsi.
   Penyandian pesan dari *plaintext* ke *ciphertext* dinamakan enkripsi, sedangkan mengembalikan pesan dari *ciphertext* ke *plaintext* dinamakan dekripsi. Enkripsi dan dekripsi dapat diterapkan pada pesan yang dikirim dan yang disimpan. *Encryption of data in motion* mengacu pada enkripsi pesan yang ditransmisikan melalui saluran komunikasi, sedangkan *encryption of data at-rest* mengacu pada enkripsi pesan yang tersimpan didalam *storage*.
d. Kriptanalis dan Kriptologi.
   Kriptografi selalu berkembang karena memiliki ilmu yang berlawanan, yaitu kriptanalisis. Kriptografi adalah ilmu dan seni memecahkan *cipherteks* menjadi *plainteks* tanpa memerlukan kunci dan pelakunya disebut kriptanalis. Kriptografer mentransformasikan *plainteks* ke *cipherteks* dengan kunci, sebaliknya kriptanalis memecahkan *cipherteks* untuk menemukan *plainteks* tanpa kunci. Jadi, kriptologi adalah studi mengenai kriptografi dan kriptanalis.

Hubungan antara kriptologi, kriptografi, dan kriptanalis sebagai berikut [5]:



Gambar 1 Hubungan Kriptologi, Kriptografi, dan Kriptanalisis

2.5.5 Jenis-Jenis Kriptografi

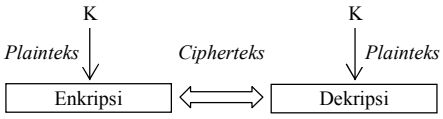
Berdasarkan kunci enkripsi dan dekripsi algoritma kriptografi dibagi menjadi [6]:

a. Kriptografi Simetris

Konsep dasar kriptografi simetris adalah kunci enkripsi dan dekripsi yang sama. Nama lain kriptografi ini adalah kriptografi kunci privat, kriptografi kunci rahasia, atau kriptografi konvensional. Kriptografi ini mengasumsikan penerima dan pengirim pesan telah berbagi kunci tertentu sebelum pesan dikirim sehingga keamanan terletak pada kerahasiaan kunci.

Umumnya *cipher* yang termasuk dalam kriptografi ini beroperasi dalam mode blok, yaitu setiap kali enkripsi atau dekripsi dilakukan pada satu blok data (yang berukuran tertentu), atau beroperasi dalam mode aliran, yaitu setiap kali enkripsi atau dekripsi dilakukan terhadap satu bit atau satu *byte* data.

Proses kriptografi ini sebagai berikut:

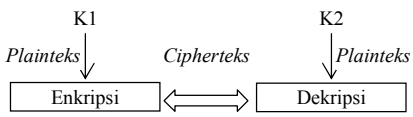


Gambar 2 Skema Kriptografi Simetris

b. Kriptografi Asimetri

Berbeda dengan kriptografi kunci simetris, kriptografi kunci publik memiliki dua kunci yang berbeda pada enkripsi dan dekripsi. Nama lain kriptografi ini adalah kriptografi kunci publik. Kunci untuk enkripsi pada kriptografi ini tidak rahasia (kunci privat). Pengirim akan mengenkripsi dengan kunci publik, sedangkan penerima mendekripsikan kunci privat.

Proses kriptografi ini sebagai berikut:



Gambar 3 Skema Kriptografi Asimetris

2.6 Algoritma *Transposition Cipher*

Algoritma *Transposition Cipher* adalah algoritma yang melakukan enkripsi dengan mengubah urutan *plainteks*. Pada algoritma ini karakter *plainteks* tidak diubah maupun dipetakan menjadi karakter lain. *Cipherteks*nya memiliki karakter yang sama dengan *plainteks* hanya urutannya berubah.

Cara kerja algoritma *Transposition Cipher* adalah membangun suatu matriks berdasarkan karakter *plainteks*, kemudian dilakukan *transpose* pada matriks dan disusunlah *cipherteks* dari hasil *transpose* tersebut. Pengubahan pesan dengan metode ini mirip anagram.

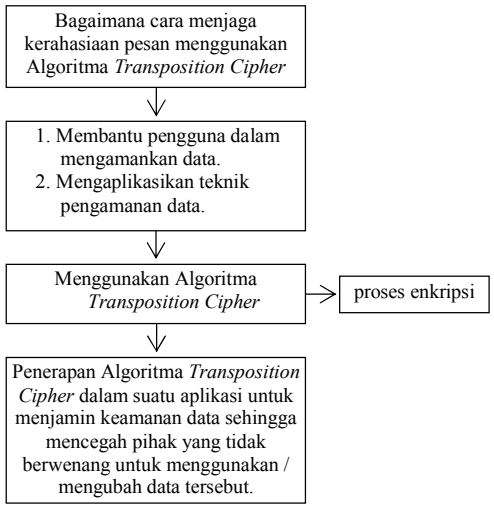
2.7 *Microsoft Visual* Studio 2012

Microsoft Visual Studio 2012 lebih dikenal sebagai VBNET adalah sebuah *software* untuk mengembangkan dan membangun aplikasi yang bergerak diatas sistem NET *Framework* yang menggunakan bahasa *Basic*. Dengan *software* ini programmer dapat membangun beberapa aplikasi yang berbeda, seperti i *Windows Forms*, *web* berbasis ASP.NET, dan *command-line*.

Software ini dapat diperoleh secara terpisah dari beberapa produk lainnya seperti *Microsoft Visual* C++, *Visual* C#, atau *Visual* J#. Dapat juga dapat diperoleh secara terpadu dalam *Microsoft Visual* Studio NET. Bahasa *Visual Basic* NET sendiri menganut paradigma bahasa pemrograman yang berorientasi pada objek yang dapat dilihat sebagai evolusi dari *Microsoft Visual Basic* versi yang sebelumnya.

2.8 Kerangka Pikir Penelitian

Kerangka pikir untuk membangun aplikasi dalam penelitian ini sebagai berikut:



Gambar 4 Kerangka Pikir Penelitian

3. Metode Penelitian

Penelitian ini termasuk jenis deskriptif yaitu penelitian yang dimaksudkan untuk menyelidiki keadaan, kondisi, situasi, peristiwa, dan hal-hal lain, yang hasilnya dipaparkan dalam bentuk deskriptif dalam bentuk laporan penelitian [7].

Untuk memperoleh data-data yang dibutuhkan, digunakan teknik sebagai berikut:

a. Studi Pustaka, yaitu mencari, mengumpulkan, dan mempelajari data-data yang berhubungan dengan penelitian ini.
b. Eksperimen, yaitu suatu percobaan yang dirancang khusus guna membangkitkan data yang diperlukan untuk menjawab pertanyaan penelitian [8]. Dilakukan dengan langkah-langkah seperti berikut [9]:
   1) Melakukan kajian secara induktif yang berkait erat dengan permasalahan.
   2) Mengidentifikasi dan mendefinisi masalah.
   3) Melakukan studi literatur dari sumber yang relevan, memformulasi hipotesis penelitian, menentukan variabel, serta merumuskan definisi operasional dan definisi istilah.
   4) Membuat rencana penelitian yang mencakup:
      a) Mengidentifikasi variabel luar yang tidak diperlukan tetapi mungkin dapat mengkontaminasi proses eksperimen.
      b) Menentukan cara mengontrol.
      c) Memilih rancangan penelitian yang tepat.
      d) Menentukan populasi serta memilih sampel dan sejumlah subjek penelitian.
      e) Membagi subjek dalam kelompok kontrol maupun kelompok eksperimen.
      f) Membuat dan memvalidasi instrumen serta melakukan studi pendahuluan agar diperoleh instrumen yang memenuhi syarat untuk mengambil data yang diperlukan.
      g) Mengidentifikasi prosedur pengumpulan data dan menentukan hipotesis.

Dalam pengembangan sistem digunakan metode *prototyping* sebagai berikut [10]:

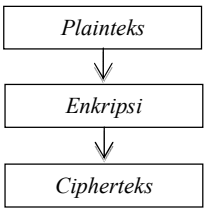
a. *Requirements*, merupakan analisis terhadap kebutuhan pemakai. Terlebih dahulu dilakukan pengumpulan data yang terkait dengan sistem yang dibangun, kemudian menganalisis data-data yang terkumpul agar dapat dilihat kebutuhan yang diinginkan pemakai.
b. *Design*, yaitu membuat desain global untuk membentuk *prototype* perangkat lunak yang akan digunakan oleh pemakai. Desain ini masih berupa *prototype* dalam bentuk rancangan.
c. *Build Prototype*, yaitu membuat *prototype* perangkat lunak, termasuk pengujian dan penyempurnaannya. Desain yang dipilih akan dibuat *prototype*nya dengan aplikasi yang sesuai keinginan pemakai. Kemudian akan diuji kebenaran dan kehandalannya sehingga dapat dibuat sebuah *prototype* yang sebenarnya.
d. *Evaluate and Refine Requirements*, yaitu mengevaluasi *prototype* dan memperhalus analisis kebutuhan pemakai. *Prototype* yang telah diuji dan disempurnakan akan dievaluasi kebenaran dan kemampuannya terhadap sistem.

4. Hasil Penelitian

4.1 Analisis

4.1.1 Analisis Permasalahan

Skema analisa rancangan dari permasalahan penelitian ini sebagai berikut:



Gambar 5 Skema Global Kriptografi Algoritma *Transposition Cipher*

Skema diatas dijelaskan sebagai berikut:

a. *Plainteks* dipermutasi menggunakan permutasi matriks.
b. Hasil permutasi matriks akan dienkripsi satu kali menggunakan kunci tertentu.
c. Proses enkripsi dengan kunci tersebut akan menghasilkan sebuah *cipherteks*.

4.1.2 Analisis Pesan/Data

Analisis pesan/data merupakan tahap dimana dilakukannya analisis terhadap data-data yang akan diolah dalam sistem atau prosedur sebuah rancangan. Data yang akan dienkripsi dengan aplikasi kriptografi Algoritma *Transposition Cipher* adalah data yang diinput langsung pada sistem yang dirancang dan berupa *file Doc*.

4.1.3 Analisis Keamanan Pesan/Data

Pertukaran informasi terjadi setiap detik di *internet* sehingga banyak terjadi pencurian informasi oleh pihak-pihak tertentu yang tidak bertanggungjawab. Agar data yang dikirimkan aman dari pihak-pihak ini maka data dapat disembunyikan dengan menggunakan kriptografi dengan Algoritma *Transposition Cipher*.

Algoritma kriptografi disebut juga *cipher*, yaitu suatu aturan untuk enkripsi dan dekripsi, atau fungsi matematika untuk proses enkripsi dan dekripsi. Keamanan data diukur dari banyaknya kerja yang dibutuhkan untuk memecahkan *cipherteks* menjadi *plainteks* tanpa kunci. Makin banyak kerja dan waktu yang dibutuhkan, makin kuat algoritma kriptografi tersebut.

4.2 Penyelesaian

4.2.1 Proses Enkripsi

Langkah-langkah dalam proses enkripsi sebagai berikut:

a. Blok *plainteks* dipermutasi dengan permutasi matriks.
b. Hasil permutasi matriks akan dienkripsi sebanyak satu kali menggunakan sebuah kunci.

c. Proses enkripsi menggunakan kunci berupa angka yang tidak kurang atau sama dengan nol dan tidak melebihi panjang *plainteks*. Proses ini akan menghasilkan blok *cipherteks*.

Contoh proses enkripsi sebagai berikut:

Plainteks =

DEPARTEMEN TEKNIK INFORMATIKA IBI

Plainteks ini akan dienkripsi menggunakan kunci = 6 sehingga menjadi bentuk sebagai berikut:

D	E	P	A	R	T
E	M	E	N	T	E
K	N	I	K	I	N
F	O	R	M	A	T
I	K	A	I	B	I

Gambar 6 Matriks *Plainteks* Dalam Enkripsi

Untuk menghasilkan *cipherteks*, *plainteks* dalam matriks diatas akan dibaca dan dituliskan secara vertikal sehingga *cipherteks* dihasilkan:

DEKFIEMNOKPEIRAANKMIRTIABTENTI

4.2.2 Proses Dekripsi

Proses dekripsi merupakan kebalikan dari proses enkripsi. Pada Algoritma *Transposition Cipher*, proses enkripsi dan deskripsi menggunakan kunci yang sama, sehingga bila dalam enkripsi menggunakan kunci 6 maka dalam deskripsi juga harus menggunakan kunci 6.

Proses dekripsi akan mengubah *cipherteks* kembali menjadi *plainteks* dengan menyusun *cipherteks* kedalam matriks yang lebarnya ditentukan dengan rumus sebagai berikut :

$$\frac{\text{Panjang } \textit{Cipherteks}}{\text{Kunci}}$$

Hasil perhitungan digunakan untuk menyusun lebar matriks *cipherteks* sehingga dapat diubah kembali menjadi *plainteks*.

Contoh proses dekripsi sebagai berikut:

Plainteks =

DEPARTEMEN TEKNIK INFORMATIKA IBI

Kunci = 6

Cipherteks =

DEKFIEMNOKPEIRAANKMIRTIABTENTI

Panjang *cipherteks* = 30

Sehingga dihitung = 30/6 = 5

Jadi, matriks *cipherteks* adalah:

D	E	K	F	I
E	M	N	O	K
P	E	I	R	A
A	N	K	M	I
R	T	I	A	B
T	E	N	T	I

Gambar 7 Matriks *Cipherteks* Dalam Dekripsi

Untuk menghasilkan *plainteks*, *chiperteks* dalam matriks diatas akan dibaca dan dituliskan secara vertikal sehingga *plainteks* yang dihasilkan:

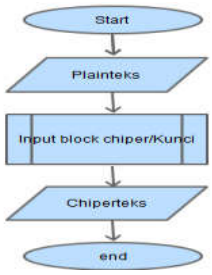
DEPARTEMENTEKNIKINFORMATIKAIBI

Plainteks yang terbentuk dari proses dekripsi tidak terpisah antara kata yang satu dengan kata g lainnya karena pada proses enkripsi pemisah kata (spasi) tidak digunakan dalam pembentukkan karakter matriks *plainteks*.

4.3 Perancangan Sistem

4.3.1 Rancangan Proses Enkripsi

Rancangan proses enkripsi digambarkan dalam bentuk *flowchart* sebagai berikut:



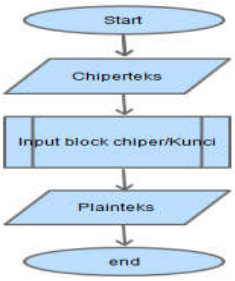
Gambar 8 Rancangan Proses Enkripsi Kriptografi Algoritma *Transposition Cipher*

Rancangan proses enkripsi diatas dijelaskan sebagai berikut:

a. Memulai proses enkripsi dengan sebuah kunci.
b. Misalkan fungsi enkripsi memiliki kunci = 6 maka *plainteks* diproses dalam matriks yang menggunakan kunci tersebut.
c. Setelah *plainteks* diproses akan menghasilkan *cipherteks*.
d. Proses enkripsi selesai.

4.3.2 Rancangan Proses Dekripsi

Rancangan proses dekripsi digambarkan dalam bentuk *flowchart* sebagai berikut:



Gambar 9 Rancangan Proses Dekripsi Kriptografi Algoritma *Transposition Cipher*

Rancangan proses dekripsi diatas dijelaskan sebagai berikut:

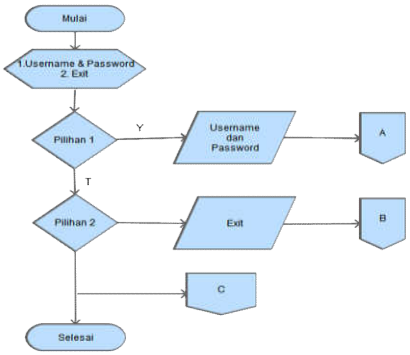
a. Memulai proses dekripsi dengan kunci yang sama dengan proses enkripsi, yaitu 6.
b. Tentukan matriks untuk memproses *cipherteks* dengan rumus:

$$\frac{\text{Panjang } \textit{Cipherteks}}{\text{Kunci}}$$

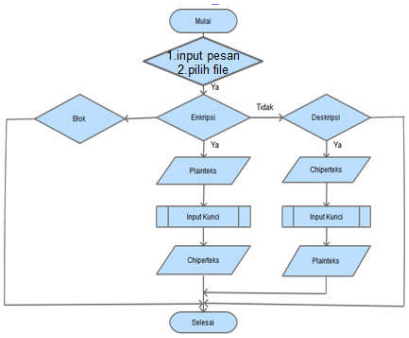
c. Setelah *cipherteks* diproses akan menghasilkan *plainteks*.
d. Proses dekripsi selesai.

4.4 *Flowchart*

Aplikasi kriptografi Algoritma *Transposition Cipher* yang dibangun dalam penelitian ini terdiri dari dua bentu *flowchart* sebagai berikut:



Gambar 10 *Flowchart Form Login*



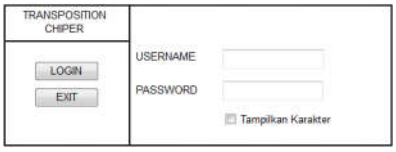
Gambar 11 *Flowchart Form* Utama dan *Form Blok*

4.5 Perancangan Desain

Rancangan desain dalam penelitian ini terdiri dari beberapa *form* sebagai berikut:

a. Rancangan *Form Login*

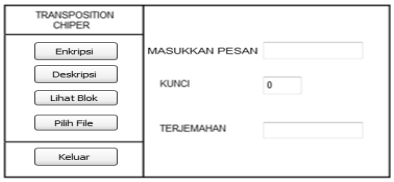
Form login untuk keamanan aplikasi agar tidak dapat dijalankan oleh orang yang tidak memiliki hak akses. Pada kolom pertama terdapat *button login* dan *button exit*. Adapun pada kolom kedua terdapat label *username*, label *password*, 2 *textbox* dan *checkbox* sebagai berikut:



Gambar 12 Rancangan *Form Login*

b. Rancangan *Form* Utama

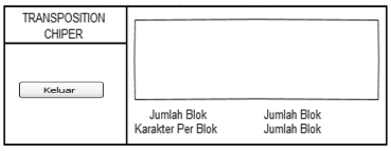
Form utama untuk memasukkan pesan yang akan dikirim dan kunci yang digunakan, serta perintah yang akan dijalankani. Pada kolom pertama terdapat *button* enkripsi, *button* deskripsi, *button* blok, *button load file*, dan *button* keluar. Adapun pada kolom kedua terdapat label *plainteks*, label kunci, label terjemahan, dan 3 *textbox* sebagai berikut:



Gambar 13 Rancangan *Form* Utama

c. Rancangan *Form* Blok

Form blok untuk melihat blok-blok kata yang terbentuk sesuai dengan kunci yang digunakan. Pada kolom pertama terdapat terdapat *button* Keluar. Adapun di kolom kedua terdapat *listbox* dan 4 label sebagai berikut:



Gambar 14 Rancangan *Form* Blok

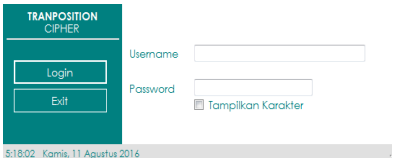
4.6 Implementasi

4.6.1 Implementasi Desain

Desain aplikasi kriptografi Algoritma *Transposition Cipher* sebagai berikut:

a. Implementasi Desain *Form Login*

Form login tampil pertama kali ketika aplikasi dijalankan untuk autentifikasi *user*. Setelah sukses *login*, ditampilkan menu-menu sesuai hak akses**.** Tampilan *form login* sebagai berikut:



Gambar 15 Tampilan *Form Login*

b. Implementasi Desain *Form* Utama

Form utama terdiri dari dua menu, yaitu Menu Enkripsi dan Menu Dekripsi. Melalui *form* ini juga *user* dapat masuk ke *form* Blok. Tampilan *form* utama sebagai berikut:

Gambar 16 Tampilan *Form* Utama

c. Implementasi Desain *Form* Blok

Form blok menunjukkan jumlah dan karakter pesan dalam blok-blok yang terbentuk setelah *user* memasukkan *plainteks* dan kunci yang digunakan. Tampilan *form* blok sebagai berikut:

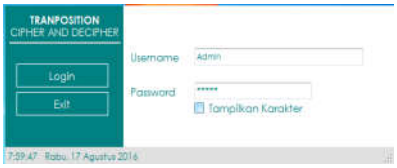
Gambar 17 Tampilan *Form* Blok

4.6.2 Implementasi Program

Implementasi program aplikasi kriptografi Algoritma *Transposition Cipher* sebagai berikut:

a. Implementasi Program *Form Login*

Program *form login* diperuntukan bagi *user*. Jika *user* ingin masuk ke *form* utama maka *user* harus mengisi *Username* dan *Password*. Pada *form login* terdapat *Chek Box* untuk menampilkan atau menyembunyikan *Password*. Tampilan program *form login* sebagai berikut:



Gambar 18 Program *Form Login*

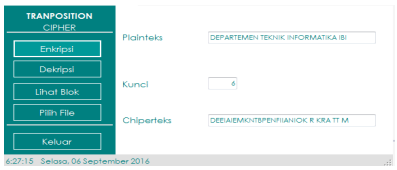
b. Implementasi Program *Form* Utama

Program *form* utama terbagi dalam dua sub program sebagai berikut:

1) Proses Enkripsi

Enkripsi pesan dapat dilakukan dengan *input* secara langsung atau dengan mencari pesan berekstensi doc yang telah ada di *database*. Enkripsi program ini berbeda dengan enkripsi manual. Pada enkripsi manual, jarak antara kata tidak dihitung dalam pembentukan matriks sehingga pesan yang terbentuk akan menyatu. Sedangkan pada program ini, jarak antara kata digunakan dalam pembentukan karakter matriks sehingga pesan yang terbentuk tidak menyatu.

Tampilan program enkripsi sebagai berikut:



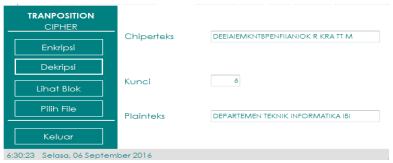
Gambar 19 Program *Form* Utama - Enkripsi

Proses enkripsi diatas menggunakan:

Plainteks :
DEPARTEMEN TEKNIK INFORMATIKA IBI
Kunci : 6
Cipherteks :
DEEIAIEMKNTBPENFIIANIOK R KRA TT M

2) Proses Dekripsi

Dekripsi merupakan proses pembentukkan kembali *cipherteks* menjadi *plainteks* dengan kunci yang sama seperti proses enkripsi. Tampilan program dekripsi sebagai berikut:



Gambar 20 Program *Form* Utama - Dekripsi

Proses dekripsi diatas menggunakan:

Cipherteks :
DEEIAIEMKNTBPENFIIANIOK R KRA TT M
Kunci : 6
Plainteks :
DEPARTEMEN TEKNIK INFORMATIKA IBI

c. Implementasi Program *Form* Blok

Program *form* blok merupakan program yang membentuk matriks karakter dari *plainteks*. Panjang matriks tersebut akan terbentuk secara horizontal sesuai dengan kunci yang digunakan. Cara kerjanya dengan membangun matriks karakter dari *plainteks*, kemudian dilakukan *transpose* pada matriks, dan disusunlah *cipherteks* dari hasil *transpose* tersebut.

Program *form* blok terbagi dalam dua sub program sebagai berikut:

Gambar 21 Program *Form* Blok - Enkripsi

Gambar 22 Program *Form* Blok – Dekripsi

4.6.2 Implementasi *Microsoft Visual Studio* 2012

Tahap terakhir adalah mengimplemantasikan hasil rancangan logika yang telah disusun ke dalam salah satu bahasa pemrograman, yaitu bahasa pemrograman *Microsoft Visual Studio* 2012. Implementasi dalam tahap ini merupakan kegiatan menulis kode program yang akan dieksekusi komputer berdasarkan dokumentasi yang dihasilkan analisis sistem.

Untuk memperoleh hasil yang berkualitas, selama proses penyusunan program harus selalu dikaji secara terus menerus untuk memastikan program tersebut harus bebas dari kesalahan, seperti kesalahan bahasa (*language error*), kesalahan waktu proses (*run time error*), atau kesalahan logika (*logical error*).

4.7 Uji Coba Aplikasi

Pengujian aplikasi kriptografi Algoritma *Transposition Cipher* dilakukan dengan teknik *Black-Box Testing*, yaitu teknik pengujian yang mengamati proses masukan dan keluaran dari sistem perangkat lunak tanpa memperhatikan apa yang terjadi didalam sistem [11].

Salah satu teknik pengujian dalam *Black-Box Testing* adalah dengan membuat tabel yang berisi skenario, *output* yang diharapkan, dan validasi untuk menguji kesesuaian antara desain dengan implementasi. Adapun hasil pengujian aplikasi kriptografi Algoritma *Transposition Cipher* ini sebagai berikut:

Tabel 1 Hasil Uji Coba Aplikasi kriptografi Algoritma *Transposition Cipher*

Form	Skenario Yang Diuji	*Output* Yang Diharapkan	Validasi
Login	Ketik *username* dan *password* kemudian klik Masuk.	Bila data benar maka masuk ke halaman menu.	Sukses
		Bila data salah muncul pesan "*Login* Salah".	Sukses
	Klik tombol *Exit.*	Aplikasi keluar.	Sukses
Utama	Klik tombol Enkripsi.	Pesan yang dimasukkan akan mengalami perubahan posisi menjadi *cipherteks*.	Sukses
	Klik tombol Dekripsi.	Pesan yang dimasukkan akan kembali normal menjadi *plainteks*.	Sukses
	Klik tombol Pilih *File*.	Menu pencarian *file* akan muncul.	Sukses
	Klik tombol Keluar.	Aplikasi keluar.	sukses
Blok	Pada *form* Utama, klik tombol Blok.	Pesan terbentuk menjadi blok-blok sesuai panjang kunci.	Sukses
	Klik tombol Keluar.	Aplikasi akan kembali ke *form* Utama.	Sukses

5. Kesimpulan

Berdasarkan proses pembuatan aplikasi kriptografi Algoritma *Transposition Cipher* dapat disimpulkan bahwa:

1. Algoritma *Transposition Cipher* merupakan algoritma yang sangat tua dan sederhana tetapi dapat menjadi alternatif dalam pengamanan data yang penting atau rahasia.
2. Penggunaan kunci adalah hal yang sangat penting dalam enkripsi dan dekripsi sehingga dibutuhkan kerahasiaan dalam pemakaiannya.
3. Penggunaan pemisah kata (spasi) pada proses enkripsi berpengaruh terhadap pembentukan karakter matriks sehingga menghasilkan *plainteks* yang sesuai dengan pesan aslinya.

6. Penutup

Aplikasi kriptografi Algoritma *Transposition Cipher* yang dibangun dalam penelitian ini mungkin masih memiliki kekurangan *tools* sehingga diharapkan ide-ide baru yang dapat mengembangkan aplikasi.

Daftar Pustaka

[1] Prastowo, Julianti. 2002. *Metode Design dan Analisis Sistem*. Edisi 6. Yogyakarta: Andi.

[2] Komarudin. 2001. *Metode Design dan Analisis Sistem*. Edisi 6. Yogyakarta: Andi.

[3] Witten, L. 2004. *Metode Design dan Analisis Sistem.* Edisi 6. Yogyakarta: Andi Offset.

[4] Herryawan. 2010. *Aplikasi Keamanan Data Menggunakan Metoda Kriptografi Gost*. TSI. Vol. 1. No.2.

[5] Munir, Rinaldi. 2006. *Diktat Kuliah IF5054 Kriptografi*. Prodi Teknik Informatika STEI.

[6] Ariyus, Dony. 2008. *Pengantar Ilmu Kripografi; Teori, Analisis, dan Implementasi*. Yogyakarta: Andi Offset.

[7] Arikunto, Suharsimi. 2009. *Prosedur Penelitian; Suatu Pendekatan Praktik*. Edisi Revisi 6. Jakarta: Rhineka Cipta.

[8] Margono. 2005. *Pengertian Eksperimental*. http:/metode penelitian/navelsblog.html.

[9] Sukardi. 2003. *Langkah-Langkah Penelitian Eksperimental*. http:/metodepenelitian/ navelsblog.html.

[10] Pressman. 2010. *Software Engineering: A Practitionerr's Approach*. 7th Ed. McGraw Hill.

[11] Wahono, Teguh. 2010. *Proses Black Box Testing*. Jakarta: Universitas Indonesia.

Nurdin, N., Stockdale, R., & Scheepers, H. (2012). *Internal Organizational Factors Influencing Sustainable Implementation of Information Systems : Experiences from a Local Government in Indonesia* Paper presented at the Australasian Conference on Information Systems (ACIS) 2012, Deakin University, Geelong, Victoria, Australia. http://dro.deakin.edu.au/view/DU:30049058