APLIKASI KRIPTOGRAFI KEAMANAN DATA MENGGUNAKAN ALGORITMA BASE64

Azlin[1], Fitriah Musadat[2], Jabal Nur[3]

[1,2,3]Dosen Fakultas Teknik Program Studi Tenik Informatika
Universitas Dayanu Ikhsanuddin Baubau

Email: [1]azlin.unidayan01@gmail.com

ABSTRAK

Penelitian ini membahas tentang keamanan data dimana keamanan data merupakan salah satu hal yang selayaknya diberikan perhatian yang lebih, khususnya bagi pemakai yang senantiasa melakukan proses *sharing* data ataupun pesan teks yang bersifat rahasia. Sistem pengamanan data yang lazim digunakan adalah *password* yang terdiri dari beberapa karakter. Sistem pengamanan tersebut masih mengalami kendala dalam mengamankan data. Salah satunya *password* mudah diretas karena mudah ditebak atau jumlah karakter yang minim. Kerahasiaan data yang tidak memiliki sistem keamanan masih sangat mudah di akses oleh pihak yang tidak berkepentingan yang akibatnya data atau pesan teks tersebut dapat disalahgunakan. Untuk mengamankan dan menjaga kerahasiaan data aplikasi dibuat dengan menggunakan kriptografi algoritma base64. Algoritma base64 merupakan salah satu algoritma untuk encoding dan decoding dalam format ASCII,yang didasarkan pada bilangan dasar 64 bit atau salah satu metode yang digunakan untuk melakukan encoding terhadap data binary. Dari proses pengujian pada aplikasi kriptografi algoritma Base64 dapat di simpulkan bahwa algoritma base64 mampu melakukan pengamanan data text dengan mengenkripsi file text menjadi sebuah karakter acak dan mengembalikan data text dengan cara mendeskripsi dari hasil enkripsi menjadi file text kebentuk semula tanpa merubah keasliannya.

Kata Kunci : Aplikasi, Algoritma Base 64, Data

A. PENDAHULUAN

Keamanan data merupakan salah satu hal yang selayaknya diberikan perhatian yang lebih, khususnya bagi pemakai yang senantiasa melakukan proses *sharing* data yang bersifat rahasia, sehingga perlu dilakukan penyadian data agar beberapa pihak yang tidak memiliki kewenangan tidak akan dapat membuka informasi yang dikirim. Banyak cara telah dilakukan untuk meningkatkan keamanan data, salah satunya dengan menggunakan teknik kriptografi. Kriptografi adalah suatu ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan, dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga. Salah satu Cara untuk mengamankan pesan dalam bentuk *text* agar tidak diketahui oleh pihak-pihak yang tidak diinginkan, dilakukan dengan cara mengenkripsi (*encrypt*) pesan (*plaintext*) tersebut menjadi karakter-karakter acak yang tidak dimengerti (*chipertext)* dan untuk memperoleh kembali pesan yang asli, dilakukan dengan cara mendeskripsi (decrypt) sehingga hanya bagi seseorang yang memiliki kunci *(key)* yang dapat mengembalikan pesan kebentuk semula.

Enkripsi itu sendiri adalah sebuah proses yang melakukan perubahan sebuah kode dari yang bisa dimengerti menjadi sebuah kode yang tidak bisa dimengerti (tidak terbaca). Enkripsi dapat diartikan sebagai kode atau chiper. Isu- isu yang terkait dengan keamanan dan kerahasiaan data adalah *privacy* (kerahasiaan), *integrity* (keutuhan), *authenticity* (keaslian), *non-repudiation* (pembuktian yang tak tersangkal).

Saat ini, banyak algoritma- algoritma kriptografi bermunculan sebagai teknik untuk mengamankan data. Algoritma ini pada dasarnya dibagi menjadi algoritma klasik dan modern. Algoritma klasik beroperasi dalam mode karakter, sedangkan
algoritma modern beroperasi dalam mode bit.

Ahmad Timbul Sholeh, Erwin Gunadhi, dan Asep Deddy Supriatna (2013) telah melakukan penelitian tentang 'Mengamankan Skrip Pada Bahasa Pemograman PHP Dengan Menggunakan Kriptografi Base64' dengan tujuan untuk mengamankan skrip dari PHP yang akan didistribusikan agar terjaga hak akses dan integritasnya. Dengan adanya cara pengamanan ini, pengembang aplikasi yang menggunakan bahasa pemograman PHP dapat menyembunyikan skrip PHP agar tidak mudah disalin, diubah oleh orang yang tidak berhak. Pada penelitian ini memiliki kelemahan sistem yaitu kecepatan *respon time script* php lebih lambat jika dibandingkan dengan *respon time script* sebelum di enkripsi dan penggunaan memory dalam mengeksekusi *file* php

yang terenkripsi bertambah karena proses dekode membutuhkan buffer.

Aldino Rahardian (2014) telah melakukan penelitian tentang 'Implementasi *Uniform Resource Locator Encryption* Pada Website Berbasis Algoritma Base64' dengan tujuan untuk mencegah SQL *injection*. Perancangan website dengan penerapan enkripsi pada variabel URL menggunakan metode base64 dapat memberikan solusi untuk mencegah terjadinya serangan SQL *injection*. Pada penelitian ini memiliki kekurangan pada proses penguncian enkripsi dan pembuka kunci pada deskripsi dimana kunci (*key)* enkripsi dan deskripsi di patenkan pada *coding* program.

Msg. Deny Ramadhan, Wiwik Andriani, Shinta Puspasari, Eka Puji Widiyanto (2015) telah melakukan penelitian tentang 'Rancang Bangun Sistem Keamanan Data Dengan Menerapkan Modifikasi Penggabungan Algoritma AES 256 dan Base64' dengan tujuan untuk mengamankan kunci dari para kriptanalis. Modifikasi penggabungan algoritma AES 256 dan Base64 pada sistem keamanan data dapat mengengkripsi data yang akan di simpan dalam database. Fitur *password key* yang dirancang pada sistem keamanan data dapat membatasi serangan pencurian data. Sistem keamanan data cukup aman dari serangan peretas, namun fitur yang diberikan dapat disalahgunakan jika server klien berhasil di *exploit* dan ditanamkan *shell backdoor*, sehingga fitur sistem keamanan data dapat dikendalikan oleh peretas menggunakan server klien yang di kendalikannya.

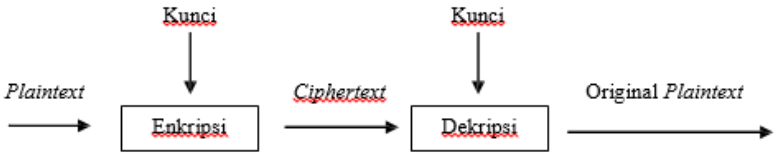
Maka dalam penelitian ini membuat sebuah Aplikasi kriptografi algoritma base64'. Aplikasi ini dapat mengamankan pesan rahasia berupa text dengan mengenkripsi *text* dan *key* sebagai kunci untuk mendeskripsi *text* ke bentuk aslinya. Algoritma base64 merupakan salah satu algoritma untuk encoding dan decoding suatu daya kedalam format ASCII, yang didasarkan pada bilangan 64. Fitur *key* yang dihasilkan dari hasil enkripsi sangat efektif, karena *key* yang di hasilkan bukan di patenkan pada coding program melainkan dari hasil enkripsi. Dengan kata lain, apabila *text* berbeda-beda maka *key* yang dihasilkan akan berbeda. Perancangan aplikasi ini dapat digunakan untuk membantu mengamankan *file text* dari pihak yang tidak berkepentingan, sehingga data aman dan tidak di salah gunakan.

B. TINJAUAN PUSTAKA

a. Kriptografi

Criptography berasal dari bahasa Yunani. Menurut bahasanya, istilah tersebut terdiri dari kata *kripto* dan *graphia*. Kripto berarti *secret* (rahasia) dan *graphia* berarti *writing* (tulisan). Menurut terminologinya, kriptografi adalah ilmu atau seni untuk menjaga keamanan pesan, ketika suatu pesan dikirim dari suatu tempat ke tempat lain, isi dari pesan tersebut kemungkinan dapat disadap oleh pihak lain. Untuk menjaga keamanan pesan, maka pesan tersebut dapat *discreamble*/diacak atau diubah menjadi kode yang tidak dapat dimengerti oleh orang lain. Tujuan dari sistem kriptografi adalah *Authentication, Integrity, Authority, Non-repudiation.*

Dasar matematis yang mendasari proses enkripsi dan dekripsi adalah relasi antara dua himpunan yaitu himpunan yang berisi elemen *plainteks* dan himpunan yang berisi elemen *chipteks*. Enkripsi dan dekripsi merupakan fungsi transformasi antara dua himpunan tersebut.



Gambar 1. Sistem Kriptografi

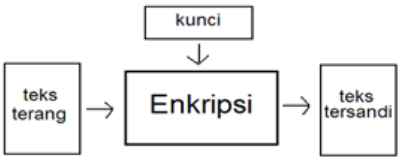
b. Enkripsi

Enkripsi adalah sebuah proses yang melakukan perubahan sebuah kode dari yang bisa dimengerti menjadi sebuah kode yang tidak bisa dimengerti (tidak terbaca). Enkripsi dapat diartikan sebagai kode atau chiper. Isu- isu yang terkait dengan keamanan dan kerahasiaan data adalah *privacy* (kerahasiaan), *integrity* (keutuhan), *authenticity* (keaslian), *non-repudiation* (pembuktian yang tak tersangkal). Di pertengahan tahun 1970-an, enkripsi kuat dimanfaatkan untuk pengamanan oleh sekretariat agen pemerintah Amerika Serikat pada domain publik, dan saat ini enkripsi telah digunakan pada sistem secara luas, seperti Internet e-commerce, jaringan Telepon bergerak dan ATM pada bank. Enkripsi dapat digunakan untuk tujuan keamanan. Ilmu yang mempelajari teknik enkripsi disebut kriptografi. Gambaran sederhana tentang enkripsi, misalnya mengganti huruf a dengan n, b dengan m dan seterusnya. Pembahasan enkripsi akan terfokus pada enkripsi password dan enkripsi komunikasi data.

Terdapat tiga kategori enkripsi yaitu :

1. Kunci enkripsi rahasia, dalam hal ini terdapat sebuah kunci yang digunakan untuk mengikrisi dan juga sekaligus mendeskripsikan informasi.
2. Kunci enkripsi *public*, dalam hal ini terdapat dua kunci yang digunakan, satu untuk proses enkripsi, satu lagi untuk proses deskripsi.

3. Fungsi *one-way*, dimana informasi dienkripsi untuk menciptakan "*signature*" dari informasi asli yang bisa digunakan untuk keperluan autentifikasi.

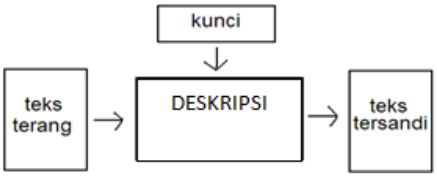


Gambar 2. Alur Enkripsi

c. Deskripsi

Deskripsi adalah satu kaedah upaya pengolahan data menjadi sesuatu yang dapat diutarakan secara jelas dan tepat dengan tujuan agar dapat dimengerti oleh orang yang tidak langsung mengalaminya sendiri. Dalam keilmuan, deskripsi diperlukan agar peneliti tidak melupakan pengalamannya dan agar pengalaman tersebut dapat dibandingkan dengan pengalaman peneliti lain, sehingga mudah untuk dilakukan pemeriksaan dan kontrol terhadap deskripsi tersebut. Pada umumnya deskripsi menegaskan sesuatu, seperti apa sesuatu itu kelihatannya, bagaimana bunyinya, bagaimana rasanya, dan sebagainya. Deskripsi yang detail diciptakan dan dipakai dalam disiplin ilmu sebagai istilah teknik.

Tulisan deskripsi adalah tulisan yang bertujuan untuk menjelaskan sebuag objek secara terperinci tanpa adanya pengaruh pendapat pendapat pengarang di dalam deskripsi tersebut (andy the gunnerz).



Gambar 3. Alur Deskripsi

d. Algoritma Base64

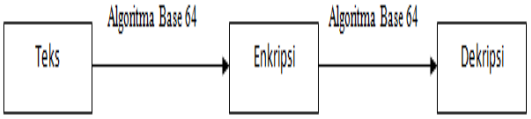
Algoritma Base64 merupakan salah satu algoritma untuk *Encoding* dan *Decoding* suatu daya ke dalam format ASCII, yang didasarkan pada bilangan dasar 64 atau bisa dikatakan sebagai salah satu metode yang digunakan untuk melakukan encoding (penyadian) terhadap data binary. Umumnya digunakan pada berbagai aplikasi seperti e-mail via MME, data XML, atau untuk keperluan encoding URL. Prinsip encodingnya adalah dengan memilih kumpulan dari 64 karakter yang dapat diprint (printable), dengan demikian data dapat disimpan dan ditransfer melewati media yang didesain untuk menangani data tekstual, penggunaan lain encoding Base64 adalah untuk melakukan *obfuscation* atau pengacakan data. Skema enkripsi Base64 biasanya juga digunakan ketika diperlukan sandi terhadap data biner yang didesain untuk menangani data berbentuk teks, hal ini ditujukan untuk menjaga data selama pengiriman ke suatu server. Karakter yang dihasilkan pada transformasi Base64 ini terdiri dari A..Z, a..z dan 0..9, serta ditambahkan dengan dua karakter terakhir yang bersimbol + dan / serta satu buah karakter sama dengan (=) yang digunakan untuk penyesuaian dan menggenapkan data binary atau istilahnya disebut sebagai pengisi pas. Karakter simbol yang akan dihasilkan akan tergantung dari proses algoritma yang berjalan.
Kriptografi Base64 banyak digunakan di dunia internet sebagai media data format untuk mengirim data, ini dikarenakan hasil dari Base64 berupa *plaintext*, maka data ini akan jauh lebih mudah dikirim, dibandingkan dengan format data yang berupa binary. Dalam *Encoding_Base64* dapat dikelompokkan dan dibedakan menjadi kriteria yang tertera dan dapat dilihat di dalam table.

C. METODOLOGI PENELITIAN

Teknik pengumpulan data pada Aplikasi kriptografi algoritma base64 ini menggunakan metode library search. Dimana metode library search yaitu metode yang digunakan dengan mencari data mengenai hal-hal yang dibutuhkan untuk menambah referensi bacaan mengenai Kriptografi Algoritma Base64.

D. HASIL DAN PEMBAHASAN

Pada penelitian ini dilakukan data uji dengan melakukan proses enkripsi dan deskripsi dengan menggunakan menggunakan algoritma base64. Dapat dilihat pada gambar blok diagram alur program.



Gambar 4. Blok diagram Alur program

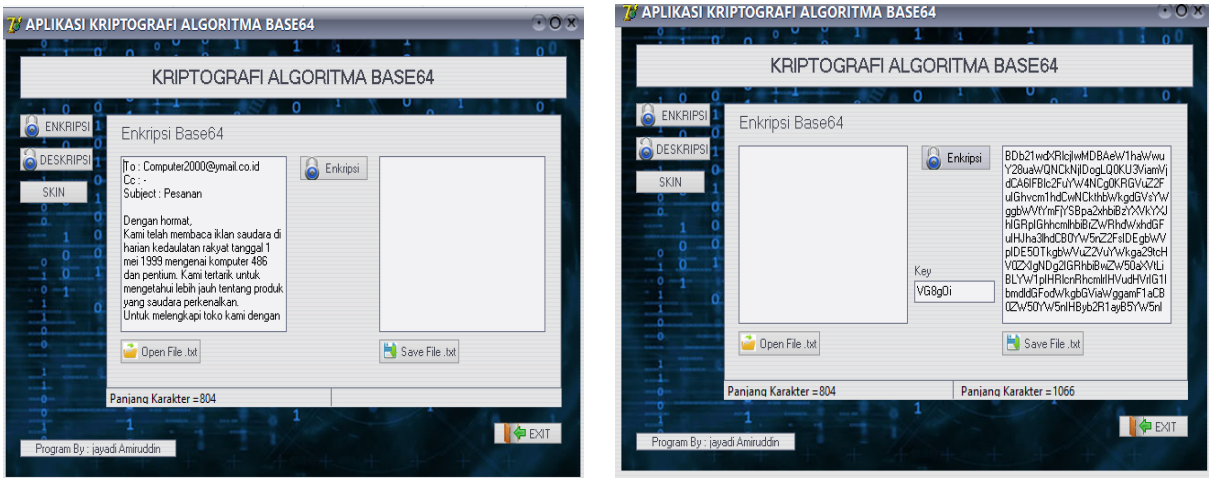
Pada langkah pertama *plaintext* di inputkan ke memo1 pada aplikasi kriptografi algoritma base64 kemuadian ketika mengklik tombol enkripsi maka plaintext di proses menjadi chipertext dengan cara :

a. Pecah *string bytes* tersebut ke per-3 *bytes*
b. Gabungankan 3 *bytes* menjadi 24 *bit.* Dengan catatan 1 *bytes* = 8 bit sehingga 3 x 8 = 24 *bit*
c. Lalu 24 *bit* yang di simpan di-*buffer* (disatukan) dipecah-pecah menjadi 6 *bit,* maka akan menghasilkan 4 pecahan.
d. Masing-masing pecahan diubah ke dalam nilai *decimal,* dimana maksimal nilai 6 *bit* adalah 63.
e. Terakhir, jadikan nilai-nilai jadikan nilai-nilai desimal tersebut menjadi indeks

untuk memilih karakter penyusun dari base64 dan maksimal adalah 63 atau indeks ke-64.

Dan seterusnya sampai akhir *string bytes* yang mau di konversikan. Jika ternyata dalam proses *encoding* terdapat sisa pembagi, maka tambahkan sebagai penggenap sisa tersebut karakter =. Maka terkadang pada base64 akan muncul satu atau dua karakter = ().

Dari penjelasan di atas maka dari plaintext yang di inputkan setelah di proses maka menghasilkan karakter acak seperti yang terlihat pada gambar dibawah ini :

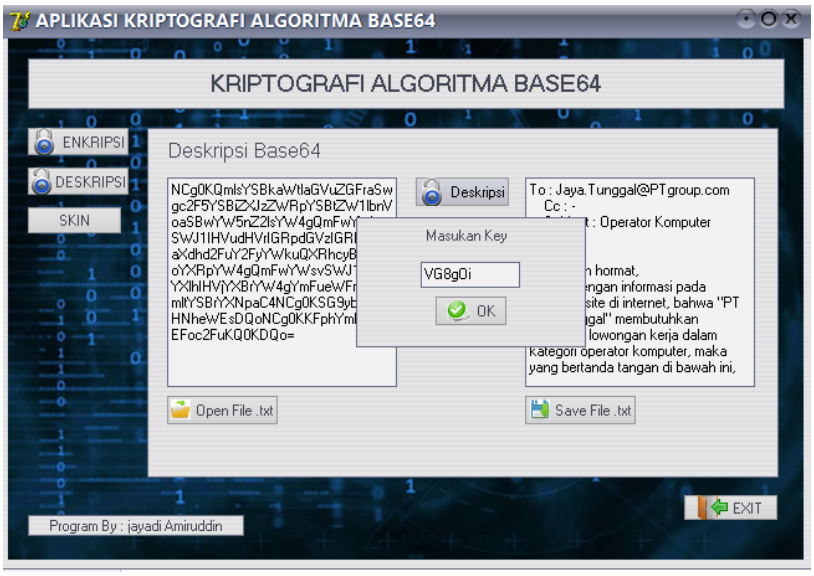


Gambar 6. Proses Enkripsi

Pada proses pengembalikan *plaintext* kebentuk aslinya maka dilakukan proses deskripsi dengan cara :

1. Sesuaikan karakter tersebut pada indeks base64 kemudian ubah ke bentuk decimal.
2. Ubah nilai decimal ke biner masing-masing 6 bit.
3. Gabungkan 6 bit tersebut kemudian pecahkan masing-masing menjadi 8 bit.
4. Setelah masing-masing menjadi 8 bit, ubah kebentuk decimal dan sesuaikan pada format ASCII.

Berikut merupakan gambar hasil deskripsi *chipertext* menjadi *plaintext :*



Gambar 7. Proses Deskripsi

E. KESIMPULAN

Dari proses pengujian pada aplikasi kriptografi algoritma Base64 dapat di simpulkan bahwa algoritma base64 mampu melakukan pengamanan data text dengan mengenkripsi file text menjadi sebuah karakter acak dan mengembalikan data text dengan cara mendeskripsi dari hasil enkripsi menjadi file text kebentuk

semula serta aplikasi kriptografi algoritma base64 mampu mengenkripsi file text lebih dari 6 karakter bahkan lebih dari 100.000 karakter menjadi *chipertext* dan mendeskripsi *chipertext* menjadi *plaintext* tanpa merubah keasliannya tetapi terjadi kesalahan apabila text yang akan di enkripsi kurang dari atau sama dengan 6 karakter.

F. SARAN

Aplikasi ini di rancang dengan menggunakan format text dengan batas lebih dari 6 karakter dan untuk penelitian lebih lanjut dapat menggunakan format lain seperti : format doc, pdf, video, image, dan sebagainya untuk dapat melihat kinerja dari algoritma base64.

DAFTAR PUSTAKA

Ahmad Timbul Sholeh & Erwin Gunadhi & Asep Deddy Supriatna (2013), *Mengamankan skrip pada bahasa pemograman PHP dengan menggunakan kriptografi Base64. jurnal Algoritma Sekolah Tinggi Teknologi Garut 2013.*

Aldino Rahardin (2014), *Impementasi Uniform Resource Locator Encryption pada Website Berbasis Algoritma Base64 Studi Kasus Pada Pimpinan Wilayah Aisyiyah Jawa Tengah.*

Ali Zaki, 2007. *Pengertian Aplikasi. Andi. Yogyakarta.*

Antony Pranata, 1998, *Pemograman Borland delphy*, andi, *Yogyakarta*

Djoko Pramono. *Pemrograman Delphi.* PT. Elex Media Komputindo, Jakarta, 1991.

Dony Arivus. *Pengantar Ilmu Kriptografi Teori, Analisis dan Implementasi*. Andi, Yogyakarta, 2008.

Fairuzabadi, Muhammad. 2010. *Implementasi Kriptografi Klasik Menggunakan Borland Delphi*. Jurnal Dinamika Informatika.

Hendrayudi, 2009. *Pengertian Aplikasi*. Andi. Yogyakarta

Kusnassriyanto. *Belajar Pemprograman Delphi. Modula*. Bandung. 2011.

Msg. Deny Ramadhan, Wiwik Andriani, Shinta Puspasari, Eka Puji Widiyanto (2015), *Rancang Bangun Sistem Keamanan Data Dengan Menerapkan Modifikasi Penggabungan Algoritma AES 256 dan Base64.* STMIK GI MDP, Palembang.