Aplikasi Pengamanan Dokumen PDF dengan Teknik Watermarking Menggunakan Metode Serpent Chiper

Chandra Himmawan Loekito[1], Tutuk Indriyani[1], Nanang Fakhrur Rozi[1]
Program Studi Teknik Informatika, Fakultas Teknik Informasi, Institut Teknologi Adhi Tama Surabaya
Email: [1]chandrahimmawan09@gmail.com

Abstract. *Advances in information and computer technology have quickened the spread of information in forms of digital document and media. The characteristic of information in PDF document is easy but reluctant to change and modify. Its originality is not safe anymore as every person can easily change, modify, and even spread it. For this reason, an application for keeping and saving the content of PDF document was built by watermarking technique and Serpent Chiper algorithm. The combination of both can create high sand unbreakable safety level. Watermarking technique is used to sign and prove the copyright of document. Meanwhile, Serpent Chiper algorithm is a cryptography method for PDF document encryption. The result of research showed that the implementation of Serpent Chiper algorithm on the application can save the inputted PDF document. The results of trial to 30 respondents were as follows: 53.3% respondents stated that the menu and feature of this application were good and easy to use, 23.3% stated that all components in this application could run well, 53.3% said that this application was beneficial for fulfilling the need of final project information, 43.3% said that this application could accommodate data inputted in a large number, and 66.5% claimed that this application was feasible enough to be implemented by an institution.*

Keywords: *PDF, copyright, encryption, watermarking, Serpent Chiper.*

Abstrak. *Seiring perkembangan teknologi informasi dan komputer saat ini, informasi dalam bentuk dokumen digital dan media dapat tersebar dengan begitu cepat. Informasi dalam bentuk dokumen PDF memiliki sifat yang mudah dan rawan untuk diubah dan dimodifikasi. Keaslian informasi dalam bentuk dokumen PDF tidak lagi aman karena setiap orang dengan bebas dapat mengubah dan memodifikasinya untuk kemudian disebarkan kembali. Maka dari itu tujuan dari penelitian ini adalah membuat sebuah aplikasi untuk menjaga dan mengamankan isi dokumen PDF menggunakan teknik watermarking dan algoritma Serpent Chiper. Peneliti menggabungkan teknik watermarking dan algoritma Serpent Chiper agar tingkat keamanannya lebih tinggi dan sulit dipecahkan. Teknik watermarking digunakan untuk menandai dan membuktikan kepemilikan dokumen (hakcipta). Sedangkan algoritma Serpent Chiper merupakan metode kriptografi yang digunakan untuk enkripsi dokumen PDF. Hasil penelitian menunjukkan bahwa penerapan algoritma tersebut pada aplikasi dapat mengamankan dokumen PDF yang diinputkan. Berdasarkan hasil pengujian responden menunjukkan dari total 30 orang 53,3% menyatakan penggunaan menu dan fitur aplikasi baik dan mudah digunakan, 23,3% menyatakan semua komponen didalam aplikasi dapat berfungsi dengan baik, 53,3% menyatakan bahwa aplikasi berperan baik dalam memenuhi kebutuhan informasi skripsi untuk pengguna, 43,3% menyatakan bahwa aplikasi cukup baik untuk menampung data yang diinputkan dalam jumlah banyak, dan 66,5% menyatakan bahwa aplikasi cukup layak diimplementasikan di lembaga atau institusi.*

Kata Kunci: PDF, Hak Cipta, Enkripsi, Watermarking, Serpent Chiper.

1. Pendahuluan

Seiring dengan perkembangan teknologi informasi dan komputer saat ini, informasi dalam bentuk dokumen digital dan media dapat tersebar dengan begitu cepat. Informasi dalam bentuk dokumen PDF memiliki sifat yang mudah dan rawan untuk diubah dan dimodifikasi, sehingga dapat menimbulkan masalahan kepemilikan informasi itu sendiri. Keaslian informasi dalam bentuk dokumen PDF tidak lagi aman karena setiap orang dengan bebas dapat mengubah dan memodifikasinya untuk kemudian disebarkan kembali. Hal ini berkaitan dengan peraturan hukum Negara UUD 1945 Pasal 28 C yang berisi tentang setiap orang berhak mengembangkan diri melalui pemenuhan kebutuhan dasarnya, berhak mendapat pendidikan dan memperoleh manfaat dari ilmu pengetahuan, teknologi, serta seni dan budaya, demi meningkatkan kualitas hidupnya dan demi kesejahteraan umat manusia. Dalam pasal tersebut juga dijelaskan tentang hak cipta (*copyright*) yang merupakan istilah legal yang menjelaskan suatu hak yang diberikan pada pencipta atas karya literatur dan artistik mereka. Tujuan utamanya adalah untuk memberikan peraturan perlindungan hak cipta serta memberikan penghargaan atas sebuah karya cipta. Dapat diambil kesimpulan bahwa peraturan hukum negara tersebut telah menjelaskan dan memberikan hak cipta atas kepemilikan informasi atau dokumen digital kepada yang telah membuat suatu karya ilmiah.

Sehubungan dengan hal tersebut penulis akan mengembangkan aplikasi yang dapat menjaga kepemilikan dan melindungi keaslian dokumen PDF dengan melakukan enkripsi yang bertujuan agar terhindar dari perubahan dan modifikasi dokumen digital secara ilegal.

Algoritma yang digunakan dalam pengembangan aplikasi kemanan dokumen PDF adalah algoritma Serpent Chiper. Algoritma Serpent Chiper merupakan Algoritma chipper block yang terdiri dari 32 putaran substitution permutation (SP) yang beroperasi pada empat word 32bit dengan ukuran bloknya adalah 128 bit. Untuk komputasi internal, semua nilai direpresentasikan dalam little-endian, plaintext ke dalam bentuk ciphertext. Pada mode ECB (*Elekctronic Codebook*), sebuah blok pada plaintext dienkripsi ke dalam sebuah *blok ciphertext* dengan panjang blok yang sama. Algoritma *serpent* merupakan algoritma kuat yang sampai saat ini dinyatakan aman karena masih belum ada serangan kriptanalisis yang benar-benar dapat mematahakan algoritma ini. Algoritma serpent juga tidak dipatenkan, sehingga penggunaannya untuk melakukan enkripsi tidak memerlukan adanya biaya.

2. Tinjauan Pustaka

2.1. *Watermarking*

Watermarking merupakan bentuk dari Steganography, yaitu ilmu yang mempelajari tentang bagaimana cara menyembunyikan suatu data pada data yang lain. *Watermarking* ini agak berbeda dengan tanda air pada uang kertas. Tanda air pada uang kertas masih terlihat oleh indera manusia (dalam posisi kertas tertentu), sedangkan Watermarking pada media digital tidak dapat dirasakan kehadirannya oleh manusia tanpa alat bantu mesin pengolah digital seperti computer. *Watermarking* ini memanfaatkan kekurangan-kekurangan sistem indera manusia seperti mata dan telinga. Dengan adanya kekurangan inilah metode *Watermarking* ini dapat diterapkan pada berbagai data digital. Jadi *Watermarking* merupakan suatu cara untuk menyembunyikan atau mengamankan suatu data/informasi tertentu ke dalam suatu data digital lainnya, tetapi tidak diketahui kehadirannya oleh indera manusia [1, 2].

2.2. Pengertian Kriptografi

Kriptografi adalah ilmu yang mempelajari tentang cara menjaga data atau pesan agar tetap aman saat dikirimkan, dari pengirim ke penerima untuk menghindari gangguan dari pihak lain. Menurut *Bruce Scheiner* dalam bukunya "*Applied Cryptography*", kriptografi merupakan ilmu pengetahuan yang digunakan untuk menjaga pesan agar tetap aman (*secure*) [3].

Konsep kriptografi sebenarnya sudah lama digunakan sejak jaman peradaban Romawi meskipun masih sangat sederhana. Prinsip-prinsip yang mendasari kriptografi salah satunya adalah *Confidelity* (kerahasiaan) yakni berupa layanan agar isi pesan yang dikirimkan tetap terjaga kerahasiaannya sehingga tidak mudah diketahui oleh pihak lain (kecuali pihak pengirim dan pihak penerima). Hal ini dilakukan dengan cara membuat suatu algoritma matematis yang mampu mengubah data hingga menjadi sulit untuk dibaca dan dipahami [4].

2.3. Algoritma *Serpent Chiper*

Algoritma serpent merupakan algoritma *block chipper* yang didesain oleh Ros Anderson, Eli Biham, dan Lars Knudsen. Algoritma ini merupakan runner-up dalam kompetisi Advanced Encryption Standart (AES) yang dimenangkan oleh algoritma Rijandael. Para perancangnya mengklaim meskipun Rijandael lebih cepat karena memiliki putaran lebih sedikit, serpent lebih aman. Meskipun lebih lambat daripada algoritma AES (Rijandael), algoritma ini masih lebih cepat daripada algoritma DES (Data Encryption Algorithm) yang telah banyak digunakan sebelumnya. Pada mesin Pentium 200MHz, algoritma serpent dapat berjalan dengan kecepatan 45 Mbit/s. Ini lebih cepat daripada DES yang memliki kecepatan 15 Mbit/s pada mesin yang sama. Serpent merupakan operasi SP-network (substitution permutation network) 32 putaran pada 4word berukuran 32 bit (blok berukuran 128 bit). Pada komputasi internal, semua nilai direpresentasikan little-endian dengan word pertama adalah least significant word dan word terakhir adalah most significant word dengan bit 0 merupakan least significant bit dari word pertama. Panjang kunci yang dapat digunakan berukuran 128, 192, atau 256 bit. Jika panjang kurang dari 256 bit, kunci tersebut ditambahkan satu bit ’1’ yang diikuti ‘0’ hingga panjangnya 256 bit [5].

2.4. Block Chiper Serpent

Serpent menggunakan S-Box dari DES yang telah banyak dipelajari selama bertahun-tahun dengan properti-properti yang dapat dipahami dengan baik, dengan struktur baru yang telah dioptimasi untuk implementasi yang lebih efisien pada Processor modern. Rancangan serpent tahan terhadap semua jenis serangan-serangan yang menggunakan teknik diferensial dan linear.

Ada beberapa varian Cipher serpent. Varian utama adalah Cipher 32 putaran yang diyakini seaman Cipher tiga kunci triple DES. Cipher serpent 32 putaran ini sedikit lebih lambat daripada DES. Cipher ini beroperasi pada empat word berukuran masing-masing 32bit sehingga ukuran blok menjadi 128 bit [6].

Varian lainnya dibuat dengan meningkatkan ukuran blok. Ukuran blok dapat ditingkatkan menjadi dua kali lipat menjadi 256bit baik dengan meningkatkan ukuran word dari 32bit menjadi 64 bit, maupun dengan menggunakan fungsi putaran pada jaringan Feistal. Dua varian Cipher serpent ini dapat dikombinasikan untuk menghasilkan Cipher dengan panjang blok 512 bit.

Semua nilai yang digunakan pada Cipher direpresentasikan dalam littleendian, termasuk urutan 32bit (0-31 dalam word berukuran 32 bit, atau 0-127 dalam blok 128 bit), dan urutan word dalam blok. Bit 0 adalah bit paling tidak berarti (Least Significant Bit), dan word 0 adalah word paling tidak berarti (LeastSignificant Word). Notasi penulisan sangat penting karena ada dia representasi serpent yang ekuivalen yaitu representasi standard dan representasi bitslice.

2.5. *Key Schedule Serpent*

Sebagaimana dekripsi pada *Cipher,* kita dapat mendeskripsikan key schedule dalam mode standard atau mode bitslice. *Cipher serpent* memerlukan 132 buah word yang masing-masing berukuran 32 bit. Pertama, kita ekspansi kunci masukan user sepanjang 256 bit menjadi 33

buah sub kunci (K0, ..., K32) dengan panjang masing-masing 128 bit.

Kita tulis K sebagai delapan word (w-8, …, w-1) yang masing-masing berukuran 32 bit lalu ekspansi menjadi intermediate key (disebut juga prekey) w0,...,w131 dengan cara rekursif sebagai berikut :

$$wi = (wi\text{-}8+wi\text{-}5+wi\text{-}3 +wi\text{-}1 +\Phi +i) <<< 11$$

Dimana Φ adalah bagian fraksional dari golden ratio (5 +1)/2 atau 0x9e3779b9 dalam heksadesimal. Polinomial x8+x7+x5+x3+1 adalah primitif dimana bersama dengan penjumlaha index putaran dipilih untuk memastikan distribusi bit kunci merata pada setiap putaran, dan untuk menghilangkan kunci lemah dan keterhubungan antar kunci.

Round key sekarang dihitung dari prekey menggunakan S-box pada mode bitslice. Input dan output S-box diambil pada jarak 33 words, untuk meminimalkan potensi serangan dengan teknik diferensial pada beberapa putaran akhir [7]. Kita menggunakan S-box untuk mentransformasi prekey wi menjadi word ki yang merupakan round key dengan membagi vektor prekey menjadi empat bagian dan mentransformasi word ke-i pada tiaptiap bagian menggunakan S(r+3-i) mod r. Dapat dilihat pada contoh untuk r = 32 sebagai berikut :

$$\{k0, k33, k66, k99\} = S3(w0, w33, w66,w99)$$
$$\{k1, k34, k67, k100\} = S3(w1, w34, w67,w100) \ldots$$
$$\{k31, k64, k97, k130\} = S3(w31, w64, w97,w130)$$
$$\{k32, k65, k98, k131\} = S3(w32, w65, w98,w131)$$

Lalu kita lakukan penomoran ulang terhadap 32 bit nilai kj sebagai128 bit kunci internal Ki (untuk i Є{0,...,r}) sebagai berikut :

$$Ki = \{k4i, k4i+1, k4i+2, k4i+3\}$$

Kemudian operasikan IP ke round key untuk menempatkan bit kunci ke dalam kolom yang benar.

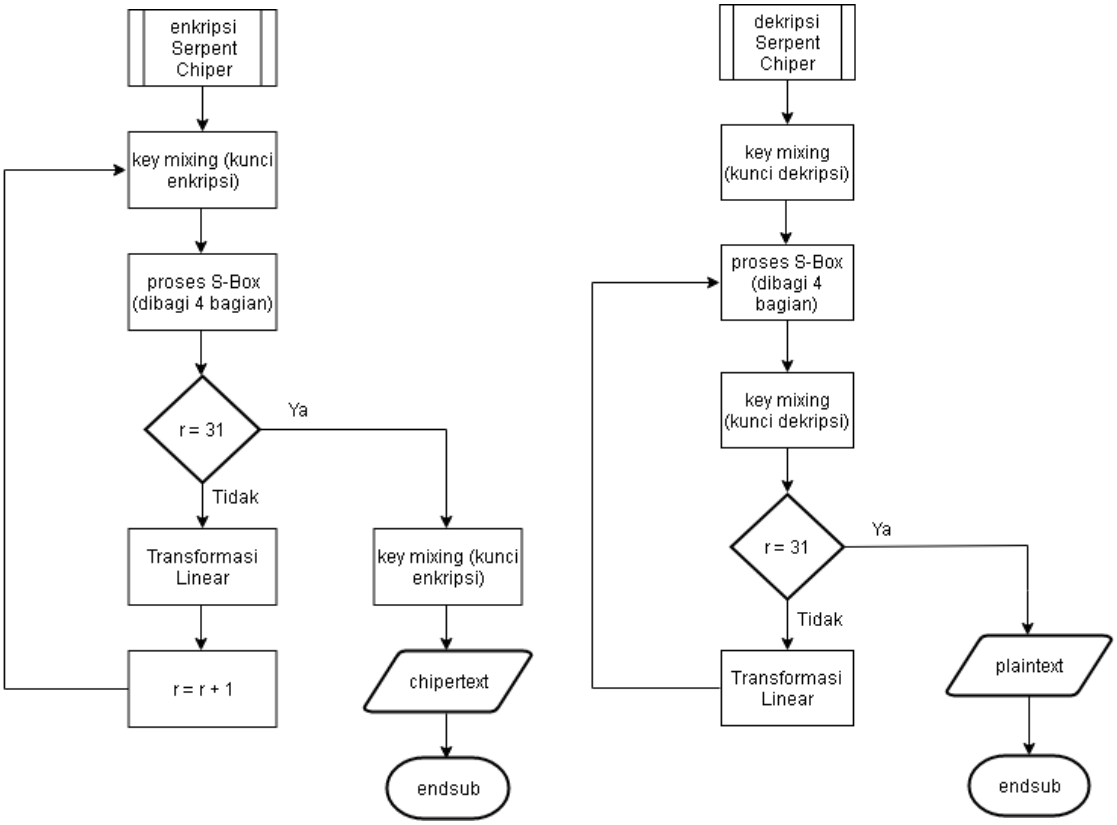
2.6. Pengertian XAMPP

XAMPP merupakan paket program web lengkap yang dapat dipakai untuk belajar pemograman web, khususnya PHP dan MySQL. XAMPP adalah perangkat lunak bebas, yang mendukung banyak sistem operasi, merupakan kompilasi dari beberapa program. Fungsinya adalah sebagai server yang berdiri sendiri (localhost), yang terdiri atas program Apache HTTP Server, MySQL database, dan penerjemah bahasa yang ditulis dengan bahasa pemrograman PHP dan Perl.

3. Metode Penelitian

Pada Gambar 3(a) menggambarkan dan mendeskripsikan alur proses enkripsi serpent chiper pada sistem. Proses tersebut dimulai dari menginputkan file plaintext yang kemudian dienkripsi dengan menggunakan key serpent yang nantinya akan menjadi chipertext atau file yang telah dienkripsi.

Sedangkan pada Gambar 3(b)menggambarkan dan mendeskripsikan alur proses dekripsi serpent chiper pada sistem. Pada proses tersebut chipertext atau file yang telah dienkripsi diproses dengan menggunakan key serpent yang nantinya file tersebut berubah menjadi plaintext atau file yang telah didekripsi.



Gambar 1. Enkripsi vs Deskripsi; (a) Enkripsi Serpent Chiper, (b) Deskripsi Serpent Chiper

4. Hasil dan Pembahasan

4.1. Pengujian Sistem Admin

Pengujian aplikasi pengamanan dokumen PDF ini dilakukan untuk mengetahui keamanan dokumen PDF yang diinputkan. Dokumen PDF dinyatakan aman apabila sistem yang dijalankan sesuai dengan yang sudah ditentukan.

Pada Tabel 1 menjelaskan tugas serta cara kerja admin didalam aplikasi. Admin tersebut melakukan login dengan username dan password yang sesuai kemudian melakukan upload data skripsi dan juga dapat melakukan edit dan menghapus data skripsi serta dapat menambahkan data skripsi yang baru. Berdasarkan data tersebut terlihat bahwa pengujian admin sesuai dengan yang diharapkan.

4.2. Pengujian Sistem *User*

Pada Tabel 2 menjelaskan cara kerja user atau mahasiswa didalam aplikasi. *User* atau mahasiswa yang mengakses dan mengunduh data skripsi tanpa melakukan *register* atau *login* akan mendapat unduhan data skripsi tidak dapat dibuka atau otomatis terenkripsi. Sebaliknya jika *user* atau mahasiswa yang ingin mendapatkan data skripsi secara valid harus melakukan *login* terlebih dahulu dan apabila tidak memiliki akun maka diharuskan untuk melakukan *register* akun.

4.3. Pengujian Fungsi Aplikasi

Pengujian fungsi aplikasi pengamanan dokumen PDF ini dilakukan untuk mengetahui apakah seluruh fungsi atau fitur yang ada didalam aplikasi berjalan sesuai yang diinginkan. Aplikasi dinyatakan sukses apabila seluruh fungsi dan fitur yang ada didalam aplikasi dapat berfungsi dengan baik.

Pada Gambar 1. menampilkan software yang digunakan untuk pengujian fungsi pada aplikasi. Software yang digunakan untuk pengujian fungsi aplikasi adalah Selenium Testing Tool. Software Selenium Testing Tool akan menampilkan seluruh fungsi dan fitur didalam aplikasi. Dengan software tersebut peneliti dapat mengetahui apakah seluruh fitur dan fungsi didalam aplikasi dapat berfungsi sesuai dengan yang diinginkan atau tidak.

Tabel 1. Pengujian Admin

No	Pengujian	Hasil Yang Diharapkan	Hasil Pengujian	Kesimpulan
1.	Admin melakukan login dengan menginputkan *username* dan *password*	Apabila admin menginputkan *username* dan *password* yang sesuai maka dapat login aplikasi. Sebaliknya apabila *username* dan *password* tidak sesuai maka tidak dapat login.	Sesuai	Valid
2.	Admin melakukan upload data skripsi berupa dokumen PDF	Data skripsi yang telah diupload oleh admin tersimpan di database aplikasi serta otomatis terenkripsi dengan menggunakan metode Serpent Chiper dan juga terwatermark	Sesuai	Valid
3.	Admin mengecek data skripsi yang sudah diupload	Admin dapat melakukan edit dan menghapus data skripsi serta dapat melakukan upload	Sesuai	Valid

Gambar 2. *Software Selenium*

Tabel 2. Perubahan karakter pertama pada *key*

No	Pengujian	Hasil Yang Diharapkan	Hasil Pengujian	Kesimpulan
1.	*User* atau mahasiswa mengakses data skripsi tanpa melakukan register atau login	*User* atau mahasiswa yang tidak melakukan register atau login dapat mengakses dan mengunduh data skripsi, akan tetapi setelah terunduh data skripsi tersebut tidak dapat dibuka atau terenkripsi oleh sistem dengan menggunakan metode Serpent Chiper	Sesuai	Valid
2.	*User* atau mahasiswa mengakses data skripsi dengan melakukan register atau login	*User* atau mahasiswa yang melakukan register atau login dapat mengakses dan mengunduh data skripsi. Setelah terunduh data skripsi dapat dibuka karena otomatis telah terdekripsi dengan menggunakan metode Serpent Chiper terwatermark.	Sesuai	Valid

4.4. Pengujian Metode Enkripsi Dan Dekripsi

Pengujian metode enkripsi dan dekripsi pada aplikasi pengamanan dokumen PDF ini dilakukan untuk mengetahui apakah metode enkripsi dan dekripsi yang digunakan didalam aplikasi berjalan sesuai yang diinginkan. Karena metode pengaman dokumen PDF didalam aplikasi menggunakan metode enkripsi dan dekripsi. Aplikasi dinyatakan sukses apabila seluruh metode yakni metode enkripsi dan dekripsi yang ada didalam aplikasi dapat berfungsi dengan baik.

Gambar 3. *Software Hex Editor Neo*

Pada Gambar 3 menampilkan software yang digunakan untuk pengujian metode enkripsi dan dekripsi. Software yang adalah Hex Editor Neo. Software Hex Editor Neo akan menampilkan hasil dari enkripsi dan dekripsi data pada aplikasi. Dengan software tersebut

peneliti dapat mengetahui apakah metode enkripsi dan dekripsi didalam aplikasi dapat berfungsi sesuai dengan yang diinginkan atau tidak.

Dari hasil pengujian enkripsi dan dekripsi menggunakan software Hex Editor Neo dapat dilihat hasil bilangan heksadesimal antara enkripsi dan dekripsi berbeda, meskipun file atau dokumen yang diproses sama. Hal tersebut dapat disimpulkan bahwa fungsi dari metode enkripsi dan dekripsi yang digunakan didalam aplikasi dapat berjalan sesuai dengan yang diinginkan. Karena metode enkripsi dan dekripsi dapat dinyatakan berhasil apabila bilangan heksa decimal antara file yang telah dienkripsi dan file yang telah didekripsi bilangannya berbeda.

4. Kesimpulan

Berdasarkan penelitian yang telah dilakukan, maka dapat diambil kesimpulan sebagai berikut:

1. Aplikasi Pengamanan Dokumen PDF ini berhasil dirancang sehingga dapat membantu user dalam mengamankan data berbentuk dokumen PDF yang tidak ingin disalahgunakan oleh pihak yang tidak bertanggungjawab.
2. Teknik watermarking yang digunakan cukup membantu menunjukkan suatu hak cipta bahwa dokumen yang diupload adalah milik yang bersangkutan.
3. Metode yang digunakan cukup membantu dalam mengenkripsi dan mendekripsi dokumen yang diupload.

Referensi

[1] Irfan. (2013). *Prototipe Teknik Penyisipan Dokumen Citra Digital Menggunakan Watermarking dengan Metode DCT (Discreate Cosine Transform).* Jakarta: Budi Luhur University.

[2] Rita Rosmawati Sitanggang. (2017). *Analisa Perlindungan Hak Cipta Pada Citra Digital Menggunakan Teknik Watermarking Dengan Metode Discreate Cosine Transform Dan Discreate Wavelet Transform.* Medan: STMIK Budidarma.

[3] Ary Hidayatullah. (2016). *Pengenalan Kriptografi Dan Pemakaiannya Sehari-Hari*. Bandung: Universitas Islam Negeri Sunan Gunung Djati.

[4] Setiaji, Bayu. (2015). *Analisis dan Implementasi Algoritma Kriptografi Kunci Publik RSA dan LUC Untuk Penyandian Data.* Yogyakarta: Setiaji, Bayu

[5] Faqihuddin Al-Anshori. (2014). *Implementasi Algoritma Kriptografi Kunci Publik ElGamal Untuk Proses Enkripsi Dan Dekripsi Guna Pengamanan File Data*. Yogyakarta: Universitas Ahmad Dahlan.

[6] Mai Hossam Taher. (2014). *Hardware Implementation of The Serpent Block Chiper Using FPGA Technology*. Egypt: Dept.Mansoura University.

[7] Maskes, Three. (2013). *Implementasi Algoritma Serpent Untuk Enkripsi dan Dekripsi Data File Pada Ponsel Berbasis Android.* STMIK MDP: Nur Rachmat.