Prosiding Seminar Ilmu Komputer dan Teknologi Informasi Vol. 1, No. 1, September 2016
ISSN 2540 – 7902

PENERAPAN KRIPTOGRAFI DENGAN ALGORITMA DATA ENCRYPTION STANDART PADA TEXT HASIL KONVERSI DARI CITRA

Nur Muhammad Dwi Oktafiansyah[*,1], Fahrul Agus[2], Septya Maharani[3]

[1,2,3] Program Studi Ilmu Komputer, FKTI Universitas Mulawarman
Kampus Gunung Kelua Barong Tongkok Samarinda, Kalimantan Timur
Email : nuwaboy@gmail.com[1], fahrulagus@yahoo.com[2], septyamaharani@yahoo.com[3]

ABSTRAK

Sistem pada keamanan data dan kerahasiaan data merupakan salah satu aspek penting dalam perkembangan kemajuan teknologi informasi namun yang cukup disayangkan adalah ketidakseimbangan antara setiap perkembangan suatu teknologi yang tidak diiringi dengan perkembangan pada sistem keamanannya itu sendiri, dengan demikian cukup banyak sistem – sistem yang masih lemah dan harus ditingkatkan keamanannya. Oleh karena itu pengamanan data yang sifatnya rahasia haruslah benar - benar diperhatikan. Untuk mengatasi masalah tersebut maka diperlukan suatu aplikasi pengamanan data yang dapat mencegah dan mengamankan data-data yang kita miliki dari orang-orang yang tidak berhak mengaksesnya. Salah satunya adalah metode algoritma kriptografi simteris, karena algoritma ini menggunakan kunci yang sama pada saat melakukan proses enkripsi dan dekripsi sehingga data yang penulis miliki akan sulit untuk dimengerti maknanya dan untuk proses enkripsi data yang sangat besar akan sangat cepat. Algoritma kriptografi (cipher) menggunakan DES.

Kata kunci : Kriptografi, Enkripsi, Dekripsi, Data Enkripsi Standar.

1. PENDAHULUAN

Pentingnya menjaga kerahasiaan suatu informasi membuat ilmu kriptografi digunakan untuk mengamankan berbagai data, baik data informasi secara umum maupun data multimedia seperti data gambar pada khususnya. Perkembangan data gambar menimbulkan berbagai permasalahan seperti penyalahgunaan akses dan penjiplakan yang telah menimbulkan dampak serius terhadap permasalahan legal, sosial dan ekonomi.Tidak semua gambar dibuat untuk konsumsi masyarakat umum, banyak dari gambar tersebut bersifat pribadi hanya ditunjukkan untuk kelompok atau masyarakat tertentu. Oleh karena itu berbagai cara dilakukan masyarakat untuk mendapatkan informasi yang terdapat pada gambar tersebut. Serta kebanyakan enkripsi pada gambar hanya menghasilkan gambar juga, belum ada ditemukan solusi atau alternatif yang lain.

Algoritma kriptografi selalu terdiri dari dua macam yaitu enkripsi dan dekripsi. Tekhnik untuk menyandikan plaintext menjadi ciphertext disebut enkripsi, sedangkan proses mengembalikan ciphertext menjadi plaintext seperti semula dinamakan dekripsi.

Salah satu media yang sering dijadikan tujuan kejahatan yaitu media gambar.Sehubungan dengan latar belakang maka diperlukan pengamanan file untuk disimpan sendiri atau untuk dikirim kepihak lain yang tidak sekedar diproteksi disk atau pengamanan secara hardware saja namun diperlukan salah satu teknik lain untuk pengamanan file.

Membahas mengenai kriptografi pada citra melalui perhitungan pada nilai RGB (Red, Green, Blue) citra tersebut. penulis bermaksud untuk mengembangkannya, yaitu dengan mengubah hasil citra menjadi huruf A-Z, a-z, dan 0-9 lalu mengenkripsinya dengan menggunakan algoritma DES.

2. TINJAUAN PUSTAKA

2.1 Kriptografi

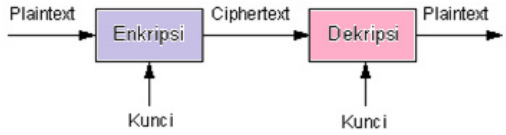
Ada berbagai definisi sistem yang berbeda diantaranya, kriptografi atau yang sering dikenal dengan sebutan ilmu penyandian data, adalah suatu bidang ilmu dan seni (art and science) yang bertujuan untuk menjaga kerahasiaan suatu pesan yang berupa data-data dari akses oleh orang-orang atau pihak-pihak lain yang tidak berhak sehingga tidak menimbulkan kerugian[3].

Kriptografi merupakan kumpulan teknik untuk Mengkode data dan pesan sedemikian rupa sehingga data dan pesan tersebut dapat disimpan dan ditransmisikan dengan aman[6]. Adapun tujuan dari sistem kriptografi adalah sebagai berikut :

1. Confidentiality : Memberikan kerahasiaan pesan dan menyimpan data dengan menyembunyikan informasi lewat teknik-teknik enkripsi.
2. Message Integrity : Memberikan jaminan untuk tiap bagian bahwa pesan tidak akan mengalami perubahan dari saat pesan dibuat sampai saat pesan dibuka.
3. Non-repudiation : Memberikan cara untuk membuktikan bahwa suatu dokumen datang dari pengirim apabila pengirim tersebut mencoba menyangkal memiliki dokumen tersebut.

*Corresponding Authors
Email : nuwaboy@gmail.com

4. Autentication : Memberikan dua layanan yaitu mengidentifikasi keaslian suatu pesan dan memberikan jaminan keautentikannya dan menguji identitas seseorang apabila memasuki sebuah sistem.



Gambar 1. Proses Enkripsi / Dekripsi Sederhana
(Sumber : Arius : 2006)

Dari gambar 1 dapat dijelaskan suatu pesan yang tidak disandikan disebut sebagai plaintext ataupun dapat disebut juga sebagai clear text. Proses yang dilakukan untuk mengubah plaintext ke dalam ciphertext disebut encryption atau encipherment. Sedangkan proses untuk mengubah ciphertext kembali ke plaintext disebut decryption atau decipherment. Secara umum operasi enkripsi dan dekripsi dapat diterangkan secara matematis sebagai berikut dimana EK (M) adalah C (Proses Enkripsi) dan DK (C) adalah M (Proses Dekripsi).

Pada saat proses enkripsi kita menyandikan pesan M dengan suatu kunci K lalu dihasilkan pesan C. Sedangkan pada proses dekripsi, pesan C tersebut diuraikan dengan menggunakan kunci K sehingga dihasilkan pesan M yang sama seperti pesan sebelumnya.

Dengan demikian keamanan suatu pesan tergantung pada kunci ataupun kunci-kunci yang digunakan dan tergantung pada algoritma yang digunakan. Hal ini menjadikan algoritma - algoritma yang digunakan tersebut dapat dipublikasikan dan dianalisis, serta produk - produk yang menggunakan algoritma tersebut dapat diproduksi massal. Tidaklah menjadi masalah apabila seseorang mengetahui algoritma yang digunakan. Selama ia tidak mengetahui kunci yang dipakai, ia tetap tidak dapat membaca pesan. Terdapat dua jenis algoritma kriptografi yang berdasarkan jenis kuncinya yaitu :

1. Algoritma Simetri

Dalam symmetric cryptosystem ini, kunci yang digunakan untuk proses enkripsi dan dekripsi pada prinsipnya identik K1 = K2 = K, tetapi satu buah kunci dapat pula diturunkan dari kunci yang lainnya. Kunci-kunci ini harus dirahasiakan. Oleh karena itulah sistem ini sering disebut sebagai secret-key ciphersystem[6]

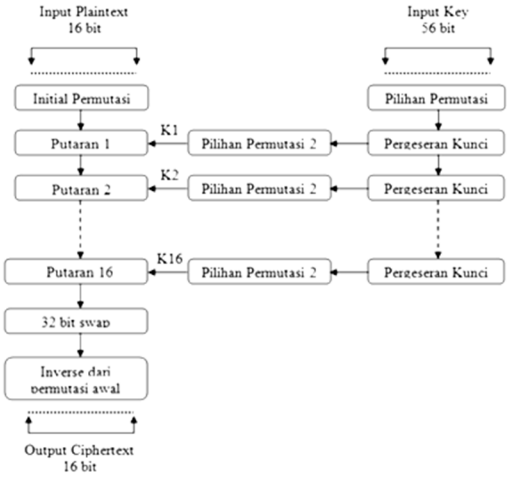
2. Algoritma Asimetri

Dalam Assymmetric Cryptosystem ini digunakan dua buah kunci. Satu kunci yang disebut kunci public (public key) dapat dipublikasikan, sedang kunci yang lain yang disebut kunci privat (private key) harus dirahasiakan. Kunci privat kadang-kadang disebut kunci rahasia. Jadi dalam membaca kunci privat harus berhati-hati.

2.2 DES (Data Enryption Standard)

Standar enkripsi data merupakan algoritma enkripsi yang paling banyak dipakai dunia, yang diadopsi oleh NIST (National Institute of Standards and Technology) sebagai standar pengolahan informasi federal AS. Secara umum standar enkripsi data terbagi menjadi tiga kelompok, yaitu pemrosesan kunci, enkripsi sandi blok kunci simetris dengan ukuran blok 64-bit, dekripsi sandi blok kunci simetris dengan ukuran blok 64-bit dan ukuran kunci internal 56-bit (interna key) atau upa-kunci (subkey), kunci internal dibangkitkan dari kunci eksternal (external key) yang panjangnya 64 bit.

DES merupakan keamanan dasar yang digunakan di seluruh dunia. Oleh karena itu ada kemungkinan DES akan tetap dilanjutkan penelitiannya hingga menjadi suatu sistem enkripsi yang kuat, baik segi kunci, penyimpanan data dan sistem kontrol akses[2].



Gambar 2. Gambaran Umum Algoritma DES
(Sumber : Munir, 2006)

Untuk mengenkripsi data dengan menggunakan algoritma DES, dimulai dengan membagi bit dari teks tersebut ke dalam blok-blok dengan ukuran blok sebesar 64-bit, yang kemudian disebut blok plaintext. Ukuran efektif dari kunci rahasia (secret key) K adalah k = 56-bit, masukan kunci (input key) K dispesifikasikan sebagai 64-bit kunci (key) dan 8-bit (bit 8, 16,…,64) digunakan sebagai parity bit. Parity bit tersebut akan mereduksi ukuran efektif key dari 64-bit menjadi 56-bit. Proses enkripsi dimulai dengan 16 pengulangan blok ciphertext (disebut juga round) dengan menggunakan initial permutation (IP) dan diakhiri dengan invers initial permutation (IP-1)

Dari masukan (input) kunci (key) K, sebanyak 16 subkey Ki yang dihasilkan dari 56-bit kunci dengan ukuran masing-masing sebesar 48-bit dan masing-masing subkey digunakan untuk setiap round. Dari 64-bit plaintext kemudian dipecah menjadi dua bagian yang masing-masing berukuran 32-bit, yang kemudian dinotasikan dengan R (kanan) dan L (kiri).

R adalah bagian yang pertama kali melalui fungsi ekspansi atau expansion function yang dinotasikan dengan E. Fungsi expansion mengambil 32-bit masukan dan menghasilkan 48-bit keluaran

dengan mereplikasi beberapa bit masukan. Keluaran E kemudian di XOR dengan 48-bit subkey.

masing-masing kotak S (S-box) mengambil 6-bit sebagai masukan untuk menghasilkan 4-bit sebagai keluaran. Pada S-box, jika satu bit berubah pada masukan maka seluruh keluaran akan berubah. Bit 1-6 melalui fungsi S1, bit 7-12 melalui S2 dan seterusnya. Ini menghasilkan 32-bit keluaran dari 48-bit masukan, yang kemudian di proses dengan fungsi permutasi P dan keluaran fungsi P juga 32-bit. Setelah di permutasi oleh fungsi P, kemudian di XOR dangan L. Bit pertama dan terakhir dari masukan untuk Si merupakan 2-bit bilangan biner untuk memilih baris pada tabel Si. Sisa 4-bit yang ditengahnya digunakan untuk memilih kolom pada tabel Si. Nilai desimal pada sel dipilih oleh baris dan kolom yang kemudian dirubah sebagai representasi 4-bit untuk menghasilkan keluaran. Sebagai contoh pada S1, untuk masukan 011011, baris adalah 01 (baris ke-1) dan kolomnya adalah 1101 (kolom ke-13). Nilai untuk baris ke-1 dan kolom-13 adalah 5, maka keluarannya adalah 0101.

Jika e notasi dari expansion E, S notasi dari fungsi S, P notasi dari permutasi P dan Ki adalah subkey ke-i, Ri nilai R ke-i, Li nilai L ke-i, r notasi proses round, dimana $r \geq 1$ dan $r \geq i \geq 1$, maka persamaannya adalah: Li = Ri-1 , Ri = Li-1 ⊕fi Ri-1. Dengan mengeliminasi Li terhadap Ri maka Ri = Ri-2 ⊕fi Ri-1. Berdasarkan persamaan, keluaran terakhir (final output) dari ciphertext adalah (Rr, Rr-1). Dengan masukan (Ri-1, R0). fi merupakan transformasi f dengan menggunakan subkey Ki. Sehingga untuk persamaan fi Ri-1 dapat juga ditulis menjadi f (Ri-1, Ki) dan persamaannya menjadi f (Ri-1, Ki) = P (S (e (Ri-1) ⊕Ki)).

2.3 Citra

Citra adalah gambar dua dimensi yang dihasilkan dari gambar analog dua dimensiyang kontinu menjadi gambar diskrit melalui proses sampling. Citra digital dapat didefinisikan sebagai fungsi dua variabel, f(x,y), dimana x dan y adalah koordinat spasial sedangkan nilai f(x,y) adalah Matrik 2D intensitas citra pada koordinat tersebut, hal tersebut diilustrasikan pada gambar di bawah.

Teknologi dasar untuk menciptakan dan menampilkan warna pada citra digital berdasarkan pada penelitian bahwa sebuah warna merupakan kombinasi dari tiga warna dasar, yaitumerah, hijau dan biru (Red, Green, Blue - RGB)[1].

Mode Warna

Menampilkan sebuah citra pada layar monitor diperlukan lebih dari sekedar informasi tentang letak dari pixel-pixel pembentuk citra. Untuk memperoleh gambar yang tepat dibutuhkan juga informasi tentang warna yang dipakai untuk menggambarkan sebuah citra digital. Beberapa mode warna yang sering digunakan adalah :

1. Bitmap mode memerlukan 1 bit data untuk menampilkan warna dan warnayang dapat ditampilkan hanya warna hitam dan putih (monokrom)
2. Indexed Color Mode, mengurutkan warna dalam jangkauan 0-255 (8 bit)
3. Grayscale Mode, menampilkan citra dalam 256 tingkat keabuan.
4. RGB Mode, menampilkan citra dalam kombinasi 3 warna dasar (Red,Green, Blue) tiap warna dasar memiliki intensitas warna 0-255 (8 bit)
5. CMYK Mode, menampilkan citra dalam kombinasi 4 warna dasar (cyan,magenta, yellow, black) tiap warna dasar memiliki intensitas warna 0-255(8 bit).

Mode warna RGB menghasilkan warna menggunakan kombinasi dari tiga warna primer merah, hijau, biru. RGB adalah model warna penambahan, yang berarti bahwa warna primer dikombinasikan pada jumlah tertentu untuk menghasilkan warna yang diinginkan. RGB dimulai dengan warna hitam (ketiadaan semua warna) dan menambahkan merah, hijau, biru terang untuk membuat putih. Kuning diproduksi dengan mencampurkan merah, hijau; warna cyan dengan mencampurkan hijau dan biru; warna magenta dari kombinasi merahdan biru. Monitor komputer dan televisi memakai RGB. Sorotan electron menghasilkan sinyal merah, hijau, biru yang dikombinasikan untuk menghasilkan berbagai warna yang dilihat pada layar[7].

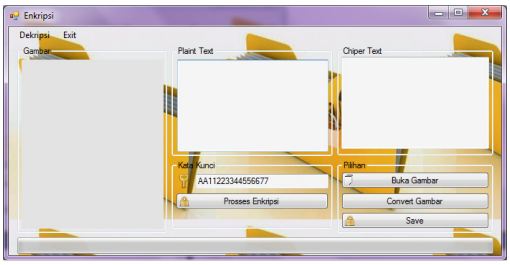
3. HASIL DAN PEMBAHASAN

3.1 IMPLENTASI SISTEM

Implementasi aplikasi berdasarkan desain yang telah dibuat menggunakan bahasa pemograman Visual Basic.net. Selanjutnya akan dijelaskan lebih lanjut mengenai implementasi sistem kriptografi pada text hasil konversi dari citra dengan menggunakan metode DES.

1. Menu Enkripsi

Panel menu enkripsi otomatis akan muncul seperti gambar 3.



Gambar **3. Panel Enkripsi**

Pada form menu enkripsi terdapat beberapa tombol untuk melakukan proses enkripsi. Pada menu enkripsi ini terdapat Picture Box yang digunakan untuk menampilkan gambar yang akan dilakukan proses konversi, serta ada 3 Text Box yang pertama untuk menampung text hasil konversi kemudian di anggap sebagai plaint text, lalu yang kedua berfungsi untuk menampung kata kunci sebanyak 16 digit, serta Text Box yang terakhir berfungsi untuk menampung chiper text hasil proses enkripsi.

2. Menu Dekripsi

Panel selanjutnya adalah panel dekripsi. Isi dari panel dekripsi hampir sama dengan panel enkripsi.

Hanya tombol proses dan tombol open file yang membedakan, jika pada panel enkripsi tombol proses enkripsi maka untuk panel dekripsi tentunya tombol dekripsi lalu jika pada panel enkripsi tombol open file untuk membuka format file citra gambar sedangkan pada panel dekripsi tombol open file berfungsi untuk membuka file dengan format text. Picture Boxdan 3 Text Box yang digunakan juga sama seperti Picture Boxdan 3 Text Box pada panel enkripsi. Panel dekripsi dapat dilihat pada gambar 4.

Gambar 4 Panel Dekripsi

3.2 PENGUJIAN SISTEM

Pengujian Berdasarkan Format Animasi dan Foto Real

Pengujian selanjutnya dilakukan berdasarkan format gambar animasi yang akan dilakukan proses kriptografi yang terdapat pada tabel 1. Format gambar yang dimaksud yaitu membandingkan antara format gambar animasi dengan format gambar foto real. Pengujian dilakukan dengan masing-masing gambar animasi dan foto real yang memiliki ukuran frame serta panjang kunci yang sama yaitu frame masing-masing dengan ukuran 50 x 50 piksel dan kunci untuk melakukan proses enkripsi dan dekripsi yang sama yaitu AA11223344556677.

Tabel 1. Perbandingan Berdasarkan Format Gambar

Foto Animasi		
1	Gambar 1	
	Key	AA11223344556677
	Text Hasil Konversi (100 Karekter Pertama)	236623662366236623662366623662366236623662366236623662366623662366236623662366623662366236623662366236623662366623662366
	Text Hasil Enkripsi (100 Karekter Pertama)	c9d354a422f11142f9653a79f499f0c8d3085fb79c469ec29053de6740b015617cdd4bd18d872d431746a9416acd451915de
	Text Hasil Deskripsi (100 Karekter Pertama)	236623662366236623662366623662366236623662366236623662366623662366236623662366623662366236623662366236623662366623662366
Foto Real		
2	Gambar 2	
	Key	AA11223344556677
	Text Hasil Konversi (100 Karekter	23472356235D233A23492350233B234D23512341235323572233A2349234C233C234B234E234223502
	Pertama)	351234823542354234F2359235A2
	Text Hasil Enkripsi (100 Karekter Pertama)	046d0ceb2b7b027f3c3669c4dccb0a5b2772af0a67ff282d74f074f3c4510ac8b27bcc7b2e99d54b0ffe4db4aabc72016a81f4699c6e0acc8e7d4f0
	Text Hasil Deskripsi (100 Karekter Pertama)	23472356235D233A23492350233B234D23512341235323572233A2349234C233C234B234E234223502351234823542354234F2359235A2

Dari tabel 1. mengenai perbandingan hasil konversi citra ke text dan proses kriptografi pada gambar animasi dan foto real dapat diketahui bahwa hasil enkripsi dan dekripsi berupa plain text yang dihasilkan terlihat bahwa gambar 2 pada kolom hasil konversi 1 baris pertama dengan format foto real memiliki plain text yang lebih bervariasi dibandingkan dengan plain text gambar 1 format animasi pada kolom hasil konversi 1 baris pertama. Pada hasil konversi citra ke text pada gambar animasi kurang menghasilkan kombinasi dan terlihat lebih monoton. Sehingga foto real jauh lebih baik dibanding kan gambar animasi ketika di konvert ke dalam text.

Tabel 4.8 Waktu Proses

No	Ukuran Gambar	Banyak Piksel	Kunci (Hexadecimal)	Waktu Proses (milidetik)	
				Enkripsi	Dekripsi
1	10 x 10	100	AA11223344556677	00:01.36	00:01.27
2	50 x 50	2500	AA11223344556677	00:02.39	00:02.30
3	100 x 50	5000	AA11223344556677	00:03.01	00:03.00
4	150 x 100	15000	AA11223344556677	00:06.11	00:06.02
5	200 x 150	30000	AA11223344556677	00:17.05	00:16.45

Berdasarkan pengujian waktu proses melakukan proses enkripsi dan dekripsi menggunakan metode DES, maka dapat dilihat hasil pada tabel 2 nomor urut 1 dan nomor urut 5 pada kolom enkripsi dan dekripsi, bahwa lama waktu yang dibutuhkan untuk melakukan proses enkripsi maupun dekripsi berbanding lurus dengan banyaknya piksel yang menyusun gambar, serta besarnya ukuran frame gambar. Jadi semakin banya piksel suatu gambar maka proses melakukan enkripsi dan dekripsi juga semakin lama karena jumlah piksel yang dilakukan proses enkripsi dan dekripsi yaitu dimensi lebar gambar di kali dimensi tinggi gambar.

Sehingga dapat disimpulkan bahwa lamanya waktu yang digunakan untuk melakukan proses enkripsi dan dekripsi antara lain besar ukuran frame. Semakin besar frame yang digunakan maka akan semakin banyak piksel yang harus diproses dan akan semakin lama waktu yang dibutuhkan.

4. KESIMPULAN DAN SARAN

4.1 Kesimpulan

Kesimpulan yang dapat diambil berdasarkan penelitian mengenai Kriptografi Pada Text Hasil Konversi Dari Citra menggunakan metode DES antara lain :

1. Gambar dapat dikonversi ke dalam format text berdasarkan kode warna RGB menggunakan tabel ASCII.

2. Gambar dengan nilai kode warna RGB yang bervariasi dapat menghasilkan format text yang bervariasi juga ketika dikonversi.
3. Gambar Animasi lebih monoton ketika dikonversi ke dalam text dari pada gambar foto real.
4. Berdasarkan penelitian diketahui bahwa lama proses untuk melakukan proses kriptografi text hasil konversi dari citra menggunakan metode DES ditentukan oleh besar frame atau banyak pixel.

4.2 Saran

Berdasarkan kesimpulan yang ada dari Kriptografi Text Hasil Konversi dari Citra menggunakan metode DES memiliki beberapa keunggulan serta kelemahan. Oleh karena itu penulis memiliki beberapa saran untuk pengembangan program selanjutnya antara lain:

1. Dibutuhkan suatu metode yang dapat lebih cepat melakukankonversi dari citra ke text.
2. Dibutuhkan suatu percobaan penerapan metode konversi citra ke text pada gambar video

5. DAFTAR PUSTAKA

[1] Ahman, U. 2005. Pengolahan Citra Digital dan Teknik Pemrogramannya. Yogyakarta : Graha Ilmu.
[2] Ariyus, D. 2006. Computer Security. Yogyakarta : Penerbit Andi.
[3] Edma saputra, B. 2012. Sistem Kriptografi pada Citra Digital Menggunakan Metode Subtitusi dan Permutasi. Skripsi Ilmu Komputer Universitas Mulawarman. Samarinda
[4] Hirin, M. 2011. Belajar Tuntas VB.Net 2010. Jakarta : Penerbit Prestasi Pustaka.
[5] Kurniawan, Y. 2004. Kriptografi Keamanan Internet dan Jaringan Komunikasi. Bandung : Penerbit Informatika
[6] Munir, R. 2006. Kriptografi. Bandung : Penerbit Informatika.
[7] Munir, R. 2004. Pengolahan Citra Dengan Pendekatan Algoritmik. Bandung : Informatika.
[8] Prabowo Wiranto, Y. 2014. Perancangan Kriptografi DES dan RSA Sebagai Media Belajar Kriptografi Berasis Mobile. Naskah Publikasi Jurusan Teknik Informatika AMIKOM. Yogyakarta
[9] Putu Herryawan, I. 2011. Analisa dan Penerapan Algoritma DES Untuk Pengamanan Data Gambar Dan Video. Jurnal Skripsi Ilmu Komputer Universitas Udayana. Denpasar Bali.
[10] Primarha, R. 2011. Penerapan Enkripsi dan Dekripsi File Menggunakan Algoritma Data Encryption Standard (DES). Jurnal Skripsi Teknik Informatika Universitas Sriwijaya. Palembang.
[11] Rosa, A. 2011. Rekayasa Perangkat Lunak. Bandung : Modula.
[12] Supriyanto, A. 2008. Penyandian File Gambar dengan Metode Substitusi dan Transposisi. Jurnal Teknologi Informasi Dinamik. Volume XIII, No.2, P : 88-97