Jurnal ELTIKOM, Vol. 1 No.1, Juni 2017, Hal 34-41
ISSN 2598-3245 (Print), ISSN 2598-3288 (Online)
Tersedia Online di http://eltikom.poliban.ac.id

PENERAPAN ALGORITMA KRIPTOGRAFI TEA DAN BASE64 UNTUK MENGAMANKAN EMAIL

Siswanto[1)], M. Anif[2)], dan Windu Gata[3)]
[1, 2)]Universitas Budi Luhur
[3)] STMIK Nusa Mandiri
e-mail: siswantobl@gmail.com[1)], m.anif91@gmail.com[2)], windu.gata@gmail.com[3)]

ABSTRACT

This data security application is designed to secure important email data at PT. Dekai Indonesia especially data policy that contains personal data of the customers. Due to the many important data of the customers then the data security be-comes very vulnerable to the theft and manipulation of data from various parties who are not responsible given the data is also often sent using email facilities. With so many important data that is often also confidential, then the data becomes vulnerable to data theft, data manipulation or email eavesdropping. Such problems may be faced by making the applica-tion to prevent irresponsible parties from reading the file contents of the transaction data. Also guarantees the authentici-ty of sensitive and important data is only acceptable and readable by those who are entitled to data. In this paper the al-gorithm used in cryptography, ie TEA cryptography algorithm (Tiny Encryption Algorithm). The use of cryptographic sys-tem is intended to make the data is not easily broken. The programming language used in building data security applica-tions is a web-based PHP programming language. As a result of this cryptographic testing, data can be secured to avoid cryptanalysis attacks. The average encrypt file size has increased by 33.29512 percent of the original file size before going through the encrypt process. The average change in file size that has gone through the decrypt process will be reduced by 25.0231 percent.

***Keywords**: Cryptography Algorithm TEA, Decript, Encrypt, Email Insurance Data Policy, PHP.*

ABSTRAK

Aplikasi pengamanan data ini dirancang untuk mengamankan email data penting pada PT. Dekai Indonesia terutama data policy yang berisi data pribadi para nasabah. Karena banyaknya data penting para nasabah maka keamanan data tersebut menjadi sangat rentan terhadap pencurian dan manipulasi data dari berbagai pihak yang tidak bertanggung jawab mengingat sering juga data tersebut dikirimkan menggunakan fasilitas email. Dengan banyaknya data penting yang sering juga bersifat rahasia tersebut, maka data tersebut menjadi rentan dengan pencurian data, manipulasi data atau penyadapan email. Permasalahan tersebut dapat dihadapi demgan membuat aplikasi untuk mencegah pihak yang tidak bertanggung jawab dapat membaca isi file dari data transaksi. Juga menjamin keaslian data sensitif dan penting hanya dapat diterima dan dibaca oleh orang-orang yang berhak mendapatkan data. Dalam penulisan ini algoritma yang digunakan dalam kriptografi, yaitu algoritma kriptografi TEA (Tiny Encryption Algorithm). Penggunaan sistem kripto-grafi ini dimaksudkan agar data tersebut tidak mudah dibobol. Bahasa pemrograman yang digunakan dalam mem-bangun aplikasi pengamanan data ini adalah bahasa pemrograman PHP yang berbasis web. Hasil dari pengujian kriptografi ini, data dapat diamankan untuk menghindari serangan cryptanalysis. Rata-rata ukuran file yang telah me-lalui proses encrypt bertambah sekitar 33,29512 persen dari ukuran asli file sebelum melalui proses encrypt. Rata-rata perubahan ukuran file yang telah melalui proses decrypt akan berkurang sebesar 25.0231 persen.

***Kata Kunci**: Algoritma kriptografi TEA, Decript, Encrypt, Email Data Policy Asuransi, PHP.*

ISSN 2598-3245 (Print)
ISSN 2598-3288 (Online)

I. PENDAHULUAN

PT. Dekai Indonesia adalah perusahaan yang bergerak di bidang *consultant* asuransi. Dengan demikian, sebagai *consultant* banyak data yang bersifat rahasia seperti data *policy* asuransi, data diri, data keluarga, data riwayat kesehatan, data penghasilan dan juga banyak dokumen lain yang bersifat rahasia, sering juga data tersebut dikirimkan menggunakan fasilitas email. Secara sederhana pengertian *email* adalah format surat dengan cara digital atau dituliskan melalui media komputer atau bisa juga gadget lainnya yang bisa diproses dengan menggunakan media internet [1].

Dengan banyaknya data penting yang sering juga bersifat rahasia tersebut, maka data tersebut menjadi rentan dengan pencurian data, manipulasi data atau penyadapan email. Saat ini penggunaan keamanan data di PT. Dekai Indonesia masih menggunakan sistem manual yaitu berupa penyimpanan *hard copy* data dalam berkas, dan juga *soft copy* tanpa ada pengamanan data pada datanya langsung. PT. Dekai Indonesia belum memiliki fasisitas keamanan berbasis kriptografi dan juga fasilitas pengamanan konten email, sehingga masih rentan terhadap dengan pencurian data, manipulasi data atau penyadapan email.

Demi keamanan data PT. Dekai Indonesia, maka salah satu cara yang harus dilakukan adalah dengan melakukan *encrypt* pada data yang akan dikirim sehingga hanya pihak yang berhak atas data tersebut yang memiliki kunci untuk membuka data. Salah satu alternatif yang dapat digunakan untuk menjaga kerahasiaan informasi tersebut adalah dengan menyamarkannya menjadi bentuk tersandi yang tidak bermakna. Hal tersebut dapat dilakukan dalam kriptografi [2].

Tiny Encryption Algorithm (TEA) merupakan suatu algoritma sandi yang diciptakan oleh David Wheeler dan Roger Needham dari Computer Laboratory, Cambridge University, England pada bulan November 1994. Algoritma ini merupakan algoritma penyandian block cipher yang dirancang untuk penggunaan memori yang seminimal mungkin dengan kecepatan proses yang maksimal [3].

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 suatu metode yang digunakan untuk melakukan encoding (penyandian) terhadap data binary [4]. Umumnya digunakan pada berbagai aplikasi seperti e-mail via MME, data XML, atau untuk keperluan encoding URL

Terdapat penelitian dimana algoritma yang digunakan adalah algoritma Tiny Encryption Algorithm. TEA merupakan algoritma jenis stream cipher yang memproses unit input data. algoritma Tiny Encryption Algorithm (TEA) juga merupakan bagian dari algoritma simetris, dimana proses enkripsi dan dekripsinya memiliki kunci yang sama. Pembuatan aplikasi ini menggunakan bahasa pemograman C#. Hasil yang akan dicapai dari penilitian ini adalah aplikasi kriptografi dokumen yang bias melakukan enkripsi dan dekripsi dengan algoritma Tiny Encryption Algorithm (TEA) [5].

Pada peneitian lain, algoritma Cryptographic yang akan digunakan adalah Algoritma Enkripsi Tiny (TEA), sedangkan algoritma steganografi yang akan digunakan adalah Least Significant Bit (LSB), data atau informasi yang pertama dienkripsi menjadi TEH, kemudian dimasukkan ke dalam gambar oleh algoritma LSB. Jadi hasil enkripsi dan steganografi tidak akan mencurigakan bagi yang lain, berdasarkan texting, perubahan gambar tidak terlihat. Oleh karena itu dapat disimpulkan dengan menggabungkan Cryptography TEA dan steganografi LSB, sehingga pendalaman data akan lebih akurat dan kinerja program yang baik [6].

Penelitian lainnya membuat sistem yang berfokus pada implementasi FPGA ringan algoritma kriptografi Enkripsi Algoritma TEA untuk beradaptasi dengan banyak kendala real time seperti memori, kehilangan data dan biaya rendah. Skema yang diusulkan menggunakan Linear Feedback Shift Register untuk menghasilkan kunci acak sehingga lebih aman untuk transfer informasi sensitif di banyak aplikasi real time [7].

Peneliti lain mengimplementasikan algoritma enkripsi yang digunakan untuk keamanan lebih komunikasi nirkabel, tetapi mengamankan data juga mengkonsumsi sumber daya. Faktor penting utama yang perlu dipertimbangkan ketika merancang sistem kriptografi adalah kinerja, kecepatan, ukuran, dan keamanan. Tiny Encryption Algorithm (TEA), dan eXtended TEA (XTEA) adalah contoh dari algoritma kriptografi. Tiny Encryption Algorithm (TEA) adalah algoritma kriptografi yang dirancang untuk meminimalkan pemakaian memori dan memaksimalkan kecepatan. Ini adalah jenis cipher feistel yang menggunakan operasi dari campuran (orthogonal) kelompok aljabar [8].

Penelitian selanjutnya menggunakan algoritma Base64 dengan mengubah struktur index-nya yang bertujuan untuk menghamburkan makna dari plaintext ketika ciphertext dicoba untuk dipecahkan oleh

pemecah kode. Pemodelan data rrpemograman C#. Dengan adanya cara pengamanan ini, pengembang aplikasi yang menggunakan bahasa pemrograman PHP dapat menyembunyikan skrip PHP supaya tidak mudah disalin, diubah sebagian/seluruhnya oleh orang yang tidak berhak dan dapat mengamankan kelemahan dari alur program aplikasi PHP [9], [10].

Oleh sebab itu penulis melakukan penerapan algoritma kriptografi tea dan base64 untuk mengamankan email data policy asuransi pada PT. Dekai Indonesia.

II. METODE PENELITIAN

A. Analisa Kebutuhan

Menganalisis masalah, kebutuhan, keperluan, dan penggunaan apa saja yang akan diperlukan untuk pengamanan dokumen di PT. Dekai Indonesia. Adapun teknik pengumpulan data yang digunakan yaitu sebagai berikut.

1) Perencanaan, mengidentifikasi masalah-masalah keamanan dokumen di PT. Dekai Indonesia.
2) Penelitian lapangan, yaitu melakukan observasi atau praktek lapangan secara langsung di perusahaan terkait guna mendapatkan data yang akurat dan dapat dipertanggung jawabkan keabsahannya. Adapun teknik pengumpulan data yang digunakan yaitu:
   a) Studi lapangan, yaitu penelitian langsung di PT. Dekai Indonesia yang diteliti untuk mendapatkan data serta informasi yang diperlukan, seperti data penting perusahaan yang memiliki format *file .pdf, .ppt, .doc, .xls, .xlsx* dan *.jpg*.
   b) Pengamatan, yaitu teknik pengumpulan data dengan mengamati langsung proses pembuatan *file* dan pengiriman *file* yang berisikan data-data penting perusahaan.
   c) Studi dokumentasi, yaitu mempelajari dokumen – dokumen yang berkaitan dengan permasalahan yang dibahas.
   d) Metode wawancara, merupakan proses tanya jawab langsung dan sistematis kepada orang yang mengetahui tentang permasalahan yang sedang diamati untuk menyakinkan hal - hal kegiatan observasi yang telah dilakukan.
   e) Penelitian kepustakaan, yaitu penelitian yang dilakukan dengan cara mempelajari literature - literatur, buku - buku, jurnal dan artikel ilmiah yang berhubungan dengan serta cara kerja algoritma TEA .

B. Desain Sistem

Persiapan rancang bangun implementasi pada PT. Dekai Indonesia yang menggambarkan bagaimana suatu sistem dibentuk yang berupa penggambaran, Desain *web* adalah tahap yang harus dilakukan sebelum mulai membuat situs web. Konsep rancangan dalam mendesain halaman web adalah tampilan pada halaman *browser* yang akan diakses oleh pengguna.

C. Ujicoba program

Ujicoba mempresentasikan ketidak normalan yang terjadi pada pengembangan program dengan bahasa pemrograman *PHP* kepada semua jenis file yang digunakan PT. Dekai Indonesia, jenis *file* yang digunakan diantaranya *.pdf, .ppt, .doc, .xls, .xlsx* dan *.jpg*. Selama definisi awal dan fase pembangunan, pengembangan berusaha untuk membangun program dari konsep yang abstrak sampai dengan implementasi yang memungkinkan.

D. Implementasi

Tahap dimana semua elemen dan aktivitas sistem disatukan dengan langkah – langkah, sebagai berikut.

1) Menyiapkan Fasilitas Fisik, fasilitas - fasilitas fisik yang disiapkan antara lain komputer dan peripheralnya, termasuk keamanan fisik untuk menjaga berlangsungnya peralatan dalam jangka waktu yang lama.
2) Menyiapkan pengguna, pemakai disiapkan dengan terlebih dahulu yaitu dengan memberikan pelatihan secara prosedural maupun tutorial mengenai program. Tujuannya adalah agar para pengguna mengerti dan mengusai cara kerja program.

ISSN 2598-3245 (Print)
ISSN 2598-3288 (Online)

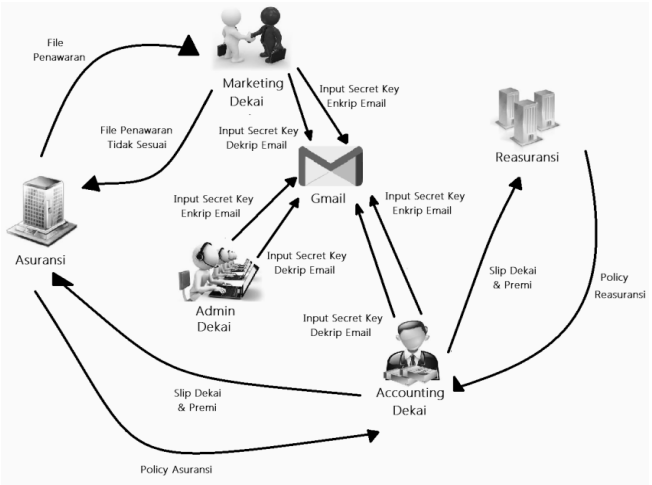
3) Melakukan Simulasi, kegiatan simulasi berupa pengujian program secara nyata yang melibatkan personil yang sesungguhnya.

III. PEMBANGUNAN PERANGKAT LUNAK

Perancangan sistem yang dibuat secara umum adalah pengiriman *mail encrypt* dan penerima *mail decrypt* menggunakan metode *TEA* berbasis *web*, adapun beberapa tahap dalam perancangan aplikasi adalah sebagai berikut.

A. Proses

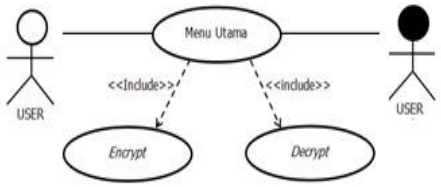
Perancangan proses yang dimaksudkan adalah bagaimana sistem akan bekerja, proses-proses yang digunakan mulai dari *user* mengakses halaman *web*, lalu menulis pesan dan *attach file* untuk dienkripsi, kemudian diproses oleh aplikasi sehingga dapat mengeluarkan *output* berupa hasil *encrypt* pesan tersebut. Perancangan proses aplikasi untuk mengamankan data *policy* asuransi dapat dilihat pada Gambar 1.



Gambar 1. *Rich Picture Diagram* aplikasi kemanan data

B. Use Case Diagram dan Activity Diagram

Tahap pertama dalam perancangan sistem adalah membuat *Use Case Diagram*. *Use Case Diagram* adalah rancangan yang digunakan untuk menggambarkan kebutuhan dan fungsionalitas dan sudut pandang user berdasarkan hasil analisa yang telah dilakukanm dapat dilihat pada Gambar 2.



Gambar 2. *Use Case Diagram* aplikasi keamanan data

C. Antar Muka Pemakai

Perancangan antar muka mengandung penjelasan tentang desain dan implementasi sistem yang digunakan dalam sistem yang dibuat. Proses perancangan aplikasi *mail encrypt* dan *decrypt* menggunakan metode enkripsi *Tea* berbasis *web* secara umum dapat diuraikan sebagai berikut :

a) Masukan pesan, *file* dan *key* yang akan dikirim lalu disandikan ke dalam aplikasi yang sedang berjalan.
b) Proses pesan dan *file* asli dengan menggunakan *encrypt* metode *Tea.*
c) Dari proses *encrypt* tersebut maka akan menghasilkan kode-kode yang acak yang di dalamnya telah disisipi pesan rahasia.
d) Proses *mail decrypt* Proses atau tahap yang dilakukan untuk membaca pesan yang telah disandikan dengan melakukan *decrypt* pesan tersebut untuk membacanya kembali.

ISSN 2598-3245 (Print)
ISSN 2598-3288 (Online)

Pada menu *encryption mail* akan langsung ditampilkan menu untuk melakukan *input* pesan dan *upload file* seperti yang terlihat pada Gambar 3.

Gambar 3. Tampilan layar *form* desain *menu encryption mail*

Pada tampilan halaman *encrypt* ini ada beberapa *menu* yang berfungsi sebagai berikut.

1) *Home*, untuk kembali ke menu utama (*home)*.
2) *Gmail ID*, kolom yang berfungsi untuk memasukan *user id Gmail.*
3) *Password*, kolom yang berfungsi untuk memasukan *password Gmail* yang telah dimasukan sebelumnya.
4) *To*, kolom berfungsi untuk memasukkan alamat *gmail* yang dituju.
5) *Subject*, kolom yang berfungsi untuk memasukan *subject email* yang akan dikirim.
6) *Choose file*, tombol yang berfungsi untuk memiih *file* yang akan diunggah.
7) *Secret Key*, kolom yang berungsi untuk memasukan *secret key.*
8) *Send*, tombol *send* berfungsi untuk mengirimkan pesan sekaligus untuk proses enkripsi.

Pada saat *user* hendak mengirimkan pesan dengan enkripsi maka diperlukan untuk memasukan *secret key* yang terdiri dari 16 character dan *case sensitif*, diwajibkan bagi *user* untuk mengingat *secret key* yang dimasukan, karena nantinya *secret key* ini akan digunakan kembali saat penerima *email* hendak membuka *email* ini kembali.

D. Algoritma encrypt TEA

```
1   INSERT plaintext
2   INSERT secret key (16 chr)
3   DO key schedule    //split key menjadi 4 subkey [K0 –K3]
4   i = 1, str = plaintext length
5   SPLIT plaintext/8 chr ← block    //text dikelompokan per 8 chr
6   IF ( i ≤ str ) then
7       SPLIT block / 4 chr ← P
8       P = y,z
9       delta = 9E3779B9, n = 1, sum = delta
10      IF ( n ≤ 32 ) then
11          y+(((ROL4 z)+K0) XOR (z+sum) XOR ((ROR5 z) + K1)) ← y
12          z+(((ROL4 y)+K2) XOR (y+sum) XOR ((ROR5 y) + K3)) ← z
13          n = n + 1, sum = sum + delta
14      ELSE
15          i = i + 8
16          JOIN all cipher ← ciphertext
17      ENDIF
18  ELSE
19      PRINT ciphertext
    ENDIF
Return
```

E. Algoritma decrypt TEA

```
1   INSERT ciphertext
2   INSERT secret key (16 chr)
3   DO key schedule   //split key menjadi 4 subkey [K0 –K3]
4   i = 1, str = ciphertext length
5   SPLIT ciphertext/8 chr ← block   //text dikelompokan per 8 chr
6   IF ( i ≤ str ) then
7       SPLIT block / 4 chr ← C
8       C = y,z
9       delta = 9E3779B9, n = 1, sum = C6EF3720
10      IF ( n ≤ 32 ) then
11          z-(((ROL4 y)+K2) XOR (y+sum) XOR ((ROR5 y) + K3)) ← z
12          y-(((ROL4 z)+K0) XOR (z+sum) XOR ((ROR5 z) + K1)) ← y
13          n = n + 1, sum = sum - delta
14      ELSE
15          i = i + 8
16          JOIN all plain ← plaintext
17      ENDIF
18  ELSE
19      PRINT plaintext
    ENDIF
Return
```

F. Algoritma proses encrypt base64

Algoritma proses *encrypt* base64 dari mulai input karakter ASCII, lalu penghitungan *padding*, lalu pemecahan menjadi per 6 bit sampai tahap konversi. Berikut adalah *pseudo code* proses *encoding* base64.

```
1   Input karakter ASCII(plaintext)
2   Hitung panjang byte(plaintext)
3   If panjang byte(plaintext) dapat dibagi 3 then
4     Hitung panjang binary(plaintext)
5     Else If penambahan padding 1 byte dapat dibagi 3 then
6           Hitung panjang binary(plaintext)
7         Else Tambakan 1 byte pada plaintext
8             Hitung panjang binary(plaintext)
9         Endif
10  Endif
11  Buat pengelompokan masing-masing 6 bit
12  Tampilkan encrypt
```

G. Algoritma proses decrypt base64

```
1   input string ciphertext
2   input key
3   hitung panjang byte(ciphertext)
4   hitung panjang binary(ciphertext)
5   hasil konversi ← kelompokkan per 8 bit
6   Hilangkan hasil konversi
7   Tampilkan decrypt
```

IV. PENGUJIAN SISTEM

Proses pengujian pada aplikasi pada sepuluh *file* dengan ukuran < 5MB, maka didapatkan hasil seperti pada Tabel 2.

TABEL I
TABEL PENGUJIAN ENCRYPT FILE < 5 MB

ISSN 2598-3245 (Print)
ISSN 2598-3288 (Online)

No	Nama File	Sebelum *Encrypt*		Ukuran file encrypt (bytes)	Lama Proses *Encrypt* (ms)	Tambahan Ukuran File (%)
		Format File	Ukuran File (bytes)			
1	Attachment of PT. DAN LIRIS - 2017 - 2018 - insurer	pdf	312066	416158	0.858	32.4207
2	PT. Sumatera Tobbaco 17.11.2014	bmp	239125	318898	0.669	33.3603
3	Dekai	jpg	21617	28894	0.064	33.6633
4	PT. LAJU PERDANA PATI	tif	239331	319174	0.666	33.3609
5	Dekai Insurance	ppt	289295	385778	0.810	33.3511
6	Final Slip - PAR - PT. DAN LIRIS and or PT. AMBASSADOR GARMINDO and or PT. EFRATA RETAILINDO and or PT. MULTIYASA ABADI SENTOSA - 2017 - 2018 - insurer	doc	45583	60830	0.13	33.4489
7	Naruto chapter 3	mp4	1561427	2081970	4,633	33.3376
8	PT. UNITED CAN COMPANY LIMITED	pdf	1607778	2143774	4.505	33.3377
9	REVISI_HARGA PERTANGGUNGAN PT KK_INDONESIA	pdf	2142906	2857266	5.985	33.336
10	SUNGAI BUDI GROUP	pdf	4322552	5763462	12.351	33.3347
Rata-rata penambahan ukuran file setelah dilakukan *encrypt* dan rata-rata kecepatan proses *encrypt* per *byte* =						33.29512

Berdasarkan hasil percobaan proses *encrypt* pada sepuluh macam *file* tersebut, didapatkan kesimpulan di bawah ini.

1) Ukuran *file* setelah melalui proses *encrypt* akan berubah menjadi lebih besar dengan rata-rata ukuran file yang telah melalui proses *encrypt* bertambah sekitar 33,29512 persen dari ukuran asli *file* sebelum melalui proses *encrypt.*
2) Waktu yang dibutuhkan untuk melakukan proses *encrypt* dengan ukuran *file* kurang dari 5 MB relatif cepat (< 15 second).

Setelah percobaan proses *encrypt*, dilakukan percobaan proses *decrypt* pada sepuluh *file* yang telah ter*encrypt* pada percobaan sebelumnya, dan didapat hasil seperti pada tabel 3,

TABEL 3
TABEL PENGUJIAN DECRYPT FILE < 5 MB

No	Nama File	Ukuran File (bytes)	Setelah *Decrypt*		Lama Proses *Decrypt* (ms)	Tambahan Ukuran File (%)
			Format File	Ukuran File (bytes)		
1	Attachment of PT. DAN LIRIS - 2017 - 2018 - insurer	416162	pdf	312066	2.9162	-25.0133
2	PT. Sumatera Tobbaco 17.11.2014	318902	bmp	239125	2.9322	-25.0161
3	Dekai	28898	jpg	21617	1.4771	-25.1955
4	PT. LAJU PERDANA PATI	319178	tif	239331	2.7752	-25.0164
5	Dekai Insurance	385782	ppt	289295	2.9282	-25.0107
6	Final Slip - PAR - PT. DAN LIRIS and or PT. AMBASSADOR GARMINDO and or PT. EFRATA RETAILINDO and or PT. MULTIYASA ABADI SENTOSA - 2017 - 2018 - insurer	60834	doc	45583	1.7501	-25.0698
7	Naruto chapter 3	2081974	mp4	1561427	7.9945	-25.0026
8	PT. UNITED CAN COMPANY LIMITED	2143778	pdf	1607778	8.0405	-25.0026
9	REVISI_HARGA PERTANGGUNGAN PT KK_INDONESIA	2857270	pdf	2142906	10.3786	-25.0016
10	SUNGAI BUDI GROUP	5763466	pdf	4322552	19.2981	-25.0008
Rata-rata penambahan ukuran file setelah dilakukan *decrypt* dan rata-rata kecepatan proses *decrypt* per *byte* =						-25.0329

Berdasarkan hasil percobaan proses decrypt pada sepuluh file didapatkan kesimpulan yaitu sebagai berikut.

1) Ukuran *file* setelah melalui proses *decrypt* akan berubah menjadi ukuran awal *file* sebelum *encrypt.* Rata-rata perubahan ukuran *file* akan berkurang sebesar 25.0329 persen, sama dengan rata-rata pada proses *encrypt*.

2) Waktu yang dibutuhkan untuk melakukan proses *decrypt* dengan ukuran *file* kurang dari 5 MB relatif cepat (< 20 second).

V. KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan serta uji coba sistem dapat disimpulkan, sebagai berikut :

a. Pegamanan email dapat diamankan dengan algortima kriptografi *TEA.*
b. Data tidak dapat dibuka oleh pihak yang tidak berhak yang tidak memiliki kunci.
c. Program sistem keamanan dengan sistem kriptografi algoritma *TEA* telah diuji coba, sehingga program dinyatakan sudah sesuai.
d. Ukuran *file* setelah melalui proses *encrypt* akan bertambah besar dibandingkan dengan ukuran *file* awal sebelum dilakukan proses *encrypt.*
e. Ukuran *file* untuk dilampirkan yang paling optimal untuk aplikasi ini adalah 5242880 bytes (5 MB) . Jika ukuran diatas 5242880 bytes (5 MB) proses akan sedikit lebih lama dan untuk ukuran file di atas10485760 bytes (10 MB) tidak bisa diproses.
f. Rata-rata ukuran *file* yang telah melalui proses *encrypt* bertambah sekitar 33,29512 persen dari ukuran asli *file* sebelum melalui proses *encrypt.*
g. Rata-rata perubahan ukuran *file* yang telah melalui proses *decrypt* akan berkurang sebesar 25.0231 persen.
h. Proses pengiriman *email encrypt* tergantung dengan koneksi *internet* yang digunakan, sehingga proses pengiriman *email encrypt* bisa cepat atau lama

DAFTAR PUSTAKA

[1] N. W. Group, “RFC 5321 – Simple Mail Transfer Protocol.” .
[2] J. Leyden, “US court test for rights not to hand over crypto keys,” Regist., 2011.
[3] W. Stallings, Network and Internetwork Security. Prentice Hall Inc, 1995.
[4] A. Kurniawan, Konsep dan Implementasi Cryptography dengan .NET. Dian Rakyat.
[5] I. Setiawan, “Aplikasi Kriptografi Dengan Algoritma Tiny Encryption Algorithm Menggunakan Microsoft Visual Basic,” Universitas Mercu Buana, 2017.
[6] D. U. Daihani, Sistem Pendukung Keputusan. Jakarta: Elex Media Komputindo, 2001.
[7] G. Qian, S. Sural, Y. Gu, and S. Pramanik, “Similarity between Euclidean and cosine angle distance for nearest neighbor queries,” in Proceedings of the 2004 ACM symposium on Applied computing - SAC ’04, 2004, p. 1232.
[8] M. Shoeb and V. K. Gupta, “A Crypt Analysis Of The Tiny Encryption Algorithm In Key Generation,” Int. J. Comput. Technol., vol. 1, no. 38, 2013.
[9] A. T. Sholeh, E. Gunadhi, and A. Supriatna, “Mengamankan Skrip Pada Bahasa Pemograman PHP Dengan Menggunakan Kriptografi Base64,” J. Algoritm. Sekol. Tinggi Teknol. Garut, vol. 10, no. 1, 2013.
[10] R. Khoirianti, N. Hidayah, and V. Widyaningsih, “Implementasi Algoritma Tea Untuk Enkripsi Dan Dekripsi Menggunakan Bahasa Pemrograman Visual Basic,” Academia, 2014.