ISBN 978-623-93343-2-1
Seminar Nasional Informatika, Sistem Informasi dan Keamanan Siber
(SEINASI-KESI)
Jakarta-Indonesia, 19-20 November 2020

PENGAMANAN SOAL UJIAN SEKOLAH *COMPUTER BASE TEST (CBT)* DENGAN ALGORITMA *ADVANCE ENCRYPTION STANDARD (AES)* DAN METODE STEGANOGRAFI *END OF FILE* (*EOF*)

Muhammad Bagus Hernowo[1], Henki Bayu Seta[2], I Wayan Widi P[3]

Fakultas Ilmu Komputer[123]
Universitas Pembangunan Nasional Veteran Jakarta
email: muh.bagus18@gmail.com, henkiseta@upnvj.ac.id, wayan.widi@unpvj.ac.id
Jl. Rs. Fatmawati, Pondok Labu, Jakarta Selatan, DKI Jakarta, 12450, Indonesia

Abstrak

Pada perkembangan teknologi yang sangat pesat, khususnya pada aliran informasi dan keamanan informasi. Data informasi yang diakses akan cepat dan efektif. Hal ini juga mempengaruhi dunia kriminalitas pada dunia maya atau lebih dikenal dengan *cyber crime*. Informasi yang penting bisa secara sengaja diambil dan sebarluaskan tanpa tanggung jawab oleh seseorang atau kelompok. Maka diperlukannya pengamanan data untuk tetap menjaga kerahasiaanya. Pengamanan data pada soal-soal ujian yang merupakan rentannya dari suatu data yang berada di komputer tanpa pengamanan khusus. Pada kalangan siswa marak beredar luasnya bocoran soal-soal ujian. Sehingga pengamanan data diperlukan untuk mengamankan soal ujian yang merupakan data penting dalam bagian hal ini. Peneliti akan menggunakan algoritma *AES (Advance Encryption Standard)* sebagai kriptografinya dan *EoF (End of File)* sebagai Metode steganografinya. Dengan demikian kerahasian data akan lebih efisien.

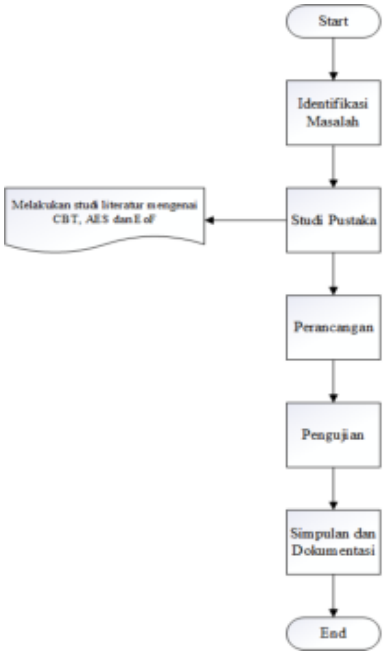
Kata Kunci : Keamanan Siber, Kriptografi, Steganografi, AES, *End of File*

1. PENDAHULUAN

Perkembangan teknologi dalam bidang informasi sangatlah cepat pada era globalisasi. Pada lembaga pemerintahan atau individual untuk mengakses informasi merupakan hal penting yang diharuskan dengan akurat dan cepat (Adetya.K. P, 2014). Dikarenakannya perkembangan teknologi yang cepat banyak kejahatan dan salah satunya adalah *cyber crime*. Pada *cyber crime* banyak macam ragamnya yaitu *cracker, hacker, phreaker* (Ariyus.D, 2008). Di internet banyak data yang disebarluaskan tetapi ada beberapa data yang hanya orang tertentu yang boleh mengaksesnya, maka dari itu pertukaran dan pengambilan data informasi membutuhkan keamanan dan kerahasiaan (Yayuk A. dan V. Dolly, 2014). Sekarang bukan hanya Ujian Nasional saja yang berbasis komputer, UTS dan UAS juga menggunakan komputerisasi (Adetya.K. P, 2014). Data dan file yang tidak teratur di dalam komputer dapat dengan mudah dibongkar jika hanya mengandalkan keamanan dasar dari komputer itu sendiri (Munir. R, 2005). Dikarenkan itu untuk meningkatkan kerahasian informasi diperlukan sebuah metode khusus (Christy A.S dan H. R. Eko, 2014). Metode yang akan digunakan untuk mengamankan data oleh penulis adalah dengan kriptografi AES *(Advance Encryption Standard)* serta teknik dari steganografi *EoF (End of File).* Maka penulis akan mengajukan judul untuk penelitian adalah "Pengamanan Soal Ujian Sekolah *Computer Base Test (CBT)* dengan algoritma *Advance Encryption Standard (AES)* dan metode steganografi *End of File (EoF)*".

2. METODE PENELITIAN

2.2 Kerangka Pemikiran



Gambar 1: Kerangka Pemikiran

2.2.1 Identifikasi Masalah

Pada tahap ini dilakukan suatu proses identifikasi masalah. Pada penelitian ini permasalahan yang terjadi adalah kurangnya pengamanan pada data ujian sekolah yang menggunakan komputer dimana data tersebut bisa di modifikasi dan hilang serta bocornya soal (Adetya.K. P, 2014).

2.2.2 Studi Pustaka

Pada tahap ini peneliti akan melakukan studi pustaka untuk mendapatkan teori-teori dasar dari setiap penelitian yang bersangkutan yaitu : AES *(Advance Encyrption Standard)*, EOF *(End of File*), CBT *(Computer Base Test*) dan PHP.

2.2.3 Perancangan

Gambar 2: Perancangan

1. Mengumpulkan data berupa database berformat .sql yang didalamnya merupakan daftar- daftar soal untuk bahan ujian.

2. Database yang berformat *.sql akan dienkripsi menggunakan kriptografi algoritma *Advance Encryption Standard (AES)* lalu menjadi format baru yaitu *.code. lalu dilakukan *encode* kepada citra gambar dalam format *.png yang menggunakan steganografi *End of File*, untuk mendapatkan *stego image*.

3. Setelah itu dilakukan *decode* untuk mendapatkan *ciphertext*. Lalu *cipertext* tersebut akan dilakukan dekripsi untuk mendapatkan informasi asli yang telah disisipkan dan dirahasiakan.

2.2.4 Pengujian

Table 1: Pengujian Besar File

No	Nama File Soal Ujian	Ukuran File Awal (KB)	AES (KB)	EoF(KB)
1	Datafile.sql	…	….	…..
Rata-Rata		…	…	….

Table 2: Pengujian Citra *End of File*

No	Nama File	Jenis *Editing*	Keterangan
1	Eof1.png	*Crop*	Korup atau Tidak
2	Eof2.png	Menaikan Kontras	Korup atau Tidak

Table 3: Pengujian Berhasil atau Tidak

No	Nama File Soal Ujian	Enkripsi *AES*	*Encode EoF*	*Decode EoF*	Dekripsi *AES*
1	Datafile.sql	…	….	…..	…..

2.2.5 Simpulan dan Dokumentasi

Pada tahap ini dilakukan penarikan simpulan akhir yang diperbolehkan setelah melakukan tahap pengujian apakah program enkripsi yang telah dibuat dengan menggunakan algoritma AES (*Advance Encryption Standard*) dan Metode Steganografi EOF *(End of File*) dapat menghasilkan keamanan pada soal ujian berbasis komputer tanpa ada kerusakan dan modifikasi. Setelah semua tahap telah selesai dilakukan maka tahapan terakhir adalah dokumentasi.

3. HASIL DAN PEMBAHASAN

3.1 Persiapan Data

Pada tahap ini merupakan data-data yang akan digunakan oleh peneliti. Peneliti memperoleh data yang merupakan kumpulan soal ujian yang diubah menjadi sebuah database dan citra sebagai objek penyisipan. Penulis memerlukan database yang berisi kumpulan soal yang sebersar 32KB, *Website CBT (Computer Base Test)* dan Data citra berformat "*.png".

3.2 *Database Website*

Ini merupakan isi database pada sebuah *website CBT(Computer Base Test)* yang menggunakan aplikasi Laragon bisa dilihat pada gambar 3.

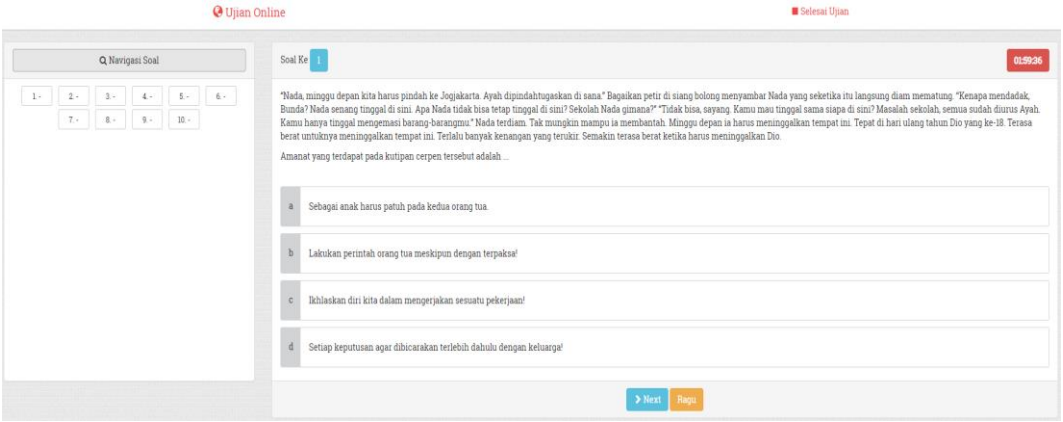
Host: 127.0.0.1 | Database: db_cat_dua | db_cat_dua.sql

Name	Rows	Size	Created	Updated	Engine	Comment	Type
hapus_guru			2020-06-10 10:11:59			AFTER DELETE...	Trig...
hapus_mapel			2020-06-10 10:11:59			AFTER DELETE...	Trig...
hapus_siswa			2020-06-10 10:11:59			AFTER DELETE...	Trig...
m_admin	3	32,0 KiB	2020-06-10 10:11:58		InnoDB		Table
m_guru	5	16,0 KiB	2020-06-10 10:11:58		InnoDB		Table
m_mapel	4	16,0 KiB	2020-06-10 10:11:59		InnoDB		Table
m_siswa	7	16,0 KiB	2020-06-10 10:11:59		InnoDB		Table
m_soal	18	96,0 KiB	2020-06-10 10:11:59	2020-06-10 19:29:31	InnoDB		Table
tr_guru_mapel	18	48,0 KiB	2020-06-10 10:11:59		InnoDB		Table
tr_guru_tes	1	48,0 KiB	2020-06-10 10:11:59	2020-06-10 19:27:33	InnoDB		Table
tr_ikut_ujian	1	48,0 KiB	2020-06-10 10:11:59	2020-06-10 19:29:31	InnoDB		Table

Gambar 3: Database Website

3.3 *Website Computer Base Test*

Pada tahap ini merupakan tampilan dari *Computer Base Test* yang akan digunakan bisa dilihat pada gambar 4.



Gambar 4: *Website Computer Base Test*

3.4 Data Citra PNG

Table 4: Data Citra PNG

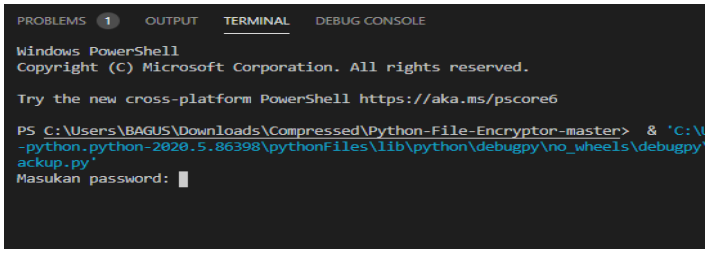
No	Data Citra	Besar File
1		584KB
2		723KB
3		300KB

3.5 Proses Enkripsi dan Penyisipan

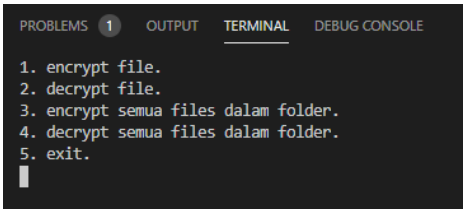
Pada peneletian ini metode yang akan digunakan adalah (AES) *Advance Encryption Standard* dengan panjang kunci 128-bit. Untuk memulai proses enkripsi maupun *encode* dalam bahasa Python dibutuhkan *Module* pendukung yang akan digunakan pada proses enkripsi dan *encode*. Pada penelitian ini digunakan *Module Pycrypto* dan *Module (PIL) Python Imaging Library*. Module ini berisi beberapa algoritma kriptografi dan steganografi yang banyak dipakai.

3.5.1 Proses Enkripsi

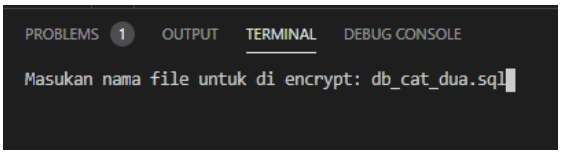
Pada penelitian ini algoritma yang digunakan merupakan (AES) *Advance Encryption Standard* dengan panjang kunci 128-bit. Proses pada enkripsi bisa dilihat pada gambar 5 sampai dengan gambar 8



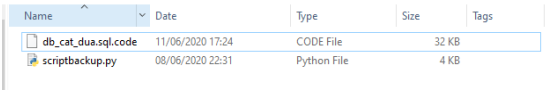
Gambar 5: Masukan *Password*



Gambar 6: Menu AES



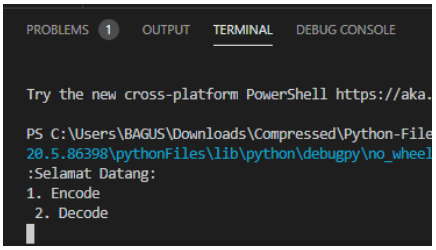
Gambar 7: Nama File



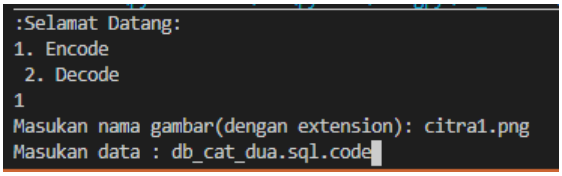
Gambar 8: Hasil Enkripsi

3.5.2 Proses Penyisipan

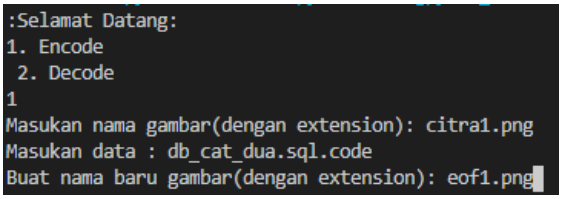
Pada tahap proses penyisipan atau *encode* data adalah tahap steganografi atau menyembunyikan data pada sebuah media. Metode yang digunakan dalam penelitian ini adalah *End of File*. proses pemanggilan fungsi penyisipan atau *encode* melalui *Visual Studio Code*, yang bisa dilihat pada gambar 9 sampai dengan gambar 12.



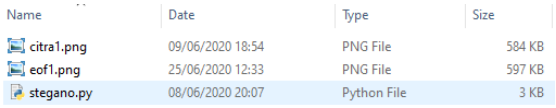
Gambar 9: Menu *End of File*



Gambar 10: Pilih Menu dan Masukan Nama Data



Gambar 11: Nama Citra Baru



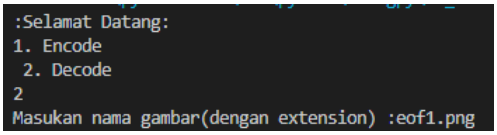
Gambar 12: Hasil *End of File*

3.6 Proses Pengembalian dan Dekripsi

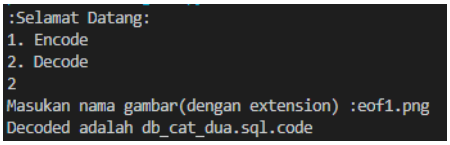
Tahap ini merupakan pengembalian/*decode* dan dekripsi dari data yang peneliti sudah enkripsi dan disisipkan/*encode.*

3.6.1 Proses Pengembalian

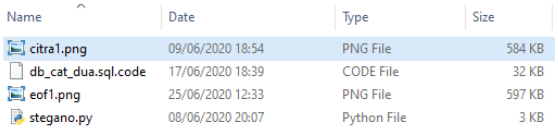
Proses ini mengabil data tersembunyi yang berada dibelakang citra steganografi *End of File* (EoF) yang bisa dilihat pada gambar 13 sampai dengan gambar 15.



Gambar 13: Menu *Decode*



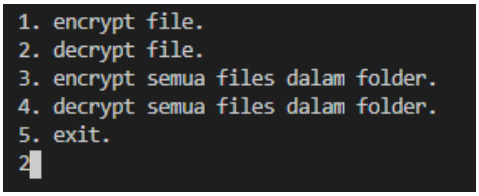
Gambar 14: *Decode* Selesai



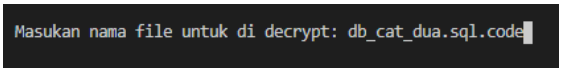
Gambar 15: Hasil Decode

3.6.2 Proses Dekripsi

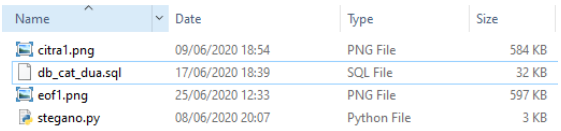
Proses dekripsi merupakan proses mengubah hasil enkripsi menjadi file awal atau data asli. Tahap bisa dilihat dari gambar 16 sampai dengan gambar 18.



Gambar 16: Menu Dekripsi



Gambar 17: Nama File Dekripsi



Gambar 18: Hasil Dekripsi

3.7 Pengujian Data

Pada tahap ini dilakukan pengujian terhadap data yang sudah di enkripsi ataupun sudah disisipkan/*encode* pada sebuah citra. Terbagi dengan 2 pengujian yaitu pengujian aplikasi dan pengujian citra.

3.7.1 Pengujian Aplikasi

Table 5: Pengujian AES

No	Nama File Soal Ujian	Ukuran File Awal (KB)	AES (KB)	Keterangan
1	db_cat_dua.sql	32	32	Berhasil
Rata-Rata		32	32	

Table 6: Pengujian EoF

No	Nama File Citra	Ukuran Citra (KB)	Nama EoF	Ukuran EoF (KB)
1	Citra1.png	584	Eof1.png	597
2	Citra2.png	724	Eof2.png	743
3	Citra3.png	349	Eof3.png	365

Table 7: Proses Pengembalian/*Decode*

No	Nama EoF	Ukuran EoF (KB)	Nama Decode	Ukuran *Decode* (KB)
1	Eof1.png	597	db_cat_dua.sql.code	32
2	Eof2.png	743	db_cat_dua.sql.code	32
3	Eof3.png	365	db_cat_dua.sql.code	32

Table 8: Proses Dekripsi

No	Nama *Decode*	Ukuran *Decode* (KB)	Nama File Awal	Ukuran File (KB)
1	db_cat_dua.sql.code	32	db_cat_dua.sql	32
2	db_cat_dua.sql.code	32	db_cat_dua.sql	32
3	db_cat_dua.sql.code	32	db_cat_dua.sql	32

3.7.2 Pengujian Citra

Table 9: Pengujian Citra

No	Nama Citra Eof	Jenis *Image Processing*	Keterangan
1	Eof1.png	Penambahan Kecerahan	Rusak/Korup
2	Eof2.png	*Cropping*	Rusak/Korup
3	Eof3.png	Penambahan Kontras	Rusak/Korup

4. KESIMPULAN

1. Pada hasil dari aplikasi, membuktikan yaitu aplikasi mampu merahasiakan informasi atau data sehingga tidak semua pihak yang bisa melihatnya.
2. Informasi atau data sebelum dan sesudah yang telah melalui enkripsi, penyisipan/*encode*, pengeluaran*/decode* dan dekripsi tidak berubah dan tidak mengalami kerusakan yang memberitahu bahwa proses sukes.
3. Informasi atau data yang diamankan menggunakan metode kriptografi *Advance Encryption System* (AES) dan Steganografi *End of File* (EoF) tidak rusak dengan syarat tidak melakukan *editing* meliputi penambahan kecerahan (*brightness)*, penambahan kontras (*contrast)* dan pemotongan (*crop).*

Referensi

Adetya .K. P., (2014), "Pengamanan Data Dengan Metode Advanced Encryption Standard Dan Metode Least Significant Bit," pada *Skripsi Teknik Informatika Universitas DIan Nuswantoro*, Semarang.

Ariyus .D., (2008). Pengantar lmu Kriptografi: Teori Analisis dan implementasi, Yogyakarta: Penerbit Andi.

Christy A. S. and H. R. Eko., (2014). "Gabungan Algoritma Vernam Cipher Dan End of File Untuk Keamanan Data," *Techno.COM*.

Gilmore .W. Jason., (2010). *Beginning PHP and MySQL From Novice to Professional Fourth Edition*.

Gupta .N., (2014). Advance Encryption Standard (AES-128) Project Report, Rajasthan: Arya institute of Engineering & Technology.

Menezesm A. J., P. C. van Oorschot, Scott A. Vanstone., (2000). *HANDBOOK of APPLIED CRYPTOGRAPHY*.

Munir .R., (2005). Pengolahan Citra Digital dengan Pendekatan Algoritmik, Bandung: Penerbit Informatika.

Munir .R., (2007). Kriptografi, Bandung: Penerbit Informatika

Yayuk A. and V. Dolly., (2014), "Penerapan Steganografi Metode End Of File (Eof) Dan Enkripsi Metode Data Encryption Standard (Des) Pada Aplikasi Pengamanan Data Gambar Berbasis Java Programming.," pada *Konferensi Nasional Sistem informasi 2014*, Makassar.