Sistem Informasi Kartu Pegawai Elektronik (SI-KPE) Berbasis Web dan Mobile KPE Berbasis Android Dengan Menggunakan Metode AES-128

Yanuar Nurdiansyah[*], Juniar Priaditama[**], Slamin[***]
Sistem Informasi, Program Studi Sistem Informasi, Universitas Jember (UNEJ)
*yanuar_pssi@unej.ac.id

ABSTRACT

East Java regional development Bank, known as the Bank of East Java was founded on august 17th 1951 in Surabaya. Bank of East Java has a lot of products and services for both civil society or non-civil servants. One of them is the product elektronic servis servant card (KPE). Data management services servants electronic card is very simple, make inefficient in terms of time and effort because the input file and file storage are still using manual system, as well as to disseminate announcements or events newest still using posters and other print media. File and information would be usefull if it is delivered to the user with an interest in the proper way. Currently, almost all file and information submitted throught the internet network. Security and confidentiality of file submitted via the internet is vulnerable to file theft by unauthorized parties. One way to maitain the security and confidentiality of such file is by using cryptographic methods. There are many cryptographic algorithms that are used to secure the file. One of which is an Algorithm Advanced Encryption Standard (AES). AES algorithm used in the reseacrh, namely AES-128 algorithm to encode digital files. So that the information contained in the file become more secure after converted into the file encrypt because the information can only be read by the party entitled. Employee card elektorinic information system (SI-KPE) and android based Mobile KPE using AES-128 method is a solution for Bank of East Java Jember branch

Keyword: Electronic employee cards, AES-128, Mobile KPE, Data Security, Cryptography

1. Introduction

Bank Pembangunan Daerah Jawa Timur yang dikenal dengan sebutan Bank Jatim, didirikan pada tanggal 17 Agustus 1961 di Surabaya. Bank Jatim memiliki banyak produk dan layanan untuk masyarakat baik PNS ataupun non PNS. Salah satunya pada produk layanan Kartu Pegawai Negeri Elektornik (KPE). Pengelolaan data layanan Kartu Pegawai Negeri Elektronik (KPE) masih terbilang sangat sederhana, menjadikan tidak efisien dalam hal waktu dan tenaga karena dalam menginputkan data dan tempat penyimpanan datanya masih menggunakan sistem manual, begitupun dalam menyebarluaskan pengumuman atau event- event terbarunya masih menggunakan poster dan media cetak lainnya. Suatu data dan informasi akan berguna jika disampaikan kepada pengguna yang berkepentingan dengan cara yang tepat. Saat ini hampir semua data dan informasi disampaikan melaui jaringan internet. Penggunaan media internet dikarenakan proses penyampaian data dan informasi dapat dilakukan dengan mudah dan lebih cepat. Keamanan dan kerahasiaan data yang disampaikan melalui media internet sangatlah rawan terhadap pencurian data oleh pihak yang tidak berkepentingan. Salah satu cara untuk menjaga keamanan dan kerahasiaan data tersebut yaitu dengan menggunakan metode kriptografi.

Penggunaan metode kriptografi bertujuan untuk mengamankan data dalam proses pengiriman, penyimpanan dan proses lainnya. Menurut Livai dkk. [1] dengan kriptografi data tidak dapat dibaca atau dimengerti oleh pihak-pihak yang tidak berwenang terhadap data tersebut, sehingga keamanan data tersebut akan terjamin. Terdapat dua proses pengamanan data dengan metode kriptografi, yaitu proses enkripsi dan

dekripsi. Terdapat banyak algoritma kriptografi yang digunakan untuk mengamankan data, salah satunya adalah algoritma *Advanced Encryption Standard* (AES). Pada penelitian yang telah dilakukan oleh Lusiana (2011), algoritma AES dipilih karena memiliki tingkat keamanan yang tinggi dengan tiga pilihan tipe kunci yaitu AES-128, AES-192 dan AES-256 [2].

Sistem Informasi Kartu Pegawai Elektronik (SI-KPE) dan Mobile KPE berbasi android dengan menggunakan Metode AES-128 menjadi solusi bagi Bank Jatim cabang Jember. penggunaan algoritma tersebut diimplementasikan pada data pengguna mobile kpe tersebut antara lain, data nama nasabah, data nomor induk pegawai, username, password daftar event yang sedang berlangsung serta data-data lainnya. Diaharapkan algoritma AES-128 dapat melindungi data-data pengguna mobile kpe tersebut .

1. Pengertian Sistem Informasi

Sistem informasi adalah suatu sistem di dalam suatu organisasi yang mempertemukan kebutuhan pengolahan transaksi harian yang mendukung fungsi organisasi yang bersifat manajerial dalam kegiatan strategi dari suatu organisasi untuk dapat menyediakan kepada pihak luar tertentu dengan laporan – laporan yang diperlukan (Sutabri, 2005:36) [3].

2. Kartu Pegawai Elektronik (KPE)

KPE adalah kartu Identitas Pegawai Negeri Sipil yang memuat data PNS dan keluarganya secara elektronik. Diberikan kepada setiap PNS secara gratis dan tetap berlaku setelah PNS yang bersangkutan pensiun dan KPE tambahan diberikan kepada suami/isteri dan anak dari penerima pensiun PNS.

3. Pengertian Keamanan Data

Keamanan data dan informasi, diperlukan penerapan dan pemeliharaan suatu program keamanan dengan memastikan tiga aspek, yaitu : *confidentiality, integrity and availability* dari sumber daya informasi *enterprise* [4].

4. Jenis Algoritma Kriptografi

Menurut Nuur & Rahman [5] berdasarkan kunci yang digunakan untuk enkripsi dan dekripsi, kriptografi dapat dibedakan menjadi 2 macam, yaitu kriptografi simetri (*symmetric cryptography*) dan kriptografi asimetri (*asymetric cryptography*). Pada sistem kriptografi simetri, kunci untuk proses enkripsi sama dengan kunci untuk proses dekripsi. Keamanan sistem kriptografi simetri terletak pada kerahasiaan kunci.

5. Pengertian Kriptografi

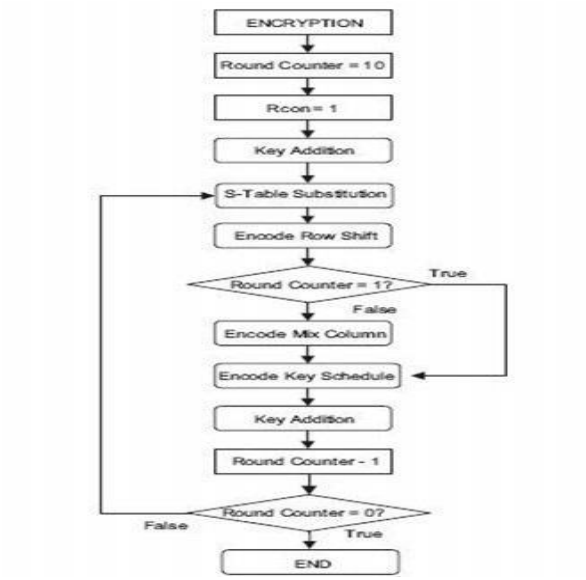
Kriptografi didefinisikan sebagai ilmu dan pelajaran untuk tulisan rahasia dengan pertimbangan bahwa komunikasi dan data dapat dikodekan untuk mencegah dari mata-mata atau orang lain yang ingin mengetahui isinya dengan menggunakan kode-kode atau aturan-aturan tertentu dan metode lainnya sehingga hanya orang yang berhak yang dapat mengetahui isi pesan sebenarnya.

6. Algoritma AES-128

Menurut Lusiana [6], proses putaran (*round*) enkripsi AES-128 dikerjakan sebanyak 10 kali (a=10), yaitu sebagai berikut:

a. Add round key
b. Putaran sebanyak a-1 kali, proses yang dilakukan pada setiap putaran adalah: Sub Bytes, Shift Rows, Mix Columns, dan Add Round Key.
c. Final round, adalah proses untuk putaran terakhir yang meliputi Sub Bytes, Shift Rows, dan Add Round Key.

Diagram alir proses enskripsi AES-128 dapat dilihat pada gambar 1.

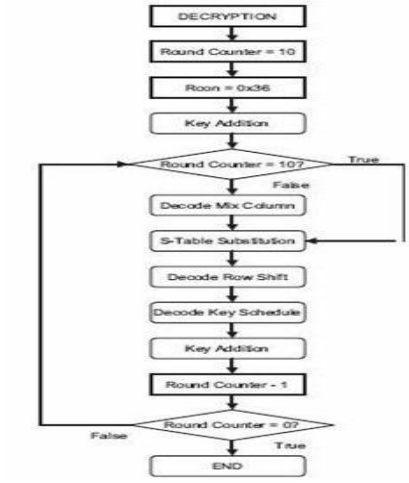


Gambar 1. Diagram Alir Enkripsi AES-128

Sedangkan pada proses dekripsi AES-128 (Lusiana, 2011), proses putaran juga dikerjakan sebanyak 10 kali (a=10), yaitu sebagai berikut:

1. *Add round key*
2. Putaran sebanyak a-1 kali, dimana pada setiap putaran dilakukan proses: *Inverse Shift Rows, Inverse Sub Bytes, Add Round Key, dan Inverse Mix Columns*.
3. Final round, adalah proses untuk putaran terakhir yang meliputi Inverse Shift Rows, Inverse Sub Bytes, dan Add Round Key.

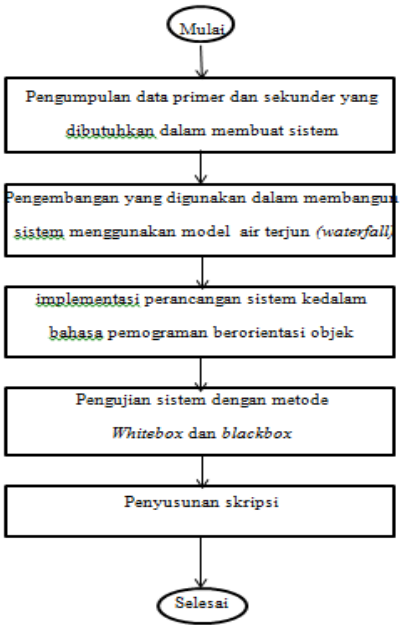
Diagram alir untuk proses dekripsi AES-128 dapat dilihat pada Gambar 2.



Gambar 2. Diagram Alir dekripsi AES-128

2. Research Method (10 PT)

Diagram alir tahapan yang akan dilakukan dalam penelitian sistem informasi kartu pegawai elektronik dan *Mobile* KPE pada Bank Jatim Jember dapat dilihat pada gambar 3.



Gambar 3 Diagram alir penelitian

1. Tahap pengumpulan data

Tahap pengumpulan data dilakukan dengan cara mencari data primer dan data sekunder yang dibutuhkan dalam membuat sistem informasi kartu pegawai elektronik berbasis web dan Mobile KPE berbasis android dengan menggunakan metode AES-128.Data primer diperoleh langsung pada objek penelitian dengan cara observasi dan wawancara pada Bank Jatim Jember. Wawancara ini dilakukan untuk mendapatkan data-data yang dibutuhkan dalam pembuatan sisten informasi kartu pegawai elektronik berbasis web dan *Mobile* KPE berbasi android ada Bank Jatim Jember.

2. Tahap Pengembangan

Tahap pengembangan yang digunakan dalam membangun sistem pada penelitian ini menggunakan model air terjun (waterfall). Model air terjun menyediakan pendekatan alur hidup perangkat lunak secara sekuensial atau terurut dimulai dari analisis, desain, pengodean, pengujian, dan tahap pendukung

3. Tahap Implementasi

Pada tahap implementasi ini, dilakukan dengan cara merubah desain sistem kedalam sebuah bahasa pemograman berorientasi objek sehingga dapat dihasilkan suatu aplikasi sistem informasi kartu pegawai elektronik berbasis web dan *Mobile* KPE berbasis android dengan menggunakan metode AES-128 untuk keamanan data pengguna

4. Tahap Pengujian

Tahapan Pengujian dilakukan apabila aplikasi yang dibuat telah selesai dan siap untuk digunakan oleh pengguna. Pengujian yang dilakukan berguna untuk mengetahui sejauh mana pengimplementasian algoritma AES-128 pada *Mobile* KPE. Tahapan pengujian dilakukan dengan mencari kesalahan-kesalahan yang mungkin terjadi, serta melakukan perbaikan untuk lebih menyempurnakan aplikasi *Mobile* KPE dalam

mengimplementasikan algoritma AES-128. Proses pengujian dilakukan dengan metode *whitebox* dan *blackbox.*

5. Tahap Penyusunan Skripsi

Tahap penyusunan skripsi merupakan langkah akhir pada penelitian ini. Pada tahapan ini akan dilakukan penyusunan laporan yang menjelaskan dasar teori dan metode apa yang digunakan dalam skripsi ini serta hasil dari sistem informasi kartu pegawai elektronik berbasi web dan *Mobile* KPE berbasi android dengan menggunakan metode AES-128.

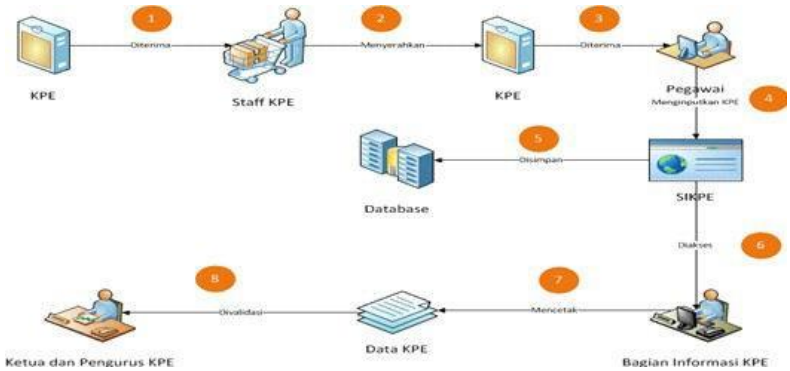
3. Result and Analysis (10 PT)

3.1. Desain dan Perancangan Sistem

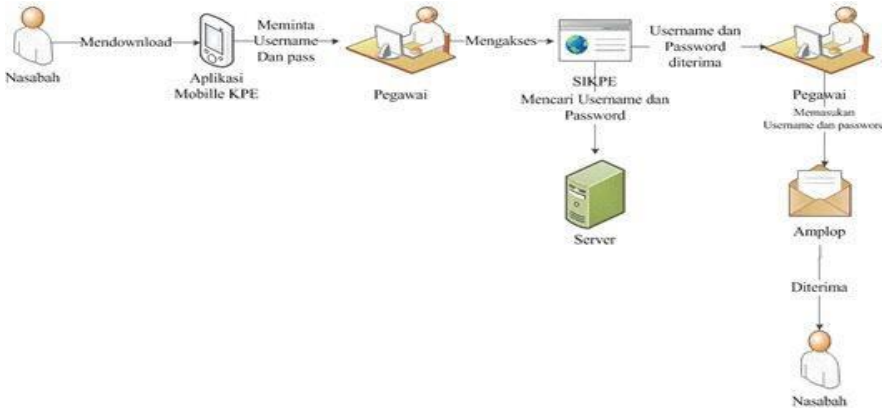
Pada bagian ini menguraikan tentang proses pendesainan dan perancangan sistem informasi kartu pegawai elektronik, serta mengimplementasi algoritma AES 128 pada *Mobille KPE.* Proses pendesainan dan perancangan sistem dimulai dari pembuatan *workflow, Context Diagram, DFD, Event Lst, Kamus Data, ERD, dan entity relation diagram* (ERD).

Desain Workflow :

Gambar 4 Workflow Manual



Gambar 5 Workflow SI KPE



Gambar 6 Workflow Pendaftaran *Mobile KPE*

1. Pengujian

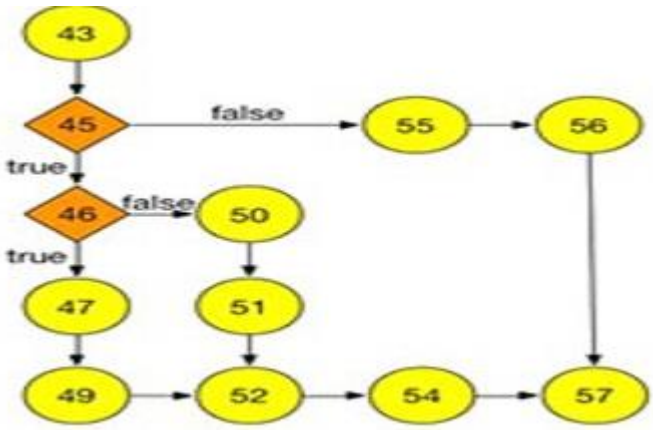
Pengujian dilakukan untuk mengevaluasi aplikasi yang telah dibuat. proses pengujian dilakukan dengan pengujian whitebox terlebih dahulu, lalu akan dilanjutkan dengan pengujian blackbox. Pengujian whitebox yang dilakukan dalam penelitian ini diutamakan dalam pengujian metode AES-128 yakni proses fungsi Enkripsi dan fungsi proses Deskripsi. Deskripsi. Listing program yang diujikan dapat dilihat pada gambar 6 dan 7 sedangkan untuk diagram alir pengujian dapat dilihat pada gambar 8 dan 9.

```
42  public static byte[] encrypt(String text) throws Exception {
43      byte[] encrypted = null;
44
45      if (text != null && text.length() != 0) {
46          try {
47              cipher.init(Cipher.ENCRYPT_MODE, keyspec, ivspec);
48
49              encrypted = cipher.doFinal(padString(text).getBytes());
50          } catch (Exception e) {
51              throw new Exception("[encrypt] " + e.getMessage());
52          }
53
54          return encrypted;
55      } else {
56          throw new Exception("Empty string");
57      }
58  }
```

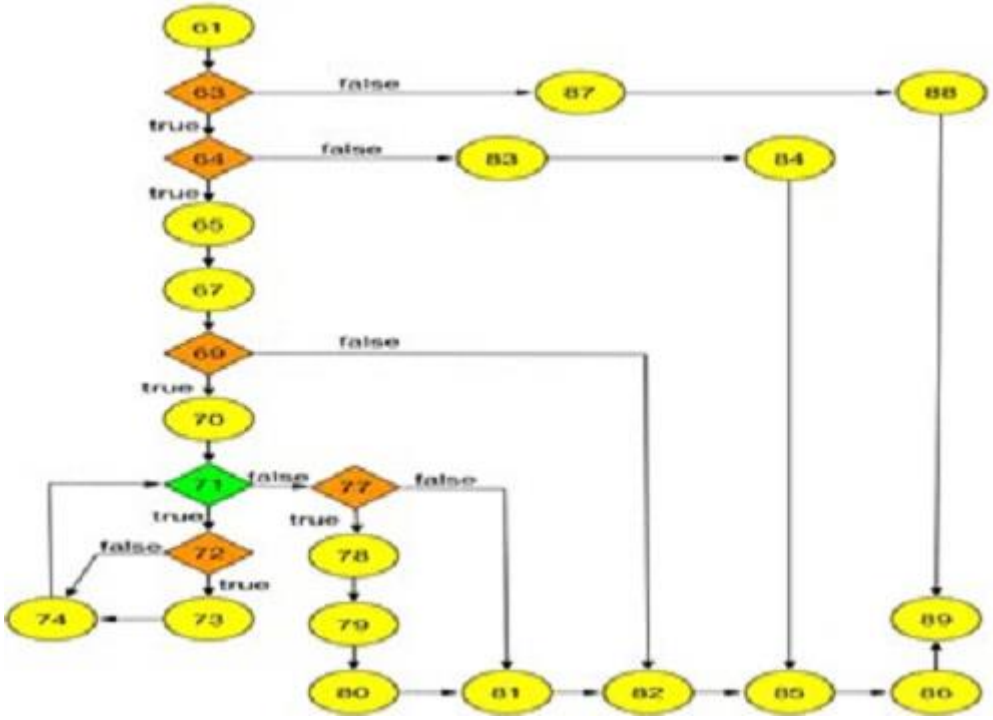
Gambar 7. listing program *Encrypt*

```
60  public static byte[] decrypt(String code) throws Exception {
61      byte[] decrypted = null;
62
63      if (code != null && code.length() != 0) {
64          try {
65              cipher.init(Cipher.DECRYPT_MODE, keyspec, ivspec);
66
67              decrypted = cipher.doFinal(hexToBytes(code));
68              // Remove trailing zeroes
69              if (decrypted.length > 0) {
70                  int trim = 0;
71                  for (int i = decrypted.length - 1; i >= 0; i--) {
72                      if (decrypted[i] == 0) {
73                          trim++;
74                      }
75                  }
76
77                  if (trim > 0) {
78                      byte[] newArray = new byte[decrypted.length - trim];
79                      System.arraycopy(decrypted, 0, newArray, 0, decrypted.length - trim);
80                      decrypted = newArray;
81                  }
82              }
83          } catch (Exception e) {
84              throw new Exception("[decrypt] " + e.getMessage());
85          }
86          return decrypted;
87      } else {
88          throw new Exception("Empty string");
89      }
90  }
```

Gambar 8 Listing program *Decrypt*



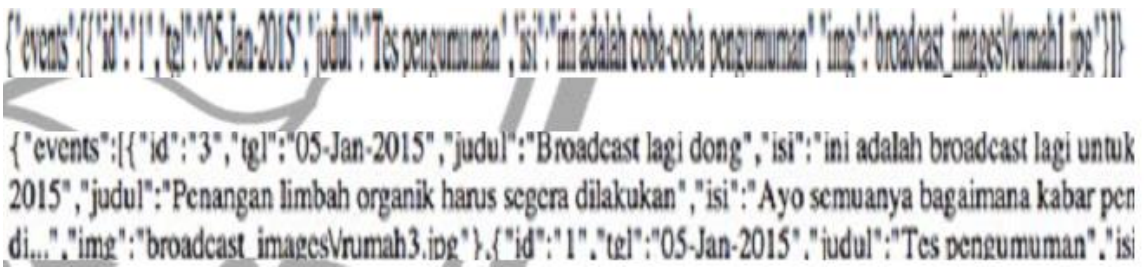
Gambar 9 Grafik Alir Fungsi Enkripsi



Gambar 10 Grafik Alir Fungsi Deskripsi

3.2. Analysis

Pada penelitian ini , implementasi AES-128 pada Mobile KPE dilakukan pengujian dengan menggunakan aplikasi tPacketCapture Pro yang memungkinkan untuk menangkap data, sehingga dengan aplikasi tPacketCapture Pro dapat digunakan untuk membandingkan keamanan data sebelum dan sesudah menggunakan AES-128 pada Mobile KPE. Hasil implementasi algoritmas AES-128 pada Mobile KPE dalam penelitian ini dapat dilihat pada gambar 11.



Gambar 11 Tampilan event tanpa AES-128

Pada gambar 11 merupakan gambar broadcast event pada Mobile KPE sebelum mengguanakan AES-128. Pada gambar tersebut sangat jelas bahwa data tersebut dapat diterjemahkan oleh siapapun. Dengan menggunakan AES- 128 data tersebut akan aman oleh semua orang yang tidak mempunyai hak untuk menerjemahkannya. Berikut hasil dengan mengguan AES 128dapat dilihat pada gambar 12

Gambar 12. Tampilan event menggunakan AES -128

4. Conclusion

1. SI KPE Bank Jatim cabang Jember berbasis web dan *Mobille KPE* berbasis android yang dirancang dan dibuat dengan struktural programming pada web, sedangkan pemrograman berorientasi objek pada android dengan tampilan sesederhana mungkin sehingga mampu membantu karyawan bank jatim melakukan pekerjaanya
2. SI KPE yang dibuat mampu mengirim informasi event terbaru setiap bulan.
3. *Mobile KPE* yang dibuat mampu menerima event terbaru setap bulan serta menjaga keamaan data pengguna ketika mengaksesnya.
4. Pemanfaatan algoritma AES 128 pada *Mobile KPE* Bank Jatim mampu mengamankan data antar server dengan aplikasi *Mobile KPE* Bank Jatim cabang Jember tanpa menggunakan algoritma AES 128 tidak akan terjamin keamanan datanya

References

[1] Livai, Vivi, and Muliawaty. Analisis Perbandingan Metode Kriptografu antara Algoritma IDEA, Blowfish, dan Hybrid. Skripsi, Jakarta: Universitas Bina Nusantara, 2004.

[2] Nurdiansyah, Yanuar, Dwiretno ST Istiyadi, and Ragilliyandi I Erick Putra. "Konferensi Nasional Ilmu Komputer (KONIK) 2014 IMPLEMENTASI ALGORITMA AES-128 PADA MOBILE LEARNING UNIVERSITAS JEMBER," n.d.

[3] Imran, and Budi Rahardjo. Studi Klasifikasi Keamanan Data untuk Enterprise. e-buletin, Sulawesi Selatan: Lembaga Penjaminan Mutu Pendidikan, 2012.

[4] Nuur, S., & Rahman, F. (2013). Analisi dan Perancangan Program Apliksai Music Player dengan Menggunakan Metode Kriptografi 3DES. 2013: Universitas Bina Nusantara

[5] Lusiana, Veronica. "Implementasi Kriptografi Pada File Dokumen Menggunakan Algoritma AES-128." Jurnal Dinamika Informatika Vol.3 No.2, 2011.

[6] Sutabri, Tata. 2013. Pengertian system informasi. [Serial Online]. http ://fisipuin.satugen.com/blog/Pengertian-Sistem- Informasi-Menurut-Para-Ahli-Definisi