P-ISSN: 2963-4008
E-ISSN: 2963-430X

IMPLEMENTASI PENGAMANAN DATA PENGARSIPAN DENGAN METODE ALGORITMA KRIPTOGRAFI AES STUDI KASUS PADA BANK BJB KCP PASTEUR BANDUNG

Muhammad Arief Jayana[1], Doni Rafael[2], Atep Aulia Rahman[3]
[1, 2]Teknik Informatika, Institut Digital Ekonomi LPKIA
[3] Manajemen Informatika, Institut Digital Ekonomi LPKIA

[1] korespondensi: 180914002@fellow.lpkia.ac.id

ABSTRACT

Bank BJB KCP Pasteur Bandung City is a BUMD engaged in the Banking Sector. With the large number of customer data at the BJB KCP Pasteur bank, it is vulnerable to data theft and data falsification. Therefore information security in it is an important aspect that needs to be considered. From the observations of this software, it is proven by the absence of security features in the software. The design of this application uses the SDLC (Software Development Life Cycle) developer methodology. One security that needs to be considered is customer archive data, archive officers enter archive data on the form and then store it in the database. As for the possible attacks. In other words, this was an attempt to monitor using a reconnaissance program. Efforts to improve security include the use of encryption techniques. AES 128-bit encryption provides fairly good security because it has a 10-round process flow where the encryption and decryption of unreadable data returns the original data that can be read later. The result of this software is to protect the data in the database using 128-bit AES encryption algorithm and insert it into the database, so that anyone who has the key used to open the archived data cannot understand the contents of the database, except the archivist.

Keywords: *Cryptographic Algorithm, AES 128 bit, Archived Data*.

ABSTRAK

Bank BJB KCP Pasteur Kota Bandung merupakan BUMD yang bergerak di Bidang Perbankan. Dengan banyaknya data nasabah pada bank BJB KCP Pasteur sehingga rentan pencurian data dan pemalsuan data. Maka dari itu keamanan informasi didalamnya adalah aspek penting yang perlu diperhatikan. Dari hasil pengamatan perangkat lunak ini dibuktikan dengan tidak adanya fitur keamanan pada perangkat lunak. Perancangan aplikasi ini menggunakan metodologi pengembang SDLC (Software Development Life Cycle). Salah satu keamanan yang perlu diperhatikan adalah data arsip nasabah, petugas arsip memasukan data arsip pada form lalu disimpan pada database. Adapun serangan yang mungkin terjadi Dengan kata lain, ini adalah upaya untuk menmantau menggunakan program pengintaian. Upaya peningkatan keamanan antara lain penggunaan teknik enkripsi. Enkripsi AES 128-bit memberikan keamanan yang cukup baik karena memiliki alur proses 10 putaran dimana proses enkripsi dan dekripsi data yang tidak terbaca mengembalikan data asli yang dapat dibaca kemudian. Hasil dari perangkat lunak ini adalah untuk melindungi data dalam database menggunakan algoritma enkripsi AES 128-bit dan memasukkannya ke dalam database, sehingga siapa pun yang memiliki kunci yang digunakan untuk membuka data arsip tidak dapat memahami isi database, kecuali petugas arsip.

Kata Kunci: *Algoritma Kriptografi, AES 128 bit, Data Arsip.*

PENDAHULUAN

Bank Pembangunan Daerah Jawa Barat dan Banten (BJB) Kantor Cabang Pembantu (KCP) Pasteur merupakan Badan Usaha Milik Daerah (BUMD) yang bergerak di Bidang Perbankan dan berperan sebagai lembaga keuangan memiliki fasilitas layanan kredit yang merupakan salah satu produk yang paling diminati. Selain kredit, bank bjb juga melayani pembukaan rekening baru bagi nasabah yang ingin menabung di bank BJB (1). Banyaknya layanan kredit yang ditawarkan hendak memunculkan bertambahnya jumlah calon debitur bank bjb

serta otomatis dokumen pokok kredit terus menjadi meningkat. Dengan bertambahnya dokumen pokok kredit hingga dibutuhkan penindakan dokumen yang efisien (1). Dalam penindakan arsipnya, hingga dibentuklah petugas pengelola arsip buat mengelola arsip. Buat sistem penyimpanan arsip, bank bjb kcp pasteur mempraktikkan sistem bersumber pada no, dalam perihal ini ialah no perjanjian kredit debitur. Seluruh dokumen pokok kredit tiap debitur ditaruh di dalam suatu amplop yang ditulis bukti diri debiturnya. Dalam satu berkas ataupun amplop, berisi seluruh dokumen- dokumen pokok yang sudah disebutkan diatas. Berkas ataupun amplop ditaruh di lemari arsip. Tetapi dalam praktiknya, penerapan sistem pengelolaan arsip di bank BJB KCP Pasteur belum seluruhnya dilaksanakan dengan baik. Perihal ini diindikasikan dengan penyimpanan dokumen pokok kredit yang dibagi jadi 2 tempat penyimpanan ialah diruang arsip serta dilaci meja karyawan. Perihal ini menimbulkan temuan kembali arsip memelurkan waktu yang lumayan lama, serta terkadang wajib mengaitkan sebagian pegawai lain (1). hingga dibutuhkan suatu aplikasi buat pengolahan informasi yang efisien serta efektif, yang didalamnya bisa memilki sistem penyimpanan informasi yang nyaman serta pastinya memenuhi aplikasi dengan metode pengamanan yang lumayan baik buat mengestimasi terdapatnya mungkin kurang baik yang hendak terjalin semacam manipulasi informasi. Dalam riset ini periset hendak mengimplementasikan sistem pengamanan dengan memakai metode kriptografi. Bersumber pada kasus yang terdapat hingga dibutuhkan buat mengamankan informasi pengarsipan di Bank BJB KCP Pasteur Bandung tersebut. Dalam perihal ini buat melindungi kerahasiaan informasi nasabah. Salah satu triknya merupakan membuat informasi data tersebut tidak terbaca ataupun tidak bisa dipahami oleh pihak lain. Buat perihal itu riset kali ini hendak memakai pengamanan dengan metode kriptografi yang bisa membuat informasi data digital tidak terbaca memakai algoritma *Advanced Encryption Standard* (AES). Dengan demikian hingga riset ini hendak berfokus buat membangun aplikasi keamanan jaringan pc memakai algoritma *Advanced Encryption Standard* (AES).

Keamanan sistem data merupakan seluruh betuk mekanisme yang wajib dijalankan dalam suatu sistem yang diperuntukan supaya sistem tersebut bebas dari seluruh ancaman yang membahayakan keamanan informasi data serta keamanan pelakon sistem. Ancaman mencakup bermacam tipe sikap karyawan semacam ketidaktahuan karyawan, kecerobohan, mengambil sandi karyawan lain serta membagikan password buat karyawan lain. Buat ancaman eksternal, ialah virus serta serbuan *spyware*, *hacker* serta penyelinap di tempat (2).

Kriptografi ialah cabang ilmu matematika yang berhubungan dengan transformasi informasi buat buatnya maksudnya tidak bisa dimengerti (buat menyembunyikan maknanya

ataupun isi dari suatu informasi), mencegahnya dari pergantian tanpa izin, ataupun mencegahnya dari pemakaian yang tidak legal. Bila transformasinya bisa dikembalikan, kriptografi pula dapat dimaksud selaku proses mengganti kembali informasi yang terenkripsi jadi wujud yang bisa dimengerti. Jadi bisa disimpulkan kalau kriptografi bisa dimaksud selaku cabang ilmu matematika buat melindungi kerahasiaan data dengan tata cara metode matematika yang mencakup, kerahasiaan, integritas informasi, autentifikasi, serta non repudiasi (3).

Algoritma kriptografi simetris sebutan lainnya yaitu algoritma kriptografi konvensional. algoritma kriptografi simetris merupakan algoritma yang menggunakan kunci yang sama untuk proses enkripsi dan proses deskripsi atau disebut juga dengan kriptografi kunci privat (4).

Dalam kriptografi ada proses didalamnya yang diucap selaku proses enkripsi serta deskripsi. Proses penyandian pesan asli(*plaintext*) jadi pesan yang tidak bisa dibaca(*chipertext*) merupakan enkripsi, sebaliknya kebalikan dari proses enkripsi yakni deskripsi ialah mengembalikan pesan yang telah disandikan tersebut serta tidak bisa terbaca jadi pesan aslinya yang bisa dibaca kembali, proses tersebut merupakan deskripsi. Pesan tersebut bisa informasi ataupun data yang berupa bacaan, dokumen, foto dan suara yang bertabiat berarti serta rahasia (5).

METODE

Metodologi penelitian yang digunakan meliputi metodologi yang digunakan adalah sebagai berikut.

System Development Life Cycle (SDLC) merupakan sesuatu pendekatan yang mempunyai sesi ataupun bertahap buat melaksanakan analisa serta membangun sesuatu rancangan sistem dengan memakai siklus yang lebih khusus terhadap aktivitas pengguna. SDLC pula ialah pusat pengembangan. sistem data yang efektif. SDLC terdiri dari 4 langkah kunci ialah, perencanaan serta pilih, analisis, desain, implementasi serta operasional. Tidak hanya itu, SDLC merupakan suatu proses menguasai gimana Sistem Data bisa menunjang kebutuhan bisnis merancang sistem, membangun sistem, serta memberikannya kepada pengguna (6).

Gambar 1: Tahapan pada *System Development Life Cycle* (6)

Berdasarkan Gambar 1, akan dijelaskan Tahapan pada *System Development Life Cycle* menurut penelitian sebelumnya (6) adalah sebagai berikut:

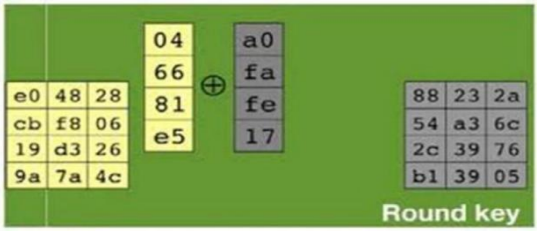
SDLC terdiri dari sebagian tahapan- tahapan. Tahapan dicoba dari analisa kebutuhan fitur lunak hendak terbuat terlebih dulu desain dari kebutuhan tersebut buat memudahkan dalam pengerjaannya. Setelah itu seluruh kebutuhan tersebut di implementasikan dengan 2 sesi ialah sesi analisa serta sesi penilaian*(User Acceptance Test)*. Sehabis melaksanakan implementasi, hingga proses tersebut hendak dikembalikan kembali ke dalam sesi desain buat pengembangan kembali fitur lunak ke tipe yang terkini.

Algoritma AES ialah algoritma simetris ialah mengunakan kunci yang sama buat proses enkripsi serta dekripsi. Algoritma AES mempunyai 3 opsi kunci ialah jenis: AES-128, AES- 192 serta AES- 256. Tiap- tiap jenis memakai kunci internal yang berbeda ialah round key buat tiap proses putaran (7).

Menurut Penelitian sebelumnya (8) Proses enkripsi dan dekripsi Algoritma AES 128-bit adalah sebagai berikut:

a) AddRoundKey

AddRoundKey Pada dasarnya, ini terdiri dari kombinasi ciphertext yang ada dan kunci enkripsi yang menggunakan operasi XOR.

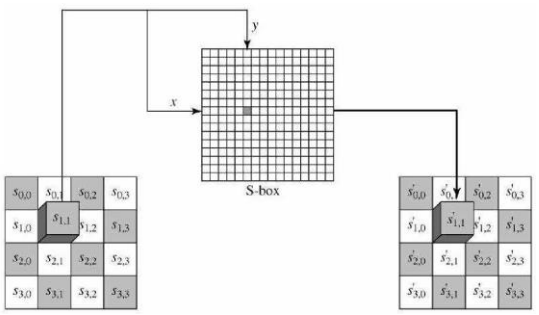


Gambar 2: Skema *AddRoundKey* (8)

Pada Gambar 2 di sebelah kiri adalah *ciphertext* dan sebelah kanan adalah *roundkey* nya. XOR dilakukan perkolom yaitu kolom-1 *ciphertext* di XOR dengan kolom-1 roundkey dan seterusnya.

b) SubBytes

Prinsip dari *SubBytes* adalah menukar isi matriks yang disebut dengan *Rijndael S-Box*. Di bawah ini adalah contoh ilustrasi *SubBytes*.



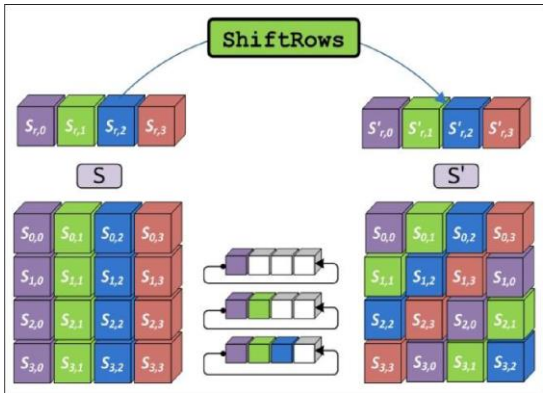
Gambar 3: Ilustrasi *SubBytes* (8)

P-ISSN: 2963-4008
E-ISSN: 2963-430X

Setiap *S-Box* memiliki nomor kolom dan nomor baris. Seperti disebutkan sebelumnya, isi dari setiap kotak cipher blok berisi informasi heksadesimal yang terdiri dari dua digit, huruf, atau angka, yang semuanya tercantum dalam *Rijndael S-Box*. Prosedurnya adalah mengambil salah satu isi kotak matriks dan mencocokkannya dengan angka di sebelah kiri sebagai baris dan angka di sebelah kanan sebagai kolom. Kemudian, setelah Anda mengetahui kolom dan baris, Anda bisa mendapatkan isi tabel dari *Rijndael S-Box*. Langkah terakhir adalah mengubah seluruh blok cipher menjadi blok baru. Isi blok ini adalah hasil dari pertukaran semua isi blok dengan isi langkah-langkah di atas.

c) ShiftRows

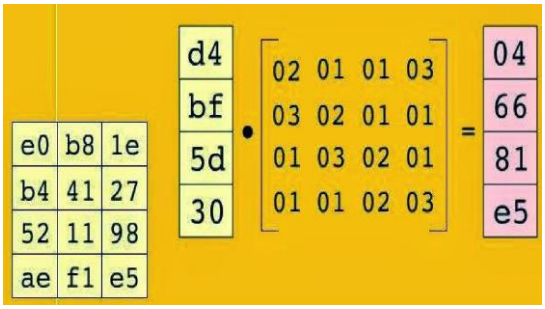
ShiftRows adalah proses menggeser atau memindahkan setiap blok atau elemen tabel baris demi baris. Artinya, baris pertama tidak digeser, baris kedua digeser 1 *byte*, baris ketiga digeser 2 *byte*, dan baris ke-4 digeser 3 byte. Pergeseran di dalam blok adalah pergeseran kiri setiap elemen sesuai dengan jumlah byte yang digeser. Setiap pergeseran 1-*byte* berarti satu pergeseran ke kiri. Gambar berikut menunjukkan diagram tahap ini.



Gambar 4 : Ilustrasi dari *ShiftRows* (8)

d) Mix Columns

Mix Column terdiri dari mengalikan setiap elemen dari blok cipher dengan matriks yang ditunjukkan pada Gambar 5 di bawah ini. Perkalian dilakukan seperti perkalian matriks normal menggunakan produk titik, dan kedua perkalian tersebut dimasukkan ke dalam block cipher yang baru.

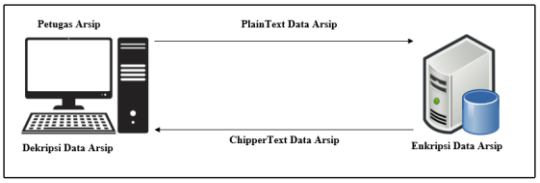


Gambar 5 : Matriks *Mix Coloumns* (8)

HASIL DAN PEMBAHASAN

Desain Penelitian

Penelitian ini berkaitan dengan proses enkripsi dan dekripsi data arsip menggunakan algoritma enkripsi AES 128 bit. Untuk memudahkan pemahaman tentang penelitian yang dilakukan, desain penelitian ditunjukkan pada Gambar 6 dan 7. Mekanisme atau operasi dari algoritma enkripsi AES 128-bit diilustrasikan pada *flowchart* pada Gambar 8. Berikut adalah skenario desain penelitiannya:



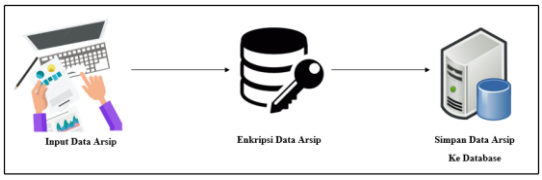
Gambar 6 : Skenario Desain Penelitian Pengiriman Data Arsip

Penjelasan gambar 6 sebagai berikut:

1) Untuk dapat masuk kedalam aplikasi. Petugas arsip harus melakukan login terlebih dahulu.
2) Setelah login, maka petugas arsip akan melakukan penginputan data arsip. Pada saat proses pengiriman data arsip yang belum dienkripsi disebut *plaintext* yang berupa text tersebut akan diproses enkripsi dengan menggunakan algoritma Kriptografi AES 128 bit dan hasil enkripsi tersebut akan dikirimkan ke server dan disimpan pada *database.*
3) Selanjutnya proses dekripsi data arsip yaitu data yang tersimpan pada *database* sudah menjadi data yang sudah dienkripsi atau disebut *chipertext.* Maka data arsip tersebut akan dikirimkan kembali ke tampilan aplikasi pengarsipan dan didekripsikan agar petugas arsip dapat membaca data arsip tersebut.

Pada proses yang telah diuraikan diatas, maka ketika ada serangan dari *Sniffing* untuk mengambil data sebelum tersimpan di *database*, Maka data yang didapat adalah data yang telah terenkripsi.

Adapun skenario penelitian berikutnya sebagai berikut:



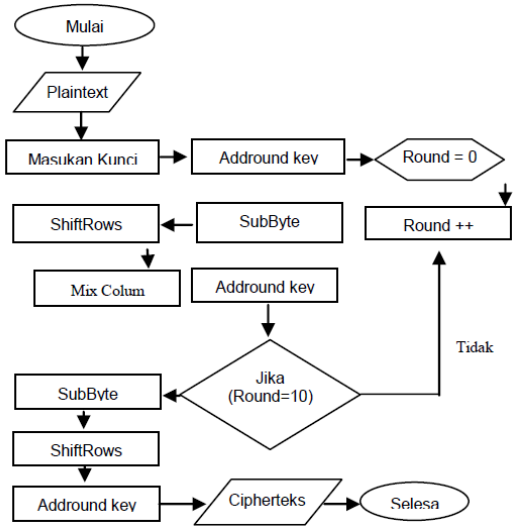
Gambar 7: Skenario Desain Penelitian Enkripsi Penyimpanan Data Arsip

Penjelasan Gambar 7 akan dijelaskan dibawah ini:

1) Petugas Arsip mengakses halaman untuk tambah data arsip baru.
2) Kemudian mengisi data arsip pada form input yang disediakan.

3) Lalu data arsip akan dikirim ke *database* dan dilakukan enkripsi dengan menggunakan algoritma Kriptografi AES 128 bit.

Adapun mekanisme enkripsi dengan algoritma Kriptografi AES 128 bit adalah sebagai berikut:



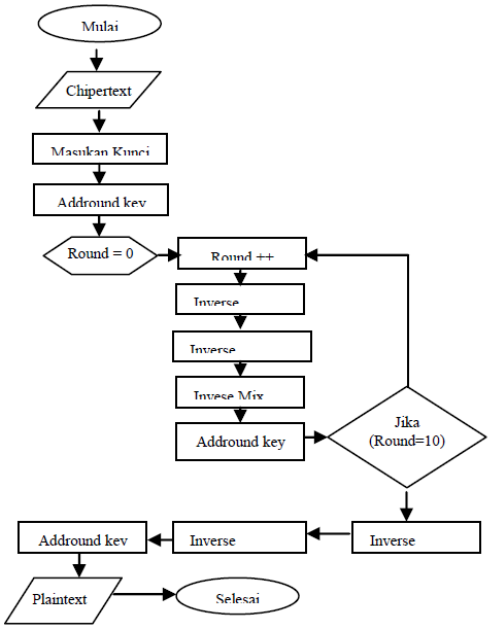
Gambar 8 : *Flowchart* Enkripsi AES 128 Bit (9)

Berdasarkan gambar 8, akan dijelaskan langkah-langkah enkripsi AES 128 bit adalah sebagai berikut:

1) Sistem akan mengambil data *plaintext* yaitu dari input data arsip.
2) *Plaintext* atau pesan masuk mentah untuk diproses dengan panjang tetap n. Namun, jika ukuran data terlalu panjang, data akan dipecah menjadi blok-blok yang lebih kecil.
3) Setelah itu *plaintext* sudah menjadi blok-blok data.
4) *Plaintext* menggunakan vektor inisialisasi IV untuk blok pertama dan XOR setiap blok dengan ekripsi dari blok sebelumnya.
5) Kemudian dilakukan enkripsi AES 128 bit prosesnya sebagai berikut:
   a) AddRoundKey : mengkombinasikan *ciphertext* yang sudah adadengan *cipherkey* dengan operasi XOR.
   b) *SubBytes* : mengganti isi matriks yang disebut dengan *Rijndael S-Box.*
   c) *ShiftRows* : Proses memindahkan atau menggeser setiap elemen dari blok atau tabel yang berjalan baris demi baris.
   d) *Mix Column* : Kalikan setiap elemen cipher blok dengan matriks.
6) Selanjtnya *AddRoundKey* 10 putaran diulang. Proses algoritma AES ini disebut fungsi pembulatan. Babak terakhir sedikit berbeda dengan babak sebelumnya dimana keadaan babak terakhir belum mengalami konversi MixColumns.
7) Kemudian periksa apakah semua blok dienkripsi. Jika tidak, proses kembali ke

nomor 4. Sementara itu, ketika semua blok selesai, ciphertext enkripsi AES 128-bit diambil.

Adapun mekanisme dekripsi dengan algoritma Kriptografi AES 128 bit adalah sebagai berikut:



Gambar 9 : *Flowchart* Deskripsi AES 128 Bit (9)

Berdasarkan gambar 9, akan dijelaskan langkah-langkah dekripsi AES 128 bit adalah sebagai berikut:

1) Sistem akan mengambil data *chipertext* yaitu dari data arsip
2) Dimasukkannya *ciphertext* dan pemrosesan dengan gerbang logika XOR.
3) Kemudian nilai Nr = 1 diambil, state array digeser ke kanan, dan *state array* diganti menggunakan *inverted S-box.*
4) Kita akan mengacak data array status dan menggunakan gerbang logika XOR untuk mengubah array status. Jika nilai Nr yang dihasilkan tidak sama dengan 9, maka langkah *sequence move* diulang. Jika nilainya sudah 9, geser *state array* ke kanan, ganti *state array* dengan *invS-box* dan lanjutkan.
5) Lanjutkan konversi menggunakan gerbang logika XOR. Teks biasa dihasilkan dan prosesnya disimpan secara otomatis.
6) Maka telah mendapatkan *plaintext* hasil dekripsi AES 128 bit.

Implementasi Metode

Penelitian ini dilakukan pada perangkat lunak data pengarsipan dikelola oleh petugas arsip bank bjb kcp pasteur kota bandung. Proses implementasi metode enkripsi untuk menjaga keamanan dari pencurian data arsip pada sistem dan database menggunakan algoritma Kriptografi AES 128 bit dilakukan pada sistem input data arsip sebelum data dikirmkan ke server. Lalu proses enkripsi pada penyimpanan data dilakukan pada sistem

input data arsip sebelum data disimpan ke database. Selanjutnya proses dekripsi data arsip yaitu data yang tersimpan pada database sudah menjadi data yang sudah dienkripsi, maka data arsip tersebut akan dikirimkan kembali ke tampilan perangkat lunak pengarsipan dan didekripsikan agar petugas arsip dapat membaca data arsip tersebut.

Skenario Eksperimen

Skenario eksperimen yang akan dilakukan sebagai berikut :

1) *Sniffing* perangkat lunak tidak menggunakan keamanan enkripsi pada proses penginputan data arsip untuk mengetahui apakah data arsip dapat dibaca oleh *tools sniffing* atau tidak.
2) *Sniffing* perangkat lunak tidak menggunakan keamanan enkripsi pada proses penginputan data arsip untuk melihat hasil enkripsi sebagai usaha melindungi data dari serangan *sniffer.*
3) Penggunaan teknik enkripsi pada penyimpanan data di *database* untuk menjaga dan melindungi kerahasiaan data perbankan.

Prosedur Eksperimen

Prosedur eksperimen yang dilakukan dalam penelitian ini sebagai berikut:

1) *Sniffing* perangkat lunak tidak menggunakan keamanan enkripsi pada proses penginputan data arsip untuk mengetahui apakah data arsip dapat dibaca oleh *tools sniffing* atau tidak yaitu dengan cara:
   a) Petugas Arsip melakukan proses penginputan data sesuai data arsip yang ada.
   b) Data yang diinputkan ke sistem yaitu kedalam bentuk *plaintext.*
   c) Pada saat yang bersamaan dilakukan proses sniffing menggunakan *tools sniffing*.
2) *Sniffing* perangkat lunak tidak menggunakan keamanan enkripsi pada proses penginputan data arsip untuk melihat hasil enkripsi sebagai usaha melindungi data dari serangan *sniffer* yaitu dengan cara:
   a) Petugas Arsip melakukan proses penginputan data sesuai data arsip yang ada.
   b) Pada seluruh *view* menu data arsip terdapat kodingan untuk proses algoritma Kriptografi AES 128 bit untuk melakukan enkripsi pada inputan data arsip sebelum data tersebut dikirm ke server.
   c) Setelah dienkripsi, *chipertext* data arsip disimpan ke *database.*
   d) Pada saat yang bersamaan dilakukan proses *sniffing* menggunakan *tools sniffing.*
3) Menambah data arsip baru, sebelum data disimpan ke *database* dienkripsi terlebih dahulu menggunakan algoritma Kriptografi AES 128 bit. Teknik enkripsi pada penyimpanan data di *database* untuk menjaga dan melindungi kerahasiaan data perbankan.

4) Analisis kodingan untuk proses algoritma kriptografi AES 128 bit untuk melihat bagaimana proses enkripsi dilakukan pada seluruh *view* menu data arsip.

Variabel Eksperimen

Beberapa variabel yang terikat dalam penelitian ini sebagai berikut:

1) *Plaintext* data arsip.
2) *Chipertext* data arsip.
3) *Library* kodingan untuk proses algoritma Kriptografi AES 128 bit sebagai metode keamanan yang digunakan.
4) *Tools Sniffing.*

Pengujian

Dalam melakukan pengujian, akan menggunakan *BlackBox Testing. BlackBox Testing* yaitu melakukan validasi *output* apakah sesuai dengan yang diharapkan dari data input yang diberikan. Manfaat dari *BlackBox Testing* dapat mengetahui seberapa baik dan kekurangan sistem melaksanakan fungsinya serta interaksi user terhadap aplikasi (10).

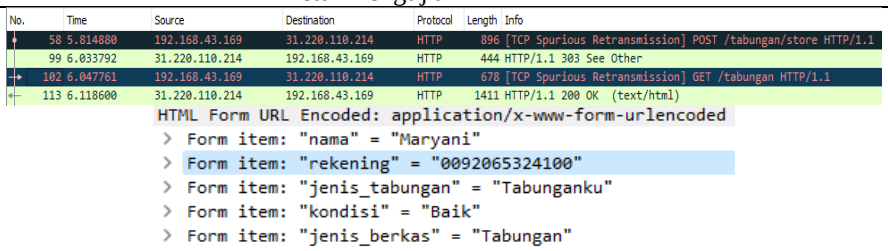
Hasil Pengujian

Hasil Pengujian ini menggunakan *BlackBox Testing.* Pengujian yang telah dilakukan implementasi algoritma Kriptografi AES 128 bit pada perangkat lunak data pengarsipan di Bank BJB KCP Pasteur Tujuannya adalah untuk menemukan masalah dan kekurangan pada perangkat lunak. Jika ada kesalahan atau bug yang ditemukan dalam perangkat lunak data pengarsipan di bank bjb kcp pasteur selama pengujian ini Pengembang kemudian dapat memperbaiki kesalahan. Ada beberapa tabel kasus uji dalam hasil pengujian untuk membantu Anda menentukan apakah sistem ini berhasil atau gagal dalam pengujian

Pengujian Tanpa Enkripsi

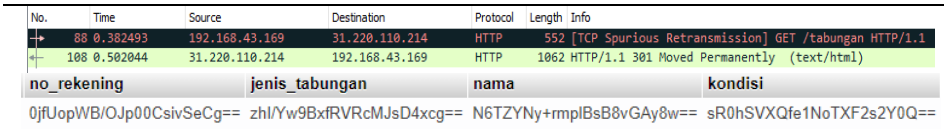
Tabel 1: Pengujian Input Data Pembukaan Rekening Baru Tanpa Enkripsi

No.		Detail Pengujian
1	Cara Pengujian	Uji input data pembukaan rekening baru dengan melakukan *sniffing* menggunakan *tools sniffing* wireshark pada form input data pembukaan rekening baru yang tidak menggunakan enkripsi. - Nomor Rekening : 0092065324100 - Nama Nasabah : Maryani - Jenis Tabungan : Tabunganku - Kondisi : Baik - Jenis Berkas : Tabungan
	Hasil yang diharapkan	*Tools Sniffing* wireshark dapat membaca inputan data pembukaan rekening baru.
		[✓] Berhasil [ ] Tidak Berhasil

No.	Detail Pengujian
	

Pengujian dengan Enkripsi

Tabel 2: Pengujian Input Data Pembukaan Rekening Baru dengan Enkripsi

No.		Detail Pengujian
1	Cara Pengujian	Uji input data pembukaan rekening baru dengan melakukan *sniffing* menggunakan *tools sniffing* wireshark pada form input data pembukaan rekening baru yang menggunakan enkripsi. - Nomor Rekening : 0092065324100 - Nama Nasabah : Maryani - Jenis Tabungan : Tabunganku - Kondisi : Baik - Jenis Berkas : Tabungan
	Hasil yang diharapkan	*Tools Sniffing* wireshark tidak dapat membaca inputan data pembukaan rekening baru dan telah terenkripsi di *database.*
		[✓] Berhasil [ ] Tidak Berhasil
		

SIMPULAN

Berdasarkan implementasi dan pengujian yang telah dilakukan, maka peroleh kesimpulan bahwa penelitian mengenai implementasi algoritma Kriptografi AES 128 bit pada perangkat lunak data pengarsipan di Bank BJB KCP Pasteur adalah:

Dengan membangun keamanan untuk data arsip pada perangkat lunak data pengarsipan di Bank BJB KCP Pasteur menggunakan algoritma Kriptografi AES 128 bit untuk enkripsi dari serangan sniffer dan memastikan bahwa yang mengakses perangkat lunak adalah petugas arsip Bank BJB KCP Pasteur saja, sehingga melindungi keamanan dan kerahasiaan data perusahaan dari orang yang tidak bertanggung jawab.

DAFTAR PUSTAKA

1. Rachman T. Perancangan Penanganan Arsip Dokumen Pokok Kredit di Bagian Adminitrasi Kredit PT Bank Pembangunan Daerah Jawa Barat dan Banten, TBK. Kantor Cabang Sukajadi KCP Pasteur. Angew Chemie Int Ed 6(11), 951–952. 2018;10–27.

2. Siagian S. Analisis Ancaman Keamanan Pada Sistem Informasi

Manajemen di Rumah Sakit Rimbo Medica Jambi. Sci J STIKES PRIMA JAMBI. 2016;4.

3. Fathurrozi A. Penerapan Algoritma Advanced Encryption Standard (AES-256) Dengan Mode CBC DanSecure Hash Algorithm (SHA-256) Untuk Pengamanan Data File. 2021;2(2):227–38.

4. Arrijal IM, Efendi R, Susilo B. Penerapan Algoritma Kriptografi Kunci Simetris Dengan Modifikasi Vigenere Cipher Dalam Aplikasi Kriptografi Teks. Pseudocode . 2016;3(1):69–82.

5. Simangunsong PBN, Fitri K. Perancangan Aplikasi Pengamanan Citra Berwarna dengan Algoritma RSA. J Tek Inform UNIKA St … [Internet]. 2018;03:99–107. Available from: http://103.76.21.184/index.php/JTIUST/article/view/295

6. Munthe IR. Perancangan Sistem Informasi Pengarsipan Data Penduduk Pada Kantor Camat Bilah Hulu Kabupaten Labuhan Batu Dengan Metode System Develovment Life Cycle (Sdlc). J Inform. 2019;5(1):22–31.

7. Lusiana V. Implementasi Kriptografi Pada File Dokumen Menggunakan Algoritma Aes-128. J Din Inform . 2011;3(2):79–83.

8. Grehasen G, Mulyati S. Pengamanan Database Pada Aplikasi Test Masuk Karyawan Baru Berbasis Web Menggunakan Algoritma Kriptografi AES-128 Dan RC4 Geri . 2017;14(1):52–60.

9. Hanafi JI, Patombongi A. Aplikasi Sms Kriptografi Menggunakan Metode Aes Berbasis Android. Simtek J Sist Inf dan Tek Komput . 2016;1(1):69–75.

10. Widia IDM, Rosalin S, Asriningtias SR, Sonalita E. Black Box Testing Menggunakan Boundary Value Analysis dan Equivalence Partitioning pada Aplikasi Pengadaan Bahan Baku Batik dengan Pendekatan Use Case . 2022;6(1):15–21.