IMPLEMENTASI PENGAMANAN DATABASE MENGGUNAKAN METODE BLOWFISH DAN AES PADA PERUSAHAAN CV. BALERONG SAKTI

Muhammad Sadli[1)] , Painem [2)]
Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
Jl. Raya Ciledug, Petukangan Utara, Kebayaroan Lama, Jakarta Selatan 12260
Telp. (021) 5853753, Fax. (021) 5866369
E-mail : sadli.dali28@gmail.com[1)], painem@budiluhur.ac.id[2)]

Abstrak

Perkembangan teknologi informasi dan telekomunikasi saat ini berkembang dengan sangat pesat berpengaruh pada penggunaan informasi data. Dimana, kemampuan untuk mengaskses dan menyediakan informasi secara cepat dan akurat menjadi efektif bagi sebuah perusahaan. Adapun dampak positif, yaitu dengan semakin canggihnya teknologi, maka dapat memudahkan seseorang untuk berinteraksi dan memudahkan pekerjaan sehingga lebih efekif dan efisien. Adapun dampak negatifnya dengan berkembangnya teknologi, yaitu dapat di pastikan semakin berkembangnya teknologi maka semakin berkembangnya pula kejahatan di dunia teknologi informasi. Data-data dalam sebuah perusahaan biasanya tersimpan dalam database perusahaan. Saat ini database yang ada didalam perusahaan belum mempunyai keamanan. Untuk mengatasi keamanan data tersebut maka diperlukan cara untuk mengamankan informasi data tersebut agar tidak dapat di salah gunakan. Salah satu cara yang dapat digunakan untuk keamanan database adalah dengan menggunakan teknik kriptografi. Metode yang akan digunakan adalah algoritma *blowfish* dan AES yang akan diimplementasikan pada aplikasi kriptografi berbasis desktop untuk mengamankan informasi database di CV. Balerong Sakti.

Kata Kunci: Enkripsi dan Dekripsi, Database, Blowfish, AES, CV. Balerong.

1. PENDAHULUAN

Perkembangan teknologi informasi dan telekomunikasi saat ini berkembang dengan sangat pesat berpengaruh pada penggunaan informasi data. Dimana, kemampuan untuk mengaskses dan menyediakan informasi secara cepat dan akurat menjadi efektif bagi sebuah perusahaan. Adapun dampak positif dan dampak negatif dari perkembangan teknologi saat ini, yaitu dengan semakin canggihnya teknologi, maka dapat memudahkan seseorang untuk berinteraksi dan memudahkan pekerjaan sehingga lebih efekif dan efisien. Adapun dampak negatifnya dengan berkembangnya teknologi, yaitu dapat di pastikan semakin berkembangnya teknologi maka semakin berkembangnya pula kejahatan di dunia teknologi informasi. Masalah keamanan dan kerahasian database merupakan suatu hal yang sangat penting untuk menjaga kerahasiaan informasi terutama yang berisi informasi database yang hanya boleh di ketahui isinya oleh pihak yang berhak saja.

CV. Balerong Sakti melayani perusahaan menengah dan perusahan besar, baik swasta dan pemerintah. CV. Balerong Sakti dalam menjalankan bisnis selalu mengutamakan mutu serta kepercayaan demi kelangsungan bisnis yang harmonis dan berkelanjutan. CV. Balerong Sakti membutuhkan

suatu pengamanan informasi database yang baik yang dapat digunakan untuk melakukan berbagai macam kegiatan perusahaan secara efektif. Mengingat banyak hal penting dalam database yang menjadi data yang sangat penting perusahaan yang akan sangat merugikan perusahaan apabila database tersebut jatuh kepada pihak yang tidak bertanggung jawab, maka di perlukan keamanan terhadap data agar pihak yang tidak bertanggung jawab tidak dapat mengetahui isi dari data tersebut.

Untuk mengatasi keamanan data tersebut maka diperlukan cara untuk mengamankan informasi data tersebut agar tidak dapat di salah gunakan. Salah satu cara yang dapat digunakan untuk keamanan data adalah dengan menggunakan teknik kriptografi. Metode yang akan digunakan adalah algoritma blowfish dan AES yang akan diimplementasikan pada aplikasi kriptografi berbasis desktop untuk mengamankan informasi database di CV. Balerong Sakti.

2. LANDASAN TEORI

2.1 Kriptografi

Kriptografi merupakan ilmu pengetahuan yang mempelajari tentang metode untuk membuat tulisan atau pesan rahasia. Sedangkan ke asliannya mencegah pihak ketiga untuk mengirim data yang salah atau mengubah data yang dikirimkan (Foelyati, 2007).

2.2 Jenis Kriptografi

Algoritma kriptografi terbagi menjadi dua bagian berdasarkan kunci yang dipakainya, yaitu :

a. Algoritma Simetris

Keamanan sistem kriptografi simetri terletak pada kerahasiaan kuncinya. Algoritma kriptografi modern yang merupakan sistem kriptografi simetri diantaranya adalah DES (*Data Encryption Standard*), *blowfish*, AES (*Advanced Encryption Standard*) dan lain-lain. (Suriski Sitinjak, 2010).

b. Algoritma Asimetris
Algoritma simetris, sering juga disebut dengan algoritma kunci rahasia atau sandi kunci rahasia. Algoritma asimetris *(asymmetric algorithm)* adalah suatu algoritma dimana kunci enkripsi yang digunakan tidak sama dengan kunci dekripsi. Pada algoritma ini menggunakan dua kunci yakni kunci publik *(public key)* dan kunci privat *(private key)*. Kunci publik disebarkan secara umum sedangkan kunci privat disimpan secara rahasia oleh si pengguna

2.3 Enkripsi Algortima Blowfish

Blowfish menggunakan subkunci berukuran besar. Kunci-kunci tersebut harus dikomputasikan pada saat awal, sebelum pengkomputasian enkripsi dan dekripsi data. Langkah-langkahnya adalah sebagai berikut (Natsir: 2017) :

a. Terdapat kotak permutasi (X-box) yang terdiri dari 18 buah 32 bit subkunci: X1, X2, X3, … X18. P-box ini telah ditetapkan sejak awal, 4 buah P-box awal adalah sebagai berikut :
X1 = 0x243f6a88
X2 = 0x85a308d3
X3 = 0x13198a2e
X4 = 0x03707344
b. Xorkan X1 dengan 32 bit awal kunci, xorkan X2 dengan 32 bit berikutnya dari kunci, dan teruskan hingga seluruh panjang kunci telah terxorkan (kemungkinan sampai X14, 14x32 = 448, panjang maskimal kunci).
c. Terdapat 64 bit dengan isi kosong, bit-bit tersebut dimasukkan ke langkah ke 2.
d. Gantikan X1 dan X2 dengan keluaran dari langkah 3.
e. Enkripsikan keluaran langkah 3 dengan langkah 2 kembali, namun kali ini dengan subkunci yang berbeda (sebab langkah 2 menghasilkan subkunci baru).
f. Gantikan X3 dan X4 dengan keluaran dari langkah 5.
g. Lakukan seterusnya hingga seluruh X-box teracak sempurna.
h. Total keseluruhan, terdapat 521 iterasi untuk menghasilkan subkunci-subkunci yang dibutuhkan. Aplikasi hendaknya menyimpannya dari pada menghasilkan ulang subkunci-subkunci tersebut.

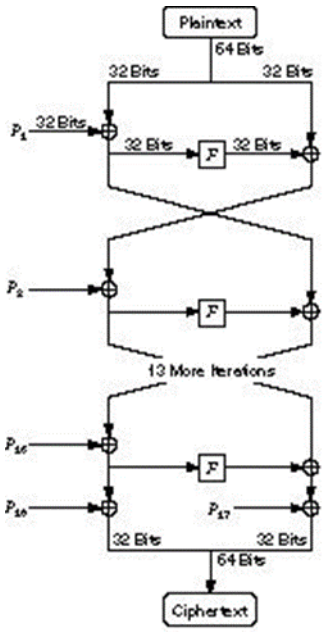
Kunci-kunci yang digunakan antara lain terdiri dari, 18 buah 32-bit subkey yang tergabung dalam X-array (X1, X2, …, X18). Selain itu, ada pula empat 32-bit Zbox yang masing-masingnya memiliki 256 entri :

Z1,0,Z1,1,…, Z1,255; Z3,0,Z3,1,…, Z3,255; Z4,0,Z4,1,…, Z4,255.

Pada proses enkripsi, Blowfish memiliki 16 iterasi, masukannya adalah 64-bit elemen data, Y. Untuk melakukan proses enkripsi:

a. Bagi Y menjadi dua bagian yang masing-masing terdiri dari 32-bit: YL, YR. For i = 1 to 16 :
YL = YL XOR Pi
YR = F (YL) XOR YR
Tukar YL dan YR
b. Setelah iterasi ke-enam belas, tukar YL dan YR lagi untuk melakukan undo pertukaran terakhir.
c. Lalu lakukan YR = YR XOR P17
YL = YL XOR P1
d. Terakhir, gabungkan kembali YL dan YR untuk mendapatkan ciperteks.

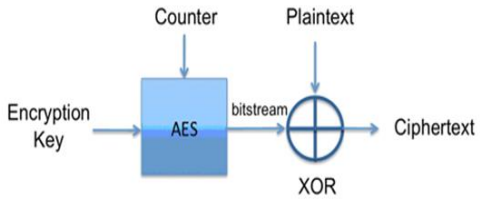
Untuk lebih jelasnya, gambaran tahapan Skema Enkripsi yang digunakan Blowfish adalah seperti pada Gambar 1



Gambar 1 Diagram Skema Enkripsi Algoritma Blowfish

Pada langkah kedua, dituliskan mengenai penggunaan fungsi F. Fungsi F adalah: Bagi YL menjadi empat bagian 8-bit: a, b, c dan d. F(YL) = ((Z1, a + Z2, b mod 232) XOR Z3, c) + Z4, d mod 232.

2.4 Algoritma AES (Advanced Encryption Standard)

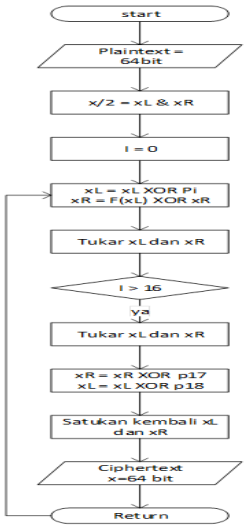


Gambar 2. Skema AES

2.5 *Flowchart* Aplikasi Blowfish dan AES

a. *Flowchart* proses Enkripsi Blowfish

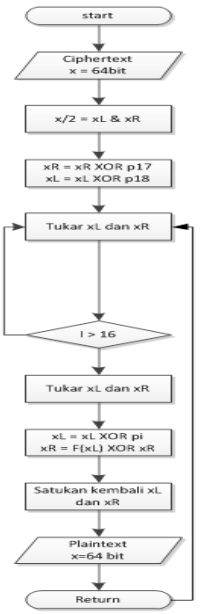
Flowchart pada Gambar 3 menjelaskan cara kerja algoritma Blowfish untuk menghasilkan ciphertext. Berikut adalah proses dari flowchart proses enkripsi Blowfish.



Gambar 3. Proses enkripsi Blowfish

b. *Flowchart* proses dekripsi *blowfish*

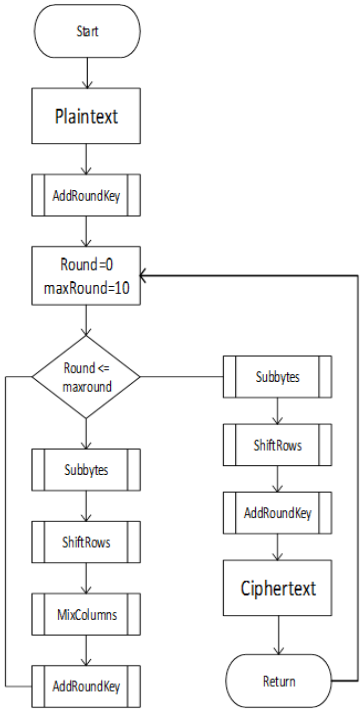
Flowchart pada Gambar. 4 menjelaskan cara kerja algoritma Blowfish untuk menghasilkan Plaintext. Berikut adalah proses dari flowchart proses dekripsi Blowfish.



Gambar 4. Proses Dekripsi Blowfish

c. Flowchart proses Enkripsi AES

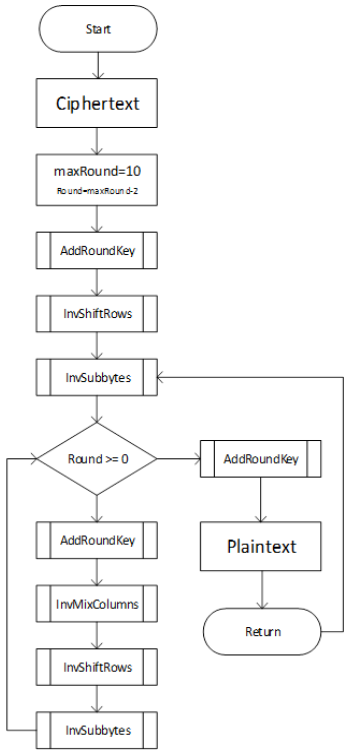
Flowchart pada Gambar 5 menjelaskan cara kerja algoritma AES untuk menghasilkan ciphertext. Berikut adalah proses dari flowchart proses enkripsi.



Gambar 5. Proses enkripsi AES

d. Flowchart proses dekripsi AES

Flowchart pada Gambar.6 menjelaskan cara kerja algoritma AES untuk menghasilkan Plaintext. Berikut adalah proses dari flowchart proses dekripsi AES.



Gambar 6. Proses Dekripsi AES

2.6 Proses Algoritma Blowfish Dan AES

a. proses enkripsi algoritma Blowfish dijelaskan seperti di bawah ini:

```
1.    Start
2.    Plaintext x = 64 bit
3.    x/2 = xL & xR
4.    I = 0
5.    xL = xl XOR Pi; xR = F(xL)
      XOR xR
6.    Tukar xL dan xR
7.    If I = 16 Then
8.      Tukar xL dan xR
9.      xR = xR XOR p17; xL = xL
      XOR p18
10.     Satukan Kembali xL dan xR
11.     Ciphertext x = 64 bit
12.     Return
13.     Kembali ke baris 5
14.   Else
15.     I = I +1
16.     Kembali ke baris 5
17.   End if
```

a. Proses dekripsi algoritma Blowfish dijelaskan seperti di bawah ini:

```
1.    Start
2.    Ciphertext x = 64 bit
3.    x/2 = xL & xR
4.    xR = xR XOR p17; xL = xL XOR
      p18
5.    I = 0
6.    Tukar xL dan xR
7.    If I = 16 Then
8.      Tukar xL dan xR
9.      xL = xl XOR Pi; xR = F(xL)
      XOR xR
10.     Satukan Kembali xL dan xR
11.     Plaintext x = 64 bit
12.     End
13.   Else
14.     I = I +1
15.     Kembali ke baris 6
16.   End if
```

b. Proses Enkripsi Algoritma AES dijelaskan seperti di bawah ini:

```
1.    Start
2.    Penambahan RoundKey
3.    Round = Round +1
4.    Subsitusi Byte data
5.    Geser baris bit data
6.    Acak kolom bit data
7.    Penambahan RoundKey
8.    If Round = 10 Then
9.      Subsitusi byte data
10.     Geser baris bit data
11.     Penambahan RoundKey
12.     Retrurn
13.     Kembali ke Baris 7
14.   Else
15.     Kembali ke baris 3
16.   End if
```

c. Proses Dekripsi Algoritma AES dijelaskan seperti di bawah ini:

```
1.    Start
2.    Penambahan RoundKey
3.    Round = Round +1
4.    Kembalikan subsitusi Byte data
5.    Kembalikan pergeseran baris bit
      data
6.    Kembalikan kolom bit data
7.    Penambahan RoundKey
8.    If Round = 10 Then
9.      Kembalikan subsitusi byte
      data
10.     Kembalikan pergeseran baris
      bit data
11.     Penambahan RoundKey
1.      Retrurn
12.     Kembali ke Baris 7
13.   Else
14.     Kembali ke baris 3
15.   End if
```

3. METODE PENELITIAN

Metode yang digunakan adalah metode sebagai berikut :

a. Studi Literatur

Melalui studi ini penulis memperoleh data atau informasi dengan mengumpulkan, mempelajari dan membaca berbagai referensi baik itu dari buku-buku, jurnal, makalah, internet dan berbagai sumber lainnya yang menunjang dalam penulisan ini.

b. Perancangan

Mengumpulkan data yang akan di perlukan, melakukan analisa dan perancanan untuk tahap implementasi.

c. Pengkodean

Pengkodean dilakukan untuk memudahkan dalammengimplementasikan rancangan aplikasi ke dalam algoritma blowfish dan AES dengan menggunakan bahasa pemrograman java.

d. Implementasi.

Implementasi pada program untuk melakukan proses enkripsi dan deskripsi database dengan menggunakan algoritma blowfish dan AES.

e. Testing atau Pengujian.

Melakukan pengujian dari sistem yang telah dibangun pada tahapan implementasi.

4. HASIL DAN PEMBAHASAN

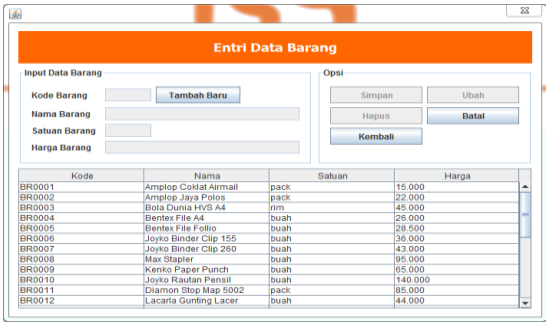
1. Implementasi Program

Implementasi aplikasi ini dibuat dengan menggunakan bahasa pemrograman java berbasis desktop. Adapun minimal spesifikasi komputer yang dibutuhkan untuk mengimplementasikan aplikasi ini adalah Windows XP/7/8 ke atas dan RAM 128.

2. Proses Sistem Aplikasi

a. Tampilan Layar form master

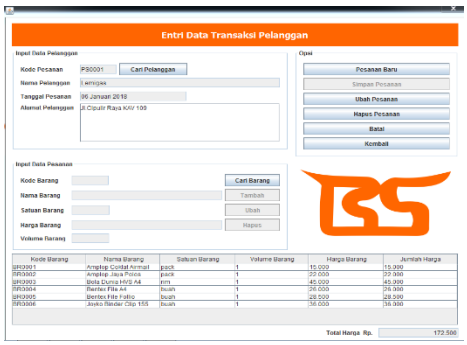
Berikut tampilan *form master* yang berhasil *login* menggunakan *user administrator*, *user* bisa meng-input jenis jenis barang dan harga. Berikut ini Gambar 7 adalah tampilan *form master*.



Gambar 7. Form Master

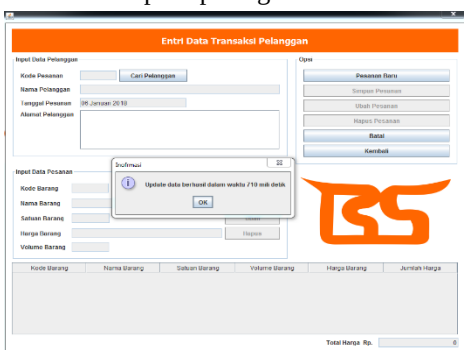
b. Tampilan Form Transaksi

Form transaksi digunakaan untuk input data pelanggan saat menyimpan data baru, mengubah data yang sudah ada atau menghapus data yang sudah ada. Pada saat menyimpan data pelanggan. Data yang akan disimpan sebelumnya di enkripsi terlebih dahulu sebelum dimasukan ke *database* dan saat ingin menampilkan data kembali dari *database* dilakukan dekripsi terlebih dahulu sebelum akhirnya ditampilkan di *form*. Berikutnya hasil pengujian *form* transaksi.



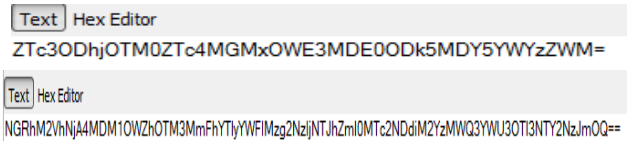
Gambar 8. Input Form Transaksi

Setelah itu klik simpan untuk menyimpan data pelanggan yang telah di-input dan akan muncul pesan berhasil seperti pada gambar 9.



Gambar 9. Transaksi berhasil disimpan

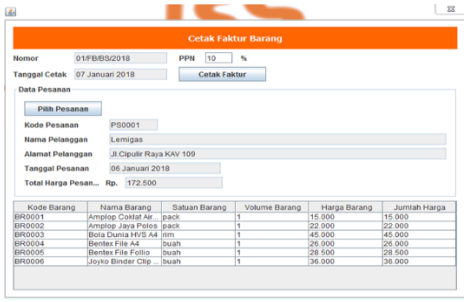
Setelah berhasil tersimpan, maka data akan dienkripsi. Seperti pada gambar 10 berikut ini



Gambar 10. Data yang tersimpan di database berbentuk cipher

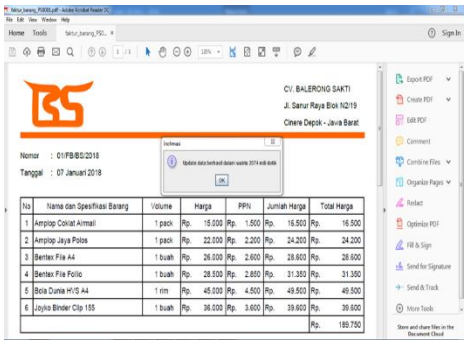
c. Tampilan Form Cetak

Pada form cetak user dapat mencetak hasil faktur barang pada setiap transaksi dengan menginput nomor pesanan, seperti pada gambar 11



Gambar 11. Tampilan form cetak

Setelah klik tombol cetak faktur maka akan tampil ke form, seperti pada gambar 12



Gambar 12. Tampilan Hasil Cetak

d. Tabel Pengujian

Dalam pengujian kali ini akan di uji coba, untuk transaksi proses enkripsi dan dekripsi, dari pengujian waktu proses untuk enkripsi dan dekripsi tersebut akan ditampilkkan rata-rata waktu proses yang dilakukan.

Tabel 1. Hasil Proses Enkripsi

NO	Jumlah Barang	Ukuran(byte)	Waktu Proses Enkripsi (ms)
1.	5 Barang Transaksi	16	142
2.	10 Barang Transaksi	16	222
3.	15 Barang Transaksi	16	324
4.	20 Barang Transaksi	16	365
5.	25 Barang Transaksi	16	428
	Rata-rata	16	296,2

Tabel 2. Hasil Proses Dekripsi

NO	Jumlah Barang	Ukuran(byte)	Waktu Proses Dekripsi (ms)
1.	5 Transaksi Cetak	16	1189
2.	10 Barang Transaksi	16	1239
3.	15 Barang Transaksi	16	1322
4.	20 Barang Transaksi	16	1561
5.	25 Barang Transaksi	16	3391
	Rata-rata	16	1740,4

5. KESIMPULAN

Sesuai dengan pembahasan penulis menarik kesimpulan dan memberikan dianalisa dan dibuat pada aplikasi "IMPLEMENTASI PENGAMANAN DATABASE MENGGUNAKAN METODE BLOWFISH DAN AES PADA PERUSAHAAN CV.BALERONG SAKTI" hasil pengujian dan analisa yang telah dilakukan dapat disimpulkan bahwa :

a. Aplikasi kriptografi ini menggunakan algoritma *blowfish* dan AES (*Advanced Encryption Standard*) sebagai sistem keamanan *database* aplikasi ini.
b. Mengamankan *database* perusahaan menjadi rahasia agar tidak bisa di ketahui oleh pihak yang tidak bertanggungjawab.
c. Dengan adanya aplikasi kriptografi ini, proses keamanan *database* menjadi lebih aman.

6. DAFTAR PUSTAKA

[1] Aulia Trianggana ,Dimas., & Latipa Sari, Herlina,. 2015. *Analisa Perbandingan Kinerja Algoritma Blowfish dan Algoritma Twofish Pada Proses Enkripsi Dan Dekripsi*. Bengkulu : Jurnal Volume 2 Nomor 1.

[2] Ariyus, D., 2006. *Kriptografi Keamanan Data dan Komunikasi*. Yogyakarta, Graha Ilmu

[3] Ariyus, D., 2008. *Pengantar Kriptografi*. Yogyakarta, ANDI.

[4] C.A. van Tilborg, Henk., 2000. *Fundamentals of Cryptology*, Kluwer Academic Publishers.

[5] Et, Al, Ramdhansya.,2014. *Implementasi Advanced Encryption Standart (AES) pada Sistem Kunci Elektronik Kendaraan Berbasis Sistem Operasi Android dan Mikrokontroler Arduino*. Bandung : Jurnal Universitas Telkom.

[6] Fahrizon, Arief, Sugianto.,2016. *Implementasi Pengamanan Data Nasabah Menggunakan Metode AES-128 di PT. Central Capital Futures*. Jakarta : Jurnal Universitas Budi Luhur.

[7] Foelyati, Rika., 2007. *Analisis Perrbandingan unjuk Kerja Algoritma Lorentz, Julia Set dan Tent Function Debagai Algoritma Chaotic*. Bandung : Tugas Akhir STTTelkom.

[8] Natsir, Mohamad., 2017. *Pengembangan Prototype Sistem Kriptografi Untuk Enkripsi Dan Dekripsi Data Office Menggunakan Metode Blowfish Dengan Bahasa Pemrograman Java*. Jakarta : Jurnal Format Vol.6 No 1.

[9] Pabokory, Fresly Nandar, dkk., 2015.

Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen , Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard (AES). Samarinda Utara : Jurnal Informatika Mulawarman Vol.10 No 1.

[10] Rifkie, Primartha., 2013. *Penerapan Enkripsi dan Dekripsi File Menggunakan Algoritma Advanced Encryption Standard (AES)*. Palembang : Journal of Research in computer science and application Vol.2 No 1.

[11] Schneier, Bruce., 1996. *Applied Cryptography, Second Edition*, John Wiley & Son, New York.

[12] Solihin, Muhammad., 2013. *Perancangan Sistem Pengamanan dan Kompresi Data Teks dengan Fibonacci Encoding dan Algoritma Shannon-Fano serta Algoritma Deflate*. Skripsi. Universitas Sumatera Utara.

[13] Suriski, Sitinjak., 2010. *Aplikasi Kriptografi File Menggunakan Algoritma Blowfish*. Yogyakarta : Jurnal Univeritas Veteran Yogakarta.

[14] Susanto., 2017. *Implementasi Keamanan Data Menggunakan Algoritma Blowfish Pada Sistem Informasi*. Lubuklinggau : Jurnal SIMETRIS, Vol 8 No 1.

[15] Wardoyo ,Siswo, Rian Fahrizal, & Zaldi Imanullah., 2014. *Aplikasi Teknik Enkripsi Dan Dekripsi File Dengan Algoritma Blowfish Pada Perangkat Mobile Berbasis Android*. Serang : Jurnal Sultan Ageng Tirtayasa.