IMPLEMENTASI ALGORITMA BLOWFISH UNTUK PENGAMANAN FILE PDF

Fritz Gamaliel[1], P. Yudi Dwi Arliyanto[2]

[1,]Program Studi Teknologi Rekayasa Perangkat Lunak, Politeknik META Industri Cikarang
[2,]Program Studi Teknik Industri, Politeknik META Industri Cikarang

Jln. Inti 1 Blok C1 No 7, Lippo Cikarang 17550
[1] fritzgamaliel@politeknikmeta.ac.id, [2] yudi@politeknikmeta.ac.id

Abstract

In communicating confidential information over the internet, there is a challenge, one of which is the possibility of unauthorized parties accessing the content of that confidential information. This results in the sender having to protect the confidential information as one of the efforts to make it more difficult for unauthorized parties to access it. Cryptography is a method to maintain the confidentiality aspects of information. In this research, confidential information is secured using a combination of alphanumeric passwords and blowfish cryptography. The application is implemented using the PHP programming language. With the presence of this research activity, it is expected that the application can increase the level of difficulty for unauthorized parties in accessing confidential information.

Keywords : *communication, password, cryptography, PHP*

Abstrak

Komunikasi antara sender dan receiver dapat dilaksanakan baik secara verbal maupun secara non-verbal. Dalam mengkomunikasikan informasi yang bersifat confidential melalui jaringan internet, terdapat kendala salah satunya yaitu adanya kemungkinan pihak yang tidak berkepentingan mengakses konten informasi confidential tersebut. Hal tersebut mengakibatkan sender harus mengamankan informasi yang bersifat confidential tersebut sebagai salah satu upaya mempersulit pihak yang tidak berkepentingan dalam mengaksesnya. Kriptografi merupakan metode untuk menjaga aspek confidentiality informasi. Dalam penelitian ini, informasi yang bersifat confidential tersebut diamankan dengan menggunakan kombinasi password alphanumeric dan kriptografi blowfish. Aplikasi diimplementasikan dengan menggunakan bahasa pemograman PHP. Dengan hadirnya kegiatan penelitian ini diharapkan aplikasi dapat menambah tingkat kesulitan kepada pihak yang tidak berkepentingan dalam mengakses informasi yang bersifat confidential.

Kata kunci : *komunikasi, password, kriptografi, PHP*

1. PENDAHULUAN

Komunikasi antara sender dan receiver bisa berupa verbal atau non-verbal. Semakin banyak komunikasi yang terjadi antara sender dan receiver, maka semakin harus memperhatikan aspek keamanannya baik aspek confidentiality, integrity, maupun availability. Menurut Alriady Tri Putra dkk, berbagai ancaman di dunia maya membuat orang khawatir akan keamanan informasi yang dikirimnya [1]. Menurut Saputra Dwi Nurcahya, bisa saja informasi yang sedang dikirim melalui media transmisi itu dicuri atau diubah oleh penyadap atau cracker untuk kepentingan tertentu [2]. Menurut Desi Fitriani Ningrum dkk,

apabila data tidak dilindungi maka orang lain dapat dengan mudah mengambil data atau informasi yang dimiliki seseorang [3]. Menurut Sri Vivi Wahdini dkk, korporasi berbasis digital memang menerima detail pribadi milik pelanggan, dan tentu saja para pelanggan mempercayai data penting itu untuk dijaga agar tetap aman dan tidak jatuh di tangah orang yang salah [4]. Menurut Siti Sofia dkk, masalah keamanan data menyebabkan kerugian tidak hanya materil tetapi juga psikis korban, dimana mereka bisa saja mendapatkan perlakuan diskriminasi di lungkungan masyarakat [5].

Kriptografi merupakan metode untuk menjaga aspek confidentiality informasi. Menurut Dimas Mayoni Aji Sasono dkk, kriptografi dibagi menjadi dua jenis yaitu kriptografi klasik dan kriptografi modern [6]. Kriptografi klasik menggunakan teknik substitusi, transposisi, kombinasi keduanya secara kompleks melatarbelakangi terbentuknya berbagai macam kriptografi modern. Contohnya adalah Caesar cipher, vigenere cipher, dan hill cipher. Kriptografi modern terdiri dari kriptografi simetris, kriptografi asimetris. Kriptografi simetris memakai kunci enkripsi yang sama dengan kunci dekripsi. Contohnya adalah algoritma DES (*Data Encryption Standard*), AES (*Advanced Encryption Standard*), dan Blowfish. Kriptografi asimetris memakai kunci enkripsi yang berbeda dengan kunci dekripsi. Contohnya adalah algoritma RSA (*Riverst Shamir Adleman*).

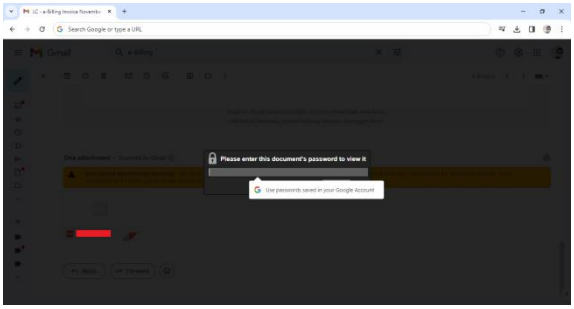
Dari halaman website Microsoft (https://support.microsoft.com/id-id/windows/ekstensi-nama-file-umum-di-windows-da4a4430-8e76-89c5-59f7-1cdbbc75cb01) kita dapat melihat bahwa terdapat sejumlah jenis file komputer yang dapat digunakan untuk saling bertukar informasi, salah satunya adalah file PDF yang digunakan oleh bagian billing customer salah satu perusahaan pengembang properti. Untuk mengatasi kemungkinan pihak yang tidak berkepentingan mengakses konten PDF yang berisi informasi confidential, maka file PDF tersebut dipassword oleh bagian billing customer sebelum dikirimkan kepada customer melalui jaringan internet. Namun hal tersebut masih terdapat kekurangan yang salah satunya adalah pihak yang tidak berkepentingan dapat langsung mengakses konten PDF yang berisi informasi confidential tersebut hanya dengan mengetahui passwordnya. Hal tersebut melatarbelakangi penelitian bagaimana jika mengenkripsi kontennya terlebih dahulu baru kemudian mempasswordnya sehingga dengan demikian membuat pihak yang tidak berkepentingan harus mendapatkan password dan kunci dekripsi nya terlebih dahulu untuk dapat mengakses konten PDF yang berisi informasi confidential tersebut. Hasil dari penelitian ini berupa sebuah aplikasi yang mana aplikasi tersebut mampu melakukan enkripsi dan dekripsi file PDF. Konten asli (plainteks) yang berisi informasi confidential akan dienkripsi ke dalam bentuk file cipher dengan menggunakan teknik enkripsi blowfish. Kemudian ketika file cipher ingin diketahui konten aslinya (plainteks) maka harus didekripsi dengan menggunakan teknik dekripsi blowfish.

2. METODOLOGI PENELITIAN

Mengenai metode penelitian yang dilakukan peneliti ada beberapa metode yang dilakukan, yaitu:

2.1. Observasi

Peneliti menggunakan metode observasi dengan cara langsung terjun ke lapangan untuk mengamati permasalahan yang terjadi dalam lapangan secara langsung. Adapun observasi yang dilaksanakan di salah satu perusahaan pengembang properti, khususnya pada bagian billing customer.



Gambar 1. Observasi

2.2. Studi Pustaka

Peneliti menggunakan metode studi pustaka dengan cara menelaah pustaka-pustaka terkait dengan penelitian.

Pada penelitian sebelumnya yang dilaksanakan oleh Kristina Pakpahan mengimplementasikan pengamanan file DOCX. Penelitian tersebut dilaksanakan untuk mengamankan file DOCX. Pada penelitian tersebut menggunakan algoritma S-DES. Adapun pada penelitian kami mengamankan file PDF.

Pada penelitian kami menggunakan algoritma blowfish.[7]

Pada penelitian sebelumnya yang dilaksanakan oleh Arif Amrulloh dan EIH Ujianto mengimplementasikan pengamanan plain teks. Penelitian tersebut dilaksanakan untuk mengamankan plain teks. Pada penelitian tersebut menggunakan algoritma Vigenere. Adapun pada penelitian kami mengamankan file PDF. Pada penelitian kami menggunakan algoritma blowfish. [8]

Pada penelitian sebelumnya yang dilaksanakan oleh Chyquitha Danuputri, Nico Santosa, Fernando Dedi Samuel mengimplementasikan pengamanan plain teks. Penelitian tersebut dilaksanakan untuk mengamankan plain teks. Pada penelitian tersebut menggunakan algoritma Vigenere. Adapun pada penelitian kami mengamankan file PDF. Pada penelitian kami menggunakan algoritma blowfish. [9]

Pada penelitian sebelumnya yang dilaksanakan oleh Muhammad Azhari, Dadang Iskandar Mulyana, Faizal Joko Perwitosari, Firhan Ali mengimplementasikan pengamanan dokumen. Penelitian tersebut dilaksanakan untuk mengamankan dokumen. Pada penelitian tersebut menggunakan algoritma AES. Adapun pada penelitian kami mengamankan file PDF. Pada penelitian kami menggunakan algoritma blowfish. [10]

Pada penelitian sebelumnya yang dilaksanakan oleh Sekar Putri Ananda, Saepul Lukman dan Irfan mengimplementasikan pengamanan berbagai jenis dokumen digital (PDF, DOCX, PPTX, XLSX, dan TXT). Penelitian tersebut dilaksanakan untuk mengamankan berbagai jenis dokumen digital. Pada penelitian tersebut menggunakan algoritma AES. Adapun pada penelitian kami mengamankan file PDF. Pada penelitian kami menggunakan algoritma blowfish. [11]

Pada penelitian sebelumnya yang dilaksanakan oleh Raka Febrianto dan Sejati Waluyo mengimplementasikan pengamanan database penilaian karyawan KJPP NDR. Penelitian tersebut dilaksanakan untuk mengamankan database penilaian karyawan KJPP NDR. Pada penelitian tersebut menggunakan algoritma AES. Adapun pada penelitian kami mengamankan file PDF. Pada penelitian kami menggunakan algoritma blowfish. [12]

Pada penelitian sebelumnya yang dilaksanakan oleh Mohammad Harun Alfirdaus dan kawan-kawan mengimplementasikan aplikasi enkripsi dekripsi. Penelitian tersebut dilaksanakan untuk mengamankan plain teks. Pada penelitian tersebut menggunakan algoritma Caesar. Adapun pada penelitian kami mengamankan file PDF. Pada penelitian kami menggunakan algoritma blowfish. [13]

Pada penelitian sebelumnya yang dilaksanakan oleh Fefiana Diny Hermawati dan kawan-kawan mengimplementasikan pengamanan e-voting. Penelitian tersebut dilaksanakan untuk mengamankan e-voting. Pada penelitian tersebut menggunakan algoritma AES. Adapun pada penelitian kami mengamankan file PDF. Pada penelitian kami menggunakan algoritma blowfish. [14]

Pada penelitian sebelumnya yang dilaksanakan oleh Roman Gusmana, Haryansyah, Adimulya Dyas Wibisono mengimplementasikan pengamanan plain teks. Penelitian tersebut dilaksanakan untuk mengamankan plain teks. Pada penelitian tersebut menggunakan algoritma Hill Cipher. Adapun pada penelitian kami mengamankan file PDF. Pada penelitian kami menggunakan algoritma blowfish. [15]

Pada penelitian sebelumnya yang dilaksanakan oleh Yosua Situmeang, Alfonsus Situmorang, Posma Lumbanraja mengimplementasikan pengamanan plain teks pada QR Code. Penelitian tersebut dilaksanakan untuk mengamankan plain teks pada QR Code. Pada penelitian tersebut menggunakan algoritma AES. Adapun pada penelitian kami mengamankan file PDF. Pada penelitian kami menggunakan algoritma blowfish. [16]

Pada penelitian sebelumnya yang dilaksanakan oleh Apriliana Tumanggor, Humuntal Rumapea, Arina Silalahi mengimplementasikan pengamanan file PDF dokumen keuangan CV Multi Kreasi Bersama. Penelitian tersebut dilaksanakan untuk mengamankan file PDF dokumen keuangan CV Multi Kreasi Bersama. Pada penelitian tersebut menggunakan algoritma AES. Adapun pada penelitian kami mengamankan file PDF. Pada penelitian kami menggunakan algoritma blowfish. [17]

Pada penelitian sebelumnya yang dilaksanakan oleh Fadlullah Fadlullah dan kawan kawan mengimplementasikan pengamanan password login. Penelitian tersebut dilaksanakan untuk mengamankan password login. Pada penelitian tersebut menggunakan algoritma AES. Adapun pada penelitian kami mengamankan file PDF. Pada penelitian kami menggunakan algoritma blowfish. [18]

Pada penelitian sebelumnya yang dilaksanakan oleh Melenia Bayu Aryanto dan

kawan kawan mengimplementasikan pengamanan file (TXT, DOCX, PPT). Penelitian tersebut dilaksanakan untuk mengamankan file. Pada penelitian tersebut menggunakan algoritma AES. Adapun pada penelitian kami mengamankan file PDF. Pada penelitian kami menggunakan algoritma blowfish. [19]

Pada penelitian sebelumnya yang dilaksanakan oleh Yusuf Ramadhan Nasution, Heri Santoso, Siti Wahyuni Amalia mengimplementasikan pengamanan file PDF. Penelitian tersebut dilaksanakan untuk mengamankan file PDF. Pada penelitian tersebut menggunakan algoritma Vernam. Adapun pada penelitian kami mengamankan file PDF. Pada penelitian kami menggunakan algoritma blowfish. [20]

Pada penelitian sebelumnya yang dilaksanakan oleh Abdul Halim Hasugian, Yusuf Ramadhan Nasution, Nadyah Almirah Simanjuntak mengimplementasikan pengamanan pesan. Penelitian tersebut dilaksanakan untuk mengamankan pesan. Pada penelitian tersebut menggunakan kombinasi kriptografi dan steganografi. Adapun pada penelitian kami mengamankan file PDF. Pada penelitian kami menggunakan algoritma blowfish. [21]

2.3. Perancangan

Perancangan aplikasi adalah pembuatan rancangan aplikasi yang berkaitan dengan fungsionalitas. Algoritma Blowfish terdiri atas 2 bagian yaitu ekspansi kunci dan enkripsi data.

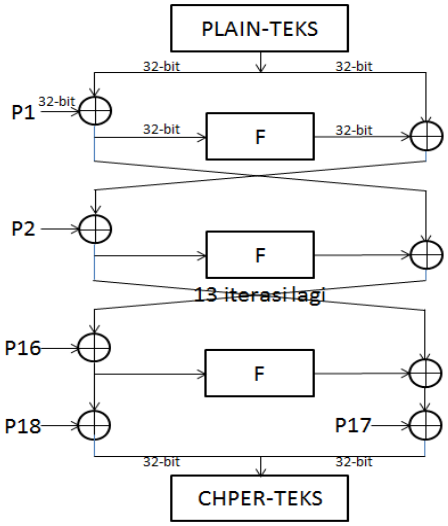
Ekspansi Kunci berfungsi merubah kunci (minimum 32-bit, maksimum 448-bit) menjadi beberapa array subkunci (subkey) dengan total 4168 byte (18x32-bit untuk P-array dan 4x256x32-bit untuk S-box sehingga totalnya 33344 bit atau 4168 byte). Langkah-langkah perhitungan atau pembangkitan subkunci tersebut adalah sebagai berikut:

1) Inisialisasi P-array yang pertama dan juga empat S-box, berurutan, dengan string yang telah pasti. String tersebut terdiri dari digit-digit heksadesimal dari phi, tidak termasuk angka tiga di awal. Contoh :
   P1= 0x243f6a88
   P2= 0x85a308d3
   P3= 0x13198a2e
   P4= 0x03707344
   dan seterusnya sampai S-box yang terakhir
2) XOR-kan P1 dengan 32-bit awal kunci, XOR-kan P2 dengan 32-bit berikutnya dari kunci, dan seterusnya untuk semua bit kunci. Ulangi siklus seluruh bit kunci secara berurutan sampai seluruh P-array ter-XOR-kan dengan bit-bit kunci. Atau jika disimbolkan :P1 = P1⊕K1, P2 = P2⊕K2, P3 = P3⊕K3, . . . P14 = P14⊕K14, P15 = P15⊕K1, . . .P18 = P18⊕K4. Keterangan :⊕ adalah simbol untuk XOR.
3) Enkripsikan string yang seluruhnya nol (all-zero string) dengan algoritma Blowfish, menggunakan subkunci yang telah dideskripsikan pada langkah 1 dan 2.
4) Gantikan P1 dan P2 dengan keluaran dari langkah 3.
5) Enkripsikan keluaran langkah 3 menggunakan algoritma Blowfish dengan subkunci yang telah dimodifikasi.
6) Gantikan P3 dan P4 dengan keluaran dari langkah 5.
7) Lanjutkan langkah-langkah di atas, gantikan seluruh elemen P-array dan kemudian keempat S-box secara berurutan, dengan hasil keluaran algoritma Blowfish yang terus-menerus berubah.
   Total keseluruhan, terdapat 521 iterasi untuk menghasilkan subkunci-subkunci dan membutuhkan memori sebesar 4KB.

Pseudocode enkripsi blowfish adalah sebagai berikut

```
For i=1 to 16{
RE(i)=LE(i-1) ⊕ P(i);
LE(i)=F[RE(i)] ⊕ RE(i-1);
}
LE(17)=RE(16) ⊕ P(18);
RE(17)=LE(16) ⊕ P(17);
```

Di mana RE(i) adalah 32-bit pecahan input sebelah kanan pada putaran ke-i, LE(i) adalah 32-bit pecahan input sebelah kiri pada putaran ke-i, dan P(i) adalah array P dengan indeks ke-i. Untuk lebih jelasnya, gambaran tahapan pada jaringan feistel yang digunakan Blowfish adalah seperti pada Gambar di bawah ini.

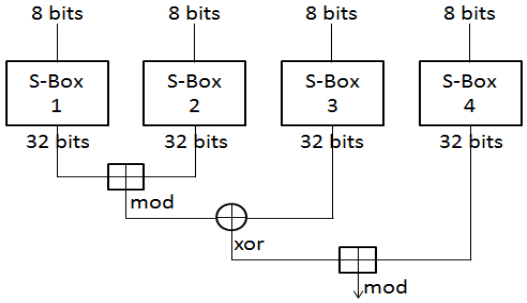


Gambar 2. Enkripsi Pada Algoritma Blowfish

Pada pseudocode tersebut, telah dituliskan mengenai penggunaan fungsi F. Fungsi F adalah: bagi XL menjadi empat bagian 8-bit: a,b,c dan d.

$F(XL) = ((S_{1,a} + S_{2,b} \bmod 2^{32}) \text{ XOR } S_{3,c}) + S_{4,d} \bmod 2^{32}$

Karena menggunakan Addition Modulo 2^{32}, maka hasil penjumlahan maksimal adalah FFFFFFFF (jika lebih dari itu, maka restart dari 0). Agar dapat lebih memahami fungsi F, tahapannya dapat dilihat pada Gambar di bawah ini.

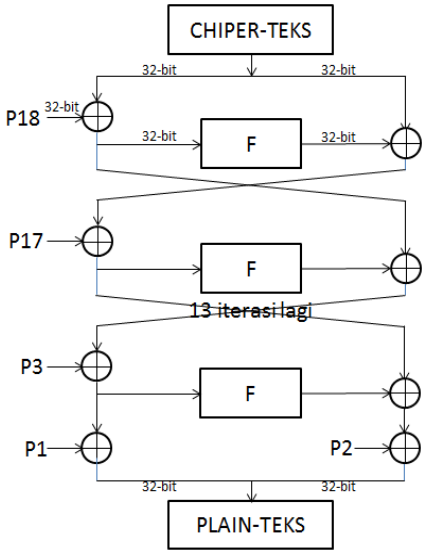


Gambar 3. Fungsi F Pada Algoritma Blowfish

Dekripsi blowfish sama persis dengan enkripsi blowfish, kecuali bahwa P1, P2,..., P18 digunakan pada urutan yang berbalik (reverse). Algoritmanya dapat dinyatakan dengan pseudocode sebagai berikut:

For i=1 to 16{
RD(i)=LD(i-1) P(19-i);
LD(i)=F[RD(i)] RD(i-1);
}
LD(17)=RD(16) P(1);
RD(17)=LD(16) P(2);

Di mana RD(i) adalah 32-bit pecahan input sebelah kanan pada putaran ke-i, LD(i) adalah 32-bit pecahan input sebelah kiri pada putaran ke-i, dan P(i) adalah array P dengan indeks ke-i. Blok diagram dekripsi seperti pada Gambar di bawah ini.



Gambar 4. Dekripsi Pada Algoritma Blowfish

3. HASIL DAN PEMBAHASAN

3.1 Tampilan Halaman Enkripsi

Halaman enkripsi digunakan oleh user untuk mengenkripsi konten asli file PDF. Tampilan halaman enkripsi dapat dilihat pada gambar berikut.

Gambar 5. Tampilan Halaman Enkripsi

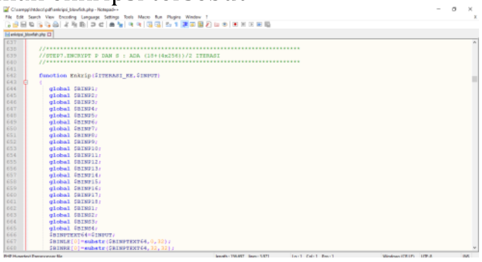
Seperti dapat dilihat pada tampilan halaman enkripsi tersebut diakses melalui alamat berikut

http://localhost/pdf/enkripsi_blowfish.php?Key=00001111001101010000111100110101000011110011010100001111001101010000111100110101000011110011010100001111001101010000111100110101000011110011010100001111001101010000111100110101000011110011010100001111001101010000111100110101000011110011010100001111001101010000111100110101000011110011010

100001111001101010000111100110101000
011110011010100001111001101010000111
100110101000011110011010100001111001101
010000111100110101000011110011010100
001111001101010000111100110101000011110
0110101

File PDF yang hendak dienkripsi diletakkan ke dalam 1 folder PDF dan kemudian dienkripsi blowfish dengan menggunakan kunci biner sepanjang 448 bit

Adapun berikut adalah potongan kode program PHP yang digunakan dalam pembuatan halaman enkripsi tersebut



Gambar 6. Kode Program PHP Halaman Enkripsi

3.2 Tampilan Halaman Dekripsi

Halaman dekripsi digunakan oleh user untuk mendekripsi konten file cipher. Tampilan halaman dekripsi dapat dilihat pada gambar berikut.

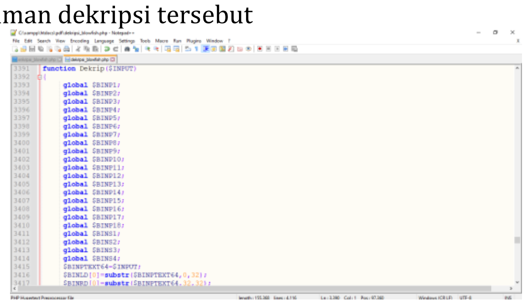
Gambar 7. Tampilan Halaman Dekripsi

Seperti dapat dilihat pada tampilan halaman dekripsi tersebut diakses melalui alamat berikut

http://localhost/pdf/dekripsi_blowfish.php
?Key=0000111100110101000011110011010100
001111001101010000111100110101000011
1100110101000011110011010100001111001
1010100001111001101010000111100110101
0000111100110101000011110011010100001
1110011010100001111001101010000111100
1101010000111100110101000011110011010
1000011110011010100001111001101010000
111100110101000011110011010100001111
0011010100001111001101010000111100110101000011110
011010100001111001101010000111100110101
010000111100110101000011110011010100
001111001101010000111100110101000011110
0110101

File PDF yang hendak didekripsi diletakkan ke dalam 1 folder PDF dan kemudian didekripsi blowfish dengan menggunakan kunci biner sepanjang 448 bit

Adapun berikut adalah potongan kode program PHP yang digunakan dalam pembuatan halaman dekripsi tersebut



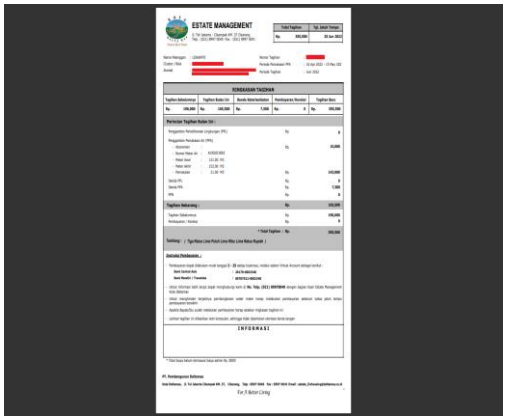
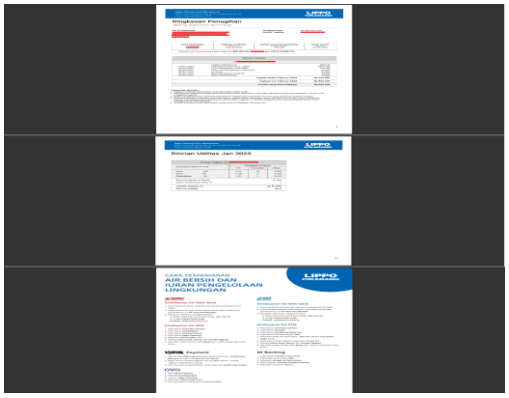
Gambar 8. Kode Program PHP Halaman Dekripsi

3.3 Tabel Pengujian Enkripsi Dekripsi

Berikut tabel pengujian enkripsi dekripsi yang telah dilaksanakan

TABEL I. TABEL PENGUJIAN ENKRIPSI DEKRIPSI

No	Keterangan
1	 **Ukuran File PDF:** 429KB **Total Waktu Enkripsi:** 0.96 menit **Ukuran File PDF Hasil Enkripsi:** 3430 KB **Total Waktu Dekripsi:** 0.94 menit **Ukuran File PDF Hasil Dekripsi:** 429KB

2	 **Ukuran File PDF:** 37KB **Total Waktu Enkripsi:** 0.09 menit **Ukuran File PDF Hasil Enkripsi:** 292 KB **Total Waktu Dekripsi:** 0.08 menit **Ukuran File PDF Hasil Dekripsi:** 37KB
3	 **Ukuran File PDF:** 336KB **Total Waktu Enkripsi:** 0.80 menit **Ukuran File PDF Hasil Enkripsi:** 2688KB **Total Waktu Dekripsi:** 0.77 menit **Ukuran File PDF Hasil Dekripsi:** 336KB

4. Kesimpulan dan Saran

Dari penelitian yang telah dilaksanakan, diambil kesimpulan sebagai berikut:

1) Algoritma blowfish merupakan salah satu algoritma kriptografi yang dapat digunakan untuk mengenkripsi maupun mendekripsi file PDF
2) Dengan mengenkripsi konten, maka pihak yang tidak berkepentingan masih harus mengeluarkan upaya untuk mendekripsi konten

Daftar Pustaka:

[1] A. T. Putra, P. L. L.B., and F. Fattah, "Penerapan Enkripsi dan Deskripsi file menggunakan algoritma Twofish," *Bul. Sist. Inf. dan Teknol. Islam*, vol. 2, no. 2, pp. 72–77, 2021, doi: 10.33096/busiti.v2i2.784.

[2] S. D. Nurcahya, K. Gedong, P. Rebo, and K. Private, "Perancangan Aplikasi Enkripsi Dan Dekripsi File Dengan Algoritma Kriptografi Berbasis Web," vol. 5, no. 4, pp. 728–735, 2022.

[3] D. F. Ningrum, M. Tahir, W. D. Angelina, and A. Permatasari, Eliza Rofiq, Fifi Rinazah Hidayati, Miftakhul Sahroh, Fatimatus Setiawan, "Implementasi Keamanan Data menggunakan Kriptografi Caesar Chiper," *ADIJAYA J. Multidisiplin*, vol. 01, no. 02, pp. 388–396, 2023.

[4] S. V. Wahdini, D. Hartama, I. O. Kirana, Poningsih, and Sumarno, "Pengamanan Data Pelanggan dan Penjualan Menggunakan Implementasi Algoritma Kriptografi," *J. Informatics Manag. Inf. Technol.*, vol. 1, no. 3, pp. 101–107, 2021.

[5] S. Sofia, E. T. Ardianto, N. Muna, and S. Sabran, "Analisis Aspek Keamanan Informasi Data Pasien Pada Penerapan RME di Fasilitas Kesehatan," *J. Rekam Med. Manaj. Inf. Kesehat.*, vol. 1, no. 2, pp. 94–103, 2022, doi: 10.47134/rmik.v1i2.29.

[6] D. M. A. Sasono, M. Tahir, F. A. M. V., M. Azizah, L. F. Utami, and N. Septiana, "Perbandingan Kriptography Klasik Caesar Cipher Dengan Kriptography Modern Aes Dalam Tingkat Keamanan Jaringan Komputer," *J. Informasi, Sains dan Teknol.*, vol. 6, no. 1, pp. 72–77, 2023, doi: 10.55606/isaintek.v6i1.93.

[7] K. Pakpahan, S. Samosir, and J. A. Simatupang, "Pengamanan File DOCX Menerapkan Algoritma Simlified Data Encryption Standart (DES)," *... Komput. Sains ...*, pp. 409–414, 2020, [Online]. Available: https://www.prosiding.seminar-id.com/index.php/sainteks/article/view/472.

[8] A. Amrulloh and E. I. H. Ujianto, "Kriptografi Simetris Menggunakan Algoritma Vigenere Cipher," *J. CoreIT*, vol. 5, no. 2, pp. 71–77, 2019.

[9] C. Danuputri, N. Santosa, and F. D. Samuel, "Pengujian Pengembangan Terhadap Algoritma Vigenere Key Kriptografi," *J. Resist. (Rekayasa Sist. Komputer)*, vol. 5, no. 1, pp. 26–37, 2022, doi: 10.31598/jurnalresistor.v5i1.822.

[10] M. Azhari, D. I. Mulyana, F. J. Perwitosari, and F. Ali, "Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES)," *J. Pendidik. Sains dan Komput.*, vol. 2, no. 1, pp. 163–171, 2022.

[11] S. P. Ananda, S. Lukman, and Irfan, "Analisa Metode Kriptografi Modern Advance Encryption Standar (AES) 128 Bit dalam Mengenkripsi dan Mendekripsi File Dokumen Digital," *J. Ilm. Komputasi*, vol. 21, no. September, pp. 333–344, 2022.

[12] R. Febrianto and S. Waluyo, "IMPLEMENTASI ALGORITME KRIPTOGRAFI ADVANCED ENCRYPTION STANDARD (AES-256) UNTUK MENGAMANKAN DATABASE PENILAIAN KARYAWAN PADA KJPP NDR," *Bit (Fakultas Teknol. Inf. Univ. Budi Luhur)*, vol. 20, no. 1, pp. 44–49, 2023.

[13] M. H. Alfirdaus, M. Tahir, and N. E. Dewanti, "Perancangan Aplikasi Enkripsi Deskripsi Mengunakan Metode Caesar Chiper Berbasis Web," *J. Tek. Mesin, Ind. Elektro dan Inform.*, vol. 2, no. 2, 2023.

[14] F. D. Hermawati *et al.*, "Keamanan E-Voting Di Indonesia Melalui Pemanfaatan Kriptografi Pada Sistem AES (Advance Encryption Standard)," *J. Tek. Mesin, Ind. Elektro dan Inform.*, vol. 2, no. 2, pp. 45–56, 2023.

[15] R. Gusmana, Haryansyah, and A. D. Wibisono, "Implementasi Algoritma Hill Cipher Menggunakan Kunci Matriks 2x2 Dalam Mengamankan Data Teks," *Gener. J.*, vol. 7, no. 3, pp. 31–39, 2023.

[16] Y. Situmeang, A. Situmorang, and P. Lumbanraja, "Implementasi Algoritma AES Rijndael Pada QR Code Untuk Validasi dan Keamanan Data Penerima Bantuan Sosial di Kelurahan Padang Bulan Selayang II," *Methotika J. Ilm. Tek. Inform.*, vol. 3, no. 2, pp. 21–30, 2023.

[17] A. Tumanggor, H. Rumapea, and A. Silalahi, "Implementasi Algoritma Advance Encryption Standard (AES) Pada Keamanan Dokumen Keuangan (Studi Kasus: CV. Multikreasi Bersama)," *Methotika J. Ilm. Tek. Inform.*, vol. 3, no. 1, pp. 83–90, 2023.

[18] F. Fadlullah *et al.*, "Implementasi Algoritma AES pada Autentikasi Login Sistem Informasi," *J. Bintang Pendidik. Indones.*, vol. 1, no. 2, pp. 251–263, 2023.

[19] M. B. Aryanto, M. Tahir, S. I. Devita, Z. N. Mustofa, Q. Ainiyah, and S. Sundoro, "Implementasi Enkrip Dan Dekrip File Menggunakan Metode Advance Encryption Standard (AES-128)," *JUISIK*, vol. 3, no. 1, pp. 89–104, 2023.

[20] Y. R. Nasution, H. Santoso, and S. W. Amalia, "Penerapan Algoritma Vernam dalam Mengamankan Dokumen PDF," *JIRE (Jurnal Inform. Rekayasa Elektron.*, vol. 6, no. 1, pp. 37–46, 2023.

[21] A. H. Hasugian, Y. R. Nasution, and N. A. Simanjuntak, "Kombinasi Algoritma Beaufort Cipher Dan Lsb2Bit Untuk Keamanan File Teks," *J. Inform. dan Rekayasa Elektron.*, vol. 6, no. 1, pp. 28–36, 2023, doi: 10.36595/jire.v6i1.730.