JNATIA Volume 1, Nomor 1, November 2022
Jurnal Nasional Teknologi Informasi dan Aplikasinya

Aplikasi Keamanan *E-Commerce* Berbasis Web Menggunakan Metode Algoritma Blowfish

Hairullah[a1], **Cokorda Rai Adi Pramartha** [b2], **Ida Ayu Gde Suwiprabayanti Putra** [a3]

Program Studi Teknik Informatika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Udayana, Badung, Bali, Indonesia

[b]Net-Centric Computing Laboratory, Universitas Udayana

hairullah.hairul2019@gmail.com
cokorda@unud.ac.id
iagsuwiprabayantiputra@unud.ac.id

Abstrak

Di era perkemabangan teknologi komputer dan teknologi saat ini yang mengalami kemajuan yang sangat pesat, pentingnya keamanan dan kerahasiaan data sebuah aplikasi e-commerce. Dulu manusia melakukan proses transaksi jual-beli masih menggunakan cara yang konvensional, yaitu harus datang ke tempat penjual produk/barang. Dengan adanya teknologi saat ini maka proses transaksi jual-beli secara jarak jauh dapat dilakukan dengan mudah dan cepat menggunakan Aplikasi e-commerce. Bermodalkan internet manusia bisa melakukan proses transaksi jual-beli menggunakan aplikasi e-commerce yang sudah sangat banyak tersedia saat ini. Namun saat ini aplikasi e-commerce masih sangat rentang terhadap penyadapan data atau informasi penting lainya. Penyadapan adalah salah satu masalah yang ditakuti oleh para pengguna aplikasi e-commerce. Maka dibuatkanlah sebuah keamanan enkripsi pada aplikasi e-commerce berbasi web. Tujuan pembuatan kemanan data ini adalah untuk menjaga kemanan data ataupun informasi yang tersimpan dalam bentuk pesan yang diketik langsung oleh customer e-commerce, mengenkripsi data customer adalah salah satu cara yang digunakan untuk mengamankan semua informasi penting dan rahasia, dengan menggunakan teknik kriptografi. Algoritma kriptografi yang digunakan adalah menggunakan metode Blowfish yang merupakan suatu algoritma yang simestris dan berbentuk chiper block. Penelitian ini telah menghasilkan aplikasi enkripsi password yang telah diuji coba dan algoritma blowfish terbukti handal dalam mengamankan password.

Kata kunci : *E-commerce*, *Kriptografi, Blowfish, Customer, Enkripsi*

1. Pendahuluan

Kemajuan dan perkembangan teknologi informasi telah berpengaruh pada seluruh aspek kehidupan manusia, terutama dalam bidang komunikasi. Segala informasi dan komunikasi dapat dengan mudah diperoleh melalui internet dan handphone, dimana keduanya tidak dapat dipisahkan dalam kehidupan manusia. Internet mempunyai banyak manfaat dalam kehidupan sehari-hari, yaitu sebagai sarana konektivitas dan komunikasi, akses informasi, edukasi, hiburan dan kemudahan dalam berbisnis. Banyak masyarakat yang memanfaatkan internet untuk berbelanja online karena disebut cukup praktis tanpa harus keluar rumah [1]. Aplikasi berbelanja online yang biasa digunakan masyarakat yaitu *e-commerce*. *E-Commerce* merupakan bentuk transaksi perdagangan yang melibatkan internet. Kelebihan dari *e-commerce* yaitu pembeli dapat bertransaksi dengan praktis dan biaya yang murah tanpa melalui proses tawar menawar, di mana pihak pembeli cukup mengakses internet kemudian mengetahui ketentuan-ketentuan yang berlaku oleh pihak penjual [2]. *E-commerce* didefinisikan sebagai proses transaksi jual-beli produk-produk secara elektronik dari penjual ke konsumen atau dari perusahaan satu ke perusahaan lainnya menggunakan komputer sebagai perantara transaksi bisnis.

Sistem *e-commerce* memiliki beberapa aturan yaitu mencakup sistem distribusi barang, sistem pembayaran dan sistem informasi yang diterapkan, namun agar semua sistem tersebut

berjalan sesuai dengan yang diharapkan maka perlu memperhatikan aspek keamanannya. Contoh hal yang tidak diinginkan pada sistem keamanan *e-commerce* yaitu pencurian data *customer* maupun kebocoran informasi rahasia dan berharga [3]. Hal tersebut menandakan bahwa pengembangan teknologi juga memiliki dampak buruk bagi kehidupan manusia yaitu mudahnya mengakses data-data dari orang lain sehingga perlu adanya informasi-informasi rahasia yang disimpan atau disampaikan melalui suatu cara tertentu agar tidak diketahui oleh pihak yang tidak dikehendaki, oleh karena itu terciptalah ilmu kriptografi. Kriptografi merupakan ilmu yang berguna untuk menjaga kerahasiaan informasi dengan metode dan teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan, integritas data, orientasi, dan anti penyangkalan (Natsir, 2017).

Salah satu mekanisme untuk meningkatkan keamanan adalah dengan menggunakan teknologi enkripsi. Enkripsi adalah proses yang dilakukan untuk mengamankan sebuah pesan (yang disebut *plaintext*) menjadi pesan yang tersembunyi (disebut *ciphertext*) adalah enkripsi (*encryption*) (Budi Raharjo, 2002). Enkripsi data tersebut dapat menggunakan metode algoritma Blowfish atau sering disebut OpenPGP.Cipher.4 [4]. Pemilihan dengan menggunakan metode ini dikarenakan Blowfish dinilai sebagai salah satu algoritma kriptografi *symetris* yang cepat dan kompak, mempunyai perhitungan sederhana sedangkan panjang kunci yang biasa digunakan yaitu bervariasi mulai dari 32 bit sampai 128 bit. Blowfish dioptimasikan untuk berbagai aplikasi dimana kunci tidak sering berubah, seperti pada jaringan komunikasi atau enkripsi file secara otomatis. Blowfish adalah algoritma simetris 64-bit yang menggunakan panjang kunci bervariasi dari 32-bit sampai 448-bit (14 bytes). Blowfish dirancang untuk mengenkripsi plain text 64-bit ke cipher text 64-bit secara efisien dan aman. Operasi yang digunakan dalam prosesnya berupa lookup table, modulus, penambahan dan XOR untuk meminimalisir waktu yang dibutuhkan dalam mengenkripsi dan mendekripsi data pada prosesor 32-bit [5].

Sebelumnya telah ada penelitain terkait mengenai Implementasi Sistem Keamanan *e-commerce* menggunakan Algoritma Blowfish (Reza dkk, 2018). Pada penelitian ini dibuat sistem keamanan *e-commerce* yang mengimplementasikan teknik kriptografi Blowfish dan tanda tangan digital dengan *Digital Signature Algoritm* (DSA) [6]. Level keamanan juga diimplementasi untuk *layer transport* dengan menggunakan *protocol* SSL (*Secure Socket Layer*). Dari hasil pengujian yang dilakukan terlihat bahwa sistem berjalan sesuai prosedur yang diharapkan. Pengujian dilakukan untuk mengetahui tingkat performasi penerapan kriptografi Blowfish dan *digital signature* DSA pada sistem. Dengan level *security* 512 bit dan SHA-1, rata-rata waktu eksekusi yang dibutuhkan dalam pembangkitan kunci 3.86 detik, enkripsi 0,73 mili detik, tanda tangan 2,42 mili detik dan dekripsi 0,85 mili detik serta verifikasi 3,37 mili detik. Total waktu yang dibutuhkan untuk satu kali transaksi penjualan adalah 224 mili detik [7].

Pada penelitian ini dalam proses enkripsi data peneliti berfokus untuk melakukan enkripsi data *customer e-commerce* pada saat melakukan registrasi akun aplikasi, dimana fokus peneliti akan melakukan enkripsi *password* dan *username customer* dengan menggunakan metode algoritma Blowfish.

Dari latar belakang diatas penulis berupaya untuk merancang sistem keamanan data *customer* pada aplikasi *e-commerce*. Dimana penulis menggunakan metode Algoritma Blowfish guna mengevaluasi sejauh mana dapat digunakan dalam mengamankan data. Dengan menggunakan metode tersebut diharapkan dapat membantu para *customer e-commerce* dalam proses menjaga keamaanan data dan segala informasi yang bersifat rahasia [8].

2. Algoritma Blowfish

Bruce Schneier merancang algoritma Blowfish pada tahun 1993 sebagai alternatif enkripsi data yang cepat dan terbuka (open-source). Sejak dicetus, algoritma ini telah dianalisa terus menerus, dan perlahan diakui sebagai algoritma enkripsi yang handal. Banyak kelebihan dari algoritma Blowfish seperti kompatibilitas dan efisiensi dalam penerapannya dan tidak ada lisensi yang diperlukan. Dasar operasi Blowfish mencakup lookup table, penambahan dan

XOR. Lookup table terdiri dari empat S-boxes dan sebuah P-array. Blowfish adalah blok cipher 64-bit yang disebut menggantikan algoritma DES, dengan operasi algoritma yang cepat dan mampu mengenkripsi data pada mikroprosesor berukuran 32-bit [1].

Blowfish adalah algoritma simetris 64-bit yang menggunakan panjang kunci bervariasi dari 32-bit sampai 448-bit (14 bytes). Blowfish dirancang untuk mengenkripsi plain text 64-bit ke cipher text 64-bit secara efisien dan aman. Operasi yang digunakan dalam prosesnya berupa lookup table, modulus, penambahan dan XOR untuk meminimalisir waktu yang dibutuhkan dalam mengenkripsi dan mendekripsi data pada prosesor 32-bit [2].

Blowfish atau disebut juga OpenPGP.Cipher.4 adalah enkripsi yang termasuk dalam golongan *Symmetric Cryptosystem*. Blowfish merupakan algoritma kunci simetrik cipher blok yang dirancang pada tahun 1993 oleh Bruce Schneier untuk menggantikan *Data EncryptionStandard* (DES) [3]. Metode enkripsi ini diciptakan oleh Bruce Schneier, seorang *Cryptanalyst* Presiden perusahaan *Counterpane Internet Security*, *Inc* pada tahun 1993. Dan dipublikasikan tahun 1994. Blowfish dibuat untuk digunakan pada komputer yang mempunyai mikroprosesor besar (32 bit ke atas dengan *cache* data yang besar).

Blowfish merupakan cipher blok, yang berarti selama proses enkripsi dan dekripsi, Blowfish bekerja dengan membagi pesan menjadi blok-blok bit dengan ukuran sama panjang yaitu 64-bit dengan panjang kunci bervariasi yang mengenkripsi data dalam 8 byte blok [4]. Pesan yang bukan merupakan kelipatan 8 byte akan ditambahkan bitbit tambahan (*padding*) sehingga ukuran untuk tiap blok sama.

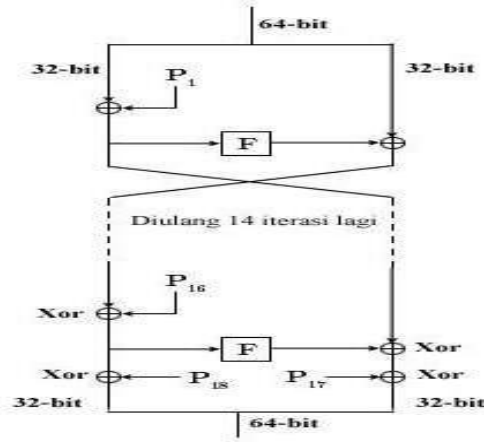
Algoritma dalam Blowfish terbagimenjadi dua bagian, yaitu *keyexpansion* dan data *encryption*. Proses *key expansion* akan melakukan konversi sebuah kunci mulai dari 56 byte sampai beberapa array subkunci dengan total mencapai 4168 byte. Blowfish dirancang dan diharapkan mempunyai kriteria perancangan yang diinginkan sebagai berikut :

- Cepat, Blowfish melakukan enkripsi data pada microprocessor 32-bit dengan rate 26 *clock cycles* per byte.
- *Compact*, Blowfish dapat dijalankan pada memory kurang dari 5K. Sederhana, Blowfish hanya menggunakan operasi – operasi sederhana, Blowfish hanya menggunakan operasi – operasi sederhana, seperti :penambahan, XOR, dan lookup tabel pada operan32- bit. 4.
- Memiliki tingkat keamanan yang bervariasi, panjang kunci yang digunakan oleh Blowfishdapat bervariasi dan bisa sampai sepanjang minimal 32-bit, maksimal 448 - bit, Multiple 8 bit, default 128 bit.

Namun, jika algoritma diterapkan dengan kunci yang sering berubah akan membutuhkan proses penurunan baru pada iterasi yang panjang, hal ini akan membuat waktu kerja Blowfish lebih panjang, sedangkan penggunaan *weak key* dapat mengganggu hasil enkripsi dan dekripsi. *Weak key m*embuat hasil enkripsi/dekripsi menjadi tidak konsisten [5]. Tingkat keamanan algoritma Blowfish ditentukan oleh jumlah iterasi dan panjang serta kerahasiaan kunci yang digunakan jumlah iterasi yang digunakan semestinya membuat jaringan feistel pada Blowfish bekerja semestinya, pengurangan jumlah iterasi akan mengurangi tingkat kesulitan suatu data untuk dipecahkan, sedangkan peran panjang dan kerahasiaan kunci menjadi sangat krusial [6]. Kunci yang panjang menjadi sama tingkat kebutuhannya dengan iterasi yang tidak dikurangi karena proses pembangkitan *subkey* akan menjadi lebih acak dan membutuhkan waktu lama untuk dipecahkan.

Ekspansi kunci pada algoritma Blowfish berfungsi untuk merubah kunci (Minimum 32-bit, Maksimum 448-bit) menjadi beberapa array subkunci (*subkey*) dengan total 4168 byte. Algoritma Blowfish terdiri dari iterasi fungsi sederhana (*Feistel Network)* sebanyak 16 kali putaran. Setiap putaran terdiri dari permutasi kunci-dependent dan substitusi- kunci dan data-dependent. Semua operasi adalah penambahan *(addition)* dan XOR pada variabel 32-bit seperti ditunjukkan pada Gambar 1 dibawah ini.

Gambar 1 Algoritma *Blowfish*



Operasi tambahan lainnya hanyalah empat penelusuran tabel *(table lookup)* array berindeks untuk setiap putaran. Untuk alur algoritma enkripsi dengan metode Blowfish dijelaskan sebagai berikut :

1. Bentuk inisial array P sebanyak 18 buah (P1,P2, P1 masing-masing bernilai 32-bit. Array P terdiri dari delapan belas kunci 32-bit subkunci : P1,P2,……..,P18
2. Bentuk S-box sebanyak 4 buah masing-masing bernilai 32-bit yang memiliki masukan 256. Empat 32-bit S-box masing- masing mempunyai 256 entri :
   S1,0,S1,1,… ,S1,255
   S2,0,S2,1,… ,S2,255
   S3,0,S3,1,… ,S3,255
   S4,0,S4,1,… ,S4,255
3. Plainteks yang akan dienkripsi diasumsikan sebagai masukan, Plainteks tersebut diambil sebanyak 64-bit, dan apabila kurang dari 64-bit maka kita tambahkan bitnya, supaya dalam operasi nanti sesuai dengan datanya.
4. Hasil pengambilan tadi dibagi 2, 32-bit pertama disebut XL, 32-bit yang kedua disebut XR.
5. Selanjutnya lakukan operasi XL = XL xor Pi dan XR = F(XL) xor XR
6. Hasil dari operasi diatas ditukar XL menjadi XR dan XR menjadi XL.
7. Lakukan sebanyak 16 kali, perulangan yang ke- 16 lakukan lagi proses penukaran XL dan XR.
8. Pada proses ke-17 lakukan operasi untuk XR = XR xor P17 dan XL = XL xor P18.
9. Proses terakhir satukan kembali XL dan XR sehingga menjadi 64-bit kembali.

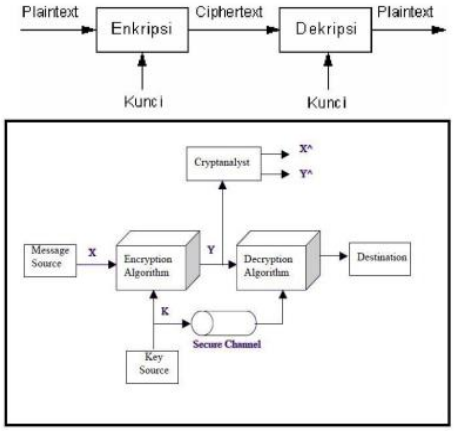
3. Metode Penelitian

3.1 Kriptografi

Kriptografi berasal dari bahasa Yunani yang terdiri *"cryptos"* yang berarti menyembunyikan sedangkan *"graphia"* berarti tulisan. Kriptografi merupkan ilmu yang mempelajari teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, autentikasi, integritas dan keabsahan data [1]. Kriptografi juga dapat diartikan sebagai ilmu untuk menjaga kerahasiaan pesan.

Kemudian, proses yang akan dibahas dalam penelitian ini meliputi 2 proses dasar pada kriptografi yaitu enkripsi dan dekripsi. Enkripsi yaitu proses mengubah data asli menjadi pesan yang tidak dapat dibaca, sedangkan dekripsi merupakan proses menjadikan data hasil manipulasi menjadi data asli [2]. Berikut ini merupakan ilustrasi sederhana dari proses kriptografi. Pada prinsipnya, Kriptografi memiliki 4 komponen utama yaitu *plaintext*, yaitu pesan yang dapat dibaca. *Ciphertext,* yaitu pesan acak yang tidak dapat dibaca. *Key*, yaitu kunci untuk melakukan teknik kriptografi. Algorithm, yaitu metode untuk melakukan enkrispi dan dekripsi.

Gambar 2 Ilustrasi Kunci Kriptografi



Gambar 2 menunjukkan proses penyembunyian pesan menggunakan teknik kriptografi. Pada kriptografi simetris, kunci yang digunakan untuk proses enkripsi dan dekripsi sama sedangkan pada kriptografi asimetris kunci yang digunakan berbeda.

Menurut terminologinya kriptografi merupakan ilmu dan seni untuk menjaga keamanan pesan ketika pesan tersebut dikirim dari suatu tempat ke tempat lain. Jika seorang kriptografer menggunakan enkripsi untuk merahasiakan pesan dan mendeskripsikannya kembali, maka kriptanalis mempelajari metode enkripsi dan cipherteks untuk menemukan plainteksnya [3].

Dalam kriptografi modern tidak mendasarkan kekuatan pada algoritmanya. Kekuatan kriptografinya terletak pada kunci, yang berupa deretan karakter atau bilangan bulat [4]. Kunci ini sama fungsinya dengan sandi lewat (*password*) pada *system computer* yang dijaga kerahasiaannya dan hanya orang yang mengetahui kunci yang dapat melakukan enkripsi dan dekripsi.

3.2 Data Penelitian

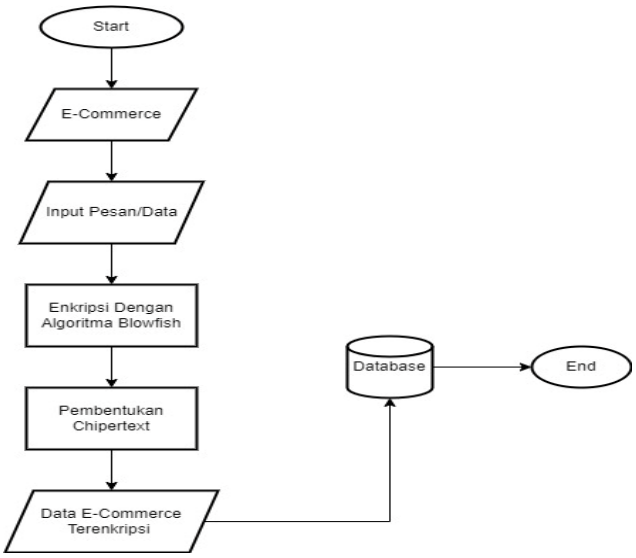
Jenis data yang digunakan dalam penelitian ini adalah data sekunder, yang memiliki arti data yang di peroleh melalui pihak lain, tidak langsung diperoleh oleh peneliti dari subjek penelitiannya. Data sekunder yang terdapat pada penelitian ini berupa data para *customer e-commerce* yang diketik langsung oleh pengguna pada saat melakukan proses registrasi akun *e-commerce*. Metode yang dilakukan penulis untuk mendapatkan data sekunder adalah menggunakan metode angket (kuisioner). Data yang dihasilkan oleh peneliti adalah melalui teknik survei dan wawancara langsung kepada para pengguna *e-commerce* [1].

Selain itu metode yang digunakan adalah Metode Studi Pustaka. Metode Studi Pustaka adalah metode pengumpulan data yang didapat dari membaca atau mempelajari teori-teori dari buku, jurnal, dan sumber lain yang relevan dengan penelitian ini [2].
Jurnal dan buku yang digunakan untuk referensi pada penelitian ini adalah jurnal dan buku yang membahas mengenai teknik enkripsi dengan metode Algoritma Blowfish pada aplikasi *e-commerce*.

3.3 Desain Sistem

Aplikasi keamanan *e-commerce* yang dikembangkan pada penelitian ini merupakan aplikasi berbasis *website* dengan bahasa pemrograman utama Python dengan *Framework* Django dengan tampilan antarmuka menggunakan HTML, CSS dengan *framework* Bootstrap dan Javascript dengan *library* JQuery. Alur sistem terbagi menjadi dua proses utama yaitu tahap enkripsi dan tahap dekripsi. Tahap enkripsi adalah tahap untuk melakukan enkripsi data *e-commerce* menggunakan algoritma Blowfish, dari proses enkripsi tersebut akan menghasilkan output berupa *ciphertext*. *Flowchart* tahap enkripsi dapat dilihat pada gambar 3.

Gambar 3 *Flowchart Enkripsi*

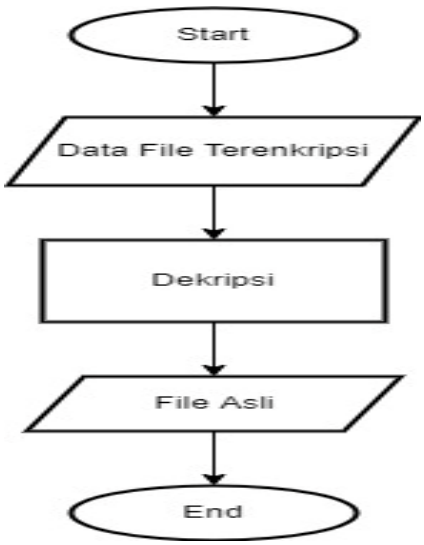


Pada tahap ini adalah proses enkripsi data *e-commerce* menggunakan algoritma Blowfish. Output yang dihasilkan pada saat enkripsi adalah berupa *ciphertext*. Adapun alur pada saat enkripsi adalah sebagai berikut:

1. Pengguna login pertama kali pada aplikasi *e-commerce*, kemudian melakukan proses registrasi.
2. Pada saat proses registrasi pengguna akan memasukkan semua data yang diminta oleh aplikasi, termasuk memasukkan username dan *password* akun.
3. Setelah proses registrasi selesai pengguna akan melakukan submit untuk menyimpan data di aplikasi.
4. Sistem akan melakukan proses enkripsi data dengan menggunakan metode algortima Blowfish, jika proses enkripsi berhasil maka;
5. Sistem akan menghasilkan output *chipertext.*
6. Setelah proses *chipertext* selesai, maka data *customer* sudah terenkripsi.
7. Proses akhir, data akan disimpan ke database sistem.

Pada tahap ini adalah proses dekripsi data *e-commerce*, menggunakan metode algortima Blowfish. Dapat dilihat pada gambar 4.

Gambar 4 *Flowchart* Dekripsi



4. Hasil dan Pembahasan

Aplikasi keamanan *e-commerce* yang dikembangkan pada penelitian ini merupakan aplikasi berbasis website dengan bahasa pemrograman utama Python dengan *Framework* Django dengan tampilan antarmuka menggunakan HTML, CSS dengan *framework* Bootstrap dan Javascript dengan *library* JQuery. Alur sistem terbagi menjadi dua proses utama yaitu tahap enkripsi dan tahap dekripsi. Tahap enkripsi adalah tahap untuk melakukan enkripsi data *e-commerce* menggunakan algoritma Blowfish.

Aplikasi ini berfungsi untuk memanipulasi *password* sebelum digunakan, sehingga orang lain tidak mengetahui. Disisi lain, *password* yang digunakan mempunyai 2 kali pertahanan.

Gambar 5. Tampilan Awal Aplikasi Enkripsi *Password*

Gambar 5 merupakan tampilan awal aplikasi pengamanan *password* menggunakan algoritma Blowfish. Terdapat pilihan opsional untuk mengaktifkan kunci yang digunakan, yaitu *hexastring* atau alfabet. Setelah kunci ditetapkan dari kunci menggenerate berdasarkan opsi yang telah dipilih maka pengguna harus mengetikkan plainteks yang akan digunakan.

Gambar 6. Proses Enkripsi *Password*

Gambar 6 merupakan proses enkripsi menggunakan algoritma Blowfish. Pada percobaan yang dilakukan, opsi dari model kunci yang digunakan adalah model alfabet.

Gambar 7. Proses Ekstraksi *Password*

Pada Gambar 7, proses ekstraksi dilakukan untuk mengevaluasi apakah proses enkripsi sudah dilakukan dengan benar. Dalam percobaan yang telah dilakukan, ekstraksi berjalan dengan baik dan menghasilkan *deciphered* yang sama dengan plainteks (file induk asli).

5. Pengujian Tabel Enkripsi dan Dekripsi

Dalam table pengujian akan terlihat perbandingan antara proses enkripsi dan dekripsi hanya menggunakan file txt. Dengan parameter meliputi ukuran awal file, waktu proses enkripsi atau dekripsi, ukuran akhir file dan hasil file yang dicapai dalam proses enkripsi maupun dekripsi.

Tabel 1. Hasil Proses Enkripsi

No	Nama File	Ukuran File Awal	Ukuran File Sesudah Enkripsi	Waktu
1.	File.txt	1 Kb	56 Bytes	0:06:4
2.	File.txt	22 Kb	29.3 Kb	0:04:9
3.	File.txt	26 Kb	34.0 Kb	0:05:6

Tabel 2. Hasil Proses Dekripsi

No	Nama File	Ukuran File Enkripsi	Ukuran File Sesudah Dekripssi	Waktu
1.	File.txt	56 Bytes	1 Kb	0:06:2
2.	File.txt	29.3 Kb	22 Kb	0:05:1
3.	File.txt	34.0 Kb	26 Kb	0:06:3

6. Kesimpulan dan Saran

6.1 Kesimpulan

Algoritma Blowfish dapat digunakan untuk mengimplementasikan aplikasi enkripsi e-commerce. Algoritma Blowfish merupakan algoritma yang cepat, tersusun secara rapi, dapat dengan mudah dijalankan, sederhana, dan terjamin keamanannya. Sampai saat ini belum ada *cryptanalysis* yang berhasil menembus keamanan yang dibuat oleh algoritma Blowfish dengan 16 kali putaran. Dari hasil percobaan yang telah dilakukan dalam penelitian ini, maka dapat disimpulkan bahwa algoritma Blowfish merupakan algoritma yang handal untuk mengamankan *password.*

6.2 Saran

a. Bisa digunakan untuk file selain ektensi : .txt.
b. Tampilan masih sederhana diharapkan ada beberapa fitur tambahan.

References :

[1] Yani Partiastuti, E. H. (2016). OPTIMASI ENKRIPSI PASSWORD MENGGUNAKAN ALGORITMA BLOWFISH. Techno.COM, 15-21.

[2] Irawan, A dan Zuli,F., 2016, Implementasi Kriptografi dengan Algoritma Blowfish dan Riverst Shamir Adleman (RSA) Untuk Proteksi File, Jurnal Format, 6(2) : 31-32

[3] Simanullang, H.G,. dan Sillahi,A.P., 2018, Algoritma Blowfish Untuk Meningkatkan Keamanan Data Base MYSQL, Jurnal Methodika, 4(1) : 14-16

[4] Asang, M.S, dan Irwan S, 2016, Keamanan Data Pada Perangkat Internet Of Things Menggunakan Metode Public-Key Cryptography, Jurnal Teknologi Informasi, 14(1) : 80-87

[5] Basri, 2015, Pendekatan Kriptografi Hybrid Pada Keamanan Dokumen Elektronik dan HypertextTransfer Protocol Secure (HTTPS) (Analisa Potensi Implementasi Pada Sistem Kemanan), Jurnal Ilmu Komputer, 1(2) : 2442-4512

[6] Rifa'i, A dan Lilis C.S, 2019, Implementasi Kriptografi Menggunakan Metode Blowfish dan Base 64 Untuk Mengamankan Database Informasi Akademik Pada Kampus Akademi Telekomunikasi Bogor Berbasis Web-Based, Jurnal Elektro Komputer Teknik, 3(2) : 87-96

[7] Sitinjak, S., Yuli F., dan Juwairiah, 2010, Aplikasi Kriptografi File Menggunakan Algortima Blowfish, Jurnal Seminar Nasional Informatika, ISSN : 1979-2328, 78-86

[8] Suhandinata, S., Reyhan. A.R., Dedy O.W., Prabhu W., dan Srinjiwi, 2019, Analisis Performa Kriptografi Hybrid Algoritma Blowfish dan Algoritma RSA, Jurnal Teknologi dan Sistem Informasi, 6(1) : 1-10

[9] Susanto, 2017, Implementasi Keamanan Data Menggunakan Algortima Blowfish Pada Sistem Informasi Koperasi Rias, Jurnal Simetris., 8(1) : 251-264

[10] Pramartha, C., et al. *Developing Semantic Ontology for Practical Digital Balinese Dictionary*. in *Proceeding International Conference on Information Technology, Multimedia, Architecture, Design, and E-Business*. 2022.

[11]
Suhandinata, S. (2019). ANALISIS PERFORMA KRIPTOGRAFI HYBRID ALGORITMA BLOWFISH DAN ALGORITMA RSA. *JURTEKSI (Jurnal Teknologi dan Sistem Informasi)*, 1-10.

[12] Rohman, F. D. (2018). IMPLEMENTASI KRIPTOGRAFI PADA PENGIRIMAN PESAN EMAIL DENGAN MENGGUNAKAN METODE RC4 DAN BLOWFISH PADA PT.DASCOM JAYA SAKTI. *SKANIKA*, 1-5.

halaman ini sengaja dibiarkan kosong