BAB II
Kerangka Teoritis

A. Rujukan Penelitian

Pada penelitian sebelumnya sudah banyak dilakukan dengan kasus yang berbeda dengan metode yang sama sebagai bahan pertimbangan pada penelitian dan untuk mengetahui perbedaan penelitian sebelumnya dengan penelitian yang akan dilakukan. Berikut ini adalah penelitian yang telah dilakukan sebelumnya :

1. Dalam penelitian yang berjudul “Implementasi Algoritma Blowfish Untuk Enkripsi Dan Dekripsi Berbasis Java Swing” oleh Rafsanjani, Muhammad Purwanto, Rachmad Martyanto dari Fakultas Teknik Informatika, Universitas PGRI Ronggolawe Tuban, Indonesia, 2016. Penelitian ini menjelaskan keamanan data enkripsi dan dekripsi document menggunakan java swing. Java Swing adalah librari java yang digunakan untuk menciptakan Grafik User Interface (GUI). Dengan Java Swing kita dapat membuat user interface yang cross platform atau OS independent. Tujuan penelitian ini adalah memanfaatkan algoritma blowfish agar dapat terintegrasi dengan java swing dalam hal keamanan document.
2. Dalam penelitian yang berjudul “Algoritma Blowfish Untuk Enkripsi Dan Dekripsi Berbasis PHP” oleh Enggy Heroedi, Puji Wahyono, Muhammad Yunus Affandi dari Universitas PGRI Ronggolawe Tuban, Indonesia, 2016. Penelitian ini menjelaskan proses yang dilakukan untuk membangun Aplikasi Kriptografi menggunakan Algoritma Blowfish Berbasis PHP dengan tujuan mengamankan data ataupun informasi yang berupa text (plaintext) dengan mengacak text tersebut sehingga tidak dapat dibaca atau dimengerti. PHP adalah bahasa pemrograman script yang paling banyak dipakai saat ini. PHP banyak dipakai untuk memrogram situs web dinamis, walaupun tidak tertutup kemungkinan digunakan untuk pemakaian lain. Tujuan penelitian ini adalah impelementasi algoritma blowfish menggunakan PHP untuk keamanan data.
3. Dalam penelitian yang berjudul “Implementasi Kriptografi Dengan Algoritma Blowfish Dan Riverst Shamir Adleman (RSA) Untuk Proteksi File” oleh Faizal Zuli, Ari Irawan dari Universitas Satya Negara Indonesia" Indonesia, 2017. Penelitian ini menjelaskan mengenai menjaga keamanan data suatu sistem kriptografi pada kerahasiaan kunci dan bukan pada kerahasiaan algoritma yang digunakan. RSA (Rivest Shamir Adleman) adalah singkatan dari para pembuatnya yaitu Ron Rivest, Adi Shamir, dan Leonard Adleman yang dibuat pada tahun 1977. RSA merupakan sistem kriptografi asimetrik. Tujuan

penelitian ini adalah implementasi algoritma blowfish menggunakan Riverst Shamir Adleman (RSA) untuk keamanan file.

4. Dalam penelitian yang berjudul “Sistem Keamanan Menggunakan Algoritma Blowfish Advance Cs Pada File Dan Folder Data” oleh Trisnawati dari Fakultas Ilmu Komputer, Universitas Sriwijaya, Indonesia, 2008. Penelitian ini menjelaskan Sistem keamanan menggunakan algoritma Blowfish Advance CS pada File dan folder yang meliputi proses enkripsi, deskripsi dan contoh simulasi data dengan menggunakan algoritma Blowfish advance CS tersebut. Dengan enkripsi, data kita disandikan (encrypted) dengan menggunakan sebuah kunci (key). Untuk membuka (decript) data tersebut digunakan juga sebuah kunci yang sama dengan kunci mengenkripsi tadi atau yang sering disebut dengan private key kriptografi.
5. Dalam penelitian yang berjudul “Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard” oleh Fresly Nandar Pabokory, Indah Fitri Astuti, Awang Harsa Kridalaksana dari Fakultas Ilmu Komputer, Universitas Mulawarman, Indonesia, 2015. Penelitian ini menjelaskan sebuah sistem keamanan data dengan mengimplementasikan kriptografi pada pesan teks, isi file dokumen, dan file dokumen dengan melakukan perhitungan algoritma Advanced Encryption Standard (AES). AES merupakan algoritma cryptographic yang dapat digunakan untuk mengamakan data dimana algoritmanya adalah blokchipertext simetrik yang dapat mengenkripsi (encipher) dan dekripsi (decipher) informasi. Hasil dari penelitian yaitu pengguna dapat mengenkripsi pesan teks kemudian disimpan menjadi sebuah file dokumen dan isi file dokumen tersebut dienkripsi lagi selanjutnya hasil enkripsi isi file dokumen tersebut, file dokumennya dienkripsikan dan selanjutnya dikompresi dan disembunyikan pada sebuah file citra (gambar) agar keamanan data informasi tersebut dapat terjaga keamanannya karena telah dilakukan pengamanan dan penyandian yang berlapislapis.
6. Dalam penelitian yang berjudul “Implementasi Algoritma DES Berbasis Blowfish Untuk Enkripsi Dan Dekripsi Data” oleh Hafid Rosianto, Lilik Anifah dari Fakultas Teknik, Universitas Negeri Surabaya, Indonesia, 2017. Penelitian ini dilakukan untuk mengimplementasikan gabungan dari dua metode algoritma yang berbeda yaitu DES dan blowfish untuk enkripsi dan dekripsi data. Proses enkripsi bertujuan untuk mengamankan data dengan mengacak bit-bit data tersebut dengan password/key masukan. Sedangkan proses dekripsi bertujuan untuk mengembalikan bit-bit acakan dari proses

enkripsi dengan kunci sama yang dipakai pada proses enkripsi. Sampel data yang digunakan adalah data yang memiliki atau sebuah ekstensi seperti berekstensi .txt, .doc, .pdf, .jpeg, .gif, .mp3, .mp4, .avi. Perancangan dan desain program menggunakan software visual studio 2012 dengan bahasa pemrograman VB.NET. Proses diawali dengan enkripsi data awal atau plaintext menggunakan algoritma blowfish, kemudian cipherfile dari enkripsi algoritma blowfish di enkripsi lagi menggunakan algoritma DES. Untuk urutan penggunaan algoritma pada proses dekripsi adalah kebalikan dari proses enkripsi dan menghasilkan plainfile/file awal. Hasil pengujian dari kedua proses enkripsi dan dekripsi data dapat digunakan dan berjalan dengan lancar untuk menjaga keaslian data (authentication) dan keutuhan data (data integrity).

Perbandingan penelitian penyusun dengan rujukan penelitian

Persamaan yang dimiliki penelitian penyusun dengan rujukan penelitian terletak pada metode yang dipakai yaitu salah satu dari algoritma enkripsi dan dekripsi, Algoritma Blowfish.

Dan perbedaannya terletak pada spesifikasi masalah yang di teliti, pada penelitian ini masalah sulitnya untuk menyebarkan data *file document* dengan aman dan penyusun menggunakan *file* pdf dengan Algoritma Blowfish bisa menggunakan smartphone, sedangan penelitian sebelumnya masih belum menggunakan smartphone.

B. Landasan Teori

Algoritma Blowfish

Menurut (Sjukani, 2014:1) Algoritma adalah langkah-langkah yang diambil dalam menyelesaikan suatu pekerjaan. Algoritma, pada dasarnya, adalah alur pikiran dalam menyelesaikan suatu pekerjaan, yang dituangkan dalam bentuk tertulis yang dapat dimengerti oleh orang lain.

Menurut (Juneadi, 2007:2) Dalam menyelesaikan masalah komputer apapun, diperlukan suatu algoritma untuk membantu mencari solusi permasalahan tersebut. Dalam bidang komputer, algoritma didefinisikan sebagai cara memecahkan masalah dalam waktu yang terbatas dan jumlah langkah yang terbatas, sehingga dalam pembuatas algoritma pasti ada titik awal sebagai dasar untuk memulai dan titik akhir yang menunjukkan akhir dari suatu algoritma.

Algoritma terbagi menjadi beberapa jenis, salah satunya adalah algoritma chipher block. Algoritma Chipher Block adalah kriptografi beroperasi pada plainteks/cipherteks dalam bentuk blok bit, yang dalam hal ini rangkaian bit dibagi menjadi blok-blok bit yang panjangnya sudah ditentukan sebelumnya. Salah satu contoh algoritma chipher block adalah Algoritma Blowfish.

Menurut (Syafari, 2007) Algoritma Blowfish diciptakan oleh seorang Cryptanalyst bernama Bruce Schneier, Presiden perusahaan Counterpane Internet Security, Inc (Perusahaan konsultan tentang kriptografi dan keamanan komputer) dan dipublikasikan tahun 1994. Dibuat untuk digunakan pada komputer yang mempunyai microposesor besar (32-bit keatas dengan cache data yang besar). Blowfish merupakan algoritma yang tidak dipatenkan dan licensefree, dan tersedia secara gratis untuk berbagai macam kegunaan.

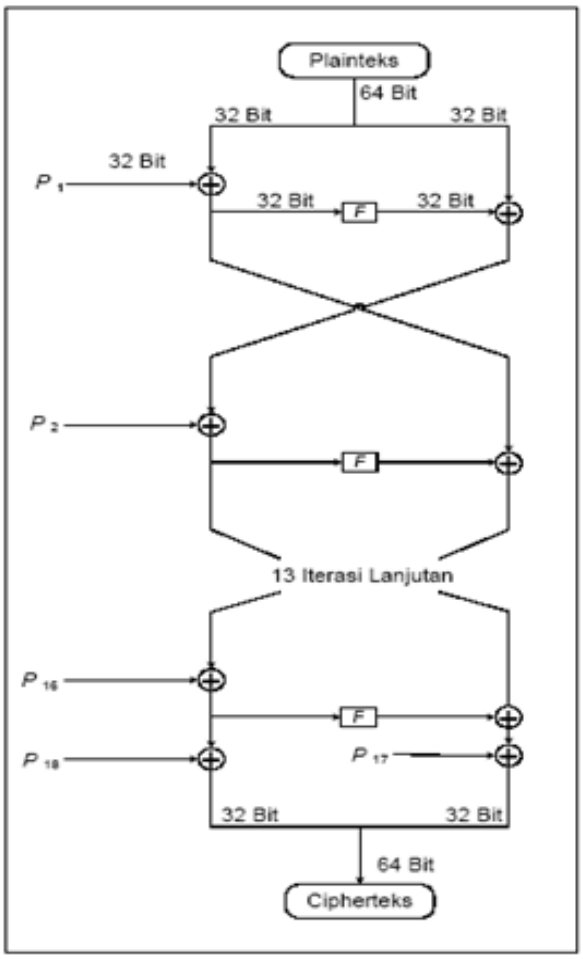
Menurut (Schneier, 1996) Pada saat Blowfish dirancang, diharapkan mempunyai kriteria perancangan sebagai berikut :

1. Cepat, Blowfish melakukan enkripsi data pada microprocessors 32-bit dengan rate 26 clock cycles perbyte.
2. Compact (ringan), Blowfish dapat dijalankan pada memori kurang dari 5K.
3. Sederhana, Blowfish hanya menggunakan operasi-operasi sederhana: penambahan, XOR, dan lookup tabel pada operan 32-bit.
4. Memiliki tingkat keamanan yang bervariasi, panjang kunci yang digunakan oleh Blowfish dapat bervariasi dan bisa sampai sepanjang 448 bit.

Enkripsi Algoritma Blowfish

Blowfish menggunakan subkunci berukuran besar. Kunci-kunsi tersebut harus dikomputasikan pada saat awal, sebelum pengkomputasian enkripsi dan dekripsi data.

Untuk lebih jelasnya, gambaran tahapan pada jaringan feistel yang digunakan Blowfish adalah seperti pada Gambar 2.1:



Gambar 2. 1 Jaringan Feistel

1. Terdapat kotak permutasi (P-box) yang terdiri dari 18 buah 32 bit subkunci: P1, P2, P3, ... P18. P-box ini telah ditetapkan sejak awal, 4 buah P-box awal adalah sebagai berikut:

   P1 = 0x243f6a88

   P2 = 0x85a308d3

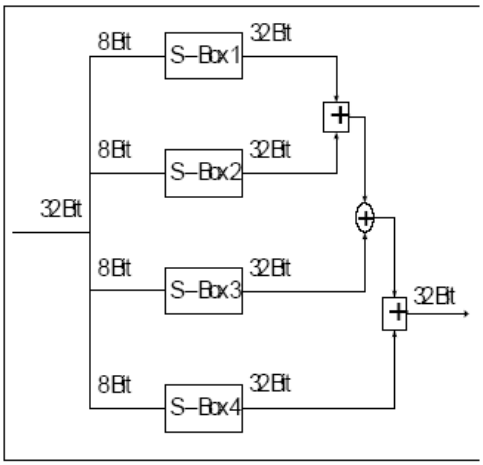
   P3 = 0x13198a2e

   P4 = 0x03707344

2. Xorkan P1 dengan 32 bit awal kunci, xorkan P2 dengan 32 bit berikutnya dari kunci, dan teruskan hingga seluruh panjang kunci telah terxorkan (kemungkinan sampai P14, 14x32 = 448, panjang maksimal kunci).
3. Terdapat 64 bit dengan isi kosong, bit-bit tersebut dimasukkan ke langkah 2.
4. Gantikan P1 dan P2 dengan keluaran dari langkah 3.
5. Enkripsikan keluaran langkah 3 dengan langkah 2 kembali, namun kali ini dengan subkunci yang berbeda (sebab langkah 2 menghasilkan subkunci baru).
6. Gantikan P3 dan P4 dengan keluaran dari langkah 5
7. Lakukan seterusnya hingga seluruh P-box teracak sempurna
8. Total keseluruhan, terdapat 521 iterasi untuk menghasilkan subkunci-subkunci yang dibutuhkan. Aplikasi hendaknya menyimpannya daripada menghasilkan ulang subkunci-subkunci tersebut.

Kunci- kunci yang digunakan antara lain terdiri dari, 18 buah 32-bit subkey yang tergabung dalam P-array (P1, P2, ..., P18). Selain itu, ada pula empat 32-bit S-box yang masing-masingnya memiliki 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. Pada jaringan feistel, Blowfish memiliki 16 iterasi, masukannya adalah 64-bit elemen data, X.

Pada langkah kedua, telah dituliskan mengenai penggunaan fungsi F. Fungsi F adalah: Bagi XL menjadi empat bagian 8-bit: a,b,c dan d. F(XL) = ((S1,a + S2,b mod 232) XOR S3,c) + S4,d mod 232.



Gambar 2. 2 Tahapan Fungsi F

Pada Algoritma Blowfish terdapat keunikan dalam hal proses dekripsinya, yaitu proses dekripsi dilakukan dengan urutan yang sama persis dengan proses enkripsi, hanya saja pada proses dekripsi P1, P2, …, P18 digunakan dalam urutan yang terbalik.

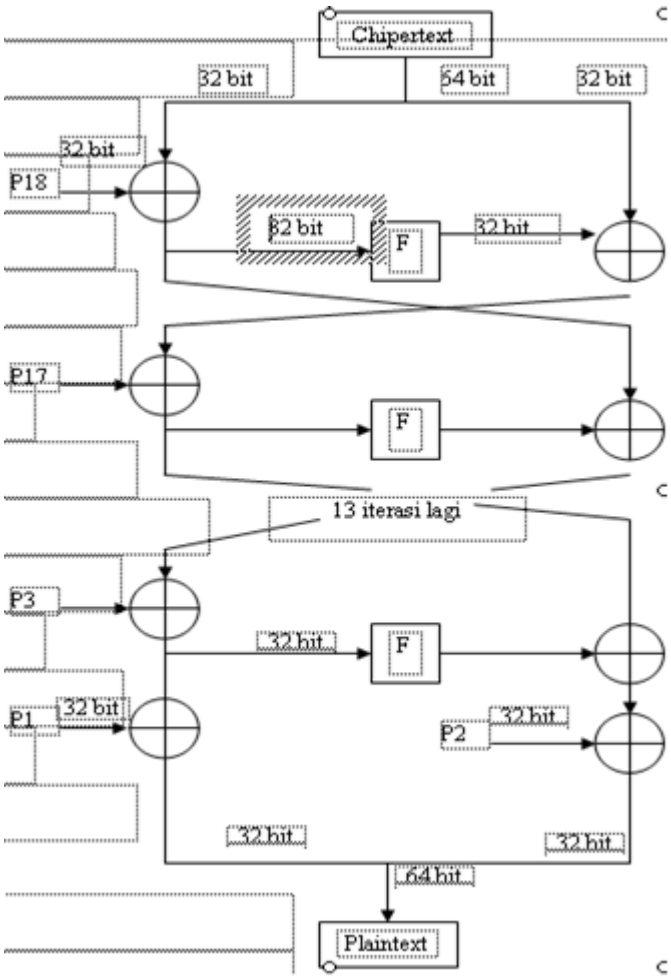
Dekripsi Algoritma Blowfish

Dekripsi sama persis dengan enkripsi, kecuali P1, P2, . . . , P18 digunakan pada urutan yang terbalik. kecuali bahwa P1, P2,…, P18. Dekripsi untuk Blowfish bersifat maju kedepan. Mengakibatkan dekripsi bekerja dalam arah algoritma yang sama seperti halnya dengan enkripsi, namun sebagai masukannya adalah chipertext. Walaupun begitu, seperti yang diharapkan, sub-kunci yang digunakan dalam urutan terbalik.

Subkunci dihitung menggunakan algoritma Blowfish, metodanya adalah sebagai berikut:

1. Pertama-tama inisialisasi P-array dan kemudian empat S-box secara berurutan dengan string yang tetap. String ini terdiri digit hexadesimal dari pi.
2. XOR P1 dengan 32 bit pertama kunci, XOR P2 dengan 32 bit kedua dari kunci dan seterusnya untuk setiap bit dari kunci (sampai P18). Ulangi terhadap bit kunci sampai seluruh P-array di XOR dengan bit kunci.
3. Enkrip semua string nol dengan algoritma Blowfiah dengan menggunakan subkunci seperti dijelaskan pada langkah (1) dan (2).
4. Ganti P1 dan P2 dengan keluaran dari langkah (3).
5. Enkrip keluaran dari langkah (3) dengan algoritma Blowfish dengan subkunci yang sudah dimodifikasi.
6. Ganti P3 dan P4 dengan keluaran dari langkah (5).
7. Lanjutkan proses tersebut, ganti seluruh elemen dari P-array, dan kemudian seluruh keempat S-box berurutan, dengan keluaran yang berubah secara kontinyu dari algoritma Blowfish.

Total diperlukan 521 iterasi untuk menghasilkan semua subkunci yang dibutuhkan. Aplikasi kemudian dapat menyimpan subkunci ini dan tidak dibutuhkan langkah-langkah proses penurunan ini berulang kali, kecuali kunci yang digunakan berubah.

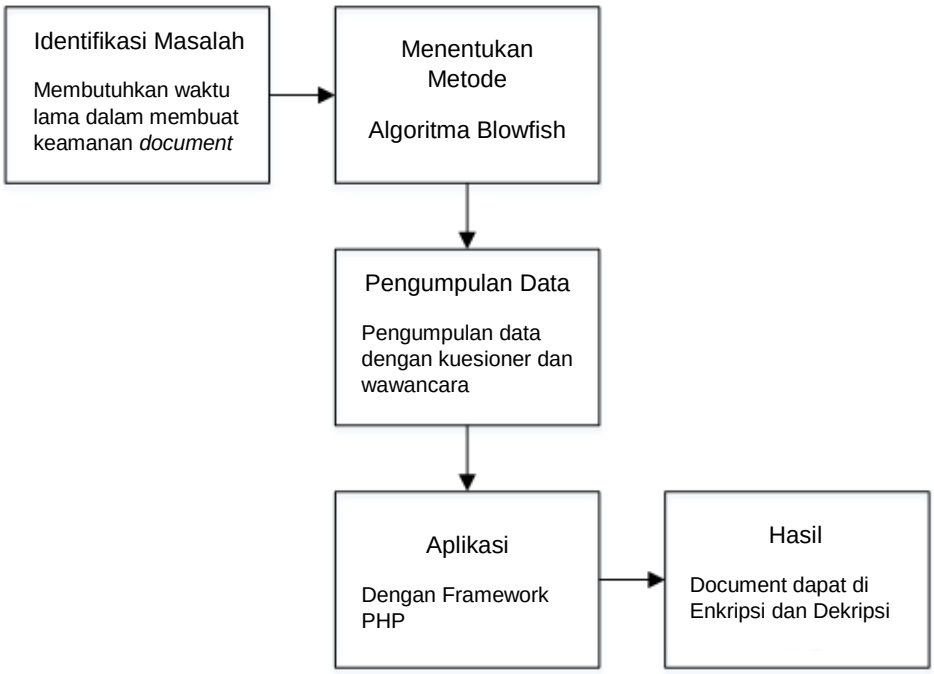


Gambar 2. 3 Diagram skema dekripsi algoritma Blowfish

Metode Algoritma Blowfish dilakukan dengan cara membalikkan 18 subskey yang ada.Yang akan kita lakuakan pertama kali adalah masalah ini nampak tidak dapat dipercaya, karena terdapat dua XOR operasi yang mengikuti pemakaian f-fungsi yang sebelumnya, dan hanya satu yang sebelumnya pemakaian pertama f-fungsi. Walupun jika kita memodifikasi algoritma tersebut sehingga pemakaian subkey 2 sampai 17 menempatkan sebelum output f-fungsi yang di-XOR-kan ke sebelah kanan blok dan dilakukan ke data yang sama sebelum XOR itu, meskipun itu berarti ia sekarang berada di sebelaha kanan blok, karena XOR subkey tersebut telah dipindahkan sebelum swap (tukar) kedua belah blok tersebut (tukar separuh blok kiri dan separuh blok kanan). Kita tidak merubah suatu apapun karena informasi yang sama di-XOR-kan ke separuh blok kiri antara setiap waktu, informasi ini digunakan sebagai input f-fungsi. Kenyataannya, kita mempunyai kebalikan yang pasti dari barisan dekripsi.

C. Kerangka Pemikiran

Kerangka pemikiran ini dibuat mewakili konsep pemecahan masalah penelitian yang meliputi objek penelitian, metode penelitian, metode penelitian adalah Algoritma Blowfish.



Gambar 2. 4 Kerangka Pemikiran

Dapat dijelaskan kerangka pemikiran sebagaimana ditunjukkan oleh Gambar 2.4.

1. Identifikasi Masalah
   Mengidentifikasi masalah yang terjadi di tempat objek penelitian.
2. Menentukan Metode
   Menentukan metode yang tepat untuk memecahkan masalah.
3. Pengumpulan Data
   Mengumpulkan data-data yang diperlukan dalam penerapan metode pada tahap selanjutnya (Aplikasi).
4. Aplikasi
   Membuktikan penerapan metode menggunakan aplikasi, disini penyusun menggunakan platform web dengan menggunakan framework PHP.
5. Hasil
   Hasil yang didapat setelah penerapan metode menggunakan aplikasi.