# SISTEM INFORMASI MANAJEMEN PENGARSIPAN DENGAN MENGGUNAKAN ALGORITMA *BLOWFISH*

**Chandra Sina Putra[1], Banni Satria Andoko [2]**

Program Studi Teknik Informatika, Jurusan Teknik Elektro, Politeknik Negeri Malang
[1]chandrasinap@gmail.com, [2]ando@polinema.ac.id

**Abstrak**

Dokumen dan arsip surat merupakan bagian terpenting bagi BPAD (Badan Perpustakaan Arsip dan Dokumentasi) Kabupaten Malang karena tugas utama adalah pengelolaan arsip. Tetapi dalam manajemennya, pengarsipan surat, serta persetujuan surat masih dilakukan secara manual dan tidak ada pengamanan data nya. Dengan adanya sistem ini diharapkan dapat membantu untuk mengelola, dan mendokumentasikan semua surat yang ada di BPAD (Badan Perpustakaan Arsip dan Dokumentasi) Kabupaten Malang. Baik surat masuk maupun surat keluar. Surat yang terdapat dalam system juga di amankan dengan cara di enkripsi menggunakan Algoritma BLOWFISH untuk mengamankan data arsip surat yang penting agar data aman dan jauh dari resiko penyalahgunaan.Aplikasi ini dapat mempermudah proses pencarian data, penyimpanan arsip dan mengamankan arsip gambar di BPAD kabupaten malang menggunakan algoritma blowfish , sehingga data aman dan jauh dari resiko penyalahgunaan.

**Kata kunci :** Sistem Informasi Manajemen Pengarsipan, Blowfish

## 1. Pendahuluan

Banyaknya organisasi berkembang pada era globalisasi dan modern seperti saat ini, menuntut organisasi tersebut untuk lebih pintar dalam mengatur manajemen sistemnya. Salah satu sistem yang penting untuk diperhatikan adalah sistem pengarsipan.

Menurut UU no. 7 tahun 1971 tentang Ketentuan-ketentuan Pokok Kearsipan. arsip atau records merupakan informasi yang direkam dalam bentuk atau media apapun, dibuat, diterima, dan dipelihara oleh suatu organisasi dalam rangka pelaksanaan kegiatan. Mengelola arsip tidak semata-mata memperlakukannya dari sudut teknis pengelolaan media rekamnya belaka melainkan dari sisi peranan arsip sebagai sumber informasi. Dari sudut pandang ini maka nilai arsip akan tampak berguna karena diperlukan sebagai informasi. Arsip sebagai informasi pengarsipan jelas menempati posisi vital dalam sebuah organisasi. Arsip akan dibutuhkan dalam seluruh proses kegiatan manajemen organisasi dari perencanaan, pelaksanaan, dan pengawasan.

Sistem Informasi pengarsipan surat dapat membantu dalam manajemen pengarsipan yang ada di perusahaan maupun instansi pemerintah termasuk salah satunya adalah BPAD (Badan Perpustakaan Arsip dan Dokumentasi) Kabupaten Malang. Arsip merupakan bagian terpenting bagi lembaga pemerintahan tersebut karena tugas utama BPAD kabupaten malang adalah pengelolaan arsip. Tetapi dalam manajemennya, ini masih dilakukan secara manual. Surat yang masuk disimpan dalam bentuk dokumen dan disimapan di rak rak penyimpanan khusus, dan di catat lokasi penyimpanannya di Microsoft access. Pencarian surat masih dilakukan secara manual sehingga memakan waktu yang lama. Surat yang ada di BPAD (Badan Perpustakaan Arsip dan Dokumentasi) Kabupaten Malang bisa berupa surat dinas seperti halnya permintaan dana dan lain-lain.

Dengan adanya sistem ini diharapkan dapat membantu mengelola, dan mendokumentasikan semua surat yang ada di BPAD (Badan Perpustakaan Arsip dan Dokumentasi) Kabupaten Malang. Baik surat masuk maupun surat keluar. Surat yang terdapat dalam system juga di amankan dengan cara di enkripsi menggunakan Algoritma *BLOWFISH* untuk mengamankan data arsip surat yang penting agar data aman dan jauh dari resiko penyalahgunaan.

## 2. Tinjauan Pustaka

### 2.1 BPAD (Badan Perpustakaan Arsip dan Dokumentasi) Kabupaten Malang

Badan Perpustakaan, Arsip dan Dokumentasi merupakan unsur pendukung pelaksana Pemerintah Kabupaten Malang yang ditetapkan dengan Peraturan Daerah Kabupaten Malang Nomor 1 Tahun 2008 tentang Organisasi Perangkat Daerah yang ditindaklanjuti dengan Peraturan Bupati Malang Nomor 33 Tahun 2008 tentang Organisasi Perangkat Daerah Badan Perpustakaan, Arsip dan Dokumentasi Kabupaten Malang.

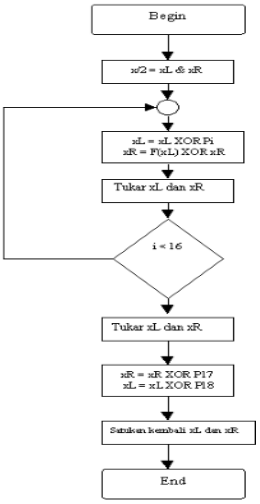
Kedudukan, tugas pokok dan fungsi Badan Perpustakaan, Arsip dan Dokumentasi Kabupaten Malang sebagai berikut :

1. Melaksanakan urusan Pemerintahan Daerah dalam penyusunan dan pelaksanaan kebijakan daerah bidang Perpustakaan, Arsip dan Dokumentasi ;
2. Melaksanakan tugas-tugas lain yang diberikan oleh Bupati sesuai dengan bidang tugas dan kewenangannya.
3. Pengumpulan, pengelolaan dan pengendalian data berbentuk data base serta analisa data untuk menyusun program kegiatan.

### 2.2 Algoritma *Blowfish*

Blowfish termasuk dalam enkripsi block Cipher 64bit dengan panjang kunci yang bervariasi antara 32-bit sampai 448-bit. Algoritma Blowfish terdiri atas dua bagian yaitu Pembangkitan sub-kunci (KeyExpansion) dan Enkripsi Data. Enkripsi Data terdiri dari iterasi fungsi sederhana (Feistel Network) sebanyak 16 kali putaran. Semua operasi adalah penambahan (addition) dan XOR pada variabel 32-bit. Operasi tambahan lainnya hanyalah empat penelusuran table (table lookup) array berindeks untuk setiap putana

Pada algoritma Blowfish, digunakan banyak subkey. Kunci-kunci ini harus dihitung atau dibangkitkan terlebih dahulu sebelum dilakukan enkripsi atau dekripsi data. Pada jaringan feistel, Blowfish memiliki 16 iterasi, masukannya adalah 64-bit elemen data atau sebut saja "X". Untuk melakukan proses enkripsi langkah-langkahnya adalah sebagai berikut:




Gambar 2.1 Flowchart proses enkripsi *Blowfish*

Proses Enkripsi dari gambar di atas, dijelaskan sebagai
berikut:

1. Bentuk inisial P-array sebanyak 18 buah (P1,P2,.....P18) masing-msing bernilai 32-bit.

Array P terdiri dari delapan belas kunci 32-bit subkunci :

$P_1,P_2,.....,P_{18}$

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 :

$S_{1,0},S_{1,1},.....,S_{1,255}$

$S_{2,0},S_{2,1},.....,S_{2,255}$

$S_{3,0},S_{3,1},.....,S_{3,255}$

$S_{4,0},S_{4,1},.....,S_{4,255}$

3. Plaintext yang akan dienkripsi diasumsikan sebagai masukan, Plaintext 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 operrasi 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.

Salah satu operator yang paling banyak digunakan pada algoritma ini adalah oerator XOR berikut adalah table kebenarannnya

Tabel 2.1 Table kebenaran XOR

| P | Q | HASIL |
|---|---|---|
| F | F | F |
| F | T | T |
| T | F | T |
| T | T | F |

Lalu untuk mencari fungsi F adalah sebagai berikut :
Bagi XL, menjadi empat bagian 8-bit : a,b,c dan d.

$F(XL)=((S1,a + S2,b \bmod 2^{32})xor\ S3,c) + S4,c \bmod 2^{32}$

Subkunci dihitung menggunakan algoritma Blowfish, metodenya adalah sebagai berikut :

1. Pertama-tama inilialisasi P-array dan kemudian empat S-box secara berurutan dengan string yang tetap. String ini terdiri atas 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 Blowfish 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, kemudian seluruh keempat S-box berurutan, dengan keluaran yang berubah secara kontiyu dari algoritma Blowfish.

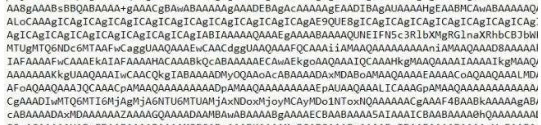
## 3. Pembahasan

Dalam penelitian ini, penulis mencoba menerapkan algoritma *blowfish* untuk mengamankan arsip gambar di BPAD kabupaten malang menggunakan

Sebelum melakukan proses enkripsi, file gambar harus di ubah terlebih dahulu kedalam bentuk string agar dapat dihitung menggunakan Algoritma B*LOWFISH,* ada beberapa cara yang bisa dilakukan, antara lain mengambil nilai RGB di setiap pixel gambar, cara ini memiliki kekurangan yaitu file hasil encode nya sangatlah besar, karena setiap pixelnya memiliki 3 nilai independen, sedangkan cara lainnya dan yang lebih praktis adalah dengan memanfaatkan BASE64 encode, selain file hasil encode yang jauh lebih kecil proses jadi lebih ringan karena mesin tidak perlu membaca setiap detil pixelnya.

Berikut adalah contoh file string asli gambar yang masih belum di proses atau bisa disebut data mentah.

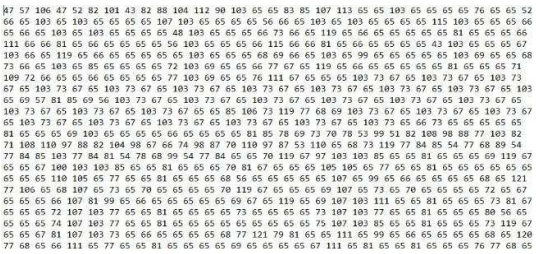
Gambar 3.1 File gambar mentah



Gambar 3.2 File hasil encode BASE64

Setelah mendapatkan file string ini, mulai proses encode dengan menggunakan base64 encode, berikut adalah contoh stringnya.

Dikarenakan proses algoritma blowfish adalah proses aritmatika maka, meubah lagi hasil setiap karakter encode BASE 64 tersebut kedalam bentuk angka decimal berdasarkan dengan karakter ASCII. Berikut adalah contoh hasilnya.



Gambar 3.3 File PlainText

Angka decimal inilah yang menjadi PlainText / Data awal yang akan di enkripsi dengan Algoritma *BLOWFISH.* Proses berikutnya sebelum enkripsi dimulai adalah menghitung subkeys, yaitu 18 buah 32bit Pbox dan 4 buah 256 entri 32bit Sbox. Yaitu XOR kan key dengan Pbox dan Sbox. Maka value pbox dan sbox akan terus berubah mengikuti kunci, berikut perhitungannya

Tabel 3.1. Menghitung SubKeys

| KEY | 3 | 5 | 2 | 7 |
|---|---|---|---|---|
| PBOX1 | 1 | 4 | 1 | 5 |
| PBOX2 | 9 | 2 | 6 | 5 |
| PBOX3 | 3 | 5 | 8 | 9 |
| dst sampai semua SBOX…. | | | | |

Setelah dilakukan perhitungan seperti tabel diatas selanjutnya di dapatkan Hasil XOR PBOX dan KEY

Tabel 3.2. hasil XOR PBOX dan KEY

| PBOX1 | 2 | 1 | 3 | 2 |
|---|---|---|---|---|
| PBOX2 | 10 | 7 | 4 | 2 |
| PBOX3 | 0 | 0 | 10 | 14 |
| dst sampai semua SBOX…. | | | | |

Setelah semua Pbox dan Sbox ter XOR dengan key mulai proses enkripsi. Dalam satu kali proses Algoritma blowfish hanya memproses 64 bit saja, berikut contoh perhitungan 64 bit pertama PlainText

Tabel 3.3 Perhitungan 64 bit pertama PlainText

| | X LEFT | | | | X RIGHT | | | |
|---|---|---|---|---|---|---|---|---|
| Plaintext | 47 | 57 | 106 | 47 | 52 | 82 | 101 | 48 |
| Pbox 1 | 2 | 1 | 3 | 2 | 21 | 27 | 18 | 10 |
| Xor Putaran 1 | 45 | 56 | 105 | 45 | 33 | 73 | 119 | 33 |
| Ulangi Sebanyak 14 Kali | | | | | | | | |
| Plaintext | 55 | 74 | 124 | 0 | 44 | 45 | 103 | 34 |
| Pbox 16 | 6 | 12 | 0 | 4 | 21 | 23 | 15 | 5 |
| Xor Putaran 16 | 49 | 70 | 124 | 4 | 57 | 58 | 104 | 39 |
| Pbox 18 | 5 | 1 | 2 | 1 | 3 | 2 | 10 | 6 |
| Xor Putaran 17 | 52 | 71 | 126 | 5 | 58 | 56 | 98 | 33 |

Tabel 3.4 Perhitngan F(x) putaran pertama

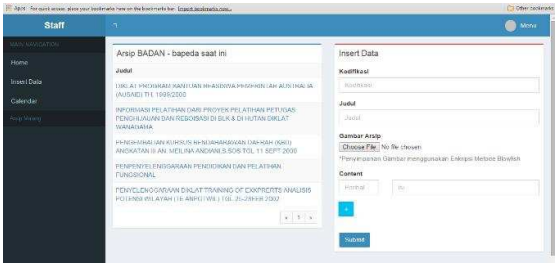
| | | | | | |
|---|---|---|---|---|---|
| SBOX 1 [45] | 5 | 13 | 3 | 7 | |
| XBOX 2 [56] | 4 | 13 | 5 | 4 | |
| | 9 | 26 | 8 | 11 | jumlah |
| SBOX 3 [105] | 7 | 2 | 7 | 15 | |
| | 14 | 24 | 15 | 4 | xor |
| SBOX 4 [45] | 7 | 3 | 3 | 6 | |
| F(X) putaran 1 | 21 | 27 | 18 | 10 | xor |

Dari table perhitungan di atas dapat dilihat kotak biru adalah awal dan hasil perhitungan

## 4. Implementasi

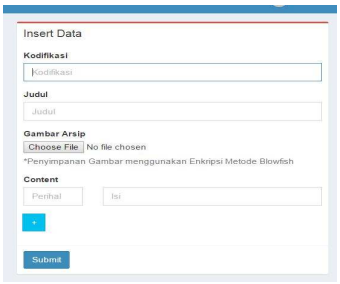
Hasil implementasi sistem informasi manajemen pengarsipan dengan menggunakan algoritma *blowfish* Sebagai Pengamanan Arsip Gambar di BPAD Kabupaten Malang. dan digambarkan secara lengkap dan terstruktur.

Halaman pertama bersi tentang penyimpanan surat dan encarian surat yang terdapat pada Sistem Informasi Manajemen Pengarsipan Dengan Menggunakan Algoritma Blowfish Sebagai Pengamanan Arsip Gambar di BPAD Kabupaten Malang.



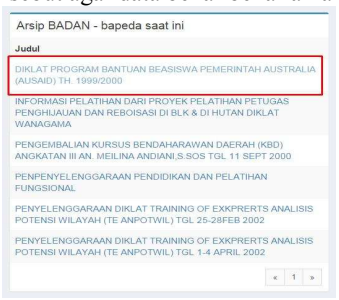

Gambar 4.1 penyimpanan data gambar

Pada sistem ini ada menu menambahkan data arsip surat yang meliputi kodifikasi , judul, gambar arsip, content. Content disini bersifat dinamis dan bisa ditambahkan sesuai kebutuhan



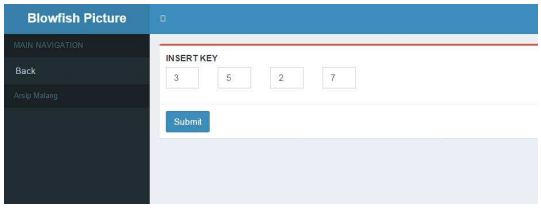

Gambar 4.2 pengisisan data

Setelah itu bisa langsung memilih judul dari arsip yang ingin dilihat dengan menekan tombol show arsip picture. Dan akan menuju ke halaman pengamanan dimana staff harus menginputkan kode untuk melihat data arsip tersebut agar data benar benar aman.



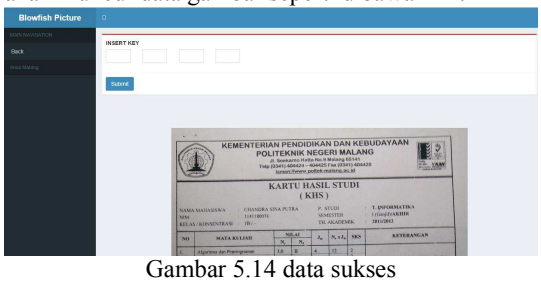

Gambar 4.3 data arsip yang masuk

Halaman inut kode untuk melihat data, halaman ini digunakan untuk media pengamanan data gambar.



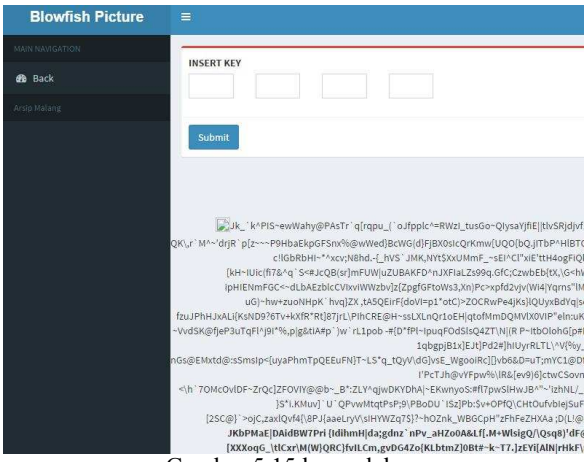

Gambar 5.13 gambar halaman melihat data

Jika key yang diisikan benar disini memakai key 3527 maka data berhasil di proses oleh system maka akan muncul data gambar seperti dibawah ini.




Gambar 5.14 data sukses

Jika key yang diisikan oleh staff salah maka data tidak berhasil di proses dan akan muncul seperti tampilan dibawah ini




Gambar 5.15 key salah

## 5. Kesimpulan dan Saran.

### 5.1 Kesimpulan

Dari aplikasi ini dapat diperoleh beberapa kesimpulan sebagai berikut :

a. Dengan adanya aplikasi ini, dapat membantu petugas pengarsipan surat untuk mempermudah dalam proses pencarian, penyimpanan arsip dan membantu untuk mendokumentasikan semua surat yang ada di BPAD Kabupaten Malang
b. Aplikasi dapat melakukan pengamanan arsip gambar di BPAD kabupaten malang menggunakan algoritma *blowfish* , sehingga agar data aman dan jauh dari resiko penyalahgunaan.

### 5.2 Saran

Kemudian saran untuk pengembangan aplikasi ini adalah sebagai berikut :

a. Bagi peneliti yang akan mengembangkan Sistem Informasi Manajemen Pengarsipan Dengan Menggunakan Algoritma Blowfish Sebagai Pengamanan Arsip Gambar (Studi Kasus : BPAD Kabupaten Malang) dapat dikembangkan menjadi sistem yang lebih baik dan lebih bervariasi dengan memakai metode serta perangkat lunak lain yang berbeda seperti android.

**Daftar Pustaka :**

Jogiyanto. 2008. *Sistem Teknologi Informasi*. Yogyakarta: Penerbit ANDI.

Joko, Mochamad. 2009. *Amazing News Website with PHP, Ajax, dan MySQL.* Yogyakarta: Penerbit ANDI.

Hakim, Lukmanul. 2009. *Trik Rahasia Master PHP*. Yogyakarta: Penerbit Lokomedia.

Hariyanto, Bambang. 2004. *Sistem Manajemen Basis Data*. Bandung: Informatika.

Hasugian, Jonner. 2009. *Pengantar Kearsipan*. Modul kuliah. Program Studi Ilmu Perpustakaan Fakultas Sastra Universitas Sumatera Utara.

Madcoms. 2009. *Menguasai XHTML, CSS, PHP, & MySQL melalui DREAMWEAVER.* Yogyakarta: Penerbit ANDI.

Muhadkly. 2007. *SMS Gateway Menggunakan Gammu.* (*online*), (http://ilmukomputer.org/2007/09/27/sms-gateway-menggunakan-gammu/*) diakses pada tanggal 26 Maret 2012.*

Nugraha WP, Antonius. 2010. *CodeIgniter: Cara Mudah Membangun Aplikasi PHP*. Jakarta Selatan: mediakita.

Pudjo Widodo, Prabowo dan Herlawati. 2011. *Menggunakan UML*. Bandung: Penerbit INFORMATIKA.

Rosa, A.S., Shalahuddin, M., 2011. *Modul Pembelajaran Rekayasa PerangkatLunak (Terstruktur dan Berorientasi Objek)*. Bandung: Modula.

Wilnic Izaac., Maraunuela . 2013. *Implementasi algoritma BLOWFISH pada basis data honorarium mengajar Dosen tidak tetap FTI UKSW* SALATIGA : FTI