SKENA TEKNOLOGI
JURNAL ILMIAH SAINS DAN TEKNOLOGI

E- ISSN: 3058-1570
Volume 2 No 2 Agustus 2025

Link Journal: https://ejournal.ibbi.ac.id/index.php/ST/index

ALGORITMA ENKRIPSI DAN DEKRIPSI MENGGUNAKAN METODE BLOWFISH DALAM KEAMANAN DATA

Tintin Chandra
Fakultas Ilmu Sains dan Teknologi Universitas IBBI
E-mail : tinuhnsbm@gmail.com

Abstrak : Pertukaran informasi sudah menjadi hal yang umum yang terjadi dalam dunia digital. Informasi yang dikirim atau diterima ada yang bersifat umum dan ada yang bersifat personal. Peranan teknologi dalam keamanan informasi tentu dibutuhkan untuk mengamankan informasi yang dikirim dalam bentuk file digital. Informasi penting berisi data rahasia tentu harus disandikan agar tidak dapat dibaca oleh pihak yang tidak berkepentingan. Data yang telah disandikan dengan teknologi dengan metode tertentu bukan data tersebut aman dari segala bentuk cobaan untuk diterobos pelaku hacker. Umumnya data sering terjadi saat ini adalah pencurian dan kebocoran data yang dilakukan oleh hacker. Penerapan kriptografi dapat mengamankan data yang tersimpan atau terkirim menjadi lebih aman sampai dengan data tersebut dibuka oleh penerima yang bersangkutan. Ada karateristik kriptografi yaitu kriptografi klasik dan kriptografi modern. Blowfish dikembangkan dengan desain yang cepat dalam penerapannya dimana pada beberapa kondisi optimal. Enkripsi adalah suatu proses yang dilakukan untuk mengubah pesan asli menjadi chipertext. proses yang dilakukan untuk mengubah pesan tersembunyi menjadi pesan asli disebut dekripsi. Enkripsi data dilakukan untuk memastikan bahwa data atau informasi dalam proses pengiriman tidak direkayasa orang lain. Blowfish merupakan enkripsi yang termasuk dalam golongan Symmetric Cryptosystem dengan menggunakan kunci yang sama untuk enkripsi dan dekripsinya. Kunci yang telah terbentuk akan digunakan pada saat enkripsi maupun dekripsi. Iterasi fungsi sederhana dilakukan 16 kali putaran, dimana setiap putaran terdiri dari permutasi kunci-dependent dan substitusi kunci dan data-dependent.

Kata Kunci: Algoritma, Keamanan Data, Blowfish

Abstract : Information exchange has become a common thing that occurs in the digital world. Information sent or received is either general or personal. The role of technology in information security is certainly needed to secure information sent in the form of digital files. Important information containing confidential data must of course be encoded so that it cannot be read by unauthorized parties. Data that has been encoded with technology with a certain method is not safe from all forms of attempts to be penetrated by hackers. Generally, data that often occurs today is theft and data leaks carried out by hackers. The application of cryptography can secure data that is stored or sent to be safer until the data is opened by the recipient concerned. There are characteristics of cryptography, namely classical cryptography and modern cryptography. Blowfish was developed with a design that is fast in its application where in some optimal conditions. Encryption is a process that is carried out to convert the original message into ciphertext. the process carried out to convert a hidden message into an original message is called decryption. Data encryption is carried out to ensure that data or information in the delivery process is not engineered by others. Blowfish is an encryption that is included in the Symmetric Cryptosystem group by using the same key for encryption and decryption. The key that has been formed will be used during encryption and decryption. Simple function iteration is performed 16 times, where each round consists of key-dependent permutations and key and data-dependent substitutions.

Keyword: Algorithm, Data Security, Blowfish

1. PENDAHULUAN

Pertukaran informasi baik dalam teks, foto, suara, atau video sudah menjadi hal yang umum yang terjadi dalam dunia digital. Informasi yang dikirim atau diterima ada yang bersifat umum dan ada yang bersifat personal. Pertukaran informasi tentu melibatkan jaringan dengan keamanan yang telah diatur sedemikian rupa baik penerima atau pengirim. Peranan teknologi dalam keamanan informasi tentu dibutuhkan untuk mengamankan informasi yang dikirim dalam bentuk file digital. Informasi penting berisi data rahasia tentu harus disandikan agar tidak dapat dibaca oleh pihak yang tidak berkepentingan. Umumnya perusaahan biasanya menggunakan teknologi penyandian baik yang sifat publik yang disediakan

E- ISSN: 3058-1570
Volume 2 No 2 Agustus 2025
Link Journal: https://ejournal.ibbi.ac.id/index.php/ST/index

oleh platform digital atau private yang berlisensi agar informasi yang terkirim lebih aman kerahasiaan. Data yang telah disandikan dengan teknologi dengan metode tertentu bukan data tersebut aman dari segala bentuk cobaan untuk diterobos pelaku hacker. Umumnya data sering terjadi saat ini adalah pencurian dan kebocoran data yang dilakukan oleh hacker atau merekayasa data tanpa seizin pengirim, maka pengguna data harus mencari solusi untuk mengamankan data tanpa melibatkan pihak administrator.

Penerapan kriptografi dapat mengamankan data yang tersimpan atau terkirim menjadi lebih aman sampai dengan data tersebut dibuka oleh penerima yang bersangkutan. Ada karateristik kriptografi yaitu kriptografi klasik dan kriptografi modern. Kriptografi klasik atau simetrik menggunakan algoritma yang menggunakan satu kunci untuk mengamankan data. Teknik dasar yang digunakan berupa substitusi dan transposisi. Kriptografi modern atau asimetrik menggunakan algoritma yang lebih kompleks daripada algoritma klasik, karena algoritma asimietrik menggunakan komputer dalam pemrosesan kunci.

Blowfish dikembangkan dengan desain yang cepat dalam penerapannya dimana pada beberapa kondisi optimal dapat mencapai 26 ccb (Clock Cycle Byte), dimana dapat berjalan pada memori kurang dari 8 KB, sederhana dalam algoritmanya sehingga mudah diketahui kesalahannya, dan keamanan yang variabel dimana panjang kunci bervariasi (paling sedikit 32 bit, paling banyak 448 bit, Multiple 8 bit, secara umum 128 bit). Untuk menangani kendala keamanan data, maka salah satu teknik yang digunakan dalam pengamanan data adalah dengan menerapkan algoritma penyandian data.

Enkripsi adalah suatu proses yang dilakukan untuk mengubah pesan asli menjadi chipertext. Sedangkan suatu proses yang dilakukan untuk mengubah pesan tersembunyi menjadi pesan asli disebut dekripsi. Pesan biasa atau pesan asli disebut plaintexts edangkan pesan yang telah diubah atau disandikan supaya tidak mudah dibaca disebut dengan chipertext.

Untuk mengatasi kendala keamanan data, peneliti memilih algoritma enkripsi dan dekrispi menggunakan metode Blowfish. Enkripsi data dilakukan untuk memastikan bahwa data atau informasi dalam proses pengiriman tidak direkayasa orang lain. Blowfish merupakan enkripsi yang termasuk dalam golongan Symmetric Cryptosystem dengan menggunakan kunci yang sama untuk enkripsi dan dekripsinya.

2. LANDASAN TEORI

Kriptografi (cryptographi) berasal dari BahasaYunani: “cryptos” artinya “secret” (rahasia), sedangkan “graphein” artinya “writing” (tulisan). Sehingga kriptografi berarti “secret writing” (tulisan rahasia). Jadi kriptografi didefinisikan sebagai ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya kebentuk yang tidak dapat dimengerti lagi maknanya. Secara umum kriptografi merupakan teknik pengamanan informasi yang dilakukan dengan cara mengolah informasi awal (plainteks) dengan suatu kunci tertentu menggunakan suatu metode enkripsi tertentu sehingga menghasilkan informasi baru (chipertext) yang tidak dapat dibaca secara langsung. Chipertext tersebut dapat dikembalikan menjadi informasi awal (plainteks) melalui proses dekripsi.

Semakin banyak informasi perusahaan yang disimpan, dikelola dan di-sharing-kan maka semakin besar pula resiko terjadi kerusakan, kehilangan atau terekspos nya data ke pihak eksternal yang tidak dinginkan. Beberapa istilah yang terdapat dalam kriptografi sebagai berikut:

1. Pesan, plaintext dan Ciphertext.
   Pesan (message) adalah data atau informasi yang dapat dibaca dan dimengerti maknanya. Nama lain untuk pesan adalah plaintext atau teks jelas (cleartext). Agar pesan tidak dimengerti oleh pihak lain yang tidak berkepentingan, maka pesan perlu disandikan menjadi bentuk lain yang tidak dapat dipahami. Bentuk pesan tersandi disebut ciphertext atau cryptogram.
   Cipherteks harus dapat ditransformasi kembali menjadi plainteks. Sebagai contoh plainteks, uang disimpan di balik buku X, maka cipherteksnya adalah j&kloP#d$gkh*7h^”tn%6^klp..t@.
2. Pengirim dan penerima
   Komunikasi data melibatkan pertukaran pesan antara dua entitas. Pengirim (sender) adalah entitas yang mengirim pesan kepada entitas lainnya. Penerima (receiver) adalah entitas yang menerima pesan. Entitas dapat berupa orang, mesin, kartu kredit dan sebagainya.
3. Enkripsi dan dekripsi
   Proses menyandikan plainteks menjadi chiperteks disebut enkripsi (encryption). Sedangkan proses mengembalikan ciphertext disebut enkripsi (encryption), sedangkan proses mengembalikan ciphertext menjadi plaintext disebut dekripsi (decryption).
4. Algoritma Kriptografi dan Kunci
   Algoritma kriptografi disebut juga chiper yaitu aturan untuk enchipering dan dechipering, atau fungsi matematika yang digunakan untuk enkripsi dan dekripsi. Kriptografi modern mengatasi masalah keamanan algoritma kriptografi dengan penggunaan kunci. Kunci (key) adalah parameter yang

SKENA TEKNOLOGI
JURNAL ILMIAH SAINS DAN TEKNOLOGI
E- ISSN: 3058-1570
Volume 2 No 2 Agustus 2025
Link Journal: https://ejournal.ibbi.ac.id/index.php/ST/index

digunakan untuk transformasi enchipering dan dechipering. Kunci biasanya berupa string atau deretan bilangan.

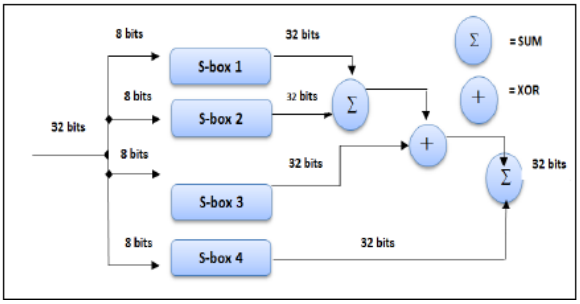
5. Sistem kriptografi
   Kriptografi membentuk sebuah sistem yang dinamakan sistem kriptografi. Menurut Schneier dan Munir, system kriptografi (cryptosystem) adalah kumpulan yang terdiri atas algoritma kriptografi, semua plainteks dan chiperteks yang mungkin serta kunci.
6. Kriptanalisis dan kriptografi
   Kriptanalisis (cryptanalysis) adalah ilmu dan seni untuk memecahkan chiperteks menjadi plainteks tanpa mengetahui kunci yang diberikan. Pelakunya disebut kriptanalis. Kriptologi (cryptology) adalah studi mengenai kriptografi dan kriptanalisis.

Algoritma blowfish menggunakan ekspansi kunci yang merubah kunci menjadi beberapa array minimum 32-bit dan maksimum 448-bit) dengan total 4168 byte (18x32-bit untuk P-array dan 4x256x32-bit untuk S-box) menjadi 33344 bit atau 4168 byte. Kunci disimpan dalam K-array:

$K_1,K_2,.....,K_j$, dimana $1 \leq j \leq 14$. Kunci ini dibangkitkan dengan menggunakan subkunci yang harus dihitung sebelum enkripsi atau dekripsi data. Sub-sub kunci yang digunakan terdiri dari :

1. Inisialisasi P-array dan kemudian empat S-box secara berurutan dengan string tetap. String ini terdiri dari digit. Hexadecimal 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. Enkripsikan semua string nol dengan algoritma Blowfish menggunakan subkunci seperti yang dijelaskan pada langkah 1 dan langkah 2.
4. Gantikan P1 dan P2 dengan keluaran dari langkah 3.
5. Enkripsikan keluaran langkah 3 dengan algoritma Blowfish dengan subkunci yang sudah termodifikasi.
6. Gantikan P3 dan P4 dengan keluaran dari langkah 5.
7. Gantikan seluruh elemen dari P-array, dan kemudian seluruh keempat S-Box berurutan, dengan keluaran yang berubah secara kontinyu dari Algoritma Blowfish.

Untuk proses pembentukan kunci dapat dilihat pada gambar 1., dimana menunjukkan tahapan penggunaan operasi XOR dan penggunaan array pada S-Box.



Gambar 1. Skema Fungsi F Algoritma Blowfish

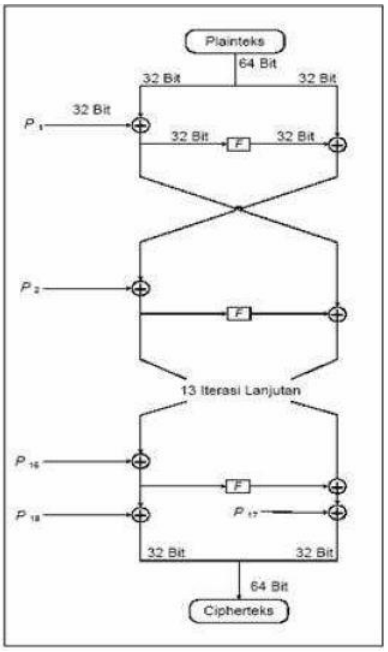
Kunci yang telah terbentuk akan digunakan pada saat enkripsi maupun dekripsi. Iterasi fungsi sederhana dilakukan 16 kali putaran, dimana setiap putaran terdiri dari permutasi kunci-dependent dan substitusi kunci dan data-dependent. Semua operasi adalah penambahan (addition) dan XOR pada variabel 32-bit. Semua Operasi adalah tambahan lainnya hanyalah empat penelusuran table (table lookup) array berindeks untuk setiap putaran.

Operasi tambahan lainnya hanyalah empat penelusuran tabel array berindeks untuk setiap putaran. Adapun langkahnya yang dikerjakan yaitu:

SKFNA TEKNOLOGI
JURNAL ILMIAH
SAINS DAN TEKNOLOGI
E- ISSN: 3058-1570
Volume 2 No 2 Agustus 2025
Link Journal: https://ejournal.ibbi.ac.id/index.php/ST/index

1. Plaintext yang akan dienkripsi diasumsikan sebagai X, X tersebut diambil sebanyak 64-bit, dan apabila kurang dari 64-bit maka ditambahkan bitnya, supaya dalam operasi nanti sesuai dengan datanya.
2. Bagi X menjadi dua bagian yang masing-masing terdiri dari 32-bit yaitu XL dan XR.
   For i = 1 to 16 :
   (a) XL = XL Xor P(i).
   (b) XR = F(XL) Xor XR.
   (c) Tukar XLdan XR.
3. Setelah iterasi keenam belas, tukar XLdan XR, lagi untuk membatalkan pertukaran terakhir.
4. Lalu lakukan :
   (a) XR = XR Xor P17
   (b) XL = XL Xor P18
5. Gabungkan kembali XL dan XR untuk mendapatkan ciphertext.

Untuk proses enkripsi iterasi algoritma blowfish dapat dilihat pada gambar 2., dimana menunjukkan tahapan pada jaringan feistel (feistel network) yang digunakan Blowfish.



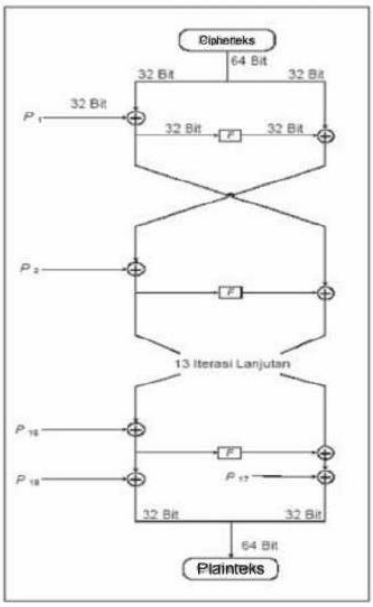
Gambar 2. Blok Diagram Enkripsi Algoritma Blowfish

Proses dekripsi Algoritma Blowfish sama seperti proses enkripsi Blowfish. Perbedaan terletak pada urutan penggunaan sub kunci P_1, P_2,..,P_{18}. Pada proses dekripsi Blowfish urutan penggunaan sub kunci dibalik dimana untuk proses enkripsi P_1, P_2,.....,P_{18} dan pada saat dekripsi menjadi P_{18}, P_{17},....., P_1. Dekripsi merupakan proses mengembalikan cipherteks menjadi plainteks semula dengan algoritma:

for i = 1 to 16 do
XRi = XLi-1 ⊕ P19-i;
XLi = F[XRi] ⊕ XRi-1;
XL17 = XR16 ⊕ P1;
XR17 = XL16 ⊕ P2;

Untuk proses dekripsi iterasi algoritma blowfish dapat dilihat pada gambar 3., dimana menunjukkan tahapan pada jaringan feistel (feistel network) yang digunakan Blowfish

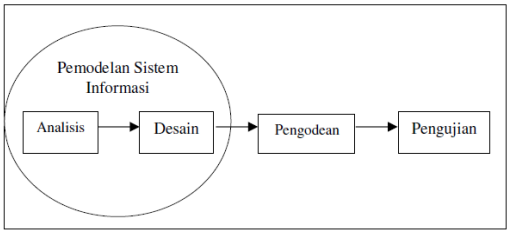
SKENA TEKNOLOGI
JURNAL ILMIAH SAINS DAN TEKNOLOGI
E- ISSN: 3058-1570
Volume 2 No 2 Agustus 2025
Link Journal: https://ejournal.ibbi.ac.id/index.php/ST/index



Gambar 3. Blok Diagram Dekripsi Algoritma Blowfish

3. METODE PENELITIAN

Metode yang diterapkan peneliti pada penelitian algoritma enkripsi dan dekripsi menggunakan metode blowfish dalam keamanan data adalah metode waterfall dapat dilihat pada gambar 4.

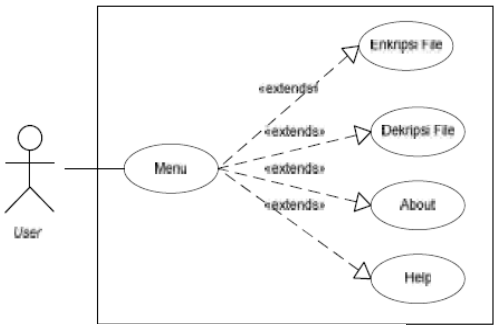


Gambar 4. Tahapan dalam Waterfall

Tahapan awal dari metode waterfall dengan proses pengumpulan kebutuhan seperti data yang di simpan dalam dokumen yang dibuat atau disimpan dalam file oleh user. Tahapan kedua dari metode waterfall adalah desain dimana proses berfokus pada desain kebutuhan program perangkat lunak, arsitektur perangkat lunak, representasi antarmuka, dan koding. Tahapan ketiga dari metode waterfall adalah pengkodean program dari tahapan desain yang dibuat dan diubah ke bahasa pemograman. Tahapan terakhir dari metode waterfall adalah pengujian dari koding yang dibuat, pengujian difokus pada proses enkripsi dan dekripsi dari segi logika dan fungsional serta memastikan semua algoritma berjalan dengan benar. Apabila pada tahap pengujian terdapat kesalahan maka perlu diperbaiki supaya file yang di-enkrispi dan di-dekripsi sesuai dengan alogirma blowfish. Setelah pengujian telah selesai, maka perlu tahapan pemeliharaan dimana tidak tertutup kemungkinan untuk penambahan atau perubahan proses S-Box maupun dalam modul yang dirancang.

Rancangan menggunakan UML yang meliputi UCase Diagram. Pada UCase Diagram seperti pada gambar 5. melibatkan 1 entitas berupa aktor yaitu user.

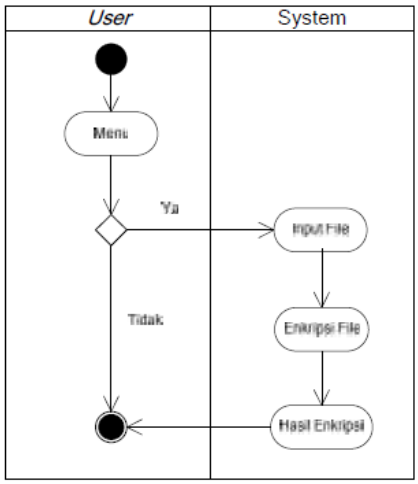
SKENA TEKNOLOGI
JURNAL ILMIAH SAINS DAN TEKNOLOGI
E- ISSN: 3058-1570
Volume 2 No 2 Agustus 2025
Link Journal: https://ejournal.ibbi.ac.id/index.php/ST/index



Gambar 5. Use Case Diagram

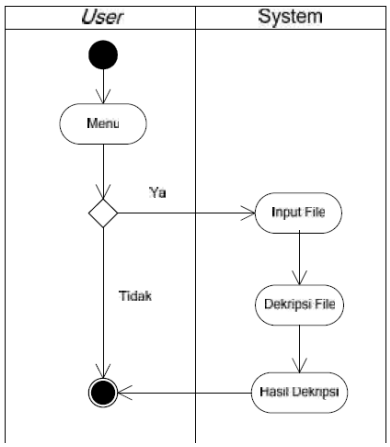
Aktor dalam entitas yaitu user dalam memiliki hak akses ke semua modul dalam penggunaan algoritma blowfish. Modul secara berfokus pada algoritma enkripsi dan dekripsi file.

Setelah merancang Ucase diagram maka peneliti melanjutkan dengan merancang aktiviti diagram dimana menggambarkan aktor berupa user melakukan proses algoritma enkripsi file melalui input file enkripsi kemudian diproses, aktor berupa user akan memperoleh file hasil enkripsi dimana isi file tersebut sudah berubah menjadi ciphertext. File ciphertext apabila dibuka maka isi file tidak dapat dibaca apabila tidak dilakukan proses dekripsi ke plaintext. Diagram aktivitas enkripsi dapat dilihat pada gambar 6.



Gambar 6. Aktiviti Diagram Enkripsi

Untuk mengembalikan ciphertext yang telah di-enkripsi maka perlu dilakukan proses dekrispi. Proses diagram aktiviti dekripsi dapat dilihat pada gambar 7. melalui proses input ciphertext. Ciphertext akan diproses menggunakan algoritma dekripsi, dengan algorima dekripsi maka ciphertext diubah menjadi plaintext seperti file semua sebelum di enkripsi. Apabila file plaintext yang telah di-dekripsi maka file tersebut bisa terbaca dan sama seperti file awal.



Gambar 7. Aktiviti Diagram Dekripsi

SKFNA TEKNOLOGI
JURNAL ILMIAH SAINS DAN TEKNOLOGI
E- ISSN: 3058-1570
Volume 2 No 2 Agustus 2025
Link Journal: https://ejournal.ibbi.ac.id/index.php/ST/index

4. HASIL DAN PEMBAHASAN

Kriptografi simetrik dapat dikatakan cukup kuat dengan menggunakan kata kunci minimal 8 karakter dengan kombinasi angka dalam pengamanan data. Kriptografi simetrik dapat digunakan untuk tujuan otentikasi agar penerima data atau informasi dapat memastikan keabsahan data tersebut dari orang yang mengirimkan data atau informasi. Pengirim akan mengirimkan sebuah data atau informasi yang terenkripsi dengan menggunakan kunci public dimana kunci private maka data diolah menajdi ciphertext. Proses pembentukan ciptertext telah terjadi proses otentikasi kepada pengirim yaitu kunci rahasia menjadi identitas dari pengirim pribadi.

Peneliti dalam melakukan proses pengujian terhadap algoritma blowfish yaitu dengan memastikan baris kode program telah dibuat berjalan dengan baik, peneliti juga melakukan pengujian terhadap beberapa tipe data atau file yang akan di-enkripsi maupun dan di-dekripsi kembali dengan ekstension docx, xlsx, mp3, ppt,dan pdf. Tahap perancangan algoritma pengamanan data menggunakan Flowchart. Pengujian algoritma terdiri dari pengujian black box, pengujian kinerja serta pengujian keamanan. Pengujian black box dilaksanakan dengan mengeksekusi modul, kemudian dair hasil dari modul tersebut apakah sesuai dengan proses berjalan sesuai algorima blowfish. Pengujian performa dilaksanakan untuk mengetahui waktu proses enkripsi dengan melakukan pengujian beberapa file. Pengujian keamanan untuk menguji sistem dikembangkan telah memenuhi aspek keamanan atau tidak meliputi confidentiality, data integrity, authentication dan non-repudiation. Langkah dalam melakukan pengubahan dari plaintext “kamu” yaitu

k = 01101011 a = 01100001
m = 01101101 u = 01110101

Sehingga plaintext “kamu” apabila dirubah menjadi biner akan menjadi “01101011011000010110110101110101”. Plaintext tersebut bernilai 32 bit dihitung berdasarkan jumlah digit yang dihasilkan. Peneliti dalam percobaan menggunakan kata kunci “kalian” dan diubah menjadi biner

k = 01101011 a = 01100001
l = 01101100 i = 01101001
a = 01100001 n = 01101110

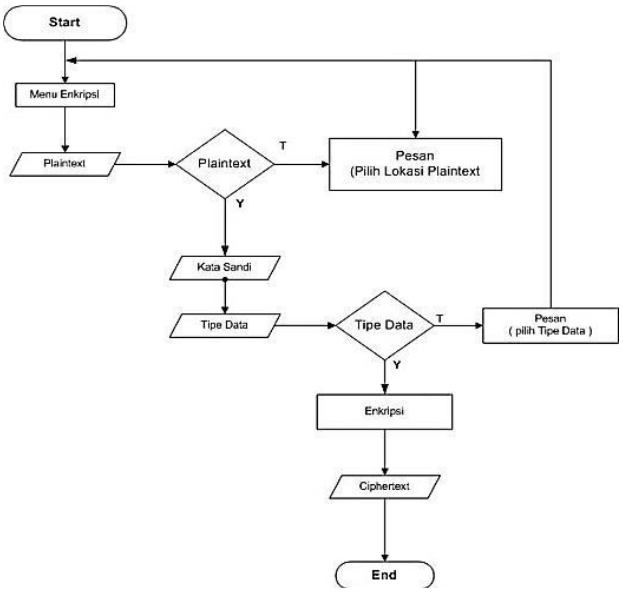
Sehingga key “kalian” apabila dirubah menjadi biner akan menjadi “01101011011000010110110001101001011000101101110”. Panjang Key bernilai 48 bit karena berdasarkan jumlah bit yang dihasilkan. Algoritma blowfish mengambil 64 bit data sehingga plaintext bertambah bit nilainya menjadi Plain-text = 0000000000000000000000000000000001101011011000010110110101110101. Pada proses pengambilan kunci harus memiliki 32 bit atau kelipatannya sehingga kunci yang digunakan peneliti bertambahan bit menjadi Key = 00000000000000000110101101100001011011000110100101100001011 01110. Plaintext 64 bit yang dibentuk kemudian dibagi 2 dimana 32 bit pertama disebut XL, 32 bit yang kedua disebut XR menjadi:

XL = 00000000000000000000000000000000
XR = 01101011011000010110110101110101

Karena key merupakan kelipatan 32 bit maka, pembagian key menjadi : P1, P3, P5, P7, P9, P11, P13, P15, P17 = 00000000000000000110101101100001, P2, P4, P6, P8, P10, P12, P14, P16, P18 = 0110110001101001011000010110110101110.

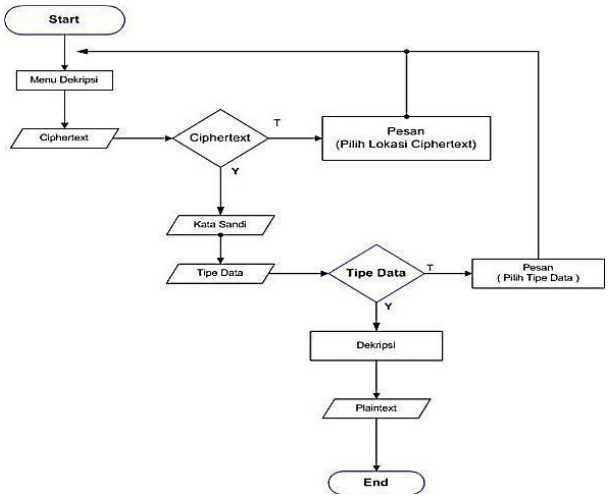
Perancangan algoritma pengamanan data dari proses enkripsi dapat dilihat pada gambar 8. Analisis algoritma bertujuan untuk memberikan gambaran proses terbentuknya ciphertext.

SKFNA TEKNOLOGI
JURNAL ILMIAH
SAINS DAN TEKNOLOGI
E- ISSN: 3058-1570
Volume 2 No 2 Agustus 2025
Link Journal: https://ejournal.ibbi.ac.id/index.php/ST/index



Gambar 8. Flowchat Proses Enkripsi

Perancangan algoritma pengamanan data dari proses dekripsi dapat dilihat pada gambar 9. Analisis algoritma bertujuan untuk memberikan gambaran proses terbentuknya ciphertext.



Gambar 9. Flowchat Proses Dekripsi

Pengujian algoritma dalam mengenkripsi beberapa ekstension file dapat dilihat pada tabel 1.

Tabel 1. Hasil Pengujian Beberapa Ekstension File

Nama *File*	Ukuran File Asli (KB)	Ukuran File Enkripsi (KB)	Waktu Enkripsi (s) Metode Blowfish	Waktu Dekripsi (s) Metode Blowfish
Daflatih Komputer.docx	43	43	4	4
RAB KOMTIK 2013.xlsx	18	18	4	4
SmartCar Android.pptx	97	97	3	3
Proposal Infotek.pdf	997	998	4	4
lagu relegi.mp3	5,078	5,078	1	1
video Corning glass.flv	15,011	15,011	4	4

SKENA TEKNOLOGI
JURNAL ILMIAH SAINS DAN TEKNOLOGI
E- ISSN: 3058-1570
Volume 2 No 2 Agustus 2025
Link Journal: https://ejournal.ibbi.ac.id/index.php/ST/index

Waktu proses enkripsi dan dekrispi secara umum lamanya sama, dan untuk ukuran file relatif sama walaupun kadang-kadang terjadi perbedaan sedikit antara file asli dengan file enkrippsi hal ini disebabkan karena sewaktu proses enkripsi dilakukan penambahan bit baik dari isi file dan kunci yang digunakan. Kecepatan enkripsi dan dekripsi juga tergantung pada besarnya file yang mau diamankan.

5. KESIMPULAN DAN SARAN

Algoritma Blowfish berfungsi untuk mengamankan data ataupun informasi yang berupa text dengan mengacak text tersebut sehingga menjadi sederetan text yang tidak memiliki arti serta tidak dimengerti. Hasil pengacakan text dengan menggunakan metode terbalik dari S-Box maka text akan di kembalikan ke text awal dengan kunci yang sama sehingga text tersebut dapat dibaca. Penggunaan algoritma Blowfish menggunakan enkripsi dan dekripsi menggunakan kata sandi untuk otentikasi, integritas dan non repudiation antara pengirim dan penerima sebagai identitas diri sebagai pemilik data yang berhak. Penggunaan algoritma enkripsi dan dekripsi menggunakan metode Blowfish merupakan salah satu metode pengacakan dalam pengamanan data. Algoritma blowfish memanfaatkan S-Box dalam pengacakan sandi yang disimpan dalam bentuk cipher sehingga pihak yang tidak berkepentingan yang mendapatkan data hanya akan mendapatkan sederetan karakter yang tidak ada artinya. File cipher yang diterima oleh penerima yang bersangkutan akan menggunakan kata sandi untuk membalikan ke data semula menjadi plain file, sehingga penerima dapat membaca isi data yang dikirim

REFERENSI

Sumarkidjo dkk., 2007, Jelajah Kriptografi, Lembaga Sandi Negara, Jakarta.

Wahana., 2003, Memahami Model Enkripsi dan Security Data, Andi Offset, Yogyakarta.

Whitten, L.J, Bentley, D.L & Dittman, C.K.. 2004, System Analysis and Design Methods, USA Mc Grawhill, Inc.

Hartini, Sri Primaini, 2013, Kriptografi Password Menggunakan Modifikasi Metode Affine Ciphers, Vol 2, No.1, AMIK SIGMA, Palembang

Natasha, Anang Eko Wicaksono, 2011, Penerapan teknik kriptografi stream-cipher untuk pengaman basis data. Jurnal Basis Data, ICT Research Center UNAS Vol. 6, No. 1, Universitas Nasional, Jakarta Selatan.

Sholeh, A.T., Erwin Gunadhi, Asep Deddy Supriatna, 2013, Mengamankan Skrip Pada Bahasa Pemograman Php Dengan Menggunakan Kriptografi Base64, Jurnal STT Garut Vol 10, No. 1, Sekolah Tinggi Teknologi Garut, Garut.