p-ISSN : 2598-0416 e-ISSN : 2615-689X

JURNAL ARMADA INFORMATIKA

STMIK Methodist Binjai

jurnal.stmikmethodistbinjai.ac.id/jai

Keamanan Informasi

PENGGUNAAN ALGORITMA TWOFISH UNTUK PENGAMANAN DATA TEKS

Jaidup Banjarnahor [1]

[1] *Program Studi Manajemen Informatika, Universitas Mandiri Bina Prestasi, Medan, Indonesia*

INFORMASI ARTIKEL

Diterima Redaksi: 01 Agustus 2023
Revisi Akhir: 10 November 2023
Diterbitkan *Online*: 01 Desember 2023

KATA KUNCI

Kriptografi, Pengamaman Pesan, Towfish

KORESPONDENSI

Phone: +62 813-7023-5302

E-mail: marbun2005@gmail.com

A B S T R A K

Komunikasi merupakan bagian dari kehidupan masyarakat pada jaman sekarang ini, dimana komunikasi dapat dilakukan dengan menggunakan komunikasi berupa suara,gambar,teks maupun bentuk bentuk yang lainnya dengan tujuan bahwa antara si pemberi pesan dan si penerima dapat saling mengerti. Kemajuan teknologi saat ini sangat memungkinkan bahwa si pemberi pesan melakukan komunikasi atau memberikan pesan kepada si tujuan berupa dokumen dalam bentuk digital sehingga informasi yang disampaikan bisa semakin banyak dan lengkap. Disamping kemudahan ini ancaman juga terjadi dimana dokumen yang dikirim dalam bentuk digital melalui jaringan komputer memungkinkan jatuh ketangan yang tidak bertanggung jawab sehingga informasi atau pesan bisa bocor ke orang lain atau bahkan orang yang mendapatkan pesan tadi memiliki kesempatan untuk mengubah pesan sehingga pesan yang disampaikan oleh si pemberi pesan berbeda dengan yang diterima oleh si penerima karena sudah diubah terlebih dahulu. Untuk mengatasi hal ini perlu penyandian atau teknik kriptografi yaitu mengubah pesan aslinya (plain teks) menjadi pesan yang tidak memiliki arti (chiper text) sehingga kalaupun jatuh ketangan orang, dia akan sulit memahami isi pesan yang dimaksud. Teknik perubahan plain teks menjadi chiper teks dan juga sebaliknya yaitu mengubah pesan yang telah diubah ke pesan aslinya. Kriptografi merupakan cara yang tepat digunakan untuk mengamankan pesan ataupun dokumen dimana teknik dan seni kriptografi dapat mengubah pesan asli menjadi pesan terenkripsi, serta mengembalikan pesan terenkripsi menjadi pesan aslinya. Dari beberapa metode kriptografi, algortima kritptografi twofish dinyatakan sebagai teknik enkripsi yang kuat karena harus menggunakan kunci untuk melakukan enkrisi maupun deskripsi, teknik ini juga melakukan enkripsi dengan metode blok yaitu bekerja dengan kode biner yang merupakan metode dari kriptografi modern. Namun demikian secara terminologinya bahwa pemberi dan penerima pesan adalah objek yang berbeda, maka dikedua belah pihak harus memiliki system masing masing dimana enkripsi atau mengubah pesan asli menjadi pesan terenkripsi ada pada si pemberi pesan, sedangkan pada si penerima harus memilki system untuk mengubah pensan yang terenkripsi menjadi pesan aslinya.

PENDAHULUAN

Data atau informasi pada era teknologi digital ini merupakan bagian yang sangat penting untuk menjalankan segalan lini kehidupan, baik itu kehidupan secara pribadi atau perorangan ataupun pada kehidupan komunitas atau kelompok. Dengan demikian pertukaran data maupun informasi baik secara orang perorang maupun antar komunitas sudah menjadi rutinitas sehari sehari.

Penggunaan teknologi digital sangat mendukung untuk melakukan pertukaran data atau informasi sehingga pegirim maupun si penerima tidak lagi terbatas dengan ruang dan waktu yang berarti sipengirim dapat mengirimkan data atau informasi yang dapat sebut sebagai pesan dimanapun dan kapanpun, dan sebaliknya sipenerima pun dapat meneriam pesan dimana pun dia berada. Dengan kondisi seperti itu, tidak menjamin bahwa pesan yang dikirim sipengirim hanya jatuh ke sipenerimma karena mengunakan media komunikasi public.

https://doi.org/

Jika pesan yang dikirim merupakan pesan rahasia bisa berdampak sangat fatal jika pesan itu jatuh ketangan orang lain, sehingga dapat digunakan sebagai sebagai alat kriminal atau pun tindakan tindakan yang dapat merugikan orang ataupun komunitas tersebut. Hal ini dapat dihindari dengan mengelabui orang yang tidak berkepentingan dengan pesan terbut diamana pesan yang diterima seakan akan tidak memiliki makna karena pesan yang dia dapat adalah pesan yang sudah di acak ataupun sudah diubah ke bentuk lainnya yang tidak dapat dipahami atau yang disebut dengan pesan terenkripsi.
Terdapat dua jenis enkripsi yang dapat digunakan, yaitu enkripsi simetris dan asimetris. Pada enrkipsi simetris, kunci yang digunakan dalam proses dekripsi sama dengan yang digunakan dalam proses enkripsi. Enkripsi juga dapat dibedakan lagi menjadi dua jenis, yaitu stream cipher dan block cipher. Stream cipher memproses data secara bit per bit, sedangkan block cipher memroses data dalam bentuk blok dengan ukuran tetap yang terdiri dari bit data. [1].
Penelitian ini akan melakukan enkripsi dengan kriptografi dengan model block chipher terhadap pesan teks dengan algoritma twofish. Untuk dokumen pesan teks yang dapat di uji pada penelitian ini adalah : Teks biasa (*.txt), Portable Document Format (*.pdf), Open Document Format Word Processing (*.odt) dan Dokumen (*.doc).

TINJAUAN PUSTAKA

Kriptografi

Kriptografi berasal dari bahasa Yunani, crypto dan graphia. Crypto berarti secret (rahasia) dan graphia berarti writing (tulisan). Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain [2]. Algoritma kriptografi merupakan langkah-langkah logis bagaimana menyembunyikan pesan dari orang-orang yang tidak berhak atas pesan tersebut. Algoritma kriptografi terdiri dari tiga fungsi dasar, yaitu :

1. *Enkripsi* : merupakan hal yang penting dalam kriptografi, merupakan pengamanan data yang dikirimkan agar terjaga kerahasiaannya. Pesan asli disebut plaintext, yang diubah menjadi kode-kode yang tidak dimengerti. Enkripsi bisa diartikan dengan cipher atau kode. Sama halnya dengan kita tidak mengerti akan sebuah kata maka kita akan melihatnya di dalam kamus atau daftar istilah. Beda halnya dengan enkripsi, untuk mengubah teks-asli ke bentuk teks-kode kita menggunakan algoritma yang dapat mengkodekan data yang kita inginkan.
2. *Dekripsi*: merupakan kebalikan dari enkripsi. Pesan yang telah dienkripsi dikembalikan ke bentuk asalnya (teks-asli), disebut dengan dekripsi pesan. Algoritma yang digunakan untuk dekripsi tentu berbeda dengan algoritma yang digunakan untuk enkripsi.
3. *Kunci*: yang dimaksud di sini adalah kunci yang dipakai untuk melakukan enkripsi dan dekripsi. Kunci terbagi menjadi dua bagian, yaitu kunci rahasia (private key) dan kunci umum (public key).

Keamanan dari algoritma kriptografi tergantung pada bagaimana algoritma itu bekerja. Algoritma kriptografi dibagi menjadi tiga bagian berdasarkan kunci yang dipakai :

1. Algorima Simetri (menggunakan satu kunci untuk enkripsi dan dekripsinya). Algoritma ini disebut algoritma klasik karena memakai kunci yang sama untuk kegiatan enkripsi dan dekripsi. Keamanan dari pesan yang menggunakan algoritma ini tergantung pada kunci. Jika kunci tersebut diketahui oleh orang lain maka orang tersebut dapat melakukan enkripsi dan dekripsi terhadap pesan. Algoritma yang memakai kunci simetri diantaranya adalah :
    a. Data Encryption Standar (DES).
    b. RC2, RC4, RC5, RC6
    c. International Data Encryption Algorithm (IDEA)
    d. Advanced Encryption Standard (AES)
    e. One Time Pad (OTP)
    f. A5, dan lain sebagainya.
2. Algorima Asimetri (menggunakan kunci yang berbeda untuk enkripsi dan dekripsinya. Algoritma asimetri sering juga disebut dengan algoritma kunci publik, dengan arti kunci kata yang digunakan untuk melakukan enkripsi dan dekripsi berbeda. Algoritma yang memakai kunci publik di antaranya adalah :
    a. Digital Signature Algorithm (DSA)
    b. RSA
    c. Diffie-Hellman (DH)
    d. Elliptic Curve Cryptography (ECC)
    e. Kriptografi Quantum, dan lain sebagainya.

3. Hash Function,Fungsi Hash sering disebut dengan fungsi Hash satu arah (one-way function), message digest, fingerprint, fungsi kompresi dan message authentication cade (MAC), merupakan suatu fungsi matematika yang mengambil masukan panjang variabel dan mengubahnya ke dalam biner dengan panjang yang tetap. Fungsi Hash biasanya diperlukan bila ingin membuat sidik jari dari suatu pesan. Sidik jari pada pesan merupakan suatu tanda bahwa pesan tersebut benar-benar berasal dari orang yang diinginkan.

Algoritma Twofish

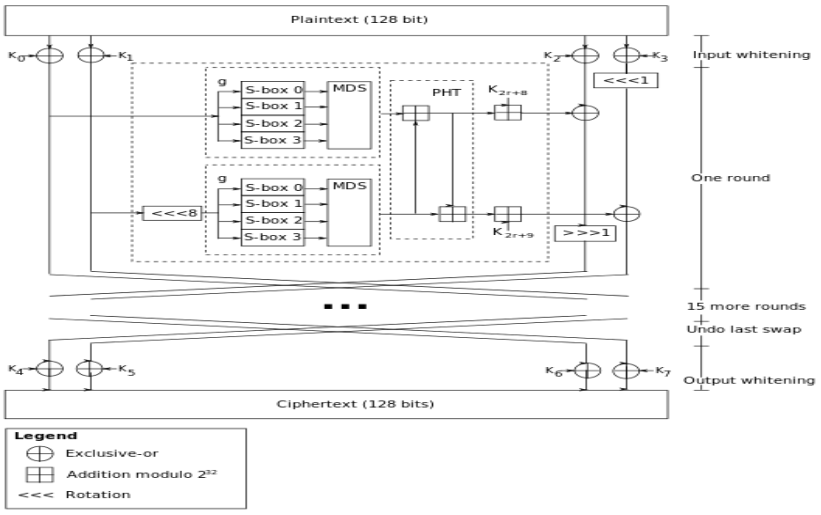
Twofish merupakan algoritrma yang beroperasi dalam mode blok. Algoritma twofish sendiri merupakan pengembangan dari algoritma Blowfish. Tujuan perancangan Twofish yang selaras dengan kriteria NIST (National Institute of Standars and Technology) untuk AES (Advanced Encryption Standard) adalah sebagai berikut [3] :

a. Merupakan blok kode dengan kunci simetri dan blok sepanjang 128 bit.
b. Panjang kunci yang digunakan adalah 128 bit, 192 bit, dan 256 bit.
c. Tidak mempunyai kunci lemah. Efisiensi algoritma, baik pada Intel Pentium Pro dan perangkat lunak lainnya serta platform perangkat keras.
d. Rancangan yang fleksibel, yang dapat diartikan, misalnya, dapat menerima panjang kunci tambahan.
e. Rancangan yang sederhana agar memudahkan proses analisis dan implementasi algoritma.

Algoritma Twofish merupakan 128-bit block sandi/cipher yang bisa menerima panjang varibel kunci/key sebesar 256 bit. Cipher tersebut berasal 16-round jaringan Feitsel dengan fungsi bijektif F yang dilanjutkan dengan empat key-dependent 8-by-b-bit S-boxes, satu fixed 4-by-4 maximum distance separable matrix over GF(28), satu pseudo-Hadamard transform, satu rotasi bitwise dan satu desain key schedule. Suatu implementasi Twofish yang dioptimalkan mengenksripsi pada Pentium Pro dengan 17,8 siklus clock per byte, dan pada smartcard akan mengenksripsi pada 1660 siklus clock per byte. Twofish dapat diimplemetsikan pada pada perangkat keras dengan 14000 gerbang. Design round function dan penjadwalan kunci mengakibatkan adanya trade off antara kecepatan, ukuran software, waktu setup key, jumlah gerbang dan memory. Twofish dapat melakukan:

1. Melakukan enkripsi data pada 285 siklus per block di atas Pentium Pro setelah menjalankan key setup 12700 siklus clock.
2. Melakukan enkripsi data pada 860 siklus per blok sdi atas Pentium Pro setelah menjalankan key setup 1250 siklus clock.
3. Melakukan enkripsi data pada 26500 siklus per block di atas sebuah 6805 smart card setelah mejalankan key setup 1750 siklus clock.

Twofish menggunakan struktur sejenis Feistel dalam 16 putaran dengan tambahan teknik whitening terhadap masukan dan keluaran. Teknik whitening adalah teknik melakukan operasi XOR terhadap materi kunci sebelum putaran pertama dan sesudah putaran akhir. Elemen di luar jaringan Feistel normal yang terdapat dalam algoritma Twofish adalah rotasi 1 bit. Proses rotasi ini dapat dipindahkan ke dalam fungsi F untuk membentuk struktur jaringan Feistel yang murni, tetapi hal ini membutuhkan tambahan rotasi kata sebelum langkah whitening keluaran. Blok diagram Twofish dapat dilihat secara global pada Gambar.1 [4] :



Gambar 1. Blok Diagram Twofish (Siddik, 2012)

Blok yang membangun Twofish seperti di bawah ini :

1. Jaringan Feistel
   Jaringan Feistel adalah metode umum untuk mentransformasi suatu fungsi menjadi bentuk permutasi.
2. Kotak-S (S-boxes)
   Kotak-S (S-boxes) adalah matriks yang berisi substitusi non-linear yang memetakan satu atau lebih bit dengan satu atau lebih bit lain dan digunakan di banyak blok kode.
3. MDS Matrices
   Kode MDS (Maximum Distance Separable) pada sebuah field adalah pemetaan linear dari x elemen field ke y elemen field, dan menghasilkan vektor komposit x + y elemen, dengan ketentuan bahwa jumlah minimum dari elemen bukan nol pada setiap vektor bukan nol paling sedikit y + 1. Dengan kata lain, jumlah elemen yang berbeda di antara dua vektor berbeda yang dihasilkan oleh pemetaan MDS paling sedikit y + 1.
4. Transformasi Pseudo-Hadamard (PHT)
   Transformasi Pseudo-Hadamard (PHT) adalah sebuah operasi pencampuran sederhana yang berjalan secara cepat dalam perangkat lunak PHT 32-bit dengan dua masukan didefinisikan sebagai :
   a. a’ = a + b mod 232
   b. b’ = a + 2b mod 232
5. SAFER menggunakan PHT 8-bit untuk difusinya. Twofish menggunakan PHT 32-bit untuk mengubah keluaran dari fungsi g-nya. PHT ini dapat dieksekusi dalam dua opcodes di mikroprosesor modern seperti keluarga pentium.
   a. Whitening
      Whitening adalah sebuah teknik meng-XOR-kan material kunci sebelum putaran pertama dan setelah putaran terakhir.
   b. Penjadwalan kunci
      Penjadwalan kunci adalah proses pengubahan bit-bit kunci menjadi upa-kunci tiap putaran yang dapat digunakan oleh kode.

Selain blok-blok pembangunan, algoritma twofish terdiri dari beberapa proses, yaitu :

1. Perubahan Pseudo-Hadamard, merupakan transformasi dua arah yang menghasilkan difusi. Difusi yang dimaksudkan disini adalah properti dari operasi cipher yang dikatakan aman. Bit masukan dari Pseudo-Hadamard harus memiliki panjang yang genap, karena akan dibagi menjadi dua bagian yang sama panjang, masing-masing sepanjang n/2 yang dilambangkan dengan a dan b. Persamaan pseudo-hadamard adalah sebagai berikut :
   1. a` = a + b (mod 2n) b` = a + 2b (mod 2n) untuk membalikkan persamaan di tersebut, persamaanya adalah :
   2. b = b` - a` (mod 2n) a = 2a` - b` (mod 2n) dimana n adalah jumlah bit yang digunakan.
2. Whitening, merupakan teknik untuk meningkatkan keamanan dari cipher blok yang menggunakan iterasi, tujuannya adalah agar input dan output dari fungsi F tidak diketahui. Whitening dilakukan dengan cara mengubah data dengan meng-XOR data dengan sebagian dari kunci sebelum iterasi pertama dan setelah iterasi terakhir dari enkripsi.
3. Penjadwalan kunci adalah proses mengubah kunci menjadi beberapa subkunci yang akan digunakan pada iterasi-iterasi

Selain unsur pembangunan di atas, ada beberapa proses penunjang lain pada implementasi algoritma twofish, yaitu :

1. Bit masukan sebanyak 128 bit akan dibagi menjadi empat bagian masing-masing sebesar 32 bit menggunakan konvensi little endlan. Dua bagian bit akan menjadi bagian kanan, dua bagian bit lainnya akan menjadi bagian kiri.
2. Bit input akan di XOR terlebih dahulu dengan empat bagian kunci, atau dengan kata lain mengalami proses whitening.
   R0,i = Pi XOR Ki i = 0, ..., 3
   Dimana K adalah kunci, Ki berarti subkunci yang ke-i.
3. Fungsi f dari twofish terdiri dari beberapa tahap, yaitu :
   a. Fungsi g, yang terdiri dari empat s-box dan matriks MDS
   b. PHT (Pseudo-Hadamard Transform)
   c. Penambahan hasil PHT dengan kunci

Blok-blok pembangunan beserta karakteristik di atas, akan digunakan pada impementasi algoritma twofish dengan tahapan-tahapan pada algoritma twofish lebih jelasnya adalah sebagai berikut:

1. Bit masukan disebut sebagai P0, P1, P2, dan P3. P0 dan P1 akan menjadi bagian kiri, dua lainnya akan menjadi masukan pada bagian kanan.

2. Kemudian akan melalui proses whitening.
3. Bagian kiri akan menjadi masukan untuk fungsi f, P0 akan langsung menjadi masukan bagi fungsi g, sementara P1 akan di-rotate 8 bit sebelum diproses oleh fungsi g.

Didalam fungsi g, bit-bit tersebut akan melalui S-box dan matriks MDS, kemudian kedua keluaran akan digabungkan oleh PHT.

4. Setelah melalui PHT, kedua bagian tersebut akan ditambah dengan bagian dari kunci sesuai dengan iterasi yang telah dilewati. Untuk keluaran dari fungsi f dengan input P1 akan ditambah dengan K2r+8. Untuk keluaran dari fungsi f dengan input P1 akan ditambah dengan K2r+9, dimana r adalah jumlah iterasi yang telah dilewati. Masing-masing ditambah delapan dan sembilan karena delapan urutan awal sudah digunakan untuk whitening input dan output.
5. Keluaran dari fungsi f dengan input P0 akan di- XOR dengan P2, kemudian hasil XOR tersebut akan di-rotate 1 bit.
6. Keluaran dari fungsi f dengan input P1 akan di- XOR dengan P3, namun P3 sebelumnya di-rotate 1 bit terlebih dahulu.
7. Setelah perhitungan bit selesai, bagian kanan yang telah dihitung tadi akan menjadi bagian kiri dan bagian kiri yang belum dihitung akan menjadi bagian kanan.
8. Kemudian setelah 16 iterasi, akan dilakukan whitening terhadap keluarannya. Whitening pada output akan meng-undo pertukaran bagian kanan dan bagian kiri pada iterasi terakhir, dan melakukan XOR data dengan 4 bagian kunci,
   Ci = R16,(i+2)mod 4 Ki+4 i = 0, ..., 3
   Bagian kunci yang digunakan disini berbeda dengan bagian kunci yang akan digunakan saat whitening pada input. Oleh karena itu urutan bagian kunci yang dipakai ditambah empat, karena empat urutan bagian kunci satu sampai empat sudah terlebih dahulu digunakan untuk whitening pada input. Keempat bagian cipherteks tersebut kemudian ditulis menjadi 16 byte C0, ...,
9. C15 menggunakan konversi little-endian seperti pada plainteks.
   Ci = mod 28 i = 0, ..., 15
   Implementasi algoritma twofish harus memperhatikan kecepatan komputasi yang diinginkan.

Twofish mempunyai karakteristik melakukan persiapan kunci dalam waktu yang lama. Karena itulah untuk menjamin kecepatan, semua proses penjadwalan kunci dapat dilakukan terlebih dahulu dan disimpan [5]. Penggunaan algoritma twofish antara lain terdapat pada :

1. Away32 Deluxe dan Away IDS Deluxe oleh BMC Engineering.
   Kedua aplikasi di atas merupakan perangkat lunak untuk enkripsi arsip dan folder pada windows.
2. CleverCrypt oleh Quantum Digital Security.
   Perangkat lunak enkripsi drive virtual on-the-fly untuk windows. Selain menggunakan algoritma twofish, aplikasi ini juga menggunakan rijndael, dan blowfish.
3. Cryptcat oleh Farm9
   Versi aplikasi netcut buatan L0pht dengan algoritma twofish. aplikasi ini memungkinkan pembangunan tunnel sederhana yang terenkripsi antar mesin, melalui jaringan internet, dan dalam kasus-kasus tertentu dapat melewati firewalls.
4. DigiSecret oleh TamoSoft.
   Aplikasi berbasiskan windows untuk membuat archive yang terenkripsi dan arsip self extracting exe, shredding, dan file sharing melalui internet.
5. FoxTrot oleh Roth Systems
   Sebuah server HTTP yang dirancang sebagai server aplikasi profesional. Dengan menggunakan aplikasi ini, pengguna dapat mengeksekusi perintah SQL langsung melalui address line pada browser.

Selain kriteria-kriteria yang telah disebutkan diatas, pada Twofish juga ditambahkan kriteria performansi berikut [4] :

1. Menerima kunci dengan panjang berapapun hingga 256 bit.
2. Mengenkripsikan data dalam waktu kurang dari 500 clock cycles per blok pada Intel Pentium, Pentium Pro, dan Pentium II, untuk versi algoritma yang teroptimasi sepenuhnya.
3. Mampu membentuk kunci 128 bit (untuk kecepatan enkripsi yang optimal) dalam waktu yang kurang dari waktu yang dibutuhkan untuk mengenkripsi 32 blok pada Pentium, Pentium Pro, dan Pentium II.
4. Tidak menggunakan operasi yang membuat Twofish tidak efisien pada mikroprosesor selain 32 bit, mikroprosesor 8 bit, dan mikroprosesor 16 bit.

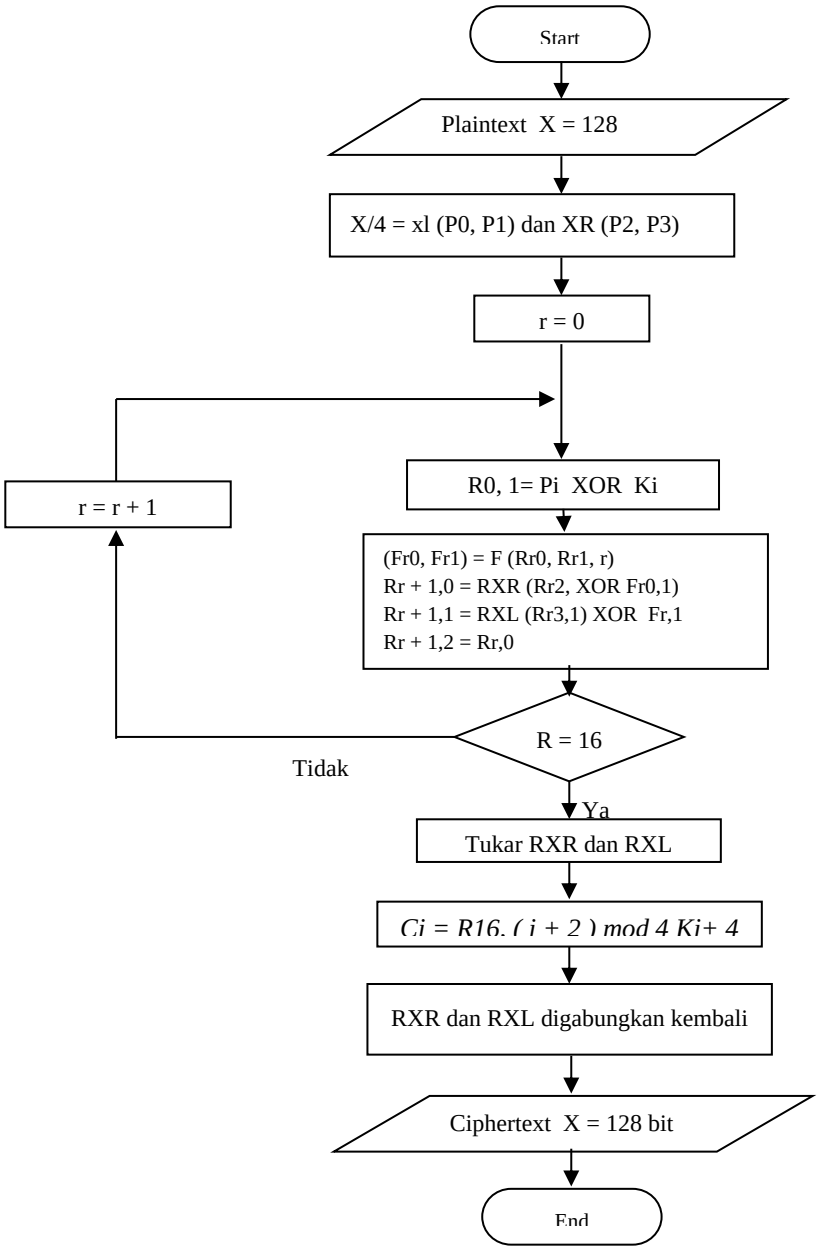
METODOLOGI

Metode dan langkah penelitian yang penulis lakukan adalah sebagai berikut :

1. Studi Pustaka :Tahapan untuk memperdalam teori dan mencari referensi-referensi yang berkaitan dengan tema penelitian ini. Sumber referensi berasal dari artikel berupa jurnal dan buku.
2. Analisa Kebutuhan :Tahapan ini untuk menganalisa apa saja kebutuhan untuk penelitian penelitian ini. Seperti pengumpulan data, analisa data, dan analisa kebutuhan software.
3. Perancangan Sistem : Dimulai pembuatan rancangan sistem. Mulai dari desain, perancangan sistem agar dapat mencapai tujuan sesuai dengan topik pembahasan.
4. Pembuatan Sistem : Dilakukan pengimplementasian rancangan yang telah disusun pada tahap sebelumnya sesuai konsep yang telah dibuat. Sistem dapat mengalami perubahan konsep dari rancangan sebelumnya maka pada tahapan ini akan dilakukan perubahan pembuatan sistem sampai mencapai hasil yang diharapkan.
5. Uji Coba Sistem : Dilakukan pengecekan apakah sistem memiliki kemampuan seperti yang diharapkan.
6. Pembuatan Kesimpulan :Tahapan ini merupakan tahap akhir setelah sistem telah berjalan seperti yang diharapkan dilakukan evaluasi dan penarikan kesimpulan.

HASIL DAN PEMBAHASAN

Proses Eknripsi

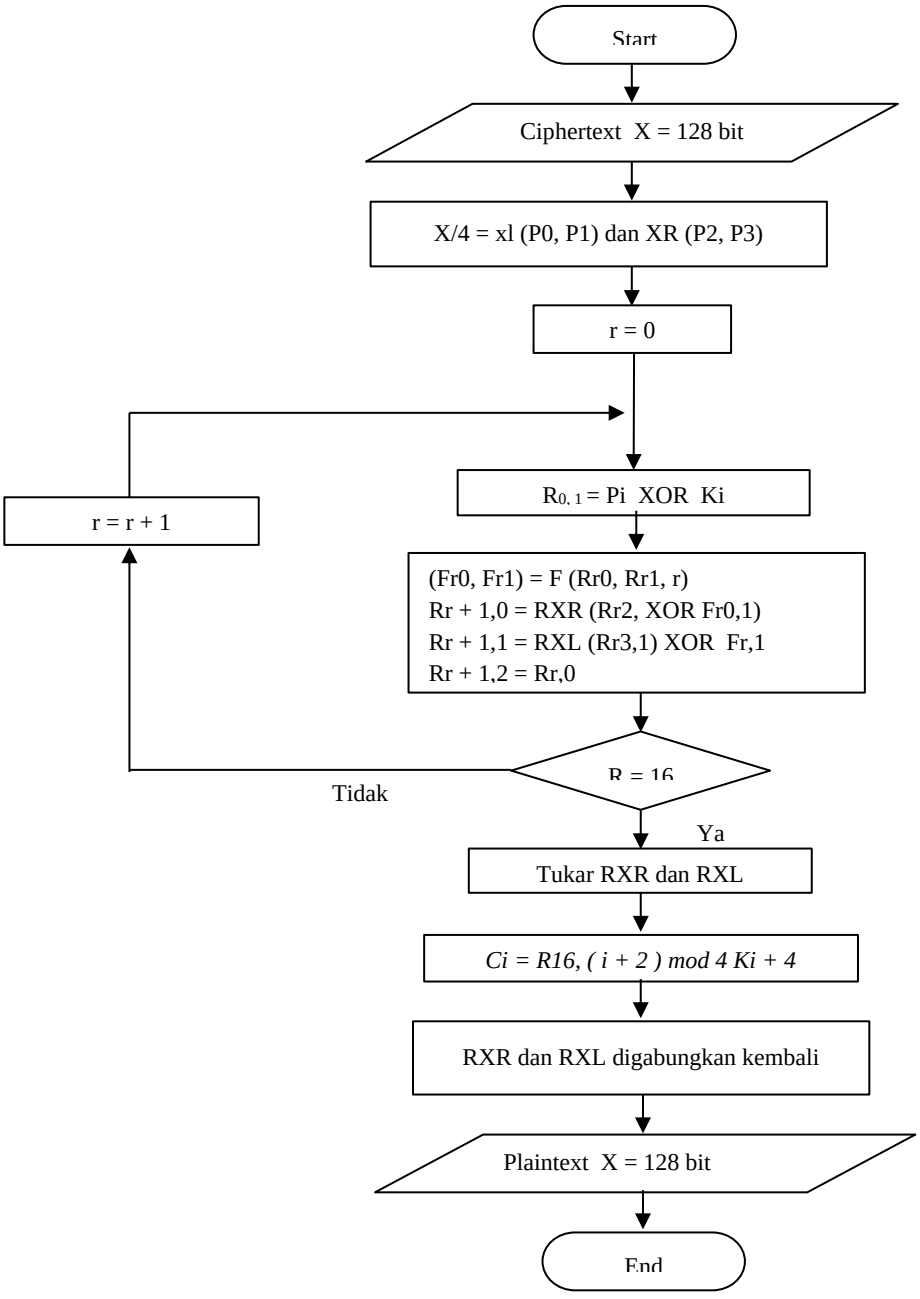


Gambar 2. Flowchart Enkripsi

Pada gambar 2 merupakan flowchart proses enkripsi pada algoritma twofish. Proses enkripsi algoritma twofish yang terjadi, yaitu sebagai berikut :

1. Memulai proses enkripsi (plaintext) dengan X = 128 bit.
2. X dibagi menjadi 4 bagian. XL = P0, P1 dan XR = P2, P3.
3. Input whitening ke-empat bagian tersebut di-XOR dengan kunci yang telah diekspansi.
4. Melakukan perulangan hingga 16 kali putaran(r= r+1), pada setiap putaran p0 dan P1 sebagai masukan dari fungsi F, P2 dilakukan operasi XOR dan dirotasikan kekanan sebanyak 1 bit, dirotasikan kekanan 1 bit dan dilakukan rotasi XOR pada keluaran fungsi F.
5. Menukarkan hasil RXR dan RXL.
6. Output whitening hasil keluaran dan melakukan operasi XOR dengan 4 buah kata darikunci yang diekspansi.
7. Menggabungkan hasil RXR dan RXL.
8. Menghasilkan cipher text X.
9. Selesai.

Proses Dekripsi



Gambar 3. Flowchart Deskripsi

Pada gambar 3 merupakan flowchart proses dekripsi pada algoritma twofish. Proses dekripsi algoritma twofish yang terjadi, yaitu sebagai berikut :

1. Memulai proses dekripsi (cipher text) dengan X= 128 bit.
2. X dibagi menjadi 4 bagian. XL = P0, P1 dan XR=P2, P3.
3. Input whitening ke-empat bagian tersebut di-XOR dengan kunci yang telah diekspansi.
4. Melakukan perulangan hingga 16 kali putaran di mulai dengan i = 0, pada setiap putaran P0 danP1 sebagai masukan dari fungsi F, P2 dilakukan operasi XOR dan dirotasikan kekanan sebanyak 1 bit, P3 dirotasikan ke kanan 1 bit dan dilakukan rotasi XOR pada keluaran fungsi F.
5. Menukarkan hasil R X R dan R X L.
6. Output whitening hasil keluaran dan melakukan operasi XOR dengan 4 buah kata dari kunci yang diekspansi.
7. Menggabungkan hasil RXR danRXL.
8. Menghasilkan plaintext X.
9. Selesai.

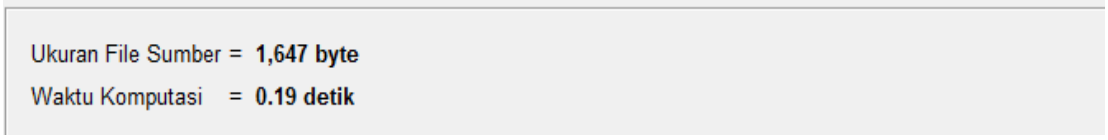
Uji Coba Sistem

Pengujian dilakukan terhadap dokumen yang dibuat dengan aplikasi ms word 2003 dan notepad.
Pengujian kesatu dilakukan pada teks yang dibuat menggunakan word 2003 dan notepad++ dengan plainteks “INI PESAN SINGKAT”, maka setelah dilakukan enkripsi maka didapat hasilnya:
Chipertext dari Notepada++
£~áÀºtp¤/3e]”JjF+Kœ¬ayVQJp

Chipertext dari word
• ©Ž}wn÷IëÄÎ##ËWñ‘Ð@› /É‹÷5)Oe§Æâc³ÇÎ
vÿ±zÈ6ñªõÇìá*f*ð“Ëð@ž¬X;®Ö†°`¯~´
ÊÃg[œi°ŒõÆò• ²â¡Ç“ÐŒ• w• .(¯}ßŠ[ìôB&Â©^&d7[³Lö§%&Äú¿0g{ÙÐðEJ5ß2¬¿JÞ©Ë?oçnY`1-I¤ßììóT@>U
¯ÈÊ)\Sö¨v¤“Z†[-²!5¬×c- vœ• Êmº'Á%bùßí„d¯_fØÑr
}q¤hÝlcŠ—• •• Ì• þpÏ,ìþöÐ7šÉ2bNÇpl‹òNøQõØ~=7¸:áñ&¨%¼ãÍ,ÝÞõÌ?‘• "ÛRaZÍšÆš¤éÚ=£†Ãž*
Æ™“³¼¥êó©-±¸iwz‡ãLèÎ rø µ<è™ÚNDÅQ®‹h¬ùÆb½N• ÷_:4-j• • ‘¡^ÐD>c¬Ñ²Æå‰
þÈ¤,B˜†ÕrÇÈÞá¯5RcSQ„LœRÌ1ë¦±Ùjÿåm É…\
¥‘5Ð[ö‡‘ÖÑÚ8©€Tn•)‹×L€ÂQ¤G;ê]<¥bH³®ÅÜP4<}q®þ¦ÝŒ;Ú…}ë7ô
‡²$@ÛuÏ;ú¸ÓdÝ“ARV_ž…¸ßÞ„¼8b-K$ÖÉ*f*W–wŽZèÕ@• mïœ\³/¤\š• ýœ
^O¡*f* ú‹´Ÿ6ÿÆT~Y;§eóÍ‹PäN÷• –0ŸÕŸœGDÅf®µ
_‰Gá-³ÿÚ¼$k¶)Gt›ÚÕ1¬• ¤R„b• ³:'µˆz´-C¯6o+»(–˜ŸÞºeoàbœÖh,-‡l(ÃÜÞ›óïö¨<Š~Ó°
a• 8DA¹eËÄ9z¦“ÉÕçà• B¾K–½„—Ñ¾ù!Û
‡Õè¶©õ‹Ãô¦˜ž¸±úÂ7°ßâHÕò• ú$ˆŸ “\¹¤Ï¿„ë¡ÌMóa¦‹\Üå«I"® Ü/¿T¤?Kb‘–@šå€Ë#fZ•|DÕéÓÈ• j• Ž$ ´r+Ë£–
Þ%#ŸghRþr¬5×KTSv'Ï
öŒ
bŒc¼ªaãAµkÊ Ã©´ïç%thœ…ÛGo„•‰• Õ3SúSþ{®¶Ng5.ô¨ÀÐ4ÿ|5ŸNBR}ûe $Âžµ8°‹ÓÝ• “K,<–|¤Õ¬zŠ¥ F&ª†fr§éz
é(æ¶3zË UÕ2[×I• b"©é
Ø,3B’a5Y"fŸçŸž¼‹;Þµ£9”(×i<¥iÉ` ÙOiÍ°{§NÜª óùGR5þ" »ˆÙ–“‡>TzïF@Ìÿa}¹‡˜‡Cœe}QNtj2´Í½ ŒÓÙ‰
QV»²×,ðïÐ l×
íþR5³ »&M6£Çvš• Y*…ÆLÌ‘žuÚ%\ÊfïcÀÐñö±xw!ò¢7kààípªpô‹ùç2œ›dØ;«>úo• —#Üœ]—
@(wMÀ#”ˆ8• Þ¢N‡0°ŠãÎ™
žK¯pîš±¡• ±\r[€ùö
†µŽŽ_a…]p• :§¦±…ù~…ž+¶•“êBû\ôèð*¶©òÌ- îã• ðbm‡ëNWE
¡~Øyfò“d-ê ®¥õ ëb8ÚâÒ'ðµ» ™€Ž¶/BlP9Ì*f*;&RiX¬Ot¹ÈXˆz9I&{…{>üšÊf·üËBpl„F6Òêš‹x&ÄüœÏd áyRÕ Ä‘
Æ3úc“¼žP »©þxâ7¥å» QY®aë „{Ô(tß¬ãt»µU5‰š • Ðšq_• ³Y7¨Z&ÃT•ÂÝ_IØêÂg,_iE ÑÃö²ë€4rY¿d×D†.˜æH’í«
ˆErœF™´²äÎ*f*I¿Ð:jß• õ}‰ñ”Ó&ú …..... dst.

Pengujian kedua dilakukan dengan tehadap plainteks berikut
Batang (ANTARA) - Kepolisian Resor Batang, Jawa Tengah, akan membatasi euforia dari masyarakat pada perayaan Hari Ulang Tahun Ke-75 RI seiring dengan adanya pandemi virus corona.
"Meski sudah diberlakukan adaptasi kehidupan baru, kami akan membatasi kegiatan perayaan HUT RI, khususnya yang menimbulkan kerumunan," kata Kepala Polres Batang AKBP Abdul Waras di Batang, Rabu.

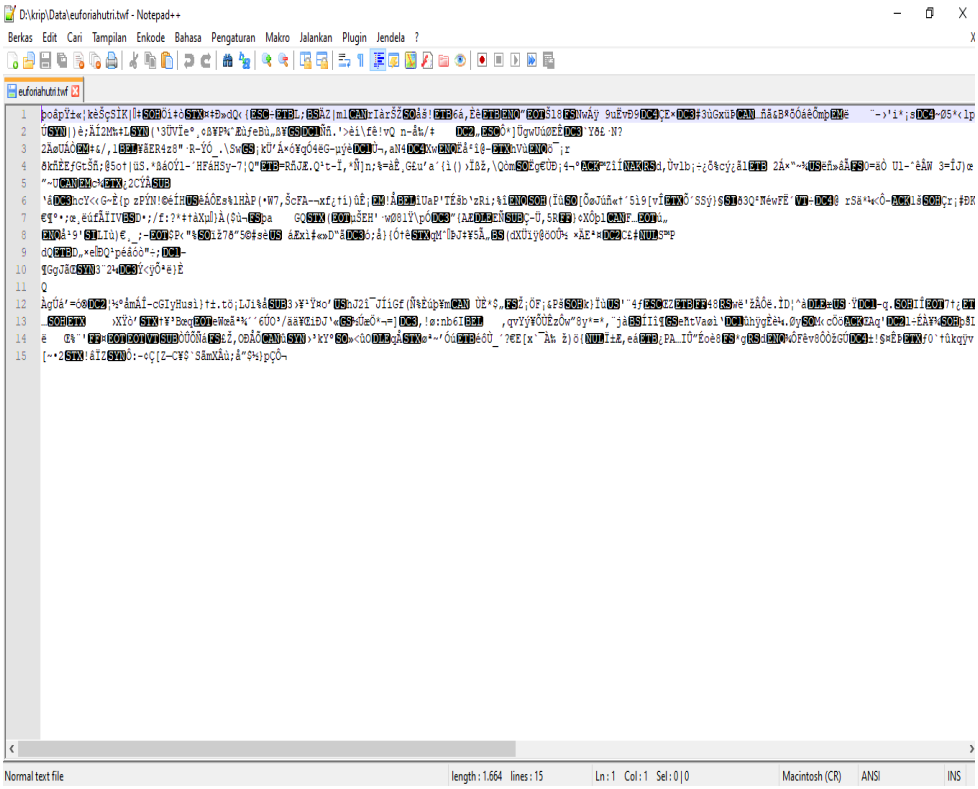
Menurut dia, masa pandemi COVID-19 yang belum diketahui kapan akan selesai ini dimungkinkan akan berdampak pada kegiatan perayaan HUT RI di wilayah ini, apalagi kasus COVID-19 di Kabupaten Batang cenderung meningkat.
"Kemungkinan kami masih akan menyesuaikan masa COVID-19 untuk membatasi kegiatan Agustusan," katanya.
Abdul Waras mengatakan bahwa rencana kebijakan pembatasan perayaan HUT RI ini sudah dibicarakan dengan pemerintah daerah setempat sebagai upaya memutus mata rantai penyebaran virus corona.
Kebiasaan masyarakat dalam merayakan HUT RI, kata dia, antara lain dengan menyelenggarakan pentas dangdut dan karnavalan. "Oleh karena itu, kegiatan yang timbulkan kerumunan akan diliburkan dahulu meski sudah diberlakukan adaptasi kehidupan baru," katanya. Ia menegaskan bahwa kebijakan itu bukan untuk menghalangi atau memutus kesenangan masyarakat untuk merayakan HUT RI, melainkan demi menjaga kebersamaan dan menjaga kesehatan warga agar tidak terpapar COVID-19. "Perlu ada kerja sama dengan masyarakat dan dukungan dari semua pihak. Jika kita disiplin dan melaksanakan protokol kesehatan, penyebaran virus corona dapat ditekan," katanya.
Pewarta : Kutnadi
Editor: Heru Suyitno
COPYRIGHT © ANTARA 2020
Pengjujian yang kedua terhadap dokumen/teks yang ditulis dengan word dan notepad, dimana data tersimpan di note dengan ukuran 1,647 byte (Gambar 4) sedangkan di word tersimpan dengan ukuran 12,856 byte (Gambar 5)



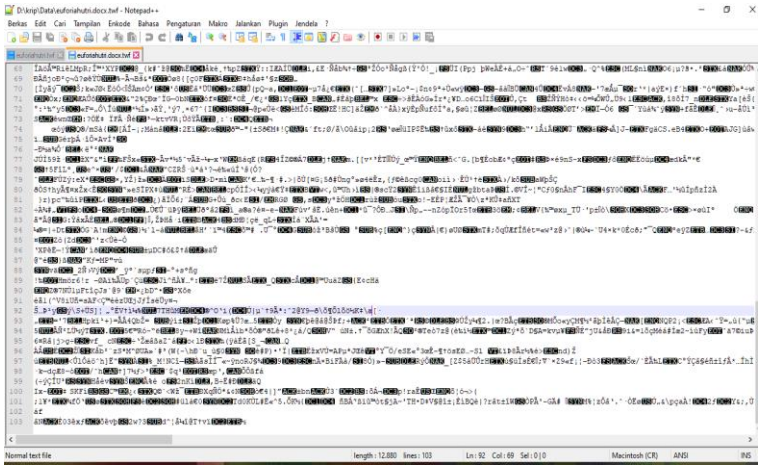
Gambar 4. Data Dengan Notepad Dan Waktu Enkripsi

Gambar 5. Data Dengan Notepad Dan Waktu Enkripsi

Hasil Enkripsi



Gambar 6. Tangkapan Layar Untuk Enkripsi Notepad



Gambar 7. Tangkapan Layar Untuk Enkripsi Word

Gambar 6 dan 7 adalah hasil tangkapan layar untuk hasil enkrisi untuk pesan yang sama namun dibuat dengan aplikasi yang berbeda yaitu notepad dan msword, jika dlihat pada ukuruan data sebelum di enkrip atau plainteks sama dengan ukuran data setelah di enkrip (chipertext). Namun demikian bahwa ukuran itu akan berbeda sesuai dengan kebutuhan dari aplikasinya untuk memberikan informasi informasi yang yang dibutuhkan oleh aplikasi tersebut.

KESIMPULAN DAN SARAN

Dari penjelasan dan pengujian sistem, maka diperoleh kesimpulan antara lain : Kriptografi merupakan teknik menyamaran pesan sehingga kalaupun jatuh ke tangan orang lain tidak akan membuka kerahasiaan pesan karena harus membutuhkan kunci yang kuat. Twofish merupakan chiper blok 128 bit yang menerima key dengan panjang variabel diatas 256 bits dan tidak memiliki kunci-kunci yang lemah. Aplikasi harus ada di kedua belah pihak yaitu pada si pembuat pesan mengubah pesan asli (plain text) menjadi pesan terekripsi (chipertext) dan juga pada sipenerima karena harus memngubah chipertext ke palin text yang dapat dipahami. Saran antara lain : Membagun aplikasi yang dapat melakukan enkripsi dan deskripsi untuk semua bentuk dokumen seperti Gambar,Audio maupun Video. Memafaatkan cloud computing sehingga tidak perlu membagun aplikasi pada kedua belah pihak.

DAFTAR PUSTAKA

[1] Fresly Nandar Pabokory, Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard, Jurnal Ilmiah Ilmu Komputer, 2015

[2] Kurniawan,Yusuf. Kriptografi: Keamanan internet dan jaringan komunikasi. Informatika Bandung, Bandung, 2004

[3] Azis, Nur. Perancangan Aplikasi Enkripsi Dekripsi Menggunakan Metode Caesar Chiper Dan Operasi XOR, Ikraith-Informatika, 2(1), 2018

[4] Ratih, Study dan Implementasi Enkripsi Pengiriman Pesan Suara Menggunakan Algoritma Twofish, Jurnal Teknik Informatika, 3(2), 2007

[5] Siddik, M.H.Saboo. Encryption and Decryption of Data Using Twofish Algorithm. NCETIT, Vol .2, 2012

[6] Edy Rahman Syahputra, Analisa Pengujian Estimasi Waktu Dan Besar Ukuran File Menggunakan Algoritma Twofish Pada Proses Enkripsi Dan Dekripsi. Jurnal TIMES, 4(2), 2015

[7] E. Ndruru and T. S. Alasi, "ALGORITMA TRIPPLE DES DALAM PENGAMANAN FILE DENGAN USB FLASHDISK," J. Inf. Komput. Log., vol. 2, no. 4, 2022.

[8] T. S. Alasi, R. Wanto, and V. H. Sitanggang, "Implementasi Kriptografi Algoritma Idea Pada Keamanan Data Teks Berbasis Android," J. Inf. Komput. Log., vol. 2, no. 1, 2020.

[9] T. S. Alasi, "Algoritma Hill Cipher Untuk Kebenaran Informasi pada Gambar dalam Media Sosial," J. Inf. Komput. Log., vol. 2, no. 2, 2021.

[10] T. S. Alasi and A. T. A. A. Siahaan, "Algoritma Vigenere Cipher Untuk Penyandian Record Informasi Pada Database," J. Inf. Komput. Log., vol. 1, no. 4, 2020.