Jurnal Mantik
Volume 3 Number 2, Agustus 2019 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

ANALISIS PERFORMA ALGORITMA BLOWFISH DAN TEA DALAM PENGAMANAN DATA

Yennimar[1], Annisa Fadhlila[1], Pratiwi[1], Anita Yose Fanny Manurung[1], Risda Amelia Amanta Br Ginting[1]

[1]Teknik Informatika, Teknologi dan Ilmu Komputer , Universitas Prima Indonesia, Medan, Indonesia

E-mail: tiwilubis.pl@gmail.com

ARTICLE INFO

Article history:
Received: 09 Aug 2019
Revised: 15 Aug 2019
Accepted:29 Aug 2019.

Keywords:
Kemanan, Blowfish, TEA

ABSTRAK

Keamanan maupun kerahasiaan data menjadi hal penting untuk diperhatikan dikarenakan keamanan data berhubungan dengan pencegahan dari pencurian data oleh pihak yang tidak bertanggung jawab. Teknik yang dapat digunakan untuk mengamankan data yaitu dengan kriptografi. Beberapa metode kriptografi memiliki performa yang baik dan buruk tergantung dengan tipe kuncinya. Maka dari itu, tujuan dari penelitian ini adalah mengukur tingkat kecepatan dari algoritm Blowfish dan algoritma TEA, dengan tipe data text dan gambar. Hasil dari penelitian ini Algoritma Blowfish dalam proses enkripsi dan dekripsi data lebih aman dan lebih unggul dari algoritma TEA. Rata-rata kecepatan enkripsi algoritma Blowfish untuk file gambar 650ms dan deskripsi 637ms sedangkan TEA waktu kecepatan enkripsi 685ms dan deskripsi 699ms. Pada file docx algoritma Blowfish memiliki kecepatan proses enkripsi 31ms dan deskripsi 94ms dan Algoritma TEA waktu kecepatan enkripsi 157ms dan deskripsi 141ms.

1. Pendahuluan

Saat ini internet sudah tidak lagi menjamin penyediaan informasi yang aman. Beberapa mesin pencarian yang terus berkembang menjadikan informasi bersifat publik, disamping itu munculnya resiko keamanan seperti : virus, penyadapan, *spam* maupun *hacker* merupakan suatu masalah yang perlu diperhatikan untuk setiap pengguna internet. Permasalahan keamanan maupun kerahasiaan data menjadi hal yang penting diperhatikan untuk saat ini dikarenakan internet sudah menjadi suatu kebutuhan bagi setiap individu [1]**.** Oleh karena itu solusi terbaik untuk melakukan perlindungan yaitu dengan teknik kriptografi. Pada kriptografi data diubah ke dalam bentuk lain dengan teknik enkripsi dan dekripsi [2]**.** Enkripsi merupakan cara utama untuk menjamin keamanan informasi yang sensitif, proses enkripsi dilakukan ketika data akan dikirim. Enkripsi yaitu dimana data asli diubah menjadi data rahasia yang tidak dapat dibaca sedangkan proses dekripsi dilakukan oleh penerima data, data rahasia yang diterima diubah kembali menjadi data asli menggunakan kunci yang diberikan oleh pengirim untuk dapat dibuka

Jurnal Mantik
Volume 3 Number 2, Agustus 2019 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

[3][4]. Algoritma enkripsi diklasifikasikan menjadi dua kelompok yaitu kunci simetris atau juga disebut kunci-rahasia dan kunci asimetris atau disebut publickey[5]. Ada berbagai jenis algoritma kriptografi yang bisa digunakan., pada dasarnya pemilihan algoritma kriptografi tergantung pada permintaan aplikasi seperti efisiensi waktu, bandwidth, kerahasiaan dan integritas. Namun, masing-masing algoritma kriptografi memiliki kekurangan dan kelebihannya [3][5].

Dalam kriptografi terdapat beberapa algoritma penyandian data. Algoritma kunci simetris merupakan algoritma yang masih sering digunakan untuk teknik pengaman data. Algoritma kunci simetris yang populer diantaranya DES, TDES, Blowfish, CAST5, IDEA, TEA, AES dan Twofish [6]. Oleh karena itu dengan teknik kriptografi diharapkan data akan tetap terjaga kerahasiaannya dan memberikan keyakinan memang benar informasi tersebut berasal dari pengirim yang asli dan pengirimpun yakin bahwa penerima informasi adalah pihak yang tepat.

[4] Mengimplementasi algoritma blowfish pada perangkat keras untuk transmisi data yang aman pada internet hasilnya untuk memberikan keamanan pengiriman informasi di internet lapisan jaringan, teknik kriptografi dapat digunakan. Dari semua algoritma kriptografi, algoritma Blowfish adalah terbaik dalam hal waktu eksekusi, penggunaan memori, throughput, konsumsi daya, dan keamanan dan dengan demikian cocok untuk IOT.

[7] Menganalisis kinerja AES dan Blowfish hasilnya Blowfish memiliki kinerja lebih unggul daripada AES karena Blowfish sejauh ini tidak memiliki titik kelemahan keamanan . Proses algoritma blowfish lebih cepat dari AES dikarenakan AES memerlukan waktu proses yang lebih besar, dengan demikian algoritma blowfish lebih sesuai untuk pengaturan nirkabel yang menukar paket ukuran kecil.

[8] Menguji efisiensi Blowfish dan AES Algoritma ini diuji dengan berbeda metrik kinerja. Hasil percobaan menunjukkan Blowfish memiliki kinerja yang lebih baik daripada AES di hampir semua semua kasus uji. Tidak ada perbedaan signifikan dalam hasil untuk pengkodean base64 dan heksadesimal teknik pengkodean. Ditemukan bahwa blowfish itu baik untuk enkripsi berbasis teks sedangkan AES lebih baik Pada enkripsi gambar.

[5] Melakukan perbandingan yang antara AES, DES, 3DES dan Blowfish dalam hal waktu Enkripsi, waktu Dekripsi dan Throughput. Hasilnya menunjukkan Blowfish memiliki performa yang lebih baik dalam hal waktu enkripsi dan waktu dekripsi.

[9] Implementasi algoritma TEA pada perangkat lunak, algoritma TEA yang dimodifikasi diusulkan menggunakan dua kunci dan dua fungsi untuk mengatasi kelemahan keamanan dan kelemahan kunci dari algoritma TEA standar. Algoritma TEA yang dimodifikasi dibandingkan dengan TEA standar. Hasilnya menunjukkan bahwa ketika menggunakan dua fungsi di setiap putaran dan masing-masing fungsi menggunakan salah satu dari dua tombol, peluang mendapatkan teks sandi yang sama untuk beberapa teks dan kunci biasa dapat dicegah.

[10] Menguji Hybrid Cryptosystem Menggunakan Algoritma TEA dan LUC hasilnya hybrid cryptosystem dengan menggunakan Algoritma TEA dan LUC memenuhi persyaratan aspek integritas pada kriptografi. Ukuran ciphertext meningkat enam belas byte karena panjang plaintext bertambah delapan karakter. Sistem ini dapat mengamankan file yang memiliki ekstensi ini: * .pdf, * .txt, * .rtf, * .doc,* .docx, dan * .otd.

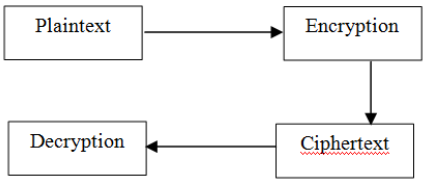
Berdasarkan penelitian-penelitian sebelumnya peneliti tertarik untuk melakukan perbandingan efiensi waktu enkripsi dan deskripsi dari algoritma Blowfish dan TEA dikarenakan kedua algoritma tersebut masih menggunakan teknik penyandian yang sama . Maka dari itu didalam penelitian ini peneliti ingin membandingan tingkat efisiensi waktu pada algoritma Blowfish dan TEA didalam enkripsi dan deskripsi pada data text dan gambar.

2. Landasan Teori

a. Kriptografi

Kriptografi biasanya disebut sebagai "cara rahasia". Enkripsi adalah proses mengubah teks normal menjadi bentuk yang tidak dapat dibaca. Dekripsi adalah proses mengubah teks terenkripsi menjadi teks normal dalam bentuk yang dapat dibaca[2]

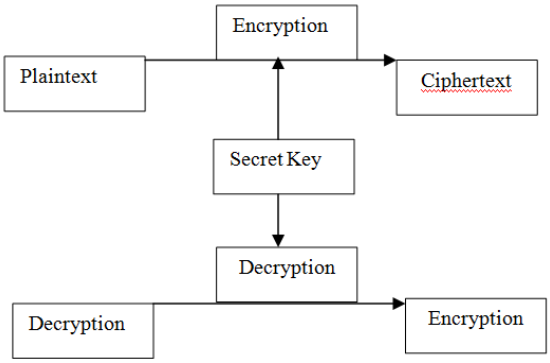
Jurnal Mantik
Volume 3 Number 2, Agustus 2019 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index



Gambar 1. Bentuk umum model enkripsi[2]

b. Enkripsi Simetris

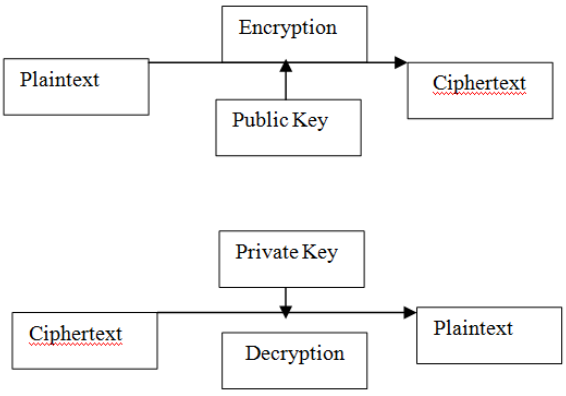
Ini juga disebut sebagai kriptografi kunci tunggal. Dalam proses enkripsi penerima dan pengirim harus menyetujui satu kunci rahasia yang dibagikan. Diberikan pesan yang disebut plaintext dan kuncinya, enkripsi menghasilkan data yang tidak dapat dipahami, yang kira-kira sama panjangnya dengan plaintext. Dekripsi adalah kebalikan dari enkripsi, dan menggunakan kunci yang sama dengan enkripsi[14]



Gambar 2. Proses Kriptografi Kunci Simetris[2]

c. Enkripsi Asimetris

Ini juga disebut sebagai kriptografi kunci publik. Ia menggunakan dua kunci: kunci public dan kunci pribadi. Kunci publik dan pribadi terkait satu sama lain dengan cara matematika apa pun. Dengan kata lain, data yang dienkripsi dengan satu kunci publik hanya dapat dienkripsi dengan kunci pribadi yang sesuai. Prosedur enkripsi dan dekripsi diilustrasikan pada gambar 3:



Gambar 3. Proses Kriptografi Kunci Publik[2]

d. Algoritma Blowfish

Algoritma Blowfish yaitu algoritma simetri yang tergolong dalam metode cipher block. Tipe dasar algoritma simetris ada dua yaitu cipher block dan stream cipher. Sebuah cipher block memproses byte

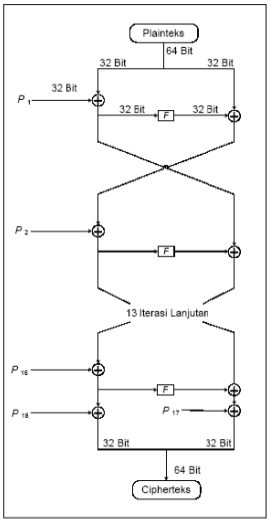
Jurnal Mantik
Volume 3 Number 2, Agustus 2019 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

block pada 64 atau 128 bit setiap satu waktu. Sebuah stream cipher memproses 1 byte atau bahkan 1 bit pada suatu waktu.

Karateristik algoritma Blowfish adalah sebagai berikut[11]:

- Cipher block dengan 64 bit block
- Variable panjang kunci mencapai 448 bit
- Melakukan enkripsi data pada microprocessor 32 bit dengan rata – rata 18 clock cycle per byte.
- Gratis
- Mampu berjalan pada memori kurang dari 5 KB
- Memiliki struktur yang sederhana dan mudah dalam implementasinya.
  Blowfish menggunakan subkunci yang besar. Sebelum enkripsi atau dekripsi data kunci tersebut harus dihitung . Pada inisial P-array sebanyak 18 buah yaitu (P1,P2,……..P18) masing-masing bernilai 32-bit . P-array terdiri dari delapan belas kunci 32-bit subkunci: P1,P2,…….,P18
- Bentuk S-Box sebanyak 4 buah masing-masing bernilai 32-bit yang memiliki masukan 256. Empat 32-bit S-Box masing-masing mempunyai 256 masukan:
- (S1,0),(S1,1),……..,(S1,255)
- (S2,0),(S2,1),……..,(S2,255)
- (S3,0),(S3,1),……..,(S3,255)
- (S4,0),(S4,1),……..,(S4,255)

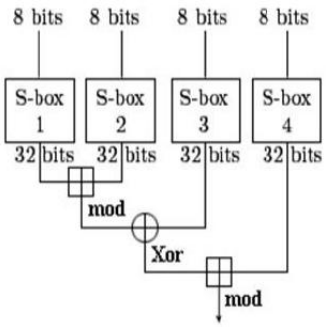
Blowfish adalah sebuah jaringan Feistel yang terdiri dari 16 putaran. Input-annya adalah elemen data 64 bit.



Gambar 4. Jaringan Feistel Algoritma *Blowfish*[11]

Fungsi F dapat dilihat sebagai berikut:

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 5. Fungsi F Pada Algoritma *Blowfish*[11]

e. Algoritma Tiny Encryption (TEA)

Jurnal Mantik
Volume 3 Number 2, Agustus 2019 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

Tiny Encryption Algorithm (TEA) adalah algoritma penyandian cipher block dimana dirancang untuk penggunaan memory yang kecil dan memilki kecepatan proses yang maksimal. Pada sistem penyandian TEA menggunakan proses fiestel network dengan menambah fungsi matematik yang berupa penambahan dan pengurangan sebagai operator pembalik selain XOR, untuk menciptakan sifat non-linearitas. Pergeseran dua arah kiri dan kanan menyebabkan semua kunci bit dan data akan bercampur secara berulang ulang.

Langkah-langkah penyandian dengan algoritma TEA yaitu [12]:

1. Pergeseran Shift

Pada kedua sisi blok teks terang sebanyak 32-bit akan bergeser ke kiri sebanyak 4 kali dan digeser ke kanan 5 kali.

2. Penambahan

Selanjutnya setelah digeser ke kiri dan kanan, maka Y dan Z yang digeser ditambahkan kunci k[0]- k[3]. Sedangkan Y dan Z awal ditambahkan dengan sum(delta).

3. Peng-XOR-an

Selanjutnya dioperasikan dengan penambahan untuk masing-masing register dan dilakukan peng-XOR-an dengan rumus untuk satu *round* yaitu :

```
y = y + (((z<<4)+k[0])^z+sum^((z>>5)+k[1]))
z = z + (((y<<4)+k[2]^y+sum^((y>>5)+k[3]))          (1)
```

dalam hal ini sum = sum + delta.

Hasil pada penyandian satu *cycle* satu blok teks terang 64-bit menjadi 64-bit teks sandi yaitu dengan menggabungkan Y dan Z. Untuk penyandian pada *cycle* selanjutnya Y dan Z ditukar posisinya, sehingga Y1 menjadi Z1 dan Z1 menjadi Y1 dan dilanjutkan prosesnya sampai dengan 16 cycle (32 round).

4. Key Schedule

Pada TEA menggunakan *key schedule*-nya sangat sederhana yaitu kunci k[0] dan k[1] konstan digunakan untuk *round* ganjil sedangkan kunci k[2] dan k[3] konstan digunakan untuk *round* genap.

5. Dekripsi

Pada proses dekripsi sama seperti pada proses penyandian berbasis feistel cipher lainnya. Hal yang berbeda adalah pada penggunaan teks sandi sebagai input dan kunci digunakan urutannya dibalik. Proses dekripsi semua round ganjil menggunakan k[1] kemudian k[0], demikian juga pada semua round genap digunakan k[3] tkemudian k[2]. Proses enkripsinya adalah : (2).

```
L0 = L0 + f (R0 , k[0], k[1], sum)
R0 = R0 + f (L0, k[2], k[3], sum)                   (2)
```

Jadi L0 merupakan hasil penjumlahan dari L0 ditambahkan dengan f (R0 , k[0], k[1], sum).

Proses enkripsi untuk satu *round* digunakan persamaan (3).

```
y = y + (((z<<4)+k[0])^z+sum^((z>>5)+k[1]))
z = z + (((y<<4)+k[2]^y+sum^((y>>5)+k[3]))          (3)
```

Proses dekripsi digunakan persamaan (4) :

```
L0 = L0 + f (R0 , k[1], k[0], sum)
R0 = R0 + f (L0, k[3], k[2], sum)                   (4)
```

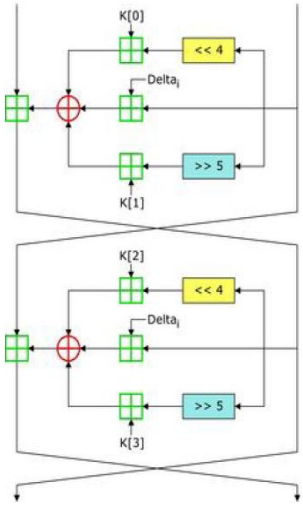
Jadi L0 merupakan hasil penjumlahan dari L0 ditambahkan dengan f (R0 , k[1], k[0], sum). Proses yang digunakan dalam satu *round* menggunakan Persamaan (5).

```
y = y + (((z<<4)+k[1])^z+sum^((z>>5)+k[0]))
z = z + (((y<<4)+k[3]^y+sum^((y>>5)+k[2]))          (5)
```

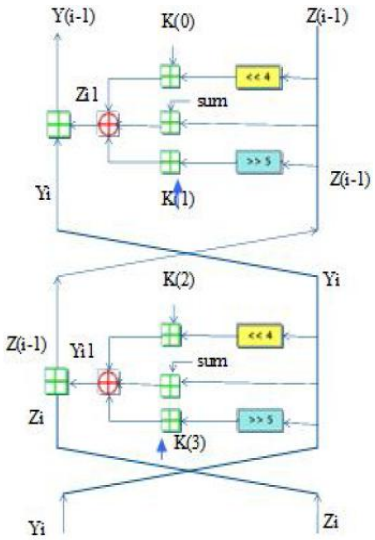
Diketahui bahwa Y merupakan hasil dari Y yang ditambahkan dengan Z yang digeser sebanyak 4 kali dengan penambahan kunci K[1]. Kemudian hasil penjumlahan tadi di-XOR-kan dengan Z yang dijumlahkan dengan sum(delta). Hasil dari peng-XOR-an dari kedua penjumlahan tadi di-XOR-kan lagi

Jurnal Mantik
Volume 3 Number 2, Agustus 2019 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

dengan Z yang digeser ke kanan sebanyak lima kali dengan penambahan kunci K[0]. Demikian juga dengan rumus Z sama halnya dengan rumus Y, hanya kunci yang menggunakan kunci K[3] dan K[2] [12].



Gambar 6. Enkripsi TEA[13]

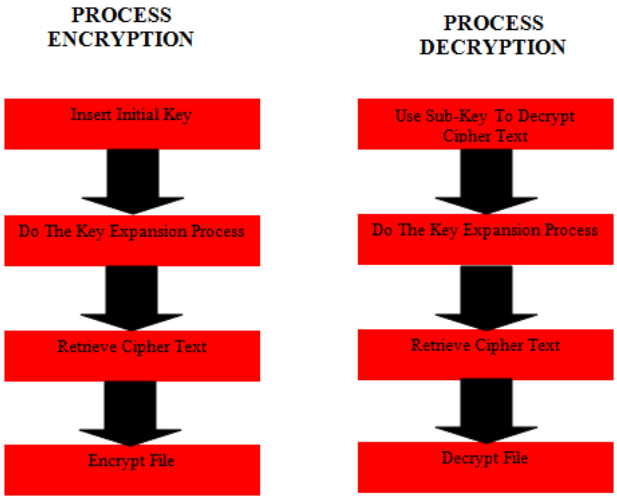


Gambar 7. Deskripsi TEA[13]

3. Metodologi Penelitian

Dalam bagian ini akan di jelaskan tahap proses dari dua algoritma yaitu : Algoritma Blowfish dan Algoritma Tiny Encryption (TEA) dalam mengenkripsi dan mengdekripsi dari suatu file.

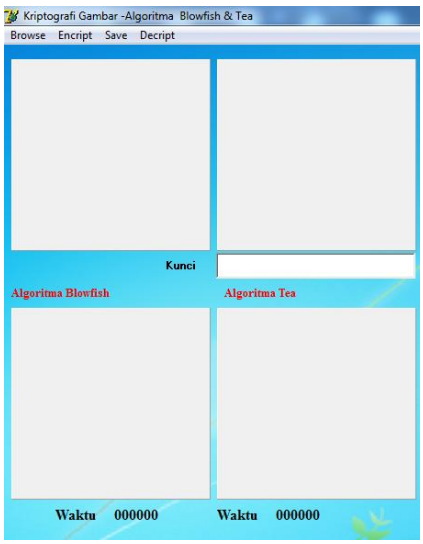
Jurnal Mantik
Volume 3 Number 2, Agustus 2019 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index



Gambar 8. Proses Enkripsi dan Dekripsi Algoritma Blowfish dan TEA

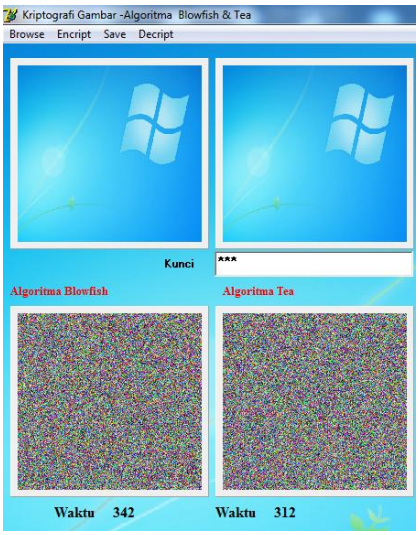
4. Hasil dan Pembahasan

Sistem yang dirancang untuk menunjang penelitian perbandingan performa kriptografi algoritma *Blowfish* dan TEA menggunakan bahasa pemrograman Delphi 7 dan pengujian dilakukan dalam sistem operasi Windows 7. Data yang diambil dari aplikasi adalah pengamatan waktu proses enkripsi dan dekripsi masing-masing algoritma. Spesifikasi perangkat keras komputer dapat mempengaruhi hasil yang didapatkan dari aplikasi.

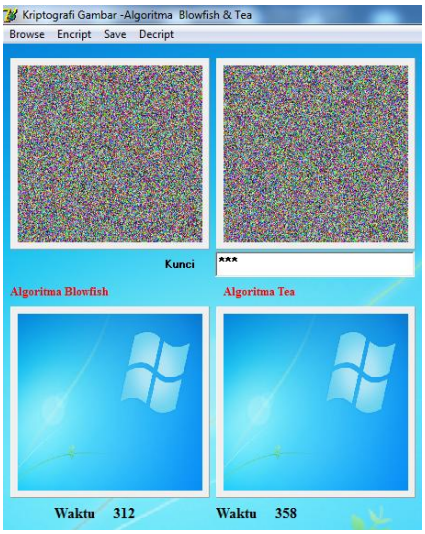


Gambar 9. Form Interface Aplikasi

Jurnal Mantik
Volume 3 Number 2, Agustus 2019 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index



Gambar 10. Proses Enkripsi Algoritma Blowfish dan TEA



Gambar 11. Proses Deskripsi Algoritma Blowfish dan TEA

Dalam penelitian ini, ada beberapa langkah yang diambil dalam menganalisis performa dari Algoritma Blowfish dan TEA. Beberapa langkah tersebut yaitu:
1. Menggunakan 3 sampel data per jenis *file* dengan ukuran berbeda.
2. Mengukur jumlah rata-rata hasil waktu enkripsi dan dekripsi masing-masing algoritma.

Hasil waktu enkripsi dan dekripsi yang didapat dari penelitian ini dapat dilihat pada tabel :

Tabel 1. Proses Enkripsi File.BMP

Besar File Gambar	Waktu Proses (s)	
	Blowfish	TEA
812Kb	284	313
1.250Kb	476	534
2.696Kb	1190	1208
Rata-Rata Waktu Kecepatan	650	685

Jurnal Mantik
Volume 3 Number 2, Agustus 2019 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

Tabel 2. Proses Deskripsi File.*BMP*

Besar File Gambar	Waktu Proses	
	Blowfish	TEA
812Kb	265	281
1.250Kb	428	442
2.696Kb	1218	1376
Rata-Rata Waktu Kecepatan	637	699

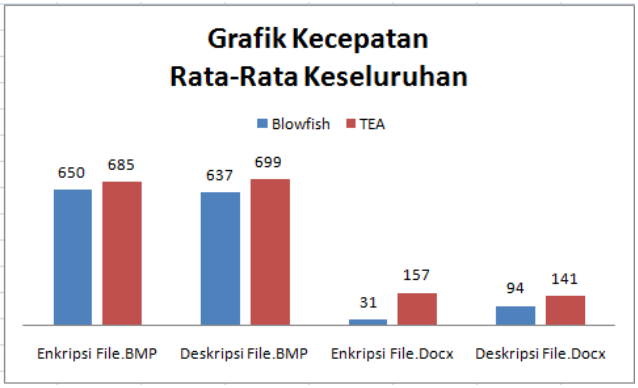
Tabel 3. Proses Enkripsi File.*Docx*

Besar File Docx	Waktu Proses	
	Blowfish	TEA
79kb	14	32
148kb	32	62
159kb	47	63
Rata-Rata Waktu Kecepatan	31	157

Tabel 3. Proses Deskripsi File.*Docx*

Besar File Docx	Waktu Proses	
	Blowfish	TEA
79kb	16	31
148kb	31	47
159kb	47	63
Rata-Rata Waktu Kecepatan	94	141

Dari hasil tabel dapat dilihat, proses enkripsi dan dekripsi TEA membutuhkan waktu yang sangat lama disbanding Blowfish. Perbandingan hasil dari masing-masing algoritma dapat dilihat pada grafik berikut ini :



Gambar 12. Grafik Perbandingan Kecepatan Algoritma Blowfish dan TEA

5. Kesimpulan

Dari analisis yang dilakukan terhadap algoritma Blowfish dan algoritma TEA maka penulis dapat mengambil kesimpulan bahwa algoritma Blowfish memiliki kecepatan proses enkripsi dan dekripsi lebih cepat dibandingkan algoritma TEA, dengan rata-rata waktu kecepatan enkripsi 650ms dan deskripsi

637ms untuk file gambar sedangkan TEA waktu kecepatan enkripsi 685ms dan deskripsi 699ms. Pada file docx algoritma Blowfish memiliki kecepatan proses enkripsi 31ms dan deskripsi 94ms dan Algoritma TEA waktu kecepatan enkripsi 157ms dan deskripsi 141ms

References

[1] Prasetiyo, B. Much, A.M. & Hendi, S. 2017. Penerapan Kriptografi Algoritma Blowfish pada Pengamanan Pesan Data Teks. Techno.COM, Vol. 16, No. 4
[2] Thakur, J. & Nagesh, K. 2011. Des, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis. International Journal of Emerging Technology and Advanced Engineering Volume 1, Issue 1,
[3] Nazeh, M.A.W. Abdulrahman, A. 2018. A Comparison of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish for Guessing Attacks Prevention. J o u r n a l o f C omputer Science Applications and Information Technology 3(2)
[4] Suresh, M.A. & Neema M.B. 2016. Hardware implementation of blowfish algorithm for the secure data transmission in Internet of Things. Procedia Technology
[5] Singh, G. Ashwani, K.S & K.S.S. 2012. Superiority of Blowfish Algorithm in Wireless Networks. International Journal of Computer Applications Volume 44– No11
[6] Styorini, W. & Dwi, H. 2015. Analisis Performansi Algoritma AES dan Blowfish Pada Aplikasi Kriptografi https://www.researchgate.net/publication/305734898
[7] Abirami, M.S.c. 2013. Performance Analysis of AES and Blowfish Encryption Algorithm. International Journal of Innovative Research in Science, Engineering and Technology Vol. 2, Issue 11
[8] Anand, M.K. & Dr, S.K. 2012. Investigating the Efficiency of Blowfish and Rejindael (AES) Algorithms. I. J. Computer Network and Information Security
[9] Aradhyamath,S. & Joy, P. 2018. Multi -key Modified Tiny Encryption Algorithm for HealthCare. International Journal of Engineering & Technology 7 (2)
[10] Rachmawati,D. Amer, S. 2018. Hybrid Cryptosystem Using Tiny Encryption Algorithm and LUC Algorithm. IOP Conference Series: Materials Science and Engineering
[11] Mujito & Anugrah, B.S. 2016. Aplikasi Kriptografi File Menggunakan Metode Blowfish dan Metode Base64 pada Dinas Kependudukan dan Pencatatan Sipil Kota Tangerang Selatan. Jurnal SISFOKOM, Volume 05, Nomor 01
[12] Asprina, T. Muh, Y & Sutardi. Pembangunan Aplikasi Keamanan Pesan Chatting Dengan Menerapkan Algoritma Tiny Encryption Algorithm (Tea) Berbasis Client Server. SemanTIK, Vol.4, No.2
[13] Shoeb,M & Vishal, K.G. 2013. A Crypt Analysis Of The Tiny Encryption Algorithm In Key Generation. International Journal of Communication and Computer Technologies Volume 01 – No.38