Volume 19 Nomor 1 (2024) 7-14
E – Link P-ISSN 1858-2109 E-ISSN 2656-5676
Jurnal Teknik Elektro dan Informatika

ANALISIS PERBANDINGAN RUANG DAN WAKTU ALGORITMA ENKRIPSI BLOWFISH DAN TWOFISH PADA ENKRIPSI DAN DESKRIPSI BERKAS MENGGUNAKAN MODUL PYTHON

Candra Kurniawan[1)], Mochammad Fadhli MS[2)], Fauziah[3)]
[1,2,3)] Magister Teknologi Informasi, Universitas Nasional
Jl. Sawo Manila, Pejaten, Ps. Minggu Jakarta Selatan 12520, Indonesia
E-mail: [1)]candra.kurniawan2022@student.unas.ac.id, [2)]mochammad.fadhli2022@student.unas.ac.id, [3)]fauziah@civitas.unas.ac.id

ABSTRAK

Perkembangan teknologi informasi yang pesat beriringan dengan meningkatnya insiden siber kebocoran data. Salah satu metode pengamanan yang dapat diterapkan dalam meningkatkan keamanan data dari kasus kebocoran data yaitu dengan menerapkan kriptografi pada sistem yang mengelola data. Kriptografi berguna untuk melakukan enkripsi *plaintext* menjadi *cipher text* sehingga data tidak mudah terbaca. Salah satu algoritma enkripsi yang banyak digunakan dalam pengamanan data yaitu Blowfish dan Twofish. Blowfish dan Twofish merupakan algoritma enkripsi simetris yang menggunakan *single key* dalam enkripsi dan dekripsi. Pada jurnal ini dilakukan pengujian enkripsi dan dekripsi pada algoritma Blowfish dan Twofish dalam kaitannya dengan kompleksitas ruang dan waktu. Hasil dari pengujian dari 3 data pada 2 perangkat yang berbeda menunjukkan bahwa algoritma Blowfish memiliki kecepatan yang lebih baik daripada Twofish dan Twofish lebih baik daripada Blowfish dalam penggunaan memori serta penggunaan *processor* mempengaruhi kecepatan proses.
Kata kunci : Blowfish, Kompleksitas, Kriptografi, Twofish

ABSTRACT

The rapid development of information technology is accompanied by an increase in cyber incidents such as data breaches. One of the security methods that can be implemented to enhance data security against data breaches is by applying cryptography to data management systems. Cryptography is useful for encrypting plaintext into ciphertext, making the data not easily readable. One of the encryption algorithms widely used in data security is Blowfish and Twofish. Blowfish and Twofish are symmetric encryption algorithms that use a single key for encryption and decryption. This journal focuses on testing the encryption and decryption of Blowfish and Twofish algorithms in relation to space and time complexity. The results of testing three sets of data on two different devices indicate that the Blowfish algorithm has better speed than Twofish, while Twofish performs better than Blowfish in terms of memory usage. Moreover, the usage of the processor affects the speed of the process.
Keywords : Blowfish, Complexity, Cryptography, Twofish

1. PENDAHULUAN

Perkembangan dan kemajuan teknologi informasi pada era digital sangatlah pesat. Perkembangan teknologi yang pesat tersebut diiringi dengan meningkatnya serangan siber yang mengancam. Salah satu ancaman siber yang meningkat yaitu ancaman kebocoran data. Pada laporan Microsoft terkait Microsoft Digital Defense Report 2022 disebutkan bahwa rata-rata pelanggaran data secara global pada tahun 2021 mencapai $4,24 juta. Kegagalan pengamanan data terjadi karena salah satunya yaitu tidak ada penerapan enkripsi pada data yang digunakan [1].

Kebocoran data menjadi salah satu Top 3 insiden siber yang terjadi di Indonesia. Hal tersebut terdapat pada laporan Lanskap Keamanan Siber Indonesia 2022. Kasus

kebocoran data pada 2022 mencapai 311 kasus yang terjadi pada 248 *stakeholder*[2].

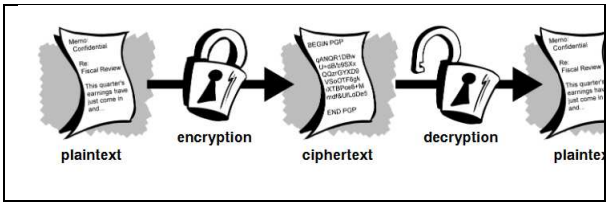
Seperti yang telah disebutkan Microsoft bahwa salah satu kegagalan pengamanan data karena tidak adanya penerapan enkripsi pada data. Dalam upaya pengamanan data dikenal metode kriptografi. Kriptografi dapat digunakan untuk mengamankan data pribadi atau informasi lain dari akses yang tidak sah. Dalam kriptografi dikenal 2 istilah yaitu enkripsi dan dekripsi. Hasil *convert plaintext* menjadi *cipher text* disebut dengan enkripsi, sedangkan proses *convert* dari *cipher text* menjadi *plaintext* disebut dengan dekripsi[3].

Algortima Blowfish dan Twofish merupakan algoritma enkripsi simetris yang dibuat oleh Bruce Schneier pada 1993. Algoritma enkripsi simetris menggunakan *single* kunci dalam melakukan enkripsi dan dekripsi. Algoritma Blowfish dan Twofish banyak digunakan dalam pengamanan data seperti *password management*, *File/disk encryption*, dan *email encryption*[4]. Berdasarkan hal tersebut penulis melakukan penelitian terkait dengan perbandingan kompleksitas ruang dan waktu yang digunakan oleh algoritma Blowfish dan Twofish dalam melakukan enkripsi dan dekripsi berkas dengan menggunakan modul Python.

2. METODE PENELITIAN

2.1. Kriptografi

Kriptografi merupakan bidang ilmu yang digunakan dalam melakukan pengamanan terhadap data dengan menggunakan perhitungan matematika untuk melakukan penyamaran data. Kriptografi memungkinkan untuk melakukan pengiriman pesan secara aman sehingga pesan tidak dapat terbaca oleh pihak yang tidak berhak. Dalam kriptografi dikenal 2 (dua) istilah yaitu *plaintext* dan *ciphertext.* Data yang dapat dibaca dan dipahami secara langsung disebut dengan *plaintext*, sedangkan data yang telah diacak atau dienkripsi sehingga data tidak dapat dibaca dan dipahami tanpa dilakukan proses dekripsi menjadi *plaintext* disebut *ciphertext* [5]. Berikut merupakan skema enkripsi dan dekripsi.



Gambar 1. Skema Enkripsi dan Dekripsi

Dalam melakukan enkripsi dikenal 2 (dua) metode yaitu *symmetric encryption* dan *asymmetric encryption*. *Symmetric encryption* merupakan metode enkripsi yang hanya memerlukan 1 (satu) kunci atau menggunakan kunci yang sama untuk dalam proses enkripsi dan dekripsi. Berbeda dengan *simetric encryption, asymmetric encryption* menggunakan menggunakan pasangan kunci untuk melakukan enkripsi dan dekripsi. Jika dibandingkan dengan *asymmetric, symmetric* lebih cepat dalam proses enkripsi serta tidak membutuhkan banyak sumber daya. Contoh algoritma kriptografi *symmetric encryption* yaitu AES, DES, 3DES, IDEA, Blowfish, dan Twofish serta untuk *asymmetric encryption* seperti RSA, ECC, DSA, dan El Gamal[5].

2.2. Blowfish

Blowfish merupakan algoritma *symmetric block cipher* yang dirancang oleh ahli keamanan komputer dan kriptografi Bruce Schneier.pada tahun 1993. Blowfish dirancang sebagai pengganti DES dan IDEA[6]. Blowfish merupakan algoritma *block cipher* dengan ukuran 64-bit, panjang kunci minimum 32-bit dan maksimum 448-bit[4].

Algoritma Blowfish terbagi menjadi 2 (dua) bagian yaitu *Key-expansion* dan *Data Encryption. Key-expansion* berfungsi sebagai pengubah kunci menjadi beberapa *array subkey* yang berjumlah 4168 *byte*. Blowfish menggunakan jaringan feistel dengan 16 iterasi sehingga diperlukan pembangkitan *subkey*. Proses pembangkitan *subkey* sebagai berikut[4][7]:

1. Inisialisasi *Array* P dan *Array* S dengan dengan nilai yang telah ditentukan dalam *hexadecimal*. *Array* P terdiri dari 18 *subkey* 32-bit yang meliputi P0, P2, ., P17.

P[0]	243f6a88	P[9]	38d01377
P[1]	85a308d3	P[10]	be5466cf
P[2]	13198a2e	P[11]	34e90c6c
P[3]	03707344	P[12]	c0ac29b7
P[4]	a4093822	P[13]	c97c50dd
P[5]	299f31d0	P[14]	3f84d5b5
P[6]	082efa98	P[15]	b5470917
P[7]	ec4e6c89	P[16]	9216d5d9
P[8]	452821e6	P[17]	8979fb1b

Gambar 2. Subkey Blowfish

Array S merupakan S-Boxes yang terdiri dari 4 Box 32-bit dengan masukan 256.

S1, 0, S1, 1,. S1, 255
S2, 0, S2, 1,. S2, 255
S3, 0, S3, 1,. S3, 255
S1, 0, S4, 1……..S4, 255

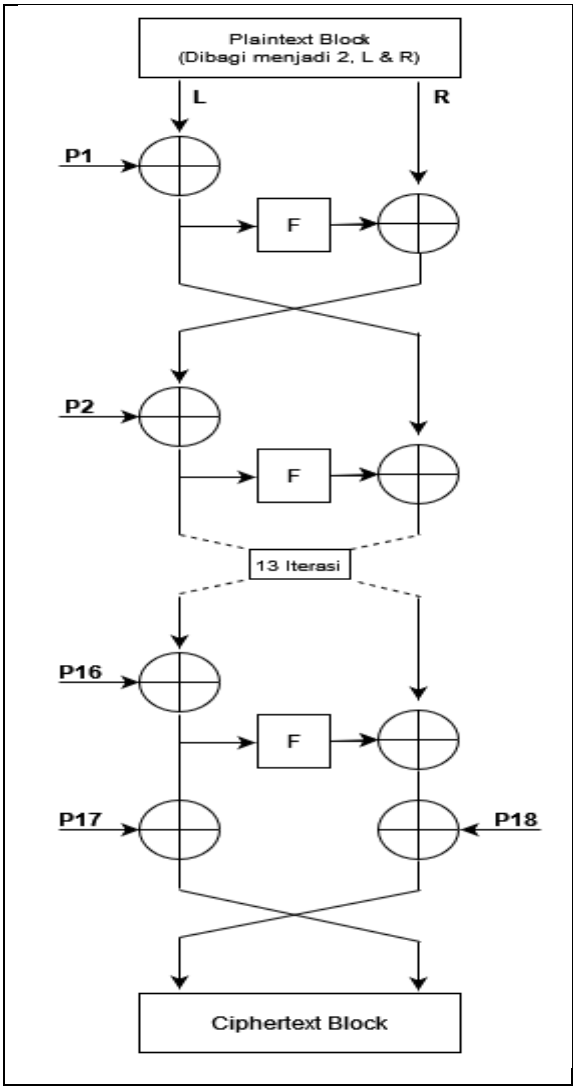
Gambar 3. S-Boxes Blowfish

2. Lakukan operasi XOR pada nilai P1 dengan 32-bit pertama kunci, XOR nilai P2 dengan 32-bit kedua kunci hingga seluruh P dilakukan XOR dengan kunci.
3. Lakukan XOR semua *string* 0 menggunakan *subkey array* P sesuai langkah 2.
4. *Replace* nilai P1 dan P2 dengan hasil dari langkah poin 3.
5. XOR hasil langkah poin 3 dengan langkah poin 2.
6. *Replace* P3 dan P4 dengan hasil dari langkah 5
7. Lakukan secara berulang hingga seluruh array P teracak.

Data Encryption, Blowfish menggunakan jaringan feistel dengan 16 iterasi. Setiap *round* terdiri dari permutasi dan subtitusi yang selanjutnya dilakukan XOR, berikut merupakan skema proses enkripsi Blowfish.

2.3. Twofish

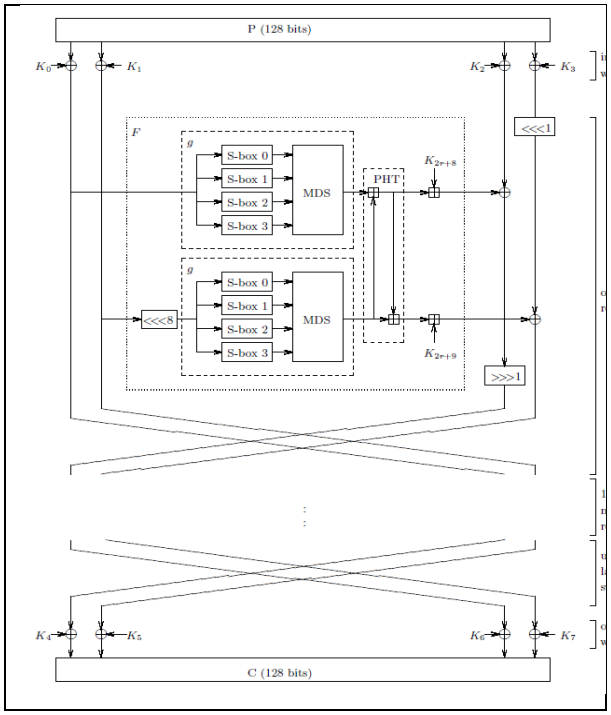
Twofish merupakan algoritma *symmetric block cipher* dengan ukuran 128-bit yang dapat menerima kunci dengan panjang 128, 192, dan 256-bit. Algoritma Twofish menggunakan struktur mirip dengan Feistel 16 round serta menggunakan subtitusi, dan transformasi linear[8]. Algoritma Twofish memiliki 16 *round* yang mana setiap *round* terdiri dari 4 (empat) tahap yaitu *F function, Key Whitening, G function*, dan *Round Whitening*. *F function* merupakan fungsi yang terdiri dari 4 (empat) operasi sederhana yaitu subtitusi, transformasi linear, permutasi dan, XOR. *F function* menerima inputan dari *Key Whitening* dan *Round Whitening*[8].



Gambar 4. Skema enkripsi Blowfish

G function merupakan fungsi yang terdiri dari operasi XOR, rotasi 1-bit, dan subtitusi. Output dari *G function* digunakan dalam operasi *F function*. *Round Whitening* merupakan tahap akhir dalam setiap *round* dan melibatkan operasi XOR untuk digunakan sebagai inputan *round* berikutnya[8].

Key Whitening merupakan tahap Twofish pada awal dan akhir dari setiap *round*. Pada proses *Key Whitening*, *block plaintext* di XOR dengan kunci yang dihasilkan dari proses *key-expansion*[8].



Gambar 5. Skema enkripsi Twofish

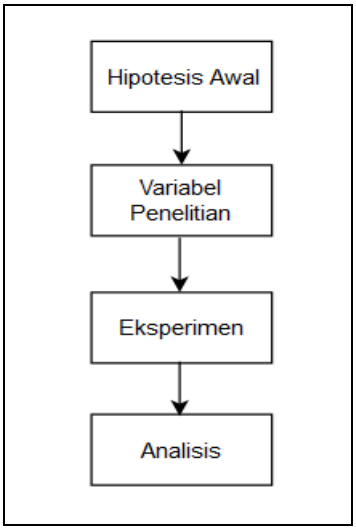
2.4. Bahasa Pemograman Python

Python merupakan Bahasa pemograman tingkat tinggi yang mudah digunakan. Pada tahun 1991, Guido van Rossum membuat bahasa pemograman Python. Semenjak dibuat, Python sering digunakan dalam pengembangan *website*, perhitungan komputasi ilmiah dan kriptografi, analisis data, *machine learning*, dan *artificial intelligence*[9].

Dalam bidang kriptografi, Python memiliki sejumlah library dan modul yang dapat dimanfaatkan untuk enkripsi, dekripsi, dan operasi kriptografi lainnya. Beberapa contoh *library* dan modul kriptografi yaitu[9][10]:

1. PyCrypto : merupakan library yang menyediakan algoritma dan protokol kriptografi seperti AES, DES, RSA, Blowfish, dan lainnya.
2. Cryptography : merupakan modul yang menyediakan kumpulan algoritma kriptografi klasik atau primitif.
3. PyCryotodome : merupakan library dan modul yang menyediakan protokol kriptografi klasik atau primitif dalam satu library.
4. Hashlib : merupakan modul yang menyediakan fungsi hash seperti SHA-1, SHA-256, MD5, dan lainnya.

Penelitian dilakukan dengan menggunakan metode eksperimen. Penelitian dengan metode eksperimen merupakan suatu penelitian yang dilakukan dengan cara melakukan manipulasi pada suatu variabel dan melakukan analisis terhadap dampak perubahan yang terjadi. Pada penelitian eksperimen terdapat beberapa komponen seperti hipotesis awal (Ho), variabel bebas, dan variabel terikat. Berikut merupakan langkah penelitian yang dilakukan.



Gambar 6. Langkah penelitian

2.5. Hipotesis Awal

Penentuan hipotesis awal merupakan hal yang penting pada penelitian eksperimen. Hipotesis awal atau Ho merupakan dugaan sementara atas hasil penelitian[11]. Pada penelitian ini penulis menentukan bahwa:

Ho : Algoritma Twofish lebih cepat dan menggunakan sedikit memori dibandingkan dengan algoritma Blowfish. Tidak ada pengaruh perubahan variabel bebas terhadap hal tersebut.

2.6. Variabel Penelitian

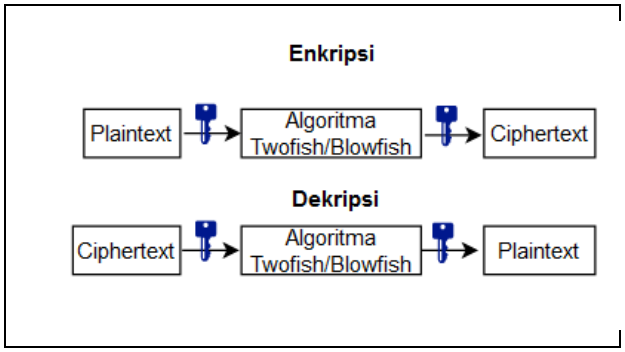
Variabel penelitian merupakan sesuatu yang dilakukan manipulasi atau sesuatu yang diamati. Pada penelitian eksperimen terdapat variabel bebas dan variabel terikat. Variabel bebas merupakan variabel yang secara sengaja dilakukan manipulasi oleh penguji, sedangkan variabel terikat merupakan variabel yang akan dipengaruhi oleh variabel bebas[11]. Berikut

merupakan penentuan variabel bebas dan variabel terikat yang dilakukan.

Variabel Bebas	:	Dilakukan perubahan atau manipulasi ukuran data yang akan dilakukan enkripsi dan dekripsi. Percobaan dilakukan pada 3 file dengan ukuran 5 kb, 50 kb, dan 500 kb.
Variabel Terikat	:	Program enkripsi dan dekripsi dalam Bahasa Python yang akan menampilkan waktu dan penggunaan memori pada proses yang berjalan.

2.7. Eksperimen

Eksperimen dilakukan dengan cara melakukan enkripsi dan dekripsi pada masing-masing data. Data yang diberikan terdiri dari 3 data dengan ukuran yang berbeda. Berikut merupakan proses pengujian yang dilakukan.



Gambar 7. Proses Pengujian

2.8. Analisis

Analisis dilakukan berdasarkan hasil percobaan yang telah dilakukan. Hasil analisis akan menunjukkan apakah Ho sesuai atau akan menghasilkan Ha (Hipotesis Baru) yang berkaitan dengan kompleksitas waktu dan ruang dalam penggunaan algoritma Twofish dan Blowfish dalam enkripsi file txt.

Bagian ini dapat berjudul Model atau Eksperimen. Dapat juga suatu *manuscript* memiliki bagian Teori dan Eksperimen sekaligus bila diperlukan. Setiap paragraf baru masuk sejauh 0,5 cm seperti paragraf ini, sedangkan paragraf lanjutan yang terpotong oleh tabel, persamaan, dan gambar tidak perlu menggunakan indentasi 0,5 cm tersebut.

3. HASIL DAN DISKUSI

Pengujian enkripsi dan dekripsi dilakukan dengan menggunakan Bahasa pemograman Python dan Modul kriptografi pycryptodome. Pengujian dilakukan pada 3 file dengan ekstensi txt yang masing-masing file 5 kb, 50 kb, dan 500 kb. Selaim dilakukan pada 3 file dengan ukuran yang berbeda, pengujian juga dilakukan pada 2 (dua) perangkat dengan spesifikasi yang berbeda. Perangkat pertama merupakan Laptop DELL yang dilengkapi dengan Processor Intel(R) Core(TM) i7-10610U CPU @1,80 GHz (8 CPUs) 2,3 GHz dan perangkat kedua merupakan PC Desktop Asus ROG yang dilengkapi dengan Processor Intel(R) Core(TM) i7-8700 CPU @3,20 GHz (12 CPUs) 3,2 GHz, dengan GPU NVIDIA GeForce GTX 1060 6GB.

Masing-masing pengujian dilakukan pada Blowfish dan Twofish dengan 16 *blocks* serta menggunakan kunci yang sama yaitu p@s5W0rd!!12345@#. Pengujian pada kedua perangkat dilakukan secara berulang sebanyak 5 (lima) kali pengujian. Hasil pengujian selanjutnya dilakukan perhitungan rata-rata dengan hasil sebagaimana pada bagian berikut.

3.1. Analisis Perbandingan Ruang dan Waktu Twofish dan Blowfish

Analisis perbandingan yang dilakukan bertujuan untuk menguji Hipotesis Awal yang telah ditentukan pada bab 3. Pada Ho disebutkan bahwa algoritma Twofish lebih cepat dan menggunakan sedikit memori dibandingkan dengan algoritma Blowfish. Serta hal tersebut tidak ada pengaruh yang diakibatkan oleh perubahan variabel bebas.

Tabel 1. Hasil Percobaan pada Laptop DELL Processor Core i7-10610U

Data	Twofish				Blowfish			
	Waktu (s)		Memori (kb)		Waktu (s)		Memori (kb)	
	Enkripsi	Dekripsi	Enkripsi	Dekripsi	Enkripsi	Dekripsi	Enkripsi	Dekripsi
5 kb	0,0034	0,0034	10,76	10,76	0,0046	0,0039	14,98	14,97
50 kb	0,0220	0,0214	10,92	10,91	0,0058	0,0039	15,052	15,032
500 kb	0,5527	1,8749	13,12	12,27	0,0210	0,0202	15,054	15,034

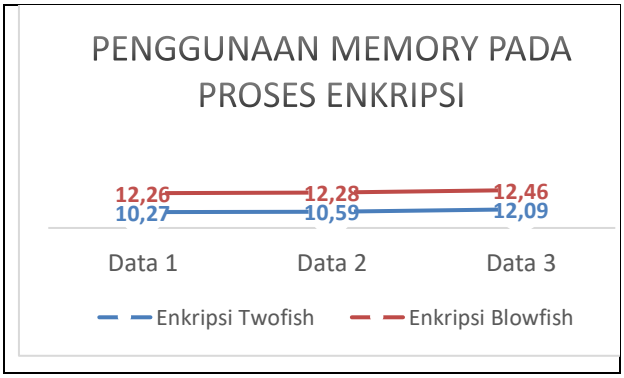
.

Tabel 1 **Error! Reference source not found.**merupakan hasil pengujian yang dilakukan pada Laptop DELL dengan *processor* Core i7-10610U (10th Gen). hasil pengujian tersebut menunjukkan bahwa Blowfish memiliki kecepatan yang lebih baik dalam melakukan proses enkripsi/dekripsi. Sedangkan untuk Twofish lebih unggul dalam penggunaan memori yang lebih sedikit. Rata-rata penggunaan memori yang digunakan oleh Twofish dalam melakukan enkripsi pada file dengan ukuran 500 kb yaitu 13,12 kb sedangkan Blowfish lebih besar dalam penggunaan memori yaitu 15,054 kb. Namun terkait dengan waktu Blowfish lebih cepat yaitu 0,0210 detik dan Twofish 0,5527 detik.

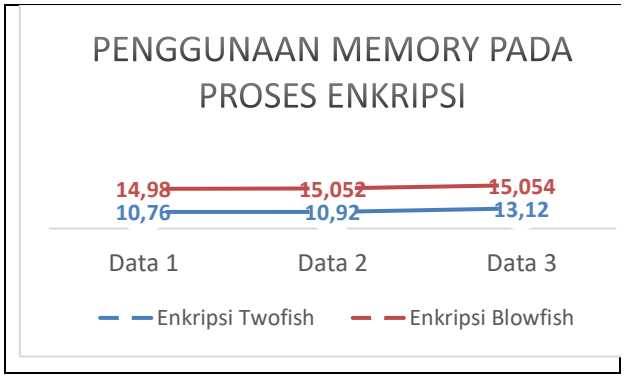
Tabel 2. Hasil Percobaan pada PC Desktop Processor Core i7-8700

Data	Twofish				Blowfish			
	Waktu (s)		Memori (kb)		Waktu (s)		Memori (kb)	
	Enkripsi	Dekripsi	Enkripsi	Dekripsi	Enkripsi	Dekripsi	Enkripsi	Dekripsi
5 kb	0,0026	0,0027	10,27	10,07	0,0030	0,0017	12,26	12,16
50 kb	0,0101	0,0097	10,59	10,28	0,0034	0,0020	12,28	12,20
500 kb	0,4271	1,7636	12,09	11,63	0,0090	0,0086	12,46	12,54

Hasil pengujian pada perangkat kedua yang merupakan PC Desktop Asus ROG dengan *processor* Core i7-8700 (8th Gen) memilik hasil yang sama seperti pada pengujian pada perangkat pertama yaitu bahwa Blowfish lebih cepat dalam melakukan proses enkripsi/dekripsi daripada Twofish. Sedangkan Twofish lebih unggul dalam penggunaan memori yang lebih sedikit. Rata-rata penggunaan memori pada 5 (lima) kali pengujian enkripsi dengan data berukuran 500 kb, Twofish menggunakan memori sebesar 12,09 kb sedangkan Blowfish menggunakan memori sebesar 12,46 kb.



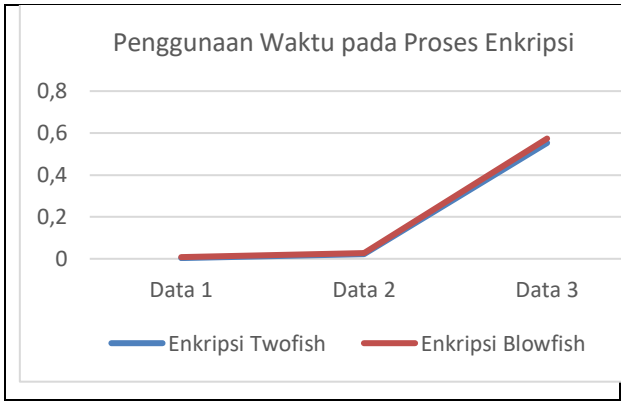
Gambar 8. Penggunaan Memori Perangkat ke-2



Gambar 9. Penggunaan Memori perangkat ke-1

Berdasarkan Gambar 8. Penggunaan Memori Perangkat ke-2 diketahui bahwa penggunaan memori pada proses enkripsi/dekrips Blowfish relatif naik stabil. Meskipun demikian, memori yang digunakan selalu naik seiring dengan besarnya data yang dilakukan proses.

Kedua tabel hasil tersebut juga menunjukkan bahwa waktu yang diperlukan dalam melakukan enkripsi atau dekripsi selalu bertambah seiring dengan penambahan ukuran data yang dilakukan pemrosesan. Dengan meningkatnya waktu serta memori yang dipengaruhi oleh perubahan ukuran data, hal ini menunjukkan bahwa kedua algoritma tersebut memiliki kompleksitas 0 (n) atau kompleksitas linier. Kompleksitas linier merupakan kompleksitas yang tumbuh secara proporsional berdasarkan data yang dilakukan proses (n).



Gambar 10. Waktu meningkat seiring dengan besar data (n)

3.2. Analisis Perbandingan Proses

Proses enkripsi serta dekripsi pada kedua algoritma yang dilakukan pengujian sangat dipengaruhi oleh perangkat yang digunakan. Hal tersebut diketahui dari perbedaan kecepatan dan penggunaan memori ketika melakukan proses kedua algoritma tersebut. Hasil pengujian sebagaimana pada tabel hasil menunjukkan bahwa penggunaan PC Desktop dengan dengan *Processor* Intel(R) Core(TM) i7-8700 yang didukung dengan GPU NVIDIA GeForce GTX 1060 6GB menghasilkan proses yang lebih cepat dan sedikit memori (efektif dan efisien).

Processor Intel(R) Core(TM) i7-8700 merupakan *processor* Intel Generasi ke-8 (8th Gen) yang memiliki 6 core dan 12 threat. *Processor* ini memiliki kecepatan 3,20,GHz serta dapat meningkat hingga 4,60 GHz pada kondisi dengan beban tinggi. Selain lebih unggul dari segi *processor*, perangkat kedua yang merupakan PC Desktop juga dilengkapi dengan GPU NVIDIA GeForce GTX 1060 dengan memori VRAM 6 GB sehingga dapat mendukung proses komputasi pararel yang tinggi.

3.3. Hipotesis Akhir (Ha)

Berdasarkan pengujian yang telah dilakukan, maka hipotesis awal (Ho) tidak berlaku. Hal tersebut disebabkan karena hasil pengujian menunjukkan bahwa Blowfish lebih cepat daripada Twofish mesikpun dilakukan perubahan pada besarnya data yang dilakukan pemrosesan. Sehingga pada pengujian ini terdapat Hipotesis baru atau hipotesis akhir (Ha) yaitu Algoritma Blowfish lebih cepat daripada Algoritma Twofish namun dalam penggunaan memori Twofish lebih baik daripada Blowfish, serta perubahan data tidak mempengaruhi hal tersebut. Proses pengujian yang dilakukan sangat dipengaruhi oleh perangkat yang digunakan.

4. KESIMPULAN DAN SARAN

Hasil pengujian kompleksitas ruang dan waktu pada enkripsi serta dekripsi algoritma Blowfish dan Twofish dilakukan pada 2 (dua) perangkat yang berbeda dan menggunakan 3 (tiga) data dengan ukuran yang berbeda. Hasil pengujian menunjukkan bahwa Algoritma Blowfish memiliki kecepatan yang lebih baik daripada Algoritma Twofish. Namun Algoritma Twofish lebih baik dari segi penggunaan memori yang sedikit.

Hasil pengujian yang dilakukan dipengaruhi oleh penggunaan perangkat yang berbeda. Pengujian kedua dengan menggunakan PC Desktop yang dilengkapi *processor* Intel(R) Core(TM) i7-8700 lebih cepat dan sedikit dalam penggunaan memori, sehingga penggunaan perangkat yang memiliki kecepatan *processor* yang baik akan mempengaruhi proses yang berjalan.

5. DAFTAR PUSTAKA

[1] T. Microsoft, "Microsoft Digital Defense Report 2022," *Microsoft*, 2023
[2] BSSN, "Lanskap Keamanan Siber Indonesia 2022," *Komunikasi Publik BSSN*, Depok, 2023.
[3] E. Jeevalatha dan S. Senthil Murugan, "Evolution of AES, blowfish and twofish encryption algorithm," *Int. J. Sci. Eng. Res*, vol. 9, no. 4, hlm. 115–118, 2018..
[4] S. K. Chinta, "Blowfish," 2015.
[5] C. PGP, "An Introduction to Cryptography", *PGP Corporation*, U.S, 2002.
[6] Arnaud, "Mailfence," Mailfence, 23 February 2023. [Online]. Available: https://blog.mailfence.com/symmetric-vs-asymmetric-encryption/. [Accessed 28 April 2023].
[7] B. Schneier, "The Blowfish Encryption Algorithm," Schneier on Security, [Online]. Available: https://www.schneier.com/academic/blowfish/. [Accessed 28 April 2023].
[8] R. Strogonovs, "Introduction to data encryption," Morf, 24 October 2014. [Online]. Available: https://morf.lv/introduction-to-data-encryption. [Accessed 2 May 2023].
[9] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall and N. Ferguson, "Twofish: A 128-Bit Block Cipher," in *University of California*, USA, 1998.
[10] S. J. Nielson and C. K.Monson, "Practical Cryptography in Python," *Apress*, USA, 2019.
[11] S. Hadi, Metodologi Research Jilid 4, *Yayasan Penerbit Fakultas Psikologi UGM*, Yogyakarta, 1985.