PERBANDINGAN ALGORITMA AES256 dan BLOWFISH

Muhammad Abdul Muin[1)], **Arief Setyanto**[2)], **Sudarmawan**[3)]
[1)] *Universitaas Amikom Yogyakarta*
[2)] *Universitaas Amikom Yogyakarta*
[3)] *Universitaas Amikom Yogyakarta*
Email : muinmuhammad@gmail.com[1)], arief_s@amikom.ac.id[2)],sudarmawan@amikom.ac.id[3)]

Abstract

Security for the moment is vital for efforts to protect organizational data against threats such as parent's destruction or accidental and unintentional. To choose the best encryption algorithm for the moment, In this research try to compare the speed of encryption and decryption in Algorima of famous encryption that is algorithm AES256 and Blowfish. In this research is done observation algorithm AES256 and Blowfish for the time of encryption and decryption. Using key lengths 4, 6, 8, 10, and 12 characters. With a combination of lowercase and large, numbers and special characters. The AES256 algorithm is faster with the blowfish algorithm for encryption, while for AES256 decryption is longer than Blowfish. Viewed from the encryption and decryption Algorithm AES256 is the best for its performance.

Keywords *: AES256, Blowfish, Encryption, Decryption*

Abstrak

Kemanan untuk saat ini sangat penting upaya yang dilakukan untuk melindungi data organisasi terhadap ancaman seperti penghancuran orang ketiga atau penyalahgunaan kerugian yang disengaja maupun tidak disengaja. Untuk memilih algoritma enkripsi yang terbaik untuk saat ini, Dalam penelitian ini mencoba membandingkan kecepatan waktu enkripsi dan dekripsi pada Algorima enkripsi yang terkenal yaitu algoritma AES256 dan Blowfish. Dalam penelitian ini yang dilakukan adalah melakukan pengamatan membandingkan algoritma AES256 dan Blowfish untuk waktu enkripsi dan dekripsinya. Dengan menggunakan panjang kunci 4, 6, 8, 10, dan 12 karakter. Dengan kombinasi huruf kecil dan besar, angka dan spesial karakter. Algoritma AES256 libih cepat dibanding dengan algoritma blowfish untuk enkripsinya, sedangkan untuk dekripsinya AES256 lebih lama dibandingkan dengan Blowfish. Dilihat dari enkripsi dan dekripsi tersebut Algoritma AES256 lah yang terbaik untuk performanya.

Kata kunci : AES256, Blowfish, Enkripsi, Dekripsi

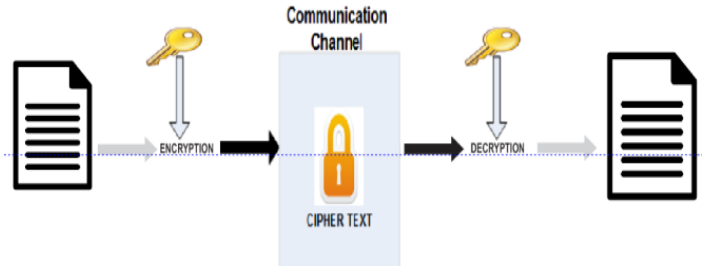
1. Pendahuluan

Saat ini, privasi dan keamanan menjadi perhatian utama teknologi elektronik (Niranjanamurthy and Chahar 2013) agar tetap aman seiring meningkatnya penggunaan sistem komputer (Jang 2010). Kemanan ini adalah upaya yang dilakukan untuk melindungi data organisasi terhadap ancaman seperti penghancuran atau penyalahgunaan kerugian yang disengaja maupun tidak disengaja. Keamanan yang dianjurkan adalah menggunakan enkripsi agar tidak dapat diakses oleh orang yang tidak bertanggung jawab (Jang 2010) (Hossain 2014). Dengan pesatnya perkembangan teknologi jaringan, serangan melalui internet juga bermacam-macam, algoritma enkripsi tradisional sudah tidak bisa membendung lagi untuk saat ini.

Untuk memilih algoritma enkripsi yang terbaik untuk saat ini, Dalam penelitian ini mencoba membandingkan kecepatan waktu enkripsi dan dekripsi pada Algorima enkripsi yang terkenal yaitu algoritma AES256 dan Blowfish

Menurut (Wardoyo, Imanullah, and Fahrizal 2014) (Maqsood , Ali , Ahmed 2017). Kriptografi adalah seni penulisan rahasia yang digunakan sejak zaman Romawi untuk merahasiakan informasi atau menjaga keamanan pesan. Metode untuk menjaga

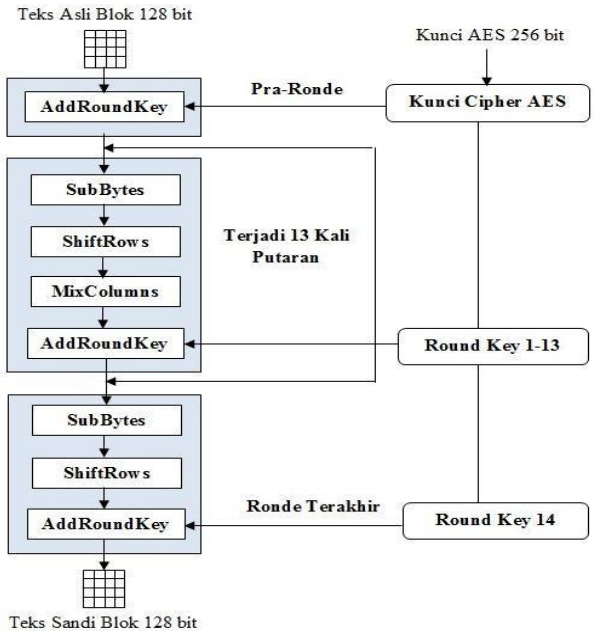
kerahasiaan informasi, adalah enkripsi/dekripsi. Untuk Alur enkripsi dan dekripsi bisa dilihat di gambar 1 dibawah ini.



Gambar 1. *Alur Enkripsi dan Dekripsi (Maqsood , Ali , Ahmed 2017)*

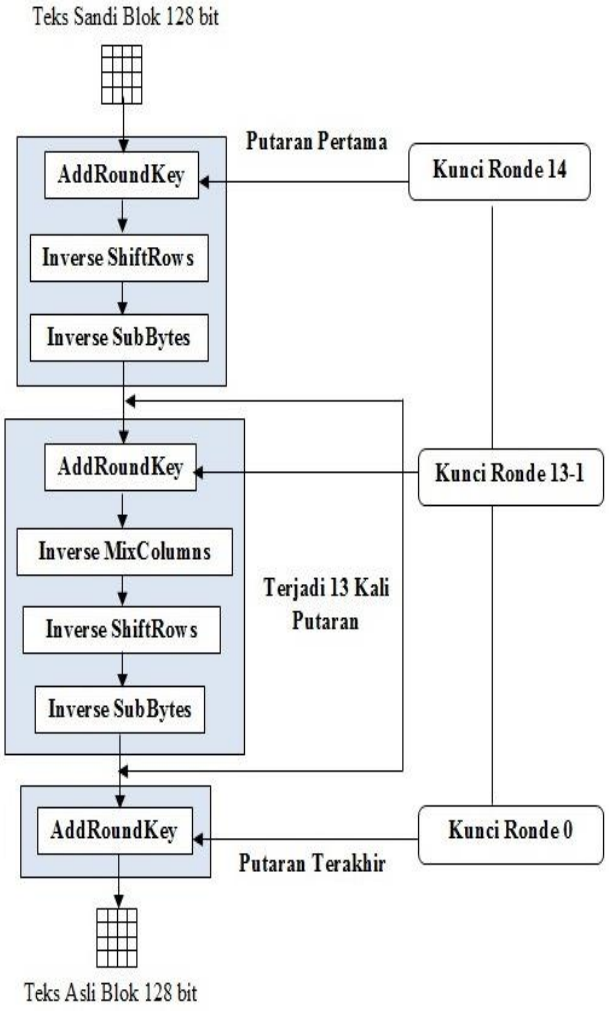
Advanced Encryption Standard (AES) adalah *cipher* blok dengan panjang blok 128 *bit* (Rihan and Osman 2015) AES (*Rijndael*) termasuk dalam jenis algoritma kriptografi yang sifatnya simetri dan *cipher block* (Bhanot and Hans 2015). Dengan demikian algoritma ini menggunakan kunci yang sama saat enkripsi dan dekripsi serta masukan dan keluarannya berupa blok dengan jumlah *bit* tertentu karena termasuk algoritma simetris. *Rijndael* mendukung berbagai variasi ukuran blok dan kunci yang akan digunakan. Namun *Rijndael* mempunyai ukuran blok dan kunci yang tetap sebesar 128, 192, 256 *bit*. Blok-blok data masukan dan kunci dioperasikan dalam bentuk *array*. Setiap anggota *array* sebelum menghasilkan keluaran *ciphertext* dinamakan dengan *state* Setiap *state* akan mengalami proses yang secara garis besar terdiri dari empat tahap yaitu, *AddRoundKey , SubBytes, ShiftRows, dan MixColumns*. Kecuali tahap *MixColumns*, ketiga tahap lainnya akan diulang pada setiap proses sedangkan tahap *MixColumns* tidak akan dilakukan pada tahap terakhir. Proses enkripsi adalah kebalikkan dari dekripsi.

Pada gambar 2 adalah proses enkrispsi AES256 dengan 14 putaran.



Gambar 2. *Proses Enkripsi AES256 (Kartika Imam Santoso 2016)*

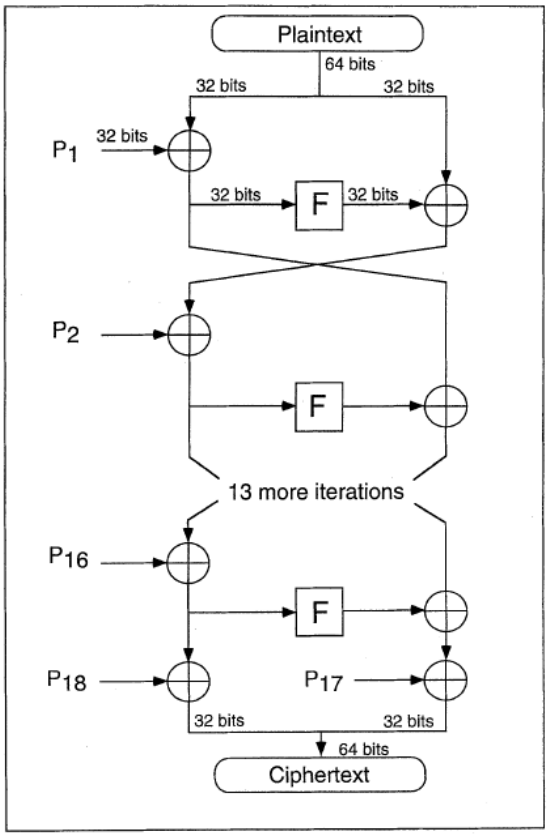
Pada Gambar.3 adalah proses dekripsi AES256 dengan melakukan putaran sebanyak 14 putaran, kebalikan dari proses enkripsi



Gambar 3. *Proses Enkripsi AES256 (Kartika Imam Santoso 2016)*

Blowfish dirancang oleh Bruce Schneier pada tahun 1993 sebagai alternatif algoritma untuk enkripsi yang cepat (Mandal 2012). *Blowfish* termasuk dalam enkripsi *block Chiper* 64-*bit* dengan panjang kunci minimal 32-*bit* sampai 448-*bit* (Wardoyo, Imanullah, and Fahrizal 2016). Dibuat untuk digunakan pada komputer yang mempunyai mikroprosesor besar (32-*bit* keatas dengan cache data yang besar) (Bruce Schneier 1994). *Blowfish* diciptakan oleh Bruce Schneier untuk digunakan oleh seseorang secara gratis (Mandal 2012).

Menurut (Bruce Schneier 1994) *Blowfish* terdiri dari iterasi fungsi sederhana (*Feistel Network*) sebanyak 16 kali putaran (iterasi), masukannya adalah 64 *bit* elemen data X seperti pada gambar 4 berikut ini.



Gambar 4. *Proses algoritma Blowfish*

Message Digest 5 (MD5) fungsi *hash* yang di bangun oleh Rivest untuk memperbarui hash sebelumnya yaitu MD4 yang sudah tidak aman dan dipublikasikan pada tahun 1992. MD5, seperti algoritma *hash* kriptografi lainnya, mengambil pesan ukuran yang bebas dan menghasilkan keluaran dengan ukuran tetap (128 *bit*) (Majumder 2012) .

2. Metode Penelitian

Jenis penelitian ini adalah eksperimental Dalam penelitian ini yang dilakukan adalah melakukan pengamatan membandingkan algoritma AES256 dan Blowfish untuk waktu enkripsi dan dekripsinya. Dengan menggunakan panjang kunci 4, 6, 8, 10, dan 12 karakter. Dengan kombinasi huruf kecil dan besar, angka dan spesial karakter. Untuk kunci dicoba dihashing dengan MD5. Sedangkan untuk panjang plaintextnya adalah 100 karakter. Komputer yang dipakai untuk program ini menggunakan komputer rumahan dengan spesifikasi *AMD Phenom* II X4 965 *Processor* 3.40 GHz, RAM 4 GB, dan AMD *Radeon* HD 5500 *memory size* 2048 MB

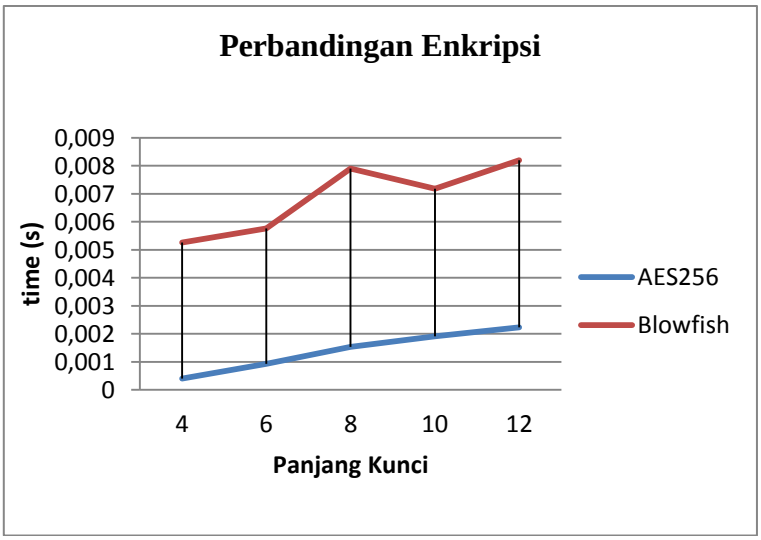
3. Hasil dan Pembahasan

Setelah melakukan ujicoba sebanyak 30 kali dengan menggunakan panjang kunci 4, 6, 8, 10, dan 12 karakter. dengan kombinasi huruf kecil dan besar, angka dan spesial karakter untuk panjang plaintext 100 karakter

Tabel 1. *Perbandingan Waktu Enkripsi (detik)*

Enkripsi	Pnjang Kunci				
	4	6	8	10	12
AES256	0,0004	0,0009333	0,00153333	0,001916667	0,002233333
Blowfish	0,0052667	0,0057667	0,0079	0,007183333	0,0082

Tabel 1 diatas apabila dibuatkan grafik akan seperti dibawah ini.

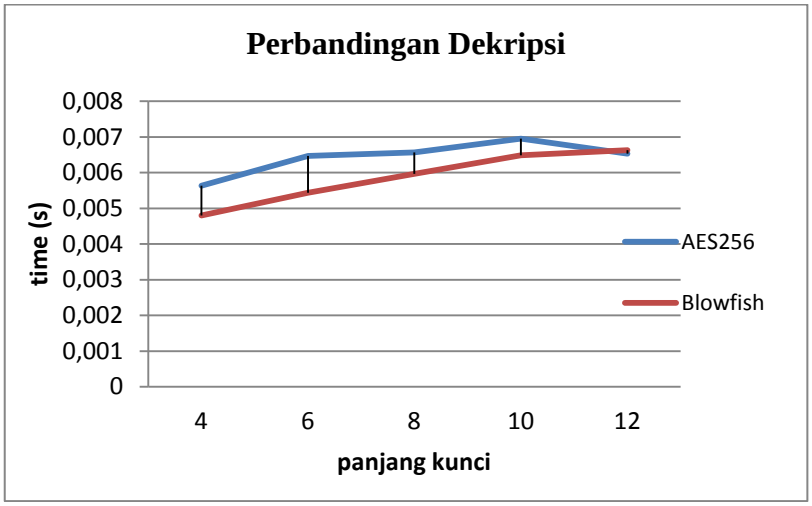


Gambar 5. *Perbandingan Enkripsi AES256 dan Blowfish*

Pada gambar 5 diatas dapat dijelaskan bahwa untuk perbandingan enkripsi, algoritma AES256 lebih Cepat dibandingkan dengan algoritma Blowfish.

Tabel 2. *Perbandingan Waktu Dekripsi (detik)*

Dekripsi	**Pnjang Kunci**				
	4	**6**	**8**	**10**	**12**
AES256	0,0056333	0,006467	0,0065667	0,00695	0,0065333
Blowfish	0,0048	0,005433	0,0059667	0,0064833	0,0066333

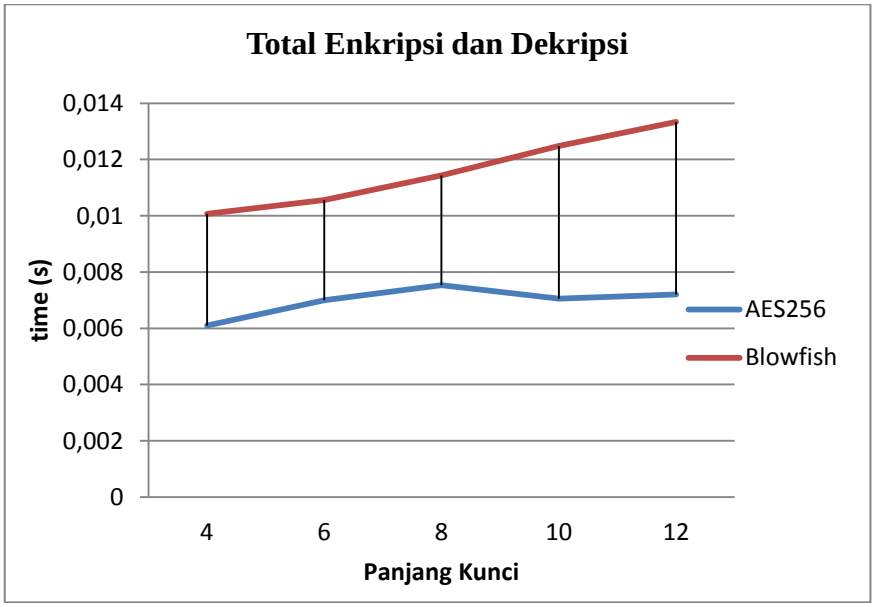


Gambar 6. *Perbandingan Dekripsi AES256 dan Blowfish*

Pada Gambar 6 dan tabel 2 diatas menunjukkan bahwa algoritma AES256 membutuhkan waktu yang lebih lama untuk dekripsinya dibandingkan dengan algorima *blowfish*.

Tabel 3. *Perbandingan Total Waktu Enkripsi dan Dekripsi (detik)*

Total Waktu Enkripsi dan Dekripsi	Panjang Kunci				
	4	6	8	10	12
AES256	0,0061	0,007	0,0075333	0,00705	0,0072
Blowfish	0,010067	0,010563	0,0114333	0,012483333	0,013333



Gambar 7. *Perbandingan Total Enkripsi dan Dekripsi AES256 dan Blowfish*

Pada gambar 7. diatas menunjukkan bahwa performa AES256 lebih bagus daripada algoritma Blowfish buatan Bruce Schneier.

4. Kesimpulan

Dengan menggunakan komputer rumahan untuk spesifikasinya *AMD Phenom* II X4 965 *Processor* 3.40 GHz, RAM 4 GB, dan AMD *Radeon* HD 5500 *memory size* 2048 MB, algoritma AES256 untuk waktu Enkripsinya lebih cepat dibandingkan dengan blowfish, sedangkan waktu dekripsinya AES256 lebih lambat dibandingkan dengan AES256.

Daftar Pustaka

Bhanot, Rajdeep, and Rahul Hans. 2015. "A Review and Comparative Analysis of Various Encryption Algorithms." 9(4): 289–306.

Bruce Schneier. 1994. "Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)."

Hossain, Monjur Ahmed and Mohammad Ashraf. 2014. "C Loud C Omputing S Ecurity in B Usiness." *International Journal of Network Security and Its Applications* 6(1): 25–36.

Jang, Seung-ju. 2010. "Developing File Security for Windows Operation System." 10(5): 36–39.

Kartika Imam Santoso, Wahyu Priyoatmoko. 2016. "Pengamanan Data Mysql Pada E-Commers Dengan Algoritma Aes 256." In *Seminar Nasional Sistem Informasi Indonesia*, , 1–8.

Majumder, Jayeeta. 2012. "Dictionary Attack on MD5 Hash." 2(3): 721–24.

Mandal, Pratap Chnadra. 2012. "Superiority of Blowfish Algorithm." *International Journal of Advance Research in Computer Science and Software Engineering* 2(9): 196–201.

Maqsood , Ali , Ahmed, & Shah. 2017. "Cryptography : A Comparative Analysis for Modern Techniques." 8(6): 442–48.

Niranjanamurthy, M., and Dharmendra Chahar. 2013. "The Study of E-Commerce Security Issues and Solutions." *International Journal of Advanced Research in Computer and Communication Engineering* 2(7): 2885–95.

Rihan, Shaza D, and Saife Eldin F Osman. 2015. "A Performance Comparison of Encryption Algorithms AES and DES." *International Journal of Engineering Research & Technology (IJERT)* 4(12): 151–54.

Wardoyo, Siswo, Zaldi Imanullah, and Rian Fahrizal. 2014. "Enkripsi Dan Dekripsi File Dengan Algoritma Blowfish Pada Perangkat Mobile Berbasis Android." *Setrum* 3(1): 43–53.

———. 2016. "Enkripsi Dan Dekripsi File Dengan Algoritma Blowfish Pada Perangkat Mobile Berbasis Android." *Jurnal Nasional Teknik Elektro* 5(1): 36–44.