# ANALISIS PERBANDINGAN PERFORMANSI ALGORITMA

# *Advance Encryption Standard* (AES) dan *Twofish*

# PADA BLOK *CIPHER*

**SKRIPSI**

Untuk Memenuhi Sebagian Persyaratan

Mencapai Drajat Sarjana S-1

Program Studi Teknik Informatika


Di Susun Oleh:

**Imam Herianto**

**10651021**



**PROGRAM STUDI TEKNIK INFORMATIKA**

**FAKULTAS SAINS DAN TEKONOLOGI**

**UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA**

**YOGYAKARTA**



**2015**

**Universitas Islam Negeri Sunan Kalijaga** **FM-UINSK-BM-05-07/R0**

**PENGESAHAN SKRIPSI/TUGAS AKHIR**

Nomor : UIN.02/D.ST/PP.01.1/ 790 /2015

Skripsi/Tugas Akhir dengan judul : Analisis Perbandingan Performansi Algoritma *Advance Encryption Standard* (AES) dan *Twofish* Pada Blok *Cipher*

Yang dipersiapkan dan disusun oleh :
Nama : Imam Herianto
NIM : 10651021
Telah dimunaqasyahkan pada : Rabu, 25 Februari 2015
Nilai Munaqasyah : A / B
Dan dinyatakan telah diterima oleh Fakultas Sains dan Teknologi UIN Sunan Kalijaga

**TIM MUNAQASYAH :**

Ketua Sidang

Bambang Sugiantoro, M.T
NIP. 19751024 200912 1 002

Penguji I

Sumarsono, M.Kom
NIP.19710209 200501 1 003

Penguji II

Nurochman, M.Kom
NIP. 19801223 200901 1 007

Yogyakarta, 24 Maret 2015
UIN Sunan Kalijaga
Fakultas Sains dan Teknologi
Dekan

Dr. Maizer Said Nahdi, M.Si
NIP. 19550427 198403 2 001

**SURAT PERSETUJUAN SKRIPSI/TUGAS AKHIR**

Hal : Permohonan
Lamp : -

Kepada
Yth. Dekan Fakultas Sains dan Teknologi
UIN Sunan Kalijaga Yogyakarta
di Yogyakarta

*Assalamu'alaikum wr. wb.*

Setelah membaca, meneliti, memberikan petunjuk dan mengoreksi serta mengadakan perbaikan seperlunya, maka kami selaku pembimbing berpendapat bahwa skripsi Saudara:

Nama : Imam Herianto
NIM : 10651021
Judul Skripsi : Analisis Perbandingan PerformansiAlgoritma *Advanced Encryption Standard* (AES) dan *Twofish* pada Blok *Cipher*.

sudah dapat diajukan kembali kepada Program Studi Tekni Informatika Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta sebagai salah satu syarat untuk memperoleh gelar Sarjana Strata Satu dalam Teknik Informatika

Dengan ini kami mengharap agar skripsi/tugas akhir Saudara tersebut di atas dapat segera dimunaqosyahkan. Atas perhatiannya kami ucapkan terima kasih.

*Wassalamu'alaikum wr. wb.*

Yogyakarta, 01 Februari 2015
Pembimbing

Bambang Sugiantoro, S.Si., MT
NIP: 19751024 200912 1 002

## PERNYATAAN KEASLIAN SKRIPSI

Yang bertanda tangan di bawah ini :

Nama : Imam Herianto

Nim : 10651021

Program Studi : Teknik Informatika

Fakultas : Sains dan Teknologi

Menyatakan bahwa skripsi dengan judul **Analisis Perbandingan Performansi Algoritma *Advanced Encryption Standard* (AES) dan *Twofish* pada Blok *Cipher*** tidak terdapat pada karya yang pernah diajukan untuk memperoleh gelar sarjana di suatu Perguruan Tinggi, dan sepengetahuan saya tidak terdapat karya atau pendapat yang pernah ditulis oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 01 Februari 2015


Menyatakan,

Imam Herianto

NIM : 10651021

## KATA PENGANTAR

*Assalamualaikum Wr.Wb.*

Segala puji bagi Allah SWT Tuhan semesta alam. Shalawat dan salam semoga tetap tercurahkan kepada junjungan kita yakni Nabi Muhammad SAW, kepada para sahabatnya, serta seluruh keluarganya, dan mudah-mudahan kita tergolong sebagai umatnya yang mendapatkan syafaat kelak di hari akhir.

*Alhamdulillah* berkat limpahan rahmat dari Allah SWT sehingga penulis dapat menyelesaikan skripsi dengan judul "Analisis Perbandingan Performansi Algoritma Kriptografi *Advanced Encryption Standard* (AES) dan *Twofish* Pada Blok *Cipher* " dengan lancar dan tanpa suatu halangan apapun.

Selanjutnya penulis mengucapkan terimaksih kepada :

1. Prof. Drs. H. Akh. Minhaji, M.A.,Ph.D, selaku Rektor UIN Sunan Kalijaga Yogyakarta.
2. Dr. Maizer Said Nahdi, M.Si, selaku Dekan Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta.
3. Bapak Agus Mulyanto, S.Si., M.Kom, selaku Ketua Program Studi Teknik Informatika UIN Sunan Kalijaga Yogyakarta.
4. Bapak Nurochman, S.Si., M.Kom, selaku Sekretaris Program Studi Teknik Informatika UIN Sunan Kalijaga Yogyakarta.
5. Bapak Bambang Sugiantoro, S.Si., MT, selaku Dosen Pembimbing yang dengan sabarnya telah membimbing saya selama ini.

6. Bapak Mustakim, M.T, selaku Dosen Pembimbing Akademik dan juga sudah memberikan saran terbaik mengenai penelitian saya.
7. Bapak dan Ibu dosen Program Studi Teknik Informatika Fakultas Sains dan Teknologi yang telah memberikan banyak ilmu dan pengalaman.
8. Teman-teman seperjuangan Program Studi Teknik Informatika, khususnya angkatan 2010 yang telah memberi dukungan, doa, motivasi, dan masukan dalam penyelesaian skripsi ini.
9. Semua pihak yang telah membantu terselesaikannya penyusunan skripsi dari awal hingga akhir.

Penulis menyadari bahwa dalam penyusunan skripsi ini masih jauh dari sempurna, maka penulis menerima segala saran dan kritik yang sifatnya membangun dari semua pihak demi kesempurnaan dimasa mendatang. Semoga skripsi ini dapat bermanfaat bagi pembaca khususnya teman-teman, adik-adik, dan pihak-pihak yang bersangkutan.

*Wassalamualaikum Wr.Wb.*

Yogyakarta, 01 Februari 2015
Yang Menyatakan

Imam Herianto
10651021

## HALAMAT PERSEMBAHAN

*Alhamdulillah . . .*

Segala puja dan puji syukur kita haturkan kepada Allah SWT atas segala rahmat dan hidayahNYA sehinga mampu menyelesaikan skripsi ini dengan selamat. Dan sholawat serta salam mudah – mudahan tetap tercurahkan kepada Nabi Besar kita Nabi Muhammad SAW, yang mana Beliau telah menuntun kita dari jalan yang gelap gulita (zaman jahiliyah) menuju jalan yang terang benderang yakni agama islam.

Skripsi ini saya persembahkan untuk :

- Kedua orang tuaku, Bapak Suwardji, Ibu Siti Aisyah, terima kasih untuk semua kebaikan, motivasi, pengorbanan, kasih saying, dan do'a yang tiada henti.
- Adik perempuanku, Farisya Irmayu, yang senantiasa memberikan do'a dan dukungannya.
- Risty Wahyuning Tyas, Terima kasih.
- Almamaterku, Teknik Informatika, Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta
- Bapak dan Ibu dosen Program Studi Teknik Informatika Fakultas Sains dan Teknologi yang telah memberikan banyak ilmu dan pengalaman.
- Kalian yang disana : Umar Kotob, Muzakki jeki, Anas Kison, Alvin, Agus Botol Fadlun, Fahmi, Aji A., Lutfi upil, Fatkur, Syamsyul Qomar, Khoirul, Fahmi Fath, dan lainnya.

- Sahabat : Alm. Fizi, Hajir, Zulkhoni, Patik, Johan, Luki, Ilek, Nasik, Doli kurus, Doli gendut, Af'am, Adi, Kak Wahyu, Emha, Dimas, Basid, dan lainnya.
- Teman semeja ngopi : Uur, Irpan, Fikri, Nuruddin, jenggol, agus, bli, barok, lemon, dan lainnya
- Seluruh warga Pondok Pesantren Al – Choiriyah : Pak Sutaman, pak mi'an, puguh, agma, nazar, kotob, charles, qifni, iyung, irfan, amin, anas, faris, gembong, pak tua, suja'ul =D
- Seluruh warga kost pak gito : Priyo, Kang Mustapa, Adam B., Rozikin, Opang, Syahir, Taha =)
- Kalian : Damar Mustiko, M. Dahlan, M. Faiz, Ucup, Fitri Su., Toni Wibowo, Najib A., Dedy S., K. Nadzif, Tama, Adi (ndut), Fajar Ramadhan, Luqman F., Arif Tuban, Yazid A., Fandi S., Hadi Ju, Dede, Pradiptya, Ikhsan Wibowo, Naufal B. (opang), Ghoni, Faizal, Maestosa, Harya B., Cincin J., Mas Purwadi, Aji K., Aziz, Iyan, Rikza, Rizki, Abid, Syahir, Putri, Fina, Erma, Siska, Sasti, Hafa, Deta, Norma, Dika, Bang Sigit, Mas Ficky, Bang Anas, Gina M., Fitria H., Nisa, Bita, dan semua Informatika angkatan 2010, 2011, dan 2012.

## HALAMAT MOTTO

“ Don’t be afraid to move,

because the distance of 1000 miles starts by a single step ”

“ Think big, feel strong, and pray hard for deep heart “

## DAFTAR ISI

## DAFTAR TABEL

## DAFTAR GAMBAR

**ANALISIS PERBANDINGAN PERFORMANSI ALGORITMA AES (*Advance Encryption Standard*) DAN *Twofish* PADA BLOK *CIPHER***

**Imam Herianto**
**NIM. 10651021**

## INTISARI

Keamanan merupakan hal yang diutamakan dalam sistem informasi, khususnya dalam pertukaran data yang bersifat penting atau rahasia. Informasi yang akan diberikan kepada pihak yang berhak terhadap informasi tersebut harus benar-benar dijaga tingkat keamanannya, jangan sampai jatuh ke tangan pihak lain yang tidak punya hak akan informasi tersebut. Salah satu upaya untuk menjaga dan menjamin keamanan informasi atau data adalah dengan menggunakan teknik kriptografi. Kriptografi merupakan seni dan ilmu untuk menyembunyikan informasi dari pihak ketiga.

*Advanced Encryption Standard* ( AES ) dan *twofish* adalah dua contoh dari beberapa algoritma kriptografi simetri berbasis blok *cipher*. Kedua sistem kriptografi menggunakan kunci yang sama simetris, 128 bit ukuran blok, dan 128, 192, 256 panjang kunci. Penelitian ini bertujuan untuk menganalisa perbandingan performansi AES dan *twofish* dalam hal kecepatan proses enkripsi dan dekripsi, nilai *avalanche effect*, dan *exhaustive key search*. Perbandingan ini difasilitasi oleh *software DP - Multicrypt*.

Berdasarkan hasil penelitian dapat disimpulkan bahwa waktu proses enkripsi dan dekripsi algoritma AES lebih cepat daripada algoritma *twofish*, karena AES memiliki struktur yang lebih sederhana. Sedangkan algoritma *twofish* lebih tangguh daripada AES terhadap *cryptanalysis* karena memiliki nilai *avalanche effect* yang lebih besar. Dan *exhaustive key search* pada kedua algoritma menghasilkan nilai waktu bongkar yang sangat besar, hal ini menyebabkan kedua algoritma dikatakan tahan terhadap *cryptanalysis*.

Kata Kunci : Twofish, Advanced Encryption Standard, Cryptography, Cipher Block, Avalanche Effect, Exhaustive Key Search.

**ANALISIS PERBANDINGAN PERFORMANSI ALGORITMA AES (*Advance Encryption Standard*) DAN *Twofish* PADA BLOK CIPHER**

**Imam Herianto**
**Nim. 10651021**

## ABSTRACT

Security is preferred in information systems, especially in the exchange of data that are important or confidential. The information will be given to the party entitled to such information should really be kept, do not fall into the hands of others who do not have a right to that information. One of the efforts to preserve and guarantee the security of information or data is to use cryptographic techniques. Cryptography is the art and science of hiding information from third parties.

Advanced Encryption Standard (AES) and Twofish are two examples of some symmetric cryptographic algorithms based on block ciphers. Both systems use the same key of symmetric cryptography, 128-bit block size, and 128, 192, 256 key length. This study aims to analyze the performance comparison AES and Twofish in speed encryption and decryption process, the value of avalanche effect, and the exhaustive key search. This comparison is facilitated by DP – Multicrypt software.

Based on the results of this study concluded that a process of encryption and decryption algorithm is faster than the AES algorithm Twofish, because AES has a simpler structure. While the Twofish algorithm tougher than AES against cryptanalysis because it has a larger avalanche effect. And exhaustive key search on both the algorithm generates a value of loading very large, this causes said second algorithm resistant to cryptanalysis.

Keywords : Advanced Encryption Standard, Avalanche Effect, Cryptography, Cipher Block, Exhaustive Key Search, Twofish.

# BAB I

# PENDAHULUAN

## 1.1. Latar Belakang

Kemudahan pengaksesan media komunikasi oleh semua orang, tentunya akan memberikan dampak bagi keamanan informasi atau pesan media komunikasi tersebut. Informasi menjadi sangat rentan untuk diketahui, diambil, dan dimanipulasi oleh pihak – pihak yang tidak bertanggung jawab.

Pengamanan komunikasi untuk mencegah pihak-pihak yang tidak berwenang dalam melakukan tindakan penyadapan terhadap data dan informasi yang dirasa sensitif, saat ini tidak hanya merupakan kebutuhan dari institusi militer ataupun pemerintah. Sektor bisnis dan bidang lainnya juga merasakan kebutuhan dalam bidang ini. Oleh sebab itu dibutuhkan suatu metode yang dapat menjaga kerahasiaan informasi dari pihak – pihak yang tidak bertanggung jawab tersebut, yang salah satunya dapat menggunakan metode kriptografi.

Pada tahun 1976 dipilihlah algoritma DES oleh *National Bureau of Standards* (NBS) milik Amerika Serikat sebagai standar enkripsi dalam pemerintahan. Sebagai efeknya, algoritma DES digunakan secara luas oleh kalangan internasional sebagai standar untuk enkripsi. Algoritma DES ini adalah algoritma kriptografi simetris yang menggunakan kunci sepanjang 56-bit. Namun, seiring dengan berkembangnya kemampuan perangkat keras untuk komputasi dan juga berkembangnya sistem terdistribusi yang bisa melakukan

komputasi menggunakan banyak komputer yang terhubung melalui suatu jaringan, DES menjadi dapat diserang melalui *exhaustive search key* atau *brute force attack* dalam waktu beberapa jam saja.

Berusaha mengatasi kelemahan algoritma DES, Bruce Schneier, seorang pakar keamanan, pada tahun 1993 merilis algoritma yang ia namakan *blowfish*. Algoritma *blowfish* ini diciptakan sebagai salah satu alternatif pengganti DES yang dirasa sudah tidak aman lagi. Algoritma *blowfish* menggunakan kunci yang panjangnya bisa bervariasi antara 32-bit hingga 448-bit. Setelah itu algoritma ini telah diterima oleh kalangan internasional sebagai suatu algoritma enkripsi yang sukar dipecahkan. *Blowfish* tidak dipatenkan dan bebas lisensi, yang berarti dapat digunakan oleh semua orang secara bebas tanpa dipungut bayaran.

Pada tahun 1997, *National Institute of Standard and Technology* (NIST) dari Amerika Serikat mengeluarkan AES untuk menggantikan DES. DES dianggap sudah tidak aman lagi, maka dari itu NIST mengusulkan kepada Pemerintah Federal AS untuk sebuah standard kriptografi baru.

Unutk menghindari kontoversi mengenai standard baru kriptografi tersebut, sebagaimana pembuatan DES (NSA sering dicurigai mempunyai "pintu belakang" untuk mengungkap cipherteks yang dihasilkan oleh DES tanpa mengetahui kunci), maka NIST mengadakan sayembara terbuka untuk membuat standard algoritma kriptografi yang baru sebagai penganti DES. Standard tersebut kelak diberi nama *Advanced Encrypion Standard* (AES).

Dan terdapat beberapa persyaratan dari NIST tentang algoritma yang baru tersebut. Dari persyaratan - persyaratan tersebut NIST menerima 15 algoritma yang masuk. Konferensi umumpun diselenggarakan untuk menilai keamanan algoritma yang diusulkan.

Dan pada tahun 2000, NIST mengumumkan memilih *rijndael*, dan pada bulan November 2001, *Rijndael* ditetapkan sebagai AES, dan diharapkan *rijndael* menjadi standard kriptografi yang dominan paling sedikit selama 10 tahun.

*Twofish* merupakan salah satu kandidat dari AES. Algoritma *twofish* dibuat oleh Bruce Schneier. Algoritma *twofish* tidak terpilih sebagai pengganti dari DES karena hanya mengumpulkan 31 suara pada konferensi umum yang diselenggarakan oleh NIST. Sebenarnya algoritma *twofish* sendiri telah memenuhi semua persyaratan dari sayembara yang dilakukan oleh NIST, yakni : Algoritma termasuk kedalam algoritma simetri, rancangan algoritma harus publik, Panjang kunci fleksibel dari 128 bit, 192 bit, dan 256 bit, ukuran blok yang dienkripsi adalah 128 bit, dan Algoritma dapat diimplementasikan baik sebagai *software* maupun *hardware*.

AES dan *twofish* merupakan blok *cipher* yang berukuran 128 bit yang dapat menerima kunci dengan panjang fleksibel, dari 128 bit, 192 bit hingga 256 bit.

Dengan banyaknya persamaaan diantara algoritma AES dan *twofish*. Penulis ingin menganalisa perbandingan antara algoritma *twofish* dan AES sebagai algoritma enkripsi kriptografi simetri dengan berbasis *cipher block*. Meskipun kedua algoritma ini memiliki basis yang sama yaitu blok *cipher*, namun keduanya memiliki metode yang berbeda dalam menyandikan data. Oleh sebab itu, kedua algoritma memiliki berbagai kelebihan dan kekurangan masing-masing dilihat dari prinsip dasar perancangan algoritma berbasis *cipher block*. Hal ini menyebabkan perbedaan dalam tingkat fleksibilitas, kesederhanaan, keamanan algoritma.

## 1.2. Rumusan Masalah

a. Bagaimana hasil perbandingan prinsip perancangan algoritma pada algoritma AES dan *twofish*?
b. Bagaimana pembangkitan kunci simetris pada algoritma AES dan *twofish*?
c. Bagaimana hasil analisis performansi dari algoritma AES dan *twofish*?

## 1.3. Batasan Masalah

a. Algoritma kriptografi yang dipakai adalah algoritma AES dan *twofish*.
b. Parameter – parameter performansi yang dibandingkan untuk algoritma AES dan *twofish* hanya prinsip perancangan algoritma, waktu proses enkripsi dan dekripsi, nilai *avalanche effect*, dan kalkulasi *exhaustive key search*.
c. Kunci yang digunakan berjenis simetris dengan panjang 128, 192, 256 bit.

## 1.4. Tujuan Penelitian

a. Menjelaskan alur kerja dari pengamanan data menggunakan algoritma AES dan twofish.
b. Menganalisa performa algoritma AES dan twofish dalam hal prinsip perancangan algoritma, waktu proses enkripsi dan dekripsi, nilai *avalanche effect*, dan kalkulasi *exhaustive key search*.

## 1.5. Manfaat Penelitian

a. Dapat membantu dalam mengamankan dokumen yang memperhitungkan kecepatan proses dan ketangguhan terhadap cryptanals.
b. Dapat digunakan sebagai referensi dalam pembahasan mengenai algoritma simetri, sehingga dapat memberikan inspirasi baru untuk pengembangan yang lebih baik.

# BAB V

# KESIMPULAN DAN SARAN

## 5.1. Kesimpulan

Berdasarkan hasil analisa dan pembahasan, diperoleh kesimpulan dari perbandingan algoritma *Advanced Encryption Standard* dan *twofish*.

### 5.1.1. Prinsip Perancangan

Dilihat dari 9 prinsip dalam pembuatan algoritma *chiper block* yang telah disebutkan sebelumnya, terdapat beberapa persamaan dan perbedaan antara perancangan algoritma *advanced encryption standard* dan *twofish*.

1) Baik algoritma *advanced encryption standard* (AES) maupun algoritma *twofish* menggunakan prinsip *confusion* dan *diffusion* dari *shanon*. Kedua algoritma telah berhasil menyembunyikan hubungan apapun yang ada antara plainteks, cipherteks, dan kunci. Untuk kedua algoritma, perubahan pada 1 bit plainteks juga menyebabkan banyak pengaruh pada cipherteks.
2) Prinsip *Chiper* berulang (*iterative chiper*) yang pada prinsipnya mengulangi proses enkripsi beberapa kali dengan kunci yang berbeda juga dilakuan pada algoritma *twofish* maupun pada Algoritma *advanced encryption standard* (AES).
3) Kedua algoritma memiliki *S-Box*. Meskipun demikian algoritma *advanced encryption standard* (AES) hanya memiliki satu *S-Box*

sedangkan algoritma *twofish* memiliki banyak *S-Box* yang dibangkitkan secara otomatis.

4) Kedua algoritma tidak memanfaatkan prinsip *P-Box* dalam merancang algoritma untuk transformasi. Akan tetapi menggunakan metode lain yaitu dengan fungsi tertentu untuk melakukan transformasi dan permutasi.
5) Algoritma *twofish* menggunakan prinsip *MDS Matrices* dan *Pseudo-Hadamard Transforms* sedangkan AES menggunakan *mixcolums*.
6) Pada kedua algoritma tidak terdapat proses ekspansi maupun kompresi.
7) Kedua algoritma tidak memiliki *weak key*. Dan kedua algoritma memiliki *keyschedule* yang terdefinisi.
8) Algoritma AES tidak menggunakan jaringan *feistel* sedangkan algoritma *twofish* menggunakan jaringan *feistel*.

### 5.1.2. Performa

1) Panjang karakter masukan dan panjang kunci berbanding lurus terhadap waktu proses enkripsi dan dekripsi kedua algoritma, hal ini karena data yang masuk ke dalam sistem semakin banyak akan mempengaruhi waktu proses sistem.
2) Waktu proses enkripsi dan dekripsi pada algoritma AES lebih rendah daripada algoritma *twofish* karena algoritma AES memilki struktur *cipher*

dan penjadwalan kunci yang relatif lebih sederhana daripada algoritma *twofish*.

3) Berdasarkan hasil pengukuran nilai *avalanche effect* kedua algoritma maka algoritma AES maupun algoritma *twofish* dikatakan tangguh terhadap *cryptanalysis* karena memiliki nilai *avalanche effet* mendekati 50 %.
4) *Brute force attack* pada kedua algoritma menghasilkan nilai waktu bongkar yang sangat besar, hal ini menyebabkan algoritma dikatakan tahan terhadap *cryptanalysis*.

## 5.2. Saran

1) Untuk pengiriman suatu dokumen penting yang lebih menekankan terhadap optimasi waktu proses maka lebih tepat digunakan algoritma kriptografi AES karena memiliki waktu proses yang relatif rendah.
2) Sedangkan untuk pengiriman suatu dokumen yang lebih menekankan terhadap daya tahan terhadap *cryptanalisis* maka lebih tepat digunakan algoritma kriptografi *twofish*.
3) Disarankan menggunakan kunci sebesar 128 bit untuk mengamankan sebuah dokumen. Dan untuk tingkat keamanan yang lebih tinggi lagi, dapat menggunakan kunci 256 bit.

# DAFTAR PUSTAKA


Alfred Menezes, P. v. (1996). *Handbook of Applied Cryptography.* Washington: CRC Press.

Ariyus, D. (2006). *Kriptografi Keamanan Data dan Komunikasi.* Yogyakarta: Graha Ilmu.

Ariyus, D. (2008). *Pengantar Ilmu Kriptografi Teori Analisis dan Implementasi.* Yogyakarta: ANDI.

Buchmann, J. A. (n.d.). Diakses pada Desember 15, 2014, from http://s29.nitroflare.com/d/b414c83899a389bb57d5d6d94aa49e63/038721156X.pdf

Buchmann, J. A. (2004). *Introduction to Cryptography; Second Edition.* USA: Springer.

Dafid. (n.d.). Diakses pada Desember 5, 2014, from http://eprints.mdp.ac.id/545/1/Jurnal%20Kriptografi%20Kunci%20Simetris.pdf

Fachrurozi, M. F. (n.d.). Diakses pada Desember 17, 2014, from http://repository.uinjkt.ac.id/dspace/bitstream/123456789/15003/1/MUHAMAD%20FARID%20FACHRUROZI-FST.pdf

*FIPS PUBS.* (n.d.). Diakses pada Desember 21, 2014, from http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

*Gunadarma.ac.id.* (n.d.). Diakses pada Januari 19, 2015, from http://elearning.gunadarma.ac.id/docmodul/diklat_kursus_spss/f.Bab_IV_Statistika_Parametrik_Uji_Beda.pdf

*Gunadarma*.ac.id (n.d.). Diakses pada Desember 13, 2014, from http://mufidnilmada.staff.gunadarma.ac.id/Downloads/files/9708/Algoritma+Brute+Force+Bagian+2.ppt

Hidayat, E. N. (2010). *Analisis Empiris Untuk Kerja Algoritma Kriptografi Block Cipher Data Encryption Standard (DES) dan GOST.* Yogyakarta: Universitas Ahmad Dahlan.

Kurniawan, Y. (2004). *Kriptografi Keamanan Internet dan Jaringan Komunikasi.* Bandung: Informatika.

Laksono, E. P. (2014). *Analisis Komparasi Algoritma Kriptografi antara Metode DES (Data Encryption Standard) dan AES (Advanced Encryption Standard).* Yogyakarta: Universitas Islam Negri Sunan Kalijaga.

Martini, E. (2008). *Analisis Empiris Unjuk Kerja Pada Algoritma Kriptografi Dengan Menggunakan Data Encryption Standard (DES) dan Rivest Code 5 (RC5).* Yogyakarta: Universitas Ahmad Dahlan.

Munir, R. (2004). *Diktat Kuliah IF5054 Kriptografi : Advanced Encryption Standard (AES).* Bandung: Departemen Teknik Informatika Institut Teknologi Bandung.

Munir, R. (2004). *Diktat Kuliah IF5054 Kriptografi : Serangan (Attack) Terhadap Kriptografi.* Bandung: Departemen Teknik Informatika Institut Teknologi Bandung.

Munir, R. (2006). *Kriptografi.* Bandung: Informatika.

Munir, R. (2007). *ALGORITMA & PEMROGRAMAN Dalam Bahasa PASCAL dan C.* Bandung: Informatika.

Pahlevi, T. R. (2010). *Analisis avalance effect terhadap algorithma kriptografi data encryption standar (DES) dan advance encryption standar (AES) dalam enkripsi data.* Malang: Universitas Brawijaya.

Rhee, M. Y. (1994). *Cryptography and Secure Communication.* New York: McGraw-Hill, Inc.

Rijmen Vincent, J. D. (2003). *AES Proposal : Rijndael.* Federal Information Processing Standards Publication.

Schneier, B. (1996). *Applied Cryptograp by : Protocols, Algorithms, and Source Code in C.* USA: John Wiley & Sons, Inc.

Setiawan, W. (n.d.). Diakses pada Januari 09, 2015, from http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2010-2011/Makalah1/Makalah1-IF3058-Sem1-2010-2011-028.pdf

Subarkah, R. (2010). *Analisis Empiris Proses Algoritma Data Encryption Standard (DES) dan Algoritma Blowfish Pada Dokumen.* Yogyakarta: Universitas Ahmad Dahlan.

Utami, R. A. (2010). *Analisis Empiris Unjuk Kerja Algoritma Rivest Code 5 (RC5) Dan Blowfish Pada Dokumen.* Yogyakarta: Universitas Ahmad Dahlan.

Viqarunnisa, P. (n.d.). Diakses pada November 20, 2014, from http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2006-2007/Makalah1/Makalah1-009.pdf