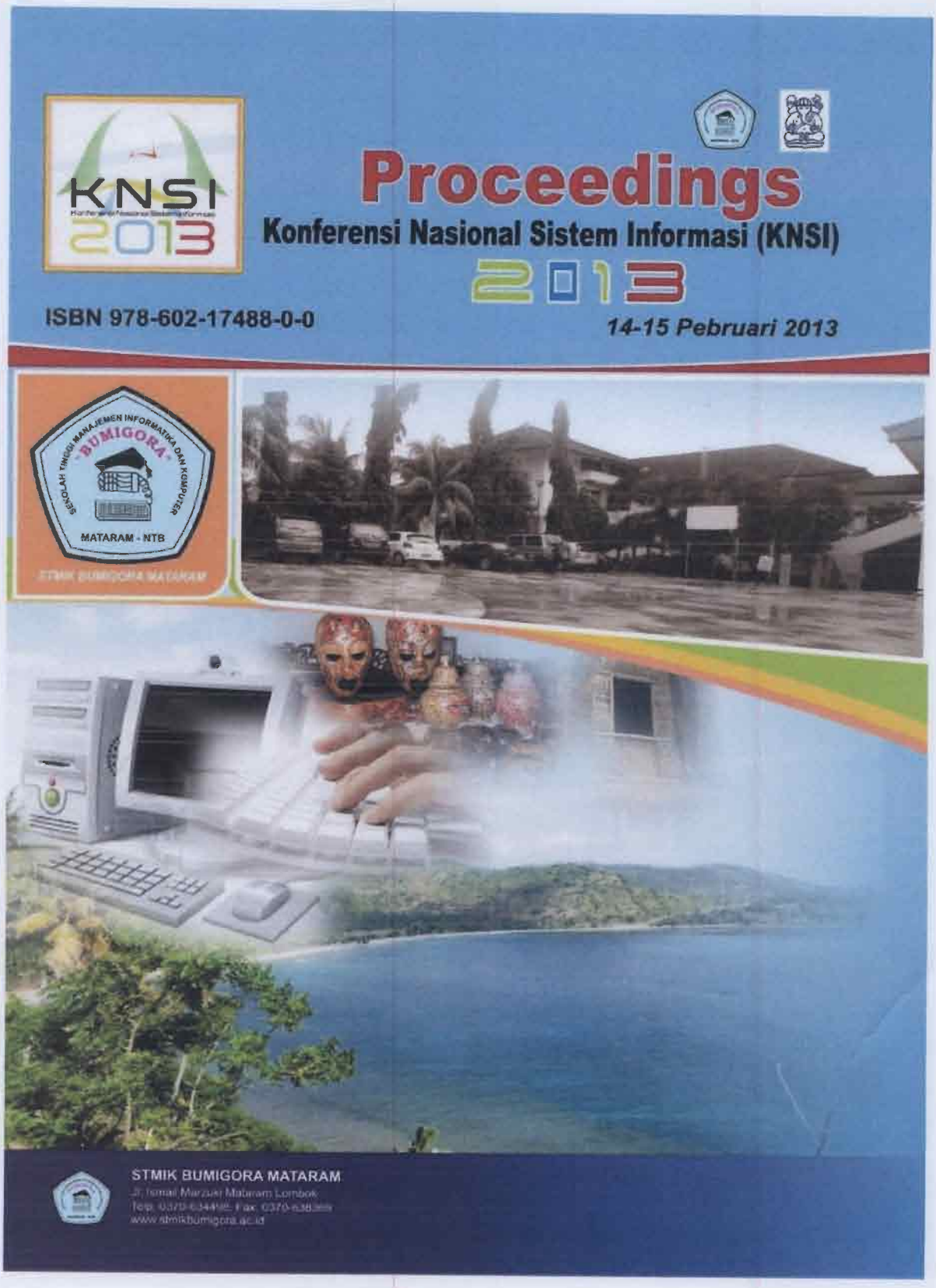


Dipublikasikan Tahun 2013 oleh :

STMIK BUMIGORA MATARAM
Mataram-Indonesia

ISBN : 978-602-17488-0-0

PROCEEDINGS
KONFERENSI NASIONAL SISTEM INFORMASI 2013

Ketua Editor
Agus Pribadi, S.T., M.Sc

Sekretaris Editor
Ir. Bambang Krismono Triwijoyo, M.Kom.

Anggota Editor
M.Yunus,S.Kom.
Ahmad Asril Rizal, S.Si.

.Makalah Nomor: KNSI- 258

PEMANFAATAN ENKRIPSI BERTINGKAT DENGAN MENGGUNAKAN ALGORITMA ADVANCED ENCRYPTION STANDARDS (AES), SERPENT, DAN TWOFISH UNTUK KEAMANAN INFORMASI

Doddy Ferdiansyah[1]

[1]Jurusan Informatika, Fakultas Teknik, Universitas Pasundan
[1]doddy2112@hotmail.com

Abstrak

Kriptografi dapat diartikan secara langsung sebagai tulisan rahasia (*secret writing*). Salah satu standar enkripsi yang terdapat dalam kriptografi adalah Advanced Encryption Standard (AES). Dalam sebuah kontes AES, terdapat dua finalis yang berhasil merancang algoritma enkripsi yang berdasarkan kriteria-kriteria dari National Institute of Standards and Technology (NAST) yaitu *Serpent* dan *Twofish*. Untuk merancang algoritma Serpent dan Twofish ini membutuhkan 256-bit key dan 128-bit block sehingga dapat mengikuti kriteria AES yaitu High Speed dan Low RAM Requirement. Pada penelitian ini dilakukan kajian teori tentang keamanan informasi dengan menggunakan algoritma kriptografi AES, Serpent, dan Twofish. Hasil akhir dari penelitian ini merupakan pemanfaatan sebuah model kriptografi dengan menggabungkan antara AES, Serpent, dan Twofish sehingga membuktikan bagaimana sebuah data/informasi akan menjadi lebih aman.

Kata kunci : *AES, Serpent, Twofish, Kriptografi*

1. Pendahuluan

Keamanan informasi sangat penting di era teknologi sekarang ini. Penyimpanan dan penyebaran informasi saat ini tidak lagi menggunakan media kertas, tetapi sudah banyak menggunakan teknologi komputer dan internet. Untuk menjaga keamanan informasi tersebut harus mengutamakan 3 faktor yaitu *Confidentiality, Integrity*, dan *Availability*. Keamanan terhadap data dan informasi yang bersifat rahasia dan pribadi dapat menggunakan Kriptografi sebagai bagian dari aspek keamanan / *security*.

Salah satu algoritma kriptografi modern saat ini yang sangat terkenal adalah Advanced Encryption Standards (AES), Serpent dan Twofish. Masing-masing dari kriptografi tersebut berdiri sendiri.

1.1 Identifikasi Masalah

Masalah-masalah yang muncul dapat di identifikasi, antara lain bagaimana menggabungkan 3 algoritma kriptografi tersebut (AES, Serpent, dan Twofish) dan bagaimana perbandingan antara enkripsi bertingkat dengan enkripsi biasa.

1.2 Tujuan Penelitian

Tujuan dari penelitian ini adalah bagaimana menggunakan enkripsi bertingkat dan menunjukan perbedaan antara enkripsi bertingkat dengan enkripsi biasa.

1.3 Metode Penelitian

Metode yang dilakukan dalam studi dan eksplorasi ini adalah sebagai berikut :

1. Studi Literatur

   Mencari dan mempelajari referensi mengenai :

   a. Konsep AES, Serpent, dan Twofish
   b. Konsep keamanan informasi

2. Analisis

   Melakukan penyelidikan atau pembelajaran lebih lanjut terhadap algoritma kriptografi, keamanan informasi dan tools yang dapat digunakan untuk

membuat algoritma AES, Serpent, dan Twofish.

3. Simulasi

Membuat contoh sebuah file yang sudah dienkripsi dengan algoritma kriptografi tersebut dengan bantuan *tools* (*software*).

2. Pemahaman Kriptografi

Kryptografi secara umum adalah ilmu dan seni untuk menjaga kerahasiaan data/informasi [2]. Ada 4 tujuan dasar dari ilmu kriptografi ini yang juga merupakan aspek keamanan informasi[3] :

i. *Confidentiality* (Kerahasiaan) : layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka/mengupas informasi yang telah disandi.

ii. *Integrity* (Integritas) : berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubsitusian data lain kedalam data yang sebenarnya.

iii. *Authentication* (Autentikasi) : berhubungan dengan identifikasi/pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan melalui kanal harus diautentikasi keaslian, isi datanya, waktu pengiriman, dan lain-lain.

iv. *Non-Repudiation* : usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman/terciptanya suatu informasi oleh yang mengirimkan/membuat.

Salah satu bentuk dari alat kriptografi yang digunakan oleh jerman pada saat perang dunia ke-2 adalah seperti gambar 1 :

Gambar 1 Alat Kriptografi Lorenz

2.1 Algoritma Sandi

Algoritma sandi adalah algoritma yang berfungsi untuk melakukan tujuan kriptografis. Algoritma tersebut harus memiliki kekuatan untuk melakukan :

1. Konfusi/pembingungan (*confusion*), dari teks terang sehingga sulit untuk direkonstruksikan secara langsung tanpa menggunakan algoritma dekripsinya.
2. Difusi/peleburan (*difusion*), dari teks terang sehingga karakteristik dari teks terang tersebut hilang.

sehingga dapat digunakan untuk mengamankan informasi.

Pada implementasinya sebuah algoritma sandi harus memperhatikan kualitas layanan/*Quality of Service* atau QoS dari keseluruhan sistem dimana dia diimplementasikan. Algoritma sandi yang handal adalah algoritma sandi yang kekuatannya terletak pada kunci, bukan pada kerahasiaan algoritma itu sendiri. Teknik dan metode untuk menguji kehandalan algoritma sandi adalah kriptanalisa.

Secara umum berdasarkan kesamaan kuncinya, algoritma sandi dibedakan menjadi :

i. kunci-simetris/*symetric-key*, sering disebut juga algoritma sandi konvensional karena umumnya diterapkan pada algoritma sandi klasik
ii. kunci-asimetris/*asymetric-key*

Berdasarkan arah implementasi dan pembagian jamannya dibedakan menjadi :

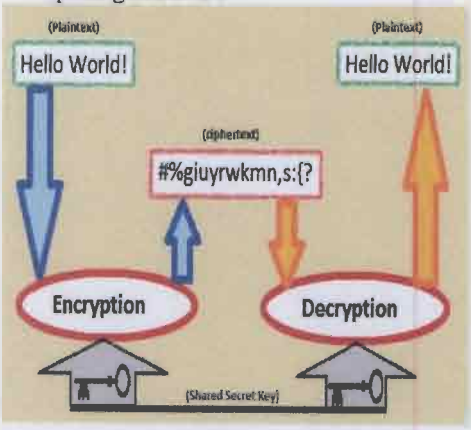
1. algoritma sandi klasik / *classic cryptography*
2. algoritma sandi modern / *modern cryptography*

Berdasarkan kerahasiaan kuncinya dibedakan menjadi :

i. algoritma sandi kunci rahasia (*secret-key*)
ii. algoritma sandi kunci publik (*publik-key*)

2.2 Algoritma Sandi Kunci-Simetris

Skema algoritma sandi akan disebut kunci-simetris apabila untuk setiap proses enkripsi maupun dekripsi data secara keseluruhan digunakan kunci yang sama. Algoritma sandi kunci simetris ini dapat diilustrasikan pada gambar 2 :



Gambar 2 Ilustrasi Algoritma Kunci Simetris

Dari Gambar 2 diatas, berdasarkan jumlah data per proses dan alur pengolahan data didalamnya dibedakan menjadi dua kelas, yaitu Block-cipher dan Stream-cipher.

A. Block-Cipher

Block-cipher adalah skema algoritma sandi yang akan membagi-bagi teks terang yang akan dikirimkan dengan ukuran tertentu (disebut blok) dengan panjang t, dan setiap blok dienkripsi dengan menggunakan kunci yang sama. Pada umumnya, block-cipher memproses teks terang dengan blok yang relatif panjang lebih dari 64 bit, untuk mempersulit penggunaan pola-pola serangan yang ada untuk membongkar kunci.

B. Stream-Cipher

Stream-cipher adalah algoritma sandi yang mengenkripsi data persatuan data, seperti bit, byte, nible atau per lima bit(saat data yang di enkripsi berupa data Boudout). Setiap mengenkripsi satu satuan data digunakan kunci yang merupakan hasil pembangkitan dari kunci sebelum.

C. Contoh Algoritma Kunci-Simetris

Beberapa contoh algoritma yang menggunakan kunci-simetris:

i. DES (Data Encryption Standard)
ii. Blowfish
iii. Twofish
iv. MARS
v. IDEA
vi. 3DES - DES diaplikasikan 3 kali
vii. AES - Advanced Encryption Standard, yang bernama asli rijndael

3. Algoritma AES, Serpent, dan Twofish

Dalam penelitian ini menggunakan 3 buah algoritma dan menggabungkannya.

3.1 AES

Advanced Encryption Standard (AES) merupakan standar enkripsi dengan kunci simetris yang diadopsi oleh pemerintah Amerika Serikat. Standar ini terdiri atas 3 blok cipher, yaitu AES-128, AES-192 and AES-256, yang diadopsi dari koleksi yang lebih besar yang awalnya diterbitkan sebagai Rijndael. Masing-masing cipher memiliki ukuran 128-bit, dengan ukuran kunci masing-masing 128, 192, dan 256 bit. AES telah dianalisis secara luas dan sekarang digunakan di seluruh dunia, seperti halnya dengan pendahulunya, Data Encryption Standard (DES).

Kecepatan yang tinggi dan kebutuhan RAM yang rendah merupakan kriteria dari algoritma AES.

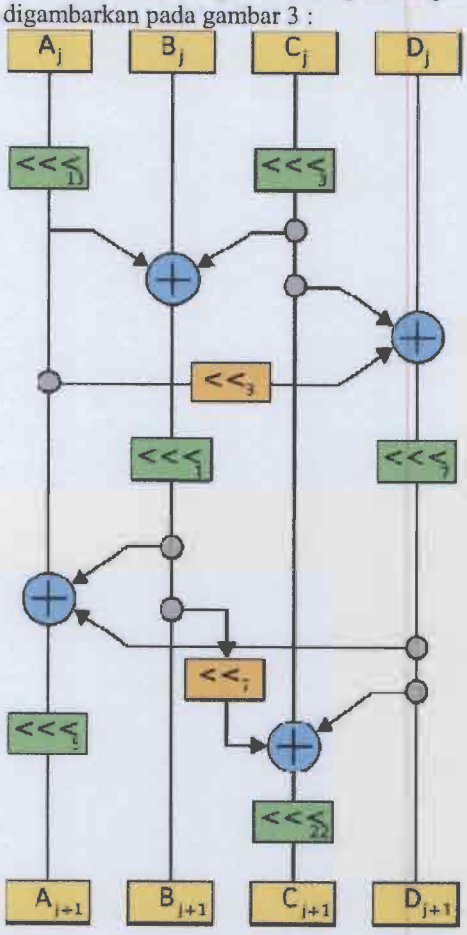
3.2 Serpent

Serpent adalah sebuah algoritma sandi kunci simetris yang merupakan salah satu finalis pada kompetisi AES. Serpent mempunyai 128 bit-block dan mendukung ukuran kunci (*key size*) 128, 192 atau 256 bit-key.

Algoritma Serpent ini terdiri dari[1]:

1. Initial Permutation (IP)
2. Terdiri dari 32 putaran, masing-masing terdiri dari sebuah operasi pengacakan kunci, operasi menggunakan S-Box, dan transformasi linear. Pada putaran terakhir, transformasi ini digantikan dengan penambahan operasi pengacakan kunci.
3. Final Permutition (FP)

Skema dari algoritma Serpent dapat digambarkan pada gambar 3 :



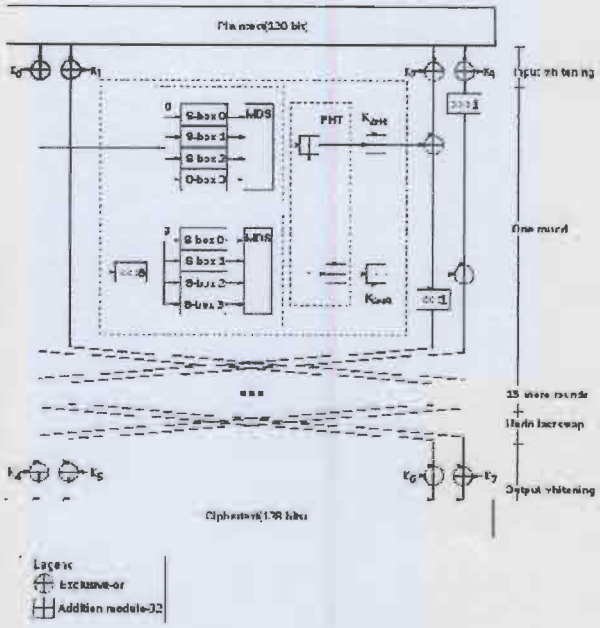
Gambar 3 Fungsi Linear pada Serpent

3.3 Twofish

Twofish merupakan algoritma kriptografi yang beroperasi dalam mode blok cipher berukuran 128 bit dengan ukuran kunci sebesar 256 bit, ukuran kunci yang besar ditujukan untuk meniadakan kemungkinan kunci lemah (*weak-key*). Algoritma Twofish sendiri merupakan pengembangan dari algoritma Blowfish. Perancangan Twofish dilakukan dengan memperhatikan kriteria-kriteria yang diajukan National Institute of Standards and Technology (NIST) untuk kompetisi Advanced Encryption Standard (AES).

Tujuan dari perancangan Twofish yang selaras dengan kriteria NIST untuk AES adalah untuk membuat suatu algoritma kriptografi yang efisien dan portabel, rancangan yang fleksibel yang dapat menerima panjang kunci tambahan sehingga dapat diterapkan pada platform dan aplikasi yang sangat bervariatif serta cocok untuk cipher aliran, fungsi hash, dan MAC, serta rancangan yang sederhana agar memudahkan proses analisis dan implementasi algoritma.

Algoritma Twofish menggunakan struktur sejenis Feistel dalam 16 putaran dengan tambahan teknik whitening terhadap input dan output. Teknik whitening sendiri adalah teknik melakukan operasi XOR terhadap materi kunci sebelum putaran pertama dan sesudah putaran akhir, seperti digambarkan pada gambar 4.



Gambar 4 Teknik Whitening pada Twofish

4. Enkripsi Bertingkat dengan AES, Serpent, dan Twofish

Seperti yang sidah diketahui bahwa algoritma AES, Serpent dan Twofish masing-masing berdiri sendiri walaupun sama-sama menggunakan bit kunci dan blok yang sama. Yang akan dieksplorasi adalah mengenkripsi sebuah file dengan cara enkripsi bertingkat dengan menggunakan ketiga algoritma kriptografi di atas. Adapun tools sebagai alat bantu adalah menggunakan TrueCrypt.

4.1 Modes of Operation pada TrueCrypt

Mode of Operation yang digunakan oleh tools TrueCrypt untuk mengenkripsi partisi, drive dan virtual volume adalah XTS. XTS ini menggunakan dua kunci independen untuk kepentingan yang berbeda.

4.2 Serpent-Twofish-AES

Dengan menggunakan TruCrypt kita dapat mengamankan file, partisi, drive, hingga virtual volume dengan maksimal

akan tetapi tidak mengurangi high speed pada proses enkripsi dan dekripsi. Cara kerja dari enkripsi bertingkat ini adalah :

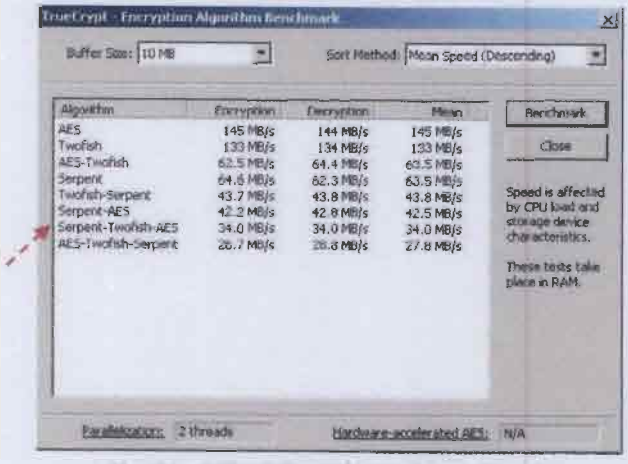
1. Setiap 128-bit blok pertama dienkripsi dengan AES (256-bit key)
2. Setelah itu di enkripsi lagi dengan Twofish (256-bit key)
3. Dan terakhir di enkripsi dengan Serpent (256-bit key)

4.3 Pengukuran Kecepatan Rata-Rata

Pengukuran yang dilakukan dengan menggunakan spesifikasi *Hardware* sebagai berikut :

a) Prosesor Core 2 Duo E7500 @2.93 GHz
b) RAM DDR3 4 Gb
c) Harddisk SATA 500 Gb

Hasil pengukuran yang didapat adalah digambarkan pada gambar 5



Gambar 5 Hasil Pengukuran *Mean Speed*

5. Kesimpulan

Setelah melakukan eksplorasi dari enkripsi bertingkat dengan menggunakan algoritma AES, Serpent, dan Twofish serta mengukur (*benchmark*) kecepatan rata-rata dari ketiga algoritma tersebut dengan menggunakan tools TrueCrypt, maka dapat diambil beberapa kesimpulan :

1. Dengan enkripsi bertingkat seperti ini dapat mengamankan informasi dengan lebih maksimal karena menggunakan 3 jenis algoritma yang berbeda.
2. Dari hasil pengukuran yang dilakukan, enkripsi bertingkat Serpent-Twofish-AES mempunyai *Mean Speed* yang cukup cepat.

Daftar Pustaka:

[1] Yusup Soleh, Moch., 2010, *Studi Perbandingan Algoritma Kunci-Simetris Serpent dan Twofish*, Bandung
[2] Rivest, Ronald L., 1990. *Handbook of Theoretical Computer Science.*
[3] AJ Menezes, PC van Oorschot, and SA Vanstone, *Handbook of Applied Cryptography*

Makalah Nomor: KNSI-247
SISTEM APLIKASI PEMINJAMAN FASILITAS UNIVERSITAS WIDYATAMA
Iwan Rijayana

Makalah Nomor: KNSI-251
PENGOLAHAN SINYAL GEOMAGNETIK SEBAGAI PREKURSOR GEMPA BUMI DI REGIONAL JEPANG
Bulkis Kanata, Teti Zubaidah, Budi Irmawati, Cipta Ramadhani

Makalah Nomor: KNSI-257
DETERMINAN FAKTOR TEKNOLOGI INFORMASI PADA PRODUKTIVITAS USAHA KECIL
Lies Handrijaningsih, Anita Wasutiningsih, E. Susy Suhendra

Makalah Nomor: KNSI-258
PEMANFAATAN ENKRIPSI BERTINGKAT DENGAN MENGGUNAKAN ALGORITMA ADVANCED ENCRYPTION STANDARDS (AES), SERPENT, DAN TWOFISH UNTUK KEAMANAN INFORMASI
Doddy Ferdiansyah

Makalah Nomor: KNSI-259
ANALISIS EFEKTIFITAS INVESTASI PROYEK TI DENGAN MENGGUNAKAN METODE INFORMATION ECONOMICS
Kaunang, Stanley D.S.Karouw, Chandra S.Rembang

Makalah Nomor: KNSI-260
SISTEM INFORMASI PENGAJUAN CUTI DAN LEMBUR STIKOM BALI BERBASIS WEB
Ni Nyoman Harini Puspita, Ni Luh Putri Srinadi, Ratna Kartika Wiyati

Makalah Nomor: KNSI-261
Implementasi dan Analisa E-mail Spam Filtering menggunakan Granular Support Vector Machines – Cumulative Margin Width (GSVM-CMW)
Pandu Fajar Mulyadi, ZK. Abdurahman Baizal, Shaufiah

Makalah Nomor: KNSI-265
PERINGKASAN OTOMATIS BERITA ONLINE BAHASA INDONESIA PADA TIMELINE TWITTER
Mohamad Ariefiandi Nugraha, Masayu Leylia Khodra, Bambang Riyanto Trilaksono

Makalah Nomor: KNSI-268
IMPLEMENTASI COBIT 5 DOMAIN BUILD, ACQUIRE, AND IMPLEMENT (BAI) PADA ELECTRONIC HEALTH RECORDS (EHR)
RS MUHAMMADIYAH BANDUNG
Arfive Gandhi, Kusuma Ayu Laksitowening, ST. MT., Angelina Prima Kurniati, ST. MT

Makalah Nomor: KNSI-269
FAKTOR-FAKTOR YANG MEMPENGARUHI KNOWLEDGE SHARING