Perbandingan Konsumsi Energi Algoritma AES (256 Bit) dan *Twofish* (256 Bit) Pada Ponsel Berbasis Android

Serli Liling Allo[1a]
M. Subali[2b]

[1]Teknik Elektro Politeknik Katolik Saint Paul
[2]Fakultas Teknologi dan Rekayasa Universitas Gunadarma,
[a]SerliLilingAllo@gmail.com, [b]subali@staff.gunadarma.ac.id

Abstraksi

Menjalankan aplikasi enkripsi/dekripsi pada ponsel akan diikuti oleh pemakaian CPU, memori, dan energi yang tersimpan dalam baterai sementara ketersediaan energi baterai terbatas, oleh karena itu cukup penting mengetahui berapa konsumsi energi dari algoritma enkripsi/dekripsi untuk menjadi salah satu bahan pertimbangan dalam pemilihan algoritma. Tujuan dari penelitian ini adalah untuk membandingkan konsumsi energi algoritma AES (256 bit) dan Twofish (256 bit) pada ponsel android.Untuk mencapai tujuan tersebut maka perlu diketahui arus, tegangan dan waktu enkripsi/dekripsi.Dalam penelitian ini arus dan tegangan diperoleh dari pengukuran langsung sedangkan waktu enkripsi/dekripsi dari algorithm benchmark pada program aplikasi SSE (Secret Space Encryptor).Konsumsi energi diperoleh dari perkalian antara arus, tegangan, dan waktu enkripsi/dekripsi.Dari hasil penelitian diperoleh konsumsi energi algoritma AES (256 bit) lebih besar dari algoritma Twofish (256 bit).

Kata kunci: *AES (256 bit), konsumsi energi enkripsi/dekripsi, Twofish (256 bit)*

A Comparative Analysis of Energy Consumption Algorhytm of AES (256 Bit) and Twofish (256 Bit) on Android-Based Cell Phone

Abstract

Running an encryption/decryption application on cell phone will be followed by the running CPU, memory, and energy stored in the battery. However, the baterry energy is limited. Therefore, it is important to observe how much energy consummed by encryption/decryption algorhytm to be one of determiners in algorhytm selecting. The study aims at comparing the energy consumption algorhytm of AES (256 bit) and Twofish (256 bit) on Android-based cell phone. To achieve that, the current, voltage, and time encryption/decryption. In the study, the current and voltage encryption/decryption are obtained from direct measurement, while time encryption/decryption is from algorithm benchmark on SSE (Secret Space Encryptor) application program. Energy consumption is obtained from the current, voltage, and time encryption/decryption multiplication. The result indicates that energy consumption algorythm of AES (256 bit) is bigger than Twofish (256 bit).

Keywords: *AES (256 bit), Encryption/Decryption Energy Consumption, Twofish (256 bit)*

PENDAHULUAN

Lembaga riset Gartner memprediksi tahun 2015 Android akan mengendalikan 48,8 % OS (*Operating System*) di dunia. Dengan semakin maraknya pengguna smartphone maka pengi-riman pesan instan melalui jaringannirkabel juga semakin banyak digunakan.Namun pesan yang dikirim melalui jaringannirkabel lebih mudah disadap oleh orang yang tidak berhak. Jika pesan yang dikirim tidak terlalu penting maka mes-kipun terjadi penyadapan pengirim/penerima tidak akan terlalu dirugikan, sebaliknya jika pesan berisi informasi penting atau rahasia maka keamanan dalam pertukaran informasi menjadi hal yang sangat penting.

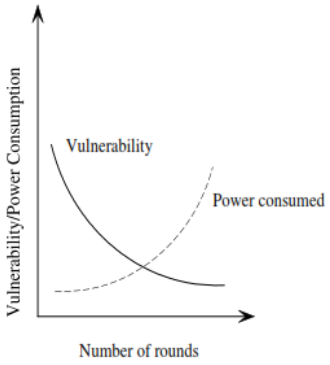
Untuk menjamin kerahasiaan pesan meski-pun berhasil disadap oleh penyerang (*attacker*) maka sebelum dikirim pesan dienkripsi terlebih dahulu sehingga menjadi pesan tersandikan yang sulit untuk dimengerti.

Menjalankan sebuah aplikasi pada ponsel dalam hal ini aplikasi enkripsi/dekripsi akan diikuti oleh konsumsi sumber daya CPU, memo-ri, dan energi baterai, di sisi lain ketersediaan energi baterai terbatas. Dengan demikian kon-sumsi energi dari setiap algoritma adalah hal yang perlu diketahui agar dapat memilih algo-ritma dengan konsumsi energi lebih rendah dan keamanannya juga tinggi.

Penelitian ini bertujuan membandingkan pemakaian energi baterai jika menggunakan algoritma AES(256 bit) dan Twofish (256 bit) pada smartphone berbasis Android. Ada bebe-rapa aplikasi enkripsi untuk ponsel android yang dapat diunduh di Google Play Store, yang digunakan dalam penelitian ini adalah SSE (*Secret Space Encryption*).

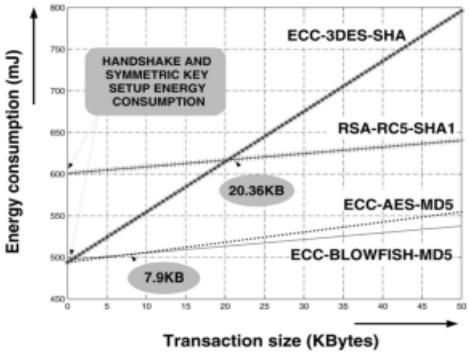
TINJAUAN PUSTAKA

Kekuatan dari sebuah algoritma enkripsi bergantung pada panjang kunci dan jumlah ronde, namun semakin besar ukuran kunci dan jumlah ronde maka konsumsi daya juga akan semakin besar [Chandramouli, 2006]. Hubungan antara *vulnerability* dan konsumsi daya untuk jumlah ronde yang bervariasi dapat dilihat pada gambar berikut :

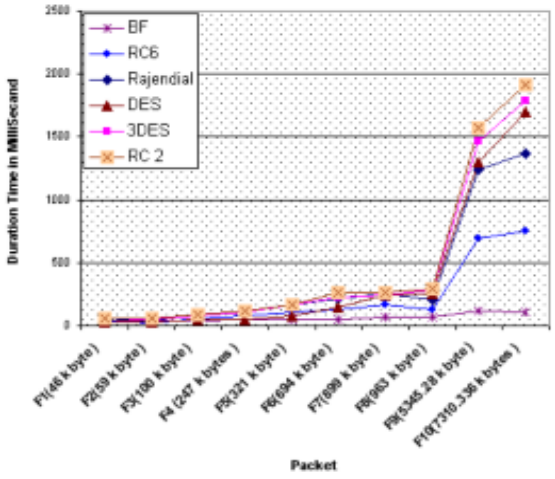


Gambar 1.Keamanan vs konsumsi daya [Chandramouli, 2006)]

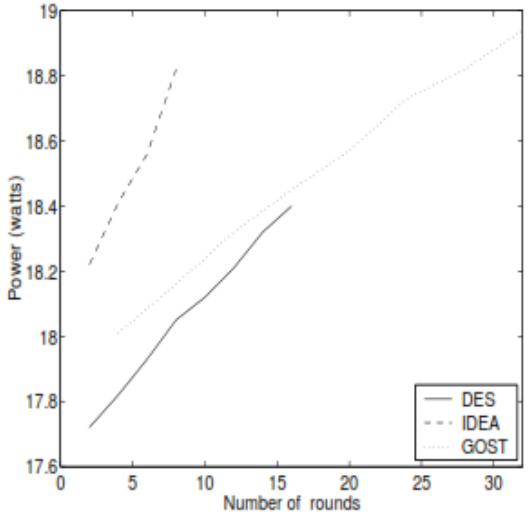
Beberapa hasil penelitian yang berhubung-an dengan konsumsi daya dan energi dari algo-ritma kriptografi dapat dilihat pada gambar-gambar berikut :



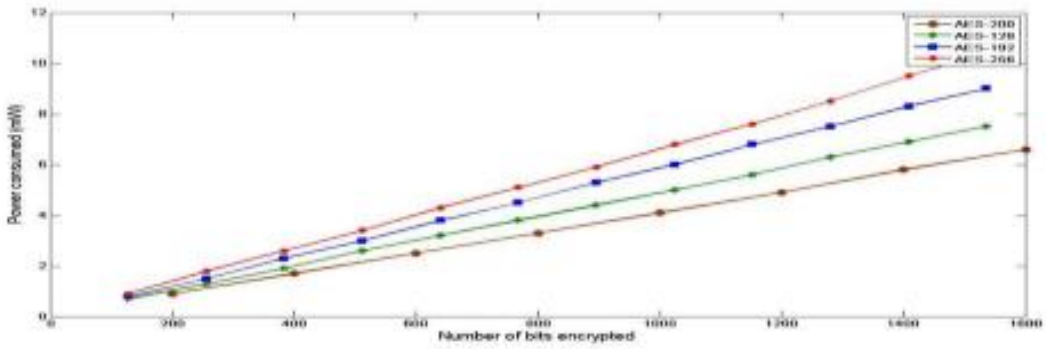
Gambar 2.Konsumsi energi selama SSL Handshake [Potlapally, 2006]



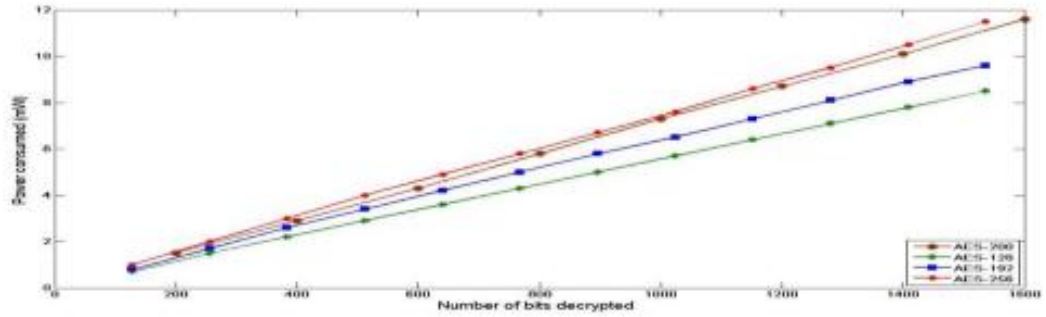
Gambar 3.Waktu enkripsi beberapa algoritma [Minaam, 2010]



Gambar 4.Konsumsi daya vs jumlah ronde dari DES, IDEA, dan GOST [Chandramouli, 2006]



Gambar 5. Konsumsi daya vs jumlah bit yang dienkripsi AES untuk panjang kunci yang bervariasi [Khatri, 2012]



Gambar 6. Konsumsi daya vs jumlah bit yang dienkripsi AES untuk panjang kunci yang bervariasi [Khatri, 2012]

Untuk memudahkan menghitung konsumsi energi dari sebuah software digunakan pe-nyederhanaan dengan menggunakan rumus:

$$E = V .I .t \quad (1)$$

E adalah energi, V adalah tegangan supply, I adalah arus, dan t adalah waktu eksekusi program.

METODE PENELITIAN

Teknik pengumpulan data yang digunakan dalam penelitian ini ada dua yaitu pengumpulan data dengan cara mengumpulkan informasi-informasi dari berbagai sumber yang mendu-kung penelitian baik itu dari buku, jurnal ilmiah, makalah, prosiding maupun artikel dari internet yang mendukung penelitian ini (*library research*) dan pengumpulan data melalui eks-perimen (*experimental research*)untuk menge-tahui kecepatan enkripsi/dekripsi, tegangan, dan arus listrik yang dibutuhkan pada saat enkripsi/dekripsi menggunakan algoritma AES (256 bit) dan Twofish (256 bit) yang kemudian digunakan untuk menghitung besar konsumsi energi baterai.

Untuk mengetahui kecepatan enkri-psi/dekripsi dari tiap algoritma maka digunakan alat dan bahan sebagai berikut :

1. Samsung Galaxy Ace Duos (GT-S6802)
   Spesifikasi ponsel ini adalah :
   - Sistem operasi yang digunakan Androd 2.3 (Gingerbread)
   - Prosesor 832 MHz
   - RAM 512MB
   - Kapasitas baterai 1300 mAh

Gambar 7. Samsung GT-S6802

2. Program aplikasi SSE (*Secret Space Encryption*)

   Program ini berfungsi untuk meng-enkripsi dan mendekripsi pesan dan dapat menampilkan tolok ukur algoritma (*bench-mark algorithm*) yang merupakan nilai estimasi kecepatan enkripsi/dekripsi dari algoritma yang digunakan. Dapat diunduh dari Google Play Store atau dari http://www.paranoiaworks.mobi/download/downloads.html.

Untuk mengetahui tegangan dan arus listrik digunakan alat-alat sebagai berikut :

Gambar 8. *Power Supply* Digital H&K-1502DD

Gambar 9. *Power Supply* Analog H&K 1501T

1. Catu daya (*Power Supply*)

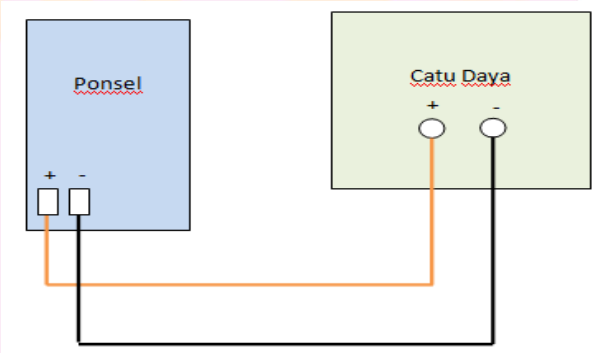
   Power supply digunakan untuk menghidupkan ponsel.Pada penelitian ini digunakan dua buah *power supply*,yaitu H&K-1502DD (digital) dan H&K 1501 T (analog). Alasan menggunakan dua *buah power supply* adalahu ntuk membandingkan hasil pengukuran masing-masing power supply sehingga diperoleh hasil yang lebih akurat.

2. Multimeter digital
   Digunakan untuk mengukur tegangan output dari *power supply* untuk memastikan tegangan output tersebut sudah benar sebelum dihubungkan ke ponsel.

Gambar 10. Multimeter Digital CD800a

Langkah-langkah percobaan :

1. Catu daya diset pada tegangan 3.7 V
2. Tegangan output catu daya diukur dengan multimeter untuk memastikan tegangan output sudah sesuai
3. Baterai ponsel dilepas kemudian positif dan negatif ponsel dihubungkan dengan positif dan negatif catu daya seperti pada gambar di bawah :



Gambar 11. Skema rangkaian pengukuran arus dan tegangan

4. Ponsel dinyalakan kemudian perubahan arus listrik yang di-tampilkan pada catu daya diamati
5. Semua aplikasi yang berjalan di belakang layar dimatikan dan kecerahan layar diatur pada posisi paling minimum.
6. Aplikasi SSE dijalankan dan besar arus listrik pada saat *idle* dan pada saat proses enkripsi/dekripsi diukur.

Untuk menghitung konsumsi baterai maka digunakan teknik yang sama dengan penelitian yang dilakukan oleh A.Sinha dan A. P. Chandrakasan (2001) dalam penelitian mereka yang berjudul "*Joule track - A webBased Tool forSoftware Energy Profiling*," [Sinha, 2001] yang juga diikuti

oleh D. S. A. Minaam, dkk.(2010) dalam penelitian yang berjudul "*Evaluating the Effect of Symmetric Cryptography Algorithms on Power Consump-tion for Different Data Types,*" yaitu untuk memperoleh besarnya konsumsi energi maka digunakan rumus (1) [Minaam, 2010]

Dalam pengukuran arus digunakan teknik yang sama dengan teknik yang digunakan oleh R. Chandramouli, dkk. dalam penelitian yang berjudul "*Battery Power-Aware Encryption*" [Chandramouli, 2006], yaitu untuk meng-hilangkan pengaruh dari aplikasi yang berjalan di balik layar (*background*) maka pengukuran arus dilakukan pada saat tidak ada aplikasi lain yang sedang berjalan. Perbedaan antara arus ketika enkripsi/dekripsi dijalankan dengan arus *idle* diasumsikan sebagai arus untuk enkrip-si/dekripsi.

HASIL DAN PEMBAHASAN

Pengukuran kecepatan algoritma AES (256 bit) dan Twofish (256 bit)

Dari beberapa percobaan diperoleh tolok ukur algoritma (*algorithm benchmark*), yang dapat dijadikan sebagai acuan untuk memperkirakan kecepatan enkripsi/dekripsi.

Tabel 1. ***Algorithm Benchmark*** **untuk AES (256 bit)**

Percobaan ke-	A = 15.360 byte		B = 262.144 byte	
	Enc. A (MB/s)	Dec. A (MB/s)	Enc. B (MB/s)	Dec. B (MB/s)
1	2,65	2,70	2,92	3,27
2	2,66	2,56	2,93	3,49
3	2,67	2,54	2,89	3,43
4	2,45	2,62	2,82	3,49
5	2,67	2,54	2,89	3,43
6	2,67	2,71	2,92	3,31
7	2,69	2.72	2.98	3,56
8	2,65	2,72	3,23	3,58
9	2,68	2,72	2,99	3,56
10	2,71	2,71	2,83	3,50
Rata-Rata Hitung	$\overline{X}_{AA}$ = **2,650**	$\overline{Y}_{AA}$ = **2,654**	$\overline{X}_{BA}$ = **2,940**	$\overline{Y}_{BA}$ = **3,462**

$\overline{X}_{AA}$ = rata-rata kecepatan enkripsi A dengan algoritma AES (256 bit)

$\overline{Y}_{AA}$ = rata-rata kecepatan dekripsi A dengan algoritma AES (256 bit)

$\overline{X}_{BA}$ = rata-rata kecepatan enkripsi B dengan algoritma AES (256 bit)

$\overline{Y}_{BA}$ = rata-rata kecepatan dekripsi B dengan algoritma AES (256 bit)

Tabel 2. ***Algorithm Benchmark*** **untuk Twofish (256 bit)**

Percobaan ke-	A = 15.360 byte		B = 262.144 byte	
	Enc. A (MB/s)	Dec. A (MB/s)	Enc. B (MB/s)	Dec. B (MB/s)
1	2,70	3,38	3,16	4,85
2	2,96	3,68	3,32	4,88

Percobaan ke-	A = 15.360 byte		B = 262.144 byte	
	Enc. A (MB/s)	Dec. A (MB/s)	Enc. B (MB/s)	Dec. B (MB/s)
3	3,09	3,51	3,37	4,40
4	3,14	3,72	3,45	4,90
5	3,15	3,55	3,75	4,75
6	3,21	3,69	3,79	4,93
7	3,10	3,66	3,48	4,96
8	3,15	3,74	3,53	4,97
9	3,15	3,69	3,88	4,97
10	3,10	3,69	3,84	4,97
Rata-Rata Hitung	$\overline{X}_{AT}$ = **3,075**	$\overline{Y}_{AT}$ = **3,631**	$\overline{X}_{BT}$ = **3,557**	$\overline{Y}_{BT}$ = **4,862**

$\overline{X}_{AT}$ = rata-rata kecepatan enkripsi A dengan algoritma Twofish (256 bit)

$\overline{Y}_{AT}$ = rata-rata kecepatan dekripsi A dengan algoritma Twofish (256 bit)

$\overline{X}_{BT}$ = rata-rata kecepatan enkripsi B dengan algoritma Twofish (256 bit)

$\overline{Y}_{BT}$ = rata-rata kecepatan dekripsi B dengan algoritma Twofish (256 bit)

Pengukuran Arus Listrik

Hasil pengukuran arus listrik pada ponsel Samsung Galaxy Ace Duos (GT-S6802) untuk tegangan input Vi=3,72 Volt :

Tabel 3. Pengukuran arus Listrik

Keadaan	Arus (A)
Start up	0,04 – 0,32
Idle	0,06
Enkripsi /Dekripsi	0,24

Analisis Kecepatan dan Waktu Enkripsi/Dekripsi AES (256 bit) dan Twofish (256 bit)

Berdasarkan Tabel 1 rata-rata kecepatan enkripsi algoritma AES (256 bit) adalah 2,65 MB/s untuk data yang berukuran 15.360 byte (Enkripsi A), rata-rata kecepatan untuk meng-enkripsi data berukuran 262.144 byte (Enkripsi B) adalah 2,94 MB/s, rata-rata kecepatan dekripsi A adalah 2,654 MB/s, dan dekripsi B adalah 3,462 MB/s. Sedangkan untuk algoritma Twofish (256 bit) rata-rata kecepatan enkripsi A = 3,075 MB/s, enkripsi B = 3,557 MB/s, enkripsi A = 3,631 MB/s, dan dekripsi B = 4,858 MB/s (Tabel 2).

Untuk memudahkan dalam perhitungan maka kecepatan enkripsi/dekripsi diasumsikan sebagai rata-rata dari enkripsi/dekripsi A dan B, dengan demikian untuk algoritma AES:

- Kecepatan enkripsi:

$$v_{enk\ AES} = \frac{\overline{X}_{AA} + \overline{X}_{BA}}{2} = \frac{2{,}650\ MB/s + 2{,}940\ MB/s}{2} = 2{,}795 MB/s$$

- Kecepatan dekripsi:

$$v_{dek\ AES} = \frac{\overline{Y}_{AA} + \overline{Y}_{BA}}{2} = \frac{2{,}654\ MB/s + 3{,}462\ MB/s}{2} = 3{,}058\ MB/s$$

Untuk algoritma *Twofish*:

- Kecepatan enkripsi:

$$v_{enk\ Twofish} = \frac{\overline{X}_{AT} + \overline{X}_{BT}}{2} = \frac{3{,}075\ MB/s + 3{,}557\ MB/s}{2} = 3{,}316 MB/s$$

- Kecepatan dekripsi:

$$v_{dek\ Twofish} = \frac{\bar{Y}_{AT} + \bar{Y}_{BT}}{2} = \frac{3{,}631\ MB/s + 4{,}858\ MB/s}{2} = 4{,}244\ MB/s$$

Waktu yang dibutuhkan untuk enkripsi/dekripsi pesan dapat dihitung dengan membagi ukuran pesan dengan kecepatan enkripsi/dekripsi. Misalnya waktu yang diper-lukan oleh algoritma AES untuk mengenkripsi pesan yang berukuran 15,360 KB adalah :

$$t_{enkripsi} = \frac{ukuran\ pesan}{kecepatan\ enkripsi} = \frac{15{,}36\ KB}{2{,}795\ MB/s} = 5{,}496\ ms$$

Sedangkan waktu dekripsi adalah :

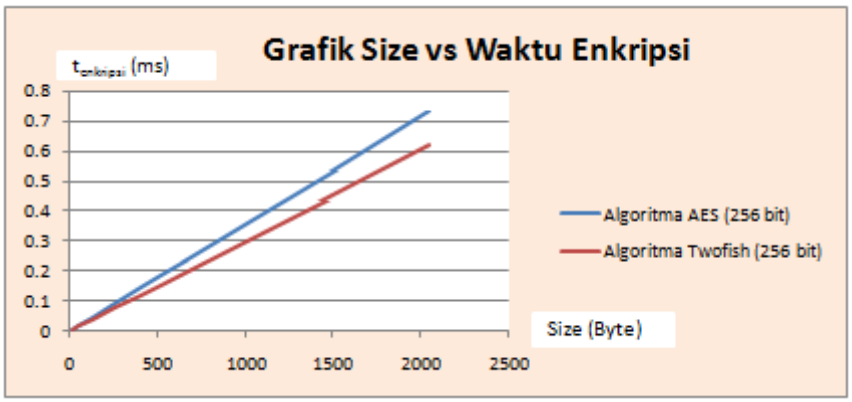
$$t_{dekripsi} = \frac{ukuran\ pesan}{kecepatan\ dekripsi} = \frac{15{,}36\ KB}{3{,}058\ MB/s} = 5{,}023\ ms$$

Dengan cara yang sama, diperoleh waktu enkripsi/dekripsi untuk beberapa ukuran pesan seperti pada tabel di bawah:

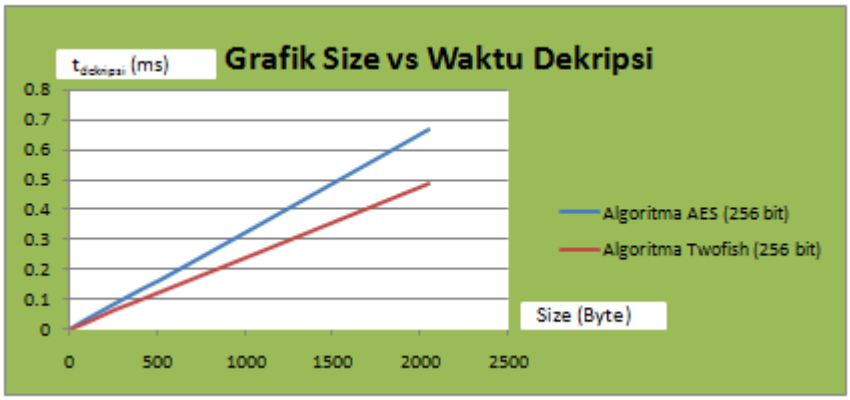
Tabel 4. Waktu enkripsi/dekripsi beberapa ukuran pesan

Ukuran Pesan (Byte)	Algoritma AES (256 bit)		Algroritma Twofish (256 bit)	
	$t_{enkripsi}$ (ms)	$t_{dekripsi}$ (ms)	$t_{enkripsi}$ (ms)	$t_{dekripsi}$ (ms)
10	0.00358	0.00327	0,00302	0.00235
50	0.01789	0.01635	0.01501	0.01178
128	0.04580	0.04186	0.03860	0.03016
256	0.09159	0.08371	0.07720	0.06032
400	0.14311	0.13080	0.12063	0.09425
512	0.18318	0.16743	0.15440	0.12064
1024	0.36637	0.33486	0.30881	0.24128
2048	0.73274	0.66972	0.61761	0.48256

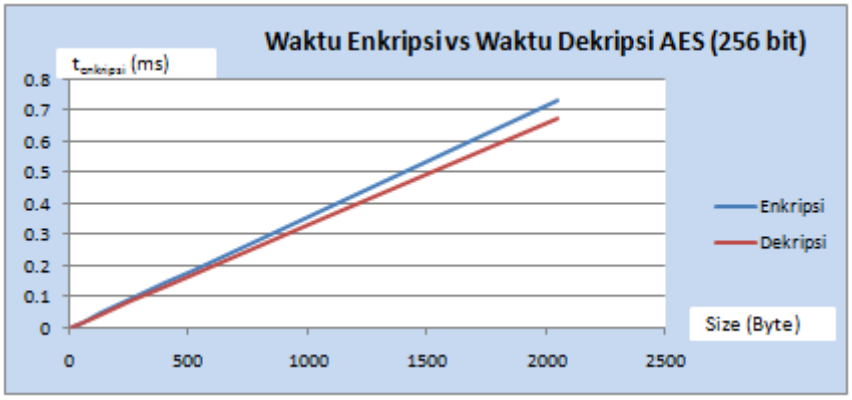
Berdasarkan Tabel 4 dapat digambarkan grafik hubungan ukuran pesan dengan waktu enkripsi, ukuran pesan vs waktu dekripsi, waktu enkripsi vs dekripsi algoritma AES (256 bit) dan algoritma Twofish (256 bit).



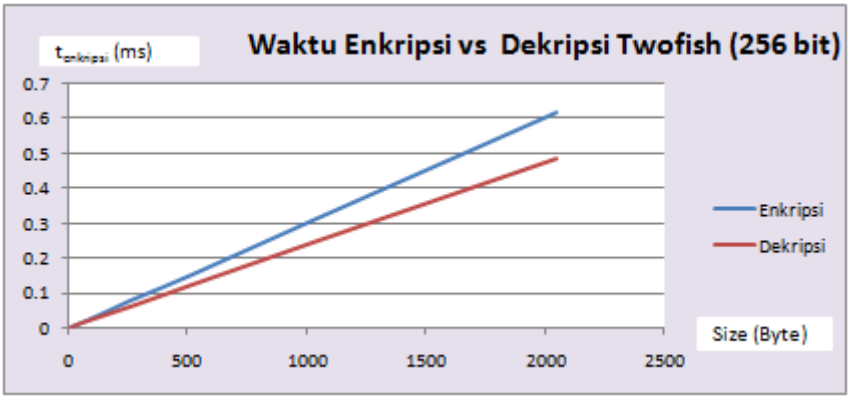
Gambar 12. Grafik *size* vs waktu enkripsi



Gambar 13. Grafik *size* vs waktu dekripsi



Gambar 14. Grafik waktu enkripsi vs dekripsi AES (256 bit)



Gambar 15. Grafik waktu enkripsi vs dekripsi Twofish (256 bit)

Analisis Konsumsi Energi Baterai Algoritma AES (256 bit) dan Twofish (256 bit)

Untuk menentukan konsumsi energi dari algoritma AES (256 bit) dan twofish (256 bit) maka digunakan rumus E = V .I . t. Dari Tabel 3, arus *idle* = 0,06 A sedangkan arus pada saat enkripsi/dekripsi = 0,24 A sehinngga arus enkripsi/dekripsi diasumsikan = 0,24 A - 0,06 A = 0,18 A. Dengan demikian konsumsi energi untuk mengenkripsi plaintext " Jam 10 am di cafe melati" dapat dihitung dengan cara:

- Dengan algoritma AES (256 bit):

Dik : size = 24 karakter = 24 Byte
Kecepatan enkripsi = 2,795 MB/s
I = 0,18 A
V = 3,72 V
maka
t = 24 Byte/2,795 MB/s = 8,587 µs
E = V.I.t = 3,72 V x 0,18 A x 8,587 µs = 5,75 µJ

- Dengan algoritma Twofish (256 bit):
Dik : size = 24 karakter = 24 Byte
Kecepatan enkripsi = 3,316 MB/s
I = 0,18 A
V = 3,72 V
maka
t = 24 Byte/3,316 MB/s = 7,238 µs
E = V.I.t = 0,18 A x 7,238 µs x 3,72 V = 4,846 µJ

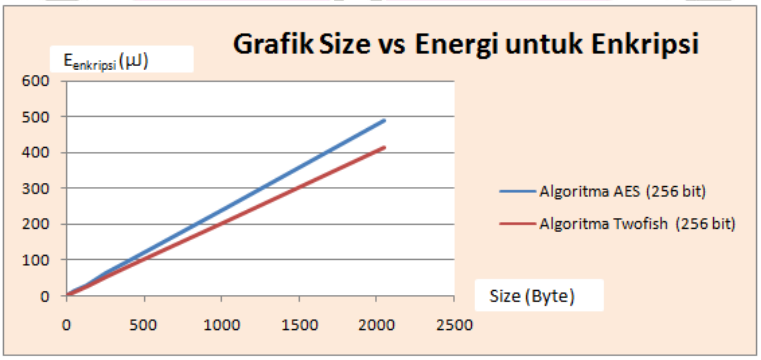
Dengan cara yang sama, konsumsi energi untuk beberapa ukuran pesan ditunjukkan pada tabel berikut;

:

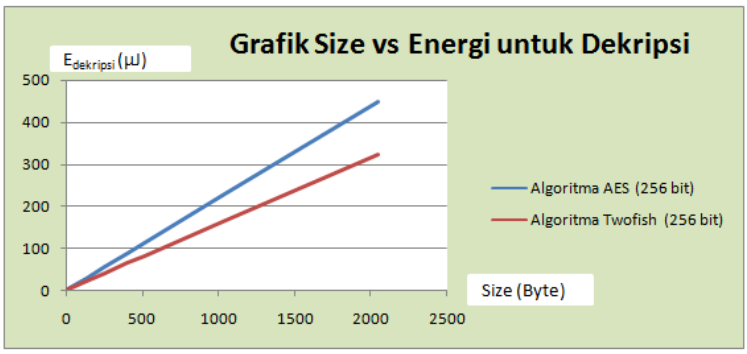
Tabel 5. Konsumsi energi algoritma AES (256 bit) dan Twofish (256) untuk beberapa ukuran pesan

Ukuran Pesan (Byte)	Konsumsi energi			
	Algoritma AES (256 bit)		Algoritma Twofish (256 bit)	
	$E_{enkripsi\ (\mu J)}$	$E_{dekripsi\ (\mu J)}$	$E_{enkripsi\ (\mu J)}$	$E_{dekripsi\ (\mu J)}$
10	2,396	2,190	2,019	1,578
50	11,979	10,948	10,097	7,889
128	30,665	28,028	25,847	20,195
256	61,330	56,055	51.694	40,391
400	95,828	87,587	80,772	63,110
512	122,660	112,111	103,388	80,781
1024	245,320	224,222	206,776	161,562
2048	490,641	448,444	413,553	323,125

Berdasarkan Tabel 5 dibuat grafik hubungan konsumsi energi dengan algoritma enkripsi dan konsumsi energi vs algoritma dekripsi.



Gambar 16. Grafik konsumsi energi vs algoritma enkripsi



Gambar 17. Grafik konsumsi energi vs algoritma dekripsi

Dari gambar di atas terlihat bahwa energi yang digunakan untuk enkripsi/denkripsi AES (256 bit) lebih besar daripada energi enkripsi/dekripsi Twofish (256 bit). Untuk tegangan (V) dan arus (I) tetap maka perubahan energi bergantung pada waktu enkripsi/dekripsi (t), karena t adalah ukuran pesan (z) dibagi kecepatan enkripsi/dekripsi (ν) sedangkan kecepatan en-kripsi/dekripsi diasumsikan konstan maka perubahan energi akan berubah secara linier terhadap perubahan ukuran pesan (z). Dengan demikian dapat dibuat persamaan linier untuk energi enkripsi/dekripsi sebagai berikut :

E = mz (2)

dengan $m = \frac{V.I}{\nu}$ (3)

Berdasarkan persamaan (2) dan (3) maka dapat dibuat persamaan linier untuk energi enkripsi/dekripsi sebagai berikut:

a. AES (256 bit)
   - Energi enkripsi

$$E = mz = \frac{V.I}{\nu} z = \frac{3{,}72\,Vx0{,}18\,A}{2{,}795\,MB/s} z = 0{,}24z \quad (\mu J)$$

   - Energi dekripsi

$$E = mz = \frac{V.I}{\nu} z = \frac{3{,}72\,Vx0{,}18\,A}{3{,}058\,MB/s} z = 0{,}22z \quad (\mu J)$$

b. Twofish (256 bit)
   - Energi enkripsi

$$E = \frac{3{,}72\,Vx0{,}18\,A}{3{,}316\,MB/s} z = 0{,}20z \quad (\mu J)$$

   - Energi dekripsi

$$E = \frac{3{,}72\,Vx0{,}18\,A}{4{,}244\,MB/s} z = 0{,}16z \quad (\mu J)$$

SIMPULAN DAN SARAN

Energi enkripsi algoritma AES (256 bit) dan Twofish (256 bit) pada ponsel Samsung Galaxy Ace Duos (GT-S6802) berubah secara linier terhadap perubahan ukuran pesan menurut persamaan E = 0.24z untuk algoritma AES (256 bit) dan E = 0.20z untuk algoritma Twofish (256 bit). Dengan demikian energi enkripsi Twofish (256 bit) adalah 83,33 % dari energi AES (256 bit) atau lebih kecil 16,67 % dari algoritma AES (256 bit).

Energi dekripsi algoritma AES (256 bit) dan Twofish (256 bit) berubah secara linier terhadap perubahan ukuran pesan menurut persamaan E = 0.22z untuk algoritma AES (256 bit) dan E = 0.16z untuk algoritma Twofish (256 bit). Dengan demikian energi dekripsi Twofish (256 bit) adalah 72,72 % dari energi AES (256 bit) atau lebih kecil 27,27 % dari algoritma AES (256 bit).

Penelitin ini hanya membandingkan AES (256 bit) dan Twofish (256 bit) dari segi konsumsi energi untuk peneliti yang berikut disarankan membandingkan keamanan algo-ritma AES (256 bit) dan Twofish (256 bit) pada ponsel berbasis android.

Daftar Pustaka

[Chandramouli , 2006] Chandramouli, R., Bapatla,S., Subbalakshmi, K.P. 2006.*"Battery Power-aware Encryption."*ACM Transactions on Information and System Security (TISSEC).Vol. 9, No. 2. New York, USA

[Khatri, 2012] Khatri, N., Dhanda, R., and Singh, J. 2012. "*Comparison of Power Consumption and Strict Avalanche Criteria at Encryption/Decryption Side of Different AES Standards*."IJCER.Vol. 2, No.4.

[Minaam, 2010] Minaam, D. S. A., Abdual-Kader, H. M., and Mohiy. 2010.*"Evaluating the Effects of Symmetric Cryptography Algorithms on Power Consumption for Different Data Types."* IJNS, Vol. 11.

[Potlapally, 2003] Potlapally, N.R, Ravi S.R.A, Jha N.K. 2003."*Analyzing the Energy Consumption of Security Protocols.*"Prosiding International Symposium on Low Power Electronics and Design. Seoul, South Korea.

[Sinha, 2001] Sinha, A andChandrakasan, A.P. 2001." *Joule Track-A WebBased Tool forSoftware Energy Profiling."*Proceedings ofthe 38th Design Automation Conference.DACLasVegas,USA.