

## **BAB V**

### **HASIL ANALISIS DAN PEMBAHASAN**

Dalam melakukan penelitian penulis menggunakan metode deskriptif dan uji coba (kuantitatif) performa kecepatan serta penggunaan memori masing-masing algoritma dalam mengenkripsi sejumlah data. Pembahasan akan dilakukan terhadap hasil temuan baik yang bersifat deskriptif maupun hasil uji coba performa (kuantitatif).

#### **5.1 Perbandingan Berdasarkan Percobaan Eksperimental**

Dalam menganalisa performa algoritma DES dan AES penulis mempersiapkan 6 buah file yang berisi kumpulan data dengan size dan isi yang berbeda, selanjutnya penulis melakukan percobaan eksperimental berdasarkan kriteria kekompleksan dalam kriptanalisis menurut Kaisar Siregar, yang memiliki 3 kriteria yaitu : waktu, memori dan data.

Data yang akan digunakan sebagai input yaitu 6 buah file dengan rincian sebagai berikut :

1. Data 1 merupakan sebuah file berukuran 8 kb yang berisikan kombinasi huruf besar (kapital) dan huruf kecil sebanyak 8.000 huruf.
2. Data 2 merupakan sebuah file berukuran 16 kb yang berisikan kombinasi huruf besar (kapital) dan huruf kecil sebanyak 16.000 huruf.
3. Data 3 merupakan sebuah file berukuran 24 kb yang berisikan kombinasi huruf besar (kapital) dan huruf kecil sebanyak 24.000 huruf.

4. Data 4 merupakan sebuah file berukuran 32 kb yang berisikan kombinasi huruf besar (kapital) dan huruf kecil sebanyak 32.000 huruf.
5. Data 5 merupakan sebuah file berukuran 40 kb yang berisikan kombinasi huruf besar (kapital) dan huruf kecil sebanyak 40.000 huruf.
6. Data 6 merupakan sebuah file berukuran 47 kb yang berisikan kombinasi huruf besar (kapital) dan huruf kecil sebanyak 48.000 huruf.

Pertama penulis akan menggunakan data 1 sebagai input kedalam algoritma DES dan AES untuk melihat berapa kecepatan dan memori yang digunakan oleh masing-masing algoritma dalam mengenkripsi data 1, data 2, data 3, data 4, data 5 dan data 6. Hal ini bertujuan untuk melihat seberapa cepat dan seberapa besar masing-masing algoritma dalam mengenkripsi sebuah pesan guna mengetahui performa masing-masing algoritma dalam mengenkripsi sebuah pesan.

Dalam melakukan percobaan penulis menggunakan alat bantu sebagai berikut :

#### Perangkat Keras (Hardware)

1. Asus S4511b
2. Processor Intel(R) Core(TM) i5-4200U CPU @1.60 GHz (4CPUs), 2,3GHz
3. RAM 4 GB
4. Hard Disk 750 GB

#### Perangkat Lunak (Software)

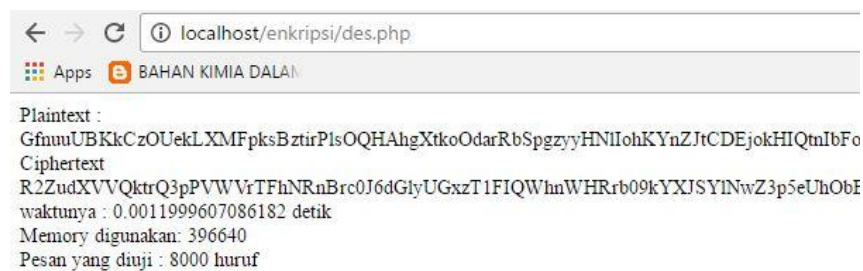
1. Sistem Operasi Windows 8 pro

2. XAMPP 7.0.3.0
3. Google Chrome 55.0.2883.87
4. Sublime Text 2
5. Microsoft Excel 2013

Didapatkan hasil sebagai berikut :

### 1, Algoritma DES

- a. Hasil percobaan menggunakan algoritma DES pada data 1

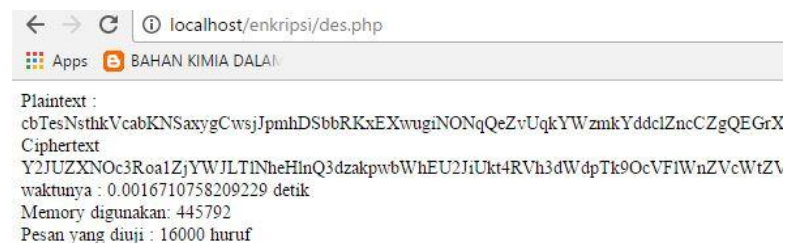


```

localhost/enkripsi/des.php
Apps BAHAN KIMIA DALAM
Plaintext :
GfnuuUBKkCzOUekLXMFpksBztirPlsOQHAhgXtkoOdarRbSpgzyyHNlIohKYnZJtCDEjokHIQtnIbFo
Ciphertext
R2ZudXVVQktrQ3pPVVvTfHNRnBrc0J6dGlyUGxzT1FIQWWhWHRrb09kYXJSYINwZ3p5eUhObf
waktunya : 0.0011999607086182 detik
Memory digunakan: 396640
Pesan yang diuji : 8000 huruf

```

- b. Hasil percobaan menggunakan algoritma DES pada data 2

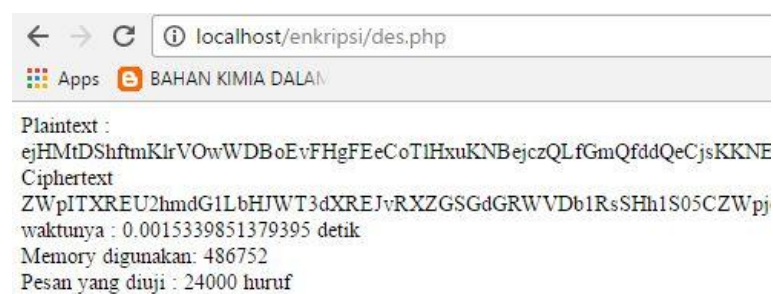


```

localhost/enkripsi/des.php
Apps BAHAN KIMIA DALAM
Plaintext :
cbTesNsthkVcabKNSaxygCwsjJpmhDSbbRKxEXwugiNONqQeZvUqkYWzmkYddclZncCZgQEGrX
Ciphertext
Y2JUZXNOc3Roa1ZjYWJLTINheHlnQ3dzakpwbWhEU2JiUkt4RVh3dWdpTk9OcVFjWnZVcWtZW
waktunya : 0.0016710758209229 detik
Memory digunakan: 445792
Pesan yang diuji : 16000 huruf

```

- c. Hasil percobaan menggunakan algoritma DES pada data 3

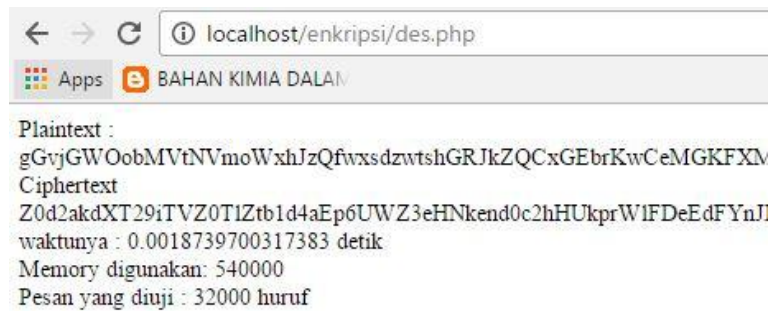


```

localhost/enkripsi/des.php
Apps BAHAN KIMIA DALAM
Plaintext :
ejHMTdShftmKlrVOwWDBoEvFHgFEcOTIHxuKNBejczQLfGmQfddQeCjsKKNE
Ciphertext
ZWpITXREU2hmdG1LbHJWt3dXREJvRXZGSgGdGRWVDb1RsSHh1S05CZWpj
waktunya : 0.0015339851379395 detik
Memory digunakan: 486752
Pesan yang diuji : 24000 huruf

```

d. Hasil percobaan menggunakan algoritma DES pada data 4

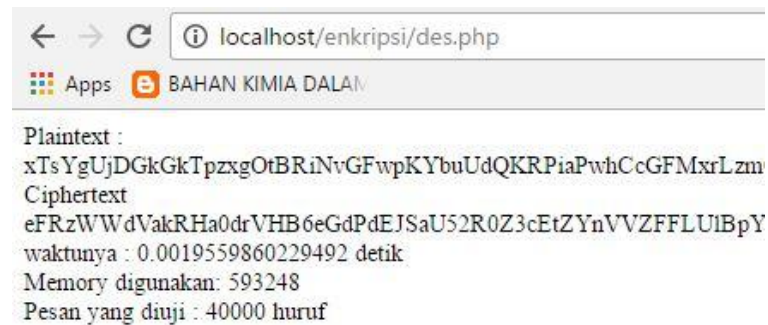


```

localhost/enkripsi/des.php
Apps BAHAN KIMIA DALAM
Plaintext :
gGvjGWoobMVtNVmoWxhJzQfwxsdzwtshGRJkZQCxGEbrKwCeMGKFXM
Ciphertext
Z0d2akdXT29iTVZ0T1Ztb1d4aEp6UWZ3eHNkenc0c2hHUkprW1FDeEdFYnJl
waktunya : 0.0018739700317383 detik
Memory digunakan: 540000
Pesan yang diuji : 32000 huruf

```

e. Hasil percobaan menggunakan algoritma DES pada data 5

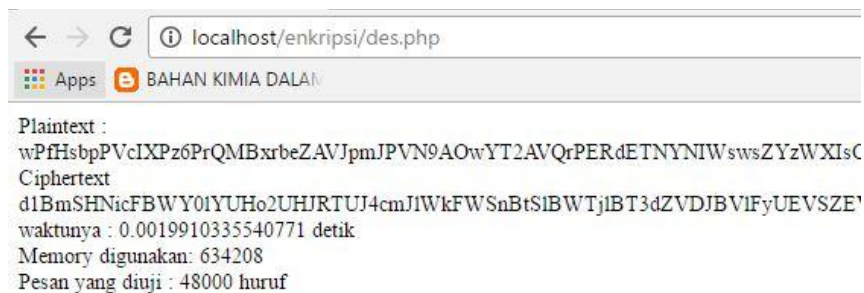


```

localhost/enkripsi/des.php
Apps BAHAN KIMIA DALAM
Plaintext :
xTsYgUjDGkGkTpzXgOtBRiNvGFwpKYbuUdQKRPIaPwhCcGFMxrLzm
Ciphertext
eFRzWWdVakRHa0drVHB6eGdPdEJSaU52R0Z3cEtZYnVVZFFLUiBpY
waktunya : 0.0019559860229492 detik
Memory digunakan: 593248
Pesan yang diuji : 40000 huruf

```

f. Hasil percobaan menggunakan algoritma DES pada data 6



```

localhost/enkripsi/des.php
Apps BAHAN KIMIA DALAM
Plaintext :
wPfhSbpPVcIXPz6PrQMBxrbeZAVJpmJPVN9AOwYT2AVQrPERdETNYNIWswsZYzWXIsC
Ciphertext
d1BmSHNicFBWY01YUHo2UHJRTUJ4cmJIWkFWSnBtSiBWTjiBT3dZVDJBViFyUEV'SZE'
waktunya : 0.0019910335540771 detik
Memory digunakan: 634208
Pesan yang diuji : 48000 huruf

```

Untuk mempermudah dalam melihat data tersebut penulis akan menyajikan data diatas kedalam tabel berikut ini :

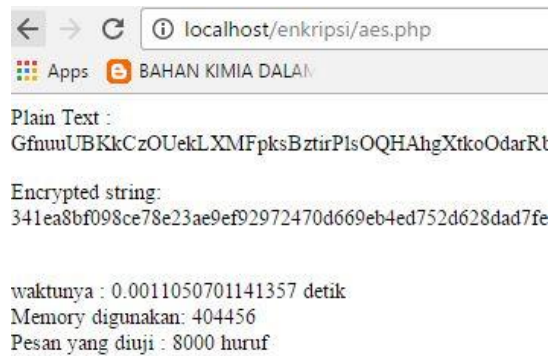
| Data        | Kecepatan (detik) | Penggunaan memori (byte) |
|-------------|-------------------|--------------------------|
| Data 1      | 0,001199          | 396.640                  |
| Data 2      | 0,001671          | 445.792                  |
| Data 3      | 0,001533          | 486.752                  |
| Data 4      | 0,001873          | 540.000                  |
| Data 5      | 0,001955          | 593.248                  |
| Data 6      | 0,001991          | 634.208                  |
| Rata – rata | 0,001704          | 516.107                  |

Kesimpulan : berdasarkan data hasil percobaan diatas dapat kita simpulkan bahwa

1. *Ciphertext* dari huruf yang sama pada *plaintext* menghasilkan output huruf yang berbeda, sebagai contoh pada gambar hasil percobaan poin d diatas pada *plaintext* dapat kita lihat pada huruf “G” pada urutan ke 2 dan ke 5 menghasilkan 2 huruf yang berbeda pada output *ciphertext*-nya dimana “G” urutan ke 2 pada *plaintext* menghasilkan “0” dan “G” pada *plaintext* urutan ke 5 menghasilkan “a” pada *ciphertext* urutan ke 5 hal tersebut menunjukkan pada kita bahwa walaupun pada pesan (*plaintext*) terdapat huruf yang sama tetapi belum tentu menghasilkan output yang sama sehingga mempersulit kita dalam menebak suatu pesan hanya dengan mengetahui output (*ciphertext*)-nya saja tanpa mengetahui *key* pesan tersebut.
2. Waktu yang dibutuhkan algoritma DES dalam mengenkripsi suatu data cenderung akan semakin besar terhadap semakin besarnya data (pesan) yang diproses.
3. Penggunaan memori pada algoritma DES berbanding lurus terhadap jumlah pesan yang diuji dimana memori yang dibutuhkan akan semakin besar seiring dengan besarnya pesan yang diuji.

## 2. Algoritma AES

### a. Hasil percobaan menggunakan algoritma AES pada data 1



← → ↻ localhost/enkripsi/aes.php

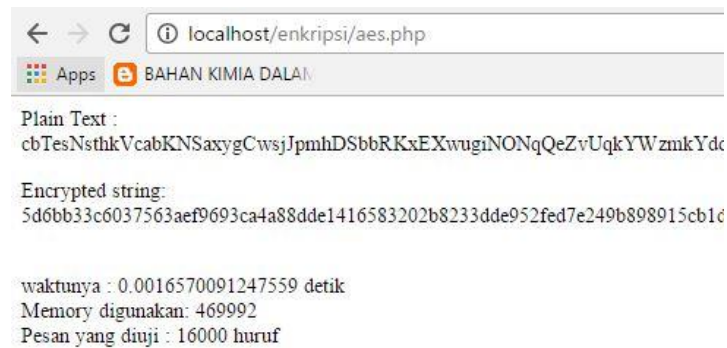
Apps BAHAN KIMIA DALAM

Plain Text :  
GfnuuUBKkCzOUekLXMFpksBztirP1sOQHAgXtkoOdarRt

Encrypted string:  
341ea8bf098ce78e23ae9ef92972470d669eb4ed752d628dad7fe

waktunya : 0.0011050701141357 detik  
Memory digunakan: 404456  
Pesan yang diuji : 8000 huruf

### b. Hasil percobaan menggunakan algoritma AES pada data 2



← → ↻ localhost/enkripsi/aes.php

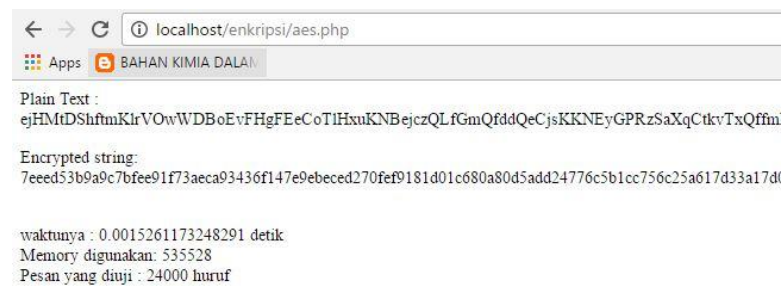
Apps BAHAN KIMIA DALAM

Plain Text :  
cbTesNsthkVcabKNSaxygCwsjJpmhDSbbRKxEXwugiNONqQeZvUqkYWzmkYdc

Encrypted string:  
5d6bb33c6037563aef9693ca4a88dde1416583202b8233dde952fed7e249b898915cb1c

waktunya : 0.0016570091247559 detik  
Memory digunakan: 469992  
Pesan yang diuji : 16000 huruf

### c. Hasil percobaan menggunakan algoritma AES pada data 3



← → ↻ localhost/enkripsi/aes.php

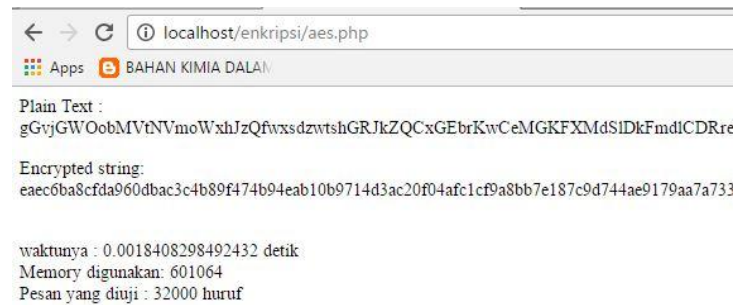
Apps BAHAN KIMIA DALAM

Plain Text :  
ejHMtDShftmKlrVOwWDBoEvFHgFEeCoTIHxuKNBejczQLfGmQfdQeCjsKKNEyGPRzSaXqCtkvTxQffm

Encrypted string:  
7eed53b9a9c7bfee91f73aeca93436f147e9ebeced270fef9181d01c680a80d5add24776c5b1cc756c25a617d33a17d

waktunya : 0.0015261173248291 detik  
Memory digunakan: 535528  
Pesan yang diuji : 24000 huruf

d. Hasil percobaan menggunakan algoritma AES pada data 4

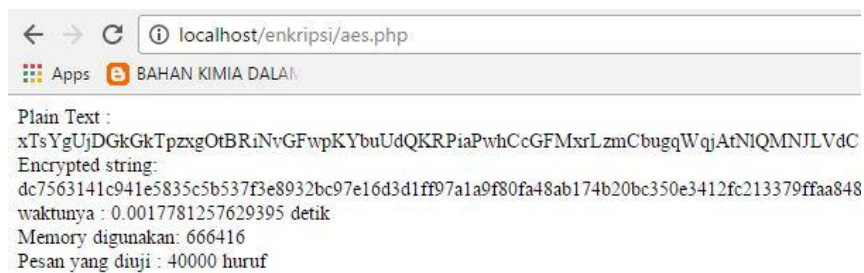


```

localhost/enkripsi/aes.php
Apps BAHAN KIMIA DALAM
Plain Text :
gGvjGWoobMVtNVmoWxhJzQfwxsdzwtshGRJkZQCxGEbrKwCeMGKFXMdSiDkFmdlCDRre
Encrypted string:
eaec6ba8cfda960dbac3c4b89f474b94eab10b9714d3ac20f04afc1cf9a8bb7e187c9d744ae9179aa7a733
waktunya : 0.0018408298492432 detik
Memory digunakan: 601064
Pesan yang diuji : 32000 huruf

```

e. Hasil percobaan menggunakan algoritma AES pada data 5

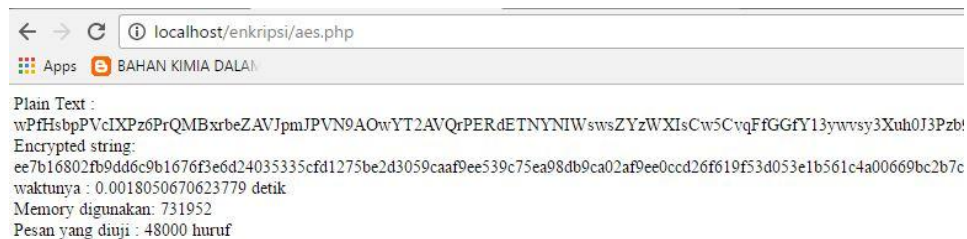


```

localhost/enkripsi/aes.php
Apps BAHAN KIMIA DALAM
Plain Text :
xTsYgUjDGkGkTpzXgOtBRiNvGFwpKYbuUdQKRPIaPwhCcGFMxLzmCbugqWqjAtNIQMNLVdC
Encrypted string:
dc7563141e941e5835c5b537f3e8932bc97e16d3d1ff97a1a9f80fa48ab174b20bc350e3412fc213379ffaa848
waktunya : 0.0017781257629395 detik
Memory digunakan: 666416
Pesan yang diuji : 40000 huruf

```

f. Hasil percobaan menggunakan algoritma AES pada data 6



```

localhost/enkripsi/aes.php
Apps BAHAN KIMIA DALAM
Plain Text :
wPfhSbpPVclXPz6PrQMBxrbeZAVJpmJPVN9AOwYT2AVQrPERdETNYNIWswsZYzWXIsCw5CvqFfGGfy13ywvsy3Xuh0J3Pzb!
Encrypted string:
ee7b16802fb9dd6c9b1676f3e6d24035335cfd1275be2d3059caaf9ee539c75ea98db9ca02af9ee0ccd26f619f53d053e1b561c4a00669bc2b7c
waktunya : 0.0018050670623779 detik
Memory digunakan: 731952
Pesan yang diuji : 48000 huruf

```

Untuk mempermudah dalam melihat data tersebut penulis akan menyajikan data

diatas kedalam tabel berikut ini :

| Data        | Kecepatan (detik) | Penggunaan memori (byte) |
|-------------|-------------------|--------------------------|
| Data 1      | 0,001105          | 404.456                  |
| Data 2      | 0,001657          | 469.992                  |
| Data 3      | 0,001526          | 535.528                  |
| Data 4      | 0,001840          | 601.064                  |
| Data 5      | 0,001778          | 666.416                  |
| Data 6      | 0,001805          | 731.952                  |
| Rata – rata | 0,001619          | 568.235                  |

Kesimpulan : berdasarkan data hasil percobaan diatas dapat kita simpulkan bahwa

1. *Ciphertext* dari huruf yang sama pada *plaintext* menghasilkan output huruf yang berbeda, sebagai contoh pada gambar hasil percobaan poin k diatas pada *plaintext* dapat kita lihat pada huruf "G" pada urutan ke 9 dan ke 11 menghasilkan 2 huruf yang berbeda pada output *ciphertext*-nya dimana "G" urutan ke 9 pada *plaintext* menghasilkan "1" dan "G" pada *plaintext* urutan ke 11 menghasilkan "9" pada *ciphertext* urutan ke 11, hal tersebut menunjukkan pada kita bahwa walaupun pada pesan (*plaintext*) terdapat huruf yang sama tetapi belum tentu menghasilkan output yang sama sehingga mempersulit kita dalam menebak suatu pesan hanya dengan mengetahui output (*ciphertext*)-nya saja tanpa mengetahui *key* pesan tersebut.
2. Waktu yang dibutuhkan algoritma AES dalam mengenkripsi suatu data cenderung lebih tidak menentu terhadap semakin besarnya data (pesan) yang diproses dikarenakan pada beberapa hasil percobaan diatas dapat kita lihat bahwa ada beberapa data yang memproses pesan lebih banyak tetapi justru lebih cepat dibandingkan dengan pesan yang lebih sedikit jumlahnya.
3. Penggunaan memori pada algoritma AES berbanding lurus terhadap jumlah pesan yang diuji dimana memori yang dibutuhkan akan semakin besar seiring dengan besarnya pesan yang diuji.

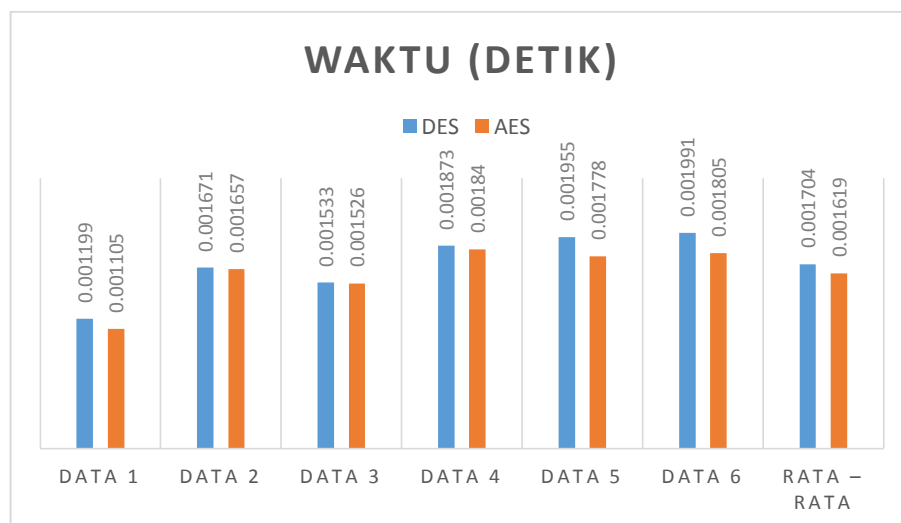


### 3. Perbandingan Algoritma DES dan AES

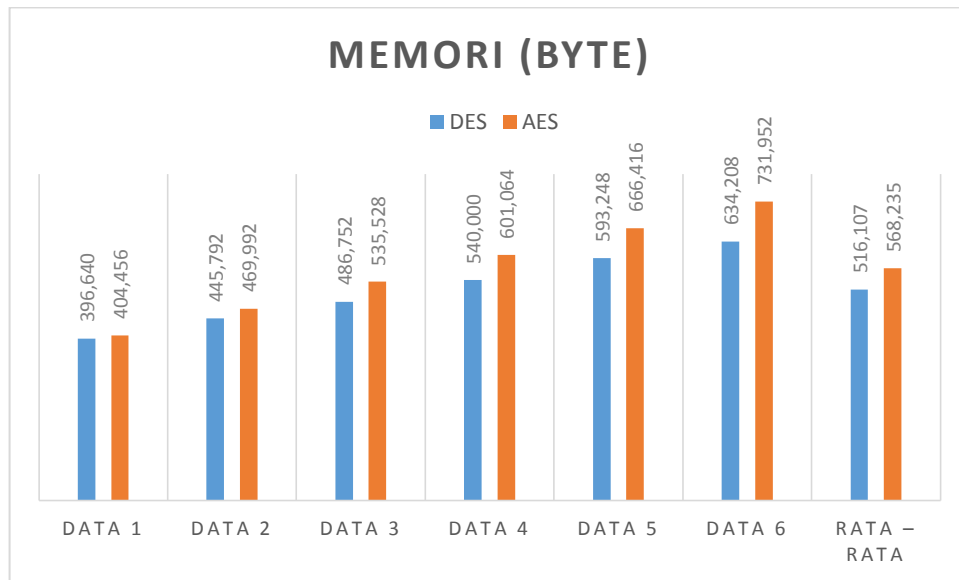
Setelah melakukan percobaan terhadap algoritma DES dan AES diatas, selanjutnya penulis menyajikan data tersebut kedalam tabel yang menjelaskan perbandingan performa kecepatan dan penggunaan memori antara algoritma DES dan AES dalam mengenkripsi kelompok data tersebut :

| Data        | DES               |                          | AES               |                          |
|-------------|-------------------|--------------------------|-------------------|--------------------------|
|             | Kecepatan (detik) | Penggunaan memori (byte) | Kecepatan (detik) | Penggunaan memori (byte) |
| Data 1      | 0,001199          | 396.640                  | 0,001105          | 404.456                  |
| Data 2      | 0,001671          | 445.792                  | 0,001657          | 469.992                  |
| Data 3      | 0,001533          | 486.752                  | 0,001526          | 535.528                  |
| Data 4      | 0,001873          | 540.000                  | 0,001840          | 601.064                  |
| Data 5      | 0,001955          | 593.248                  | 0,001778          | 666.416                  |
| Data 6      | 0,001991          | 634.208                  | 0,001805          | 731.952                  |
| Rata – rata | 0,001704          | 516.107                  | 0,001619          | 568.235                  |

Berikut adalah data hasil percobaan algoritma DES dan AES yang disajikan dalam bentuk diagram batang :



**Gambar 5.1 Perbandingan waktu algoritma DES dan AES**



**Gambar 5.2 Perbandingan penggunaan memori algoritma DES dan AES**

Berdasarkan data di atas dapat kita lihat bahwa algoritma DES membutuhkan waktu yang lebih lama ketimbang algoritma AES dalam mengenkripsi data yang sama atau dengan kata lain algoritma AES memiliki waktu enkripsi yang lebih kecil atau lebih cepat dibandingkan algoritma DES.

Dan berdasarkan grafik perbandingan penggunaan memori masing-masing algoritma dalam mengenkripsi diatas kita dapat melihat bahwa algoritma AES membutuhkan alokasi memori yang lebih besar dibandingkan algoritma DES dalam setiap proses enkripsi data yang sama. Hal ini dapat dimengerti karena dalam mengenkripsi data tersebut algoritma DES memiliki ukuran *block* sepanjang 64 bit sedangkan AES sepanjang 128 yaitu sebesar 2 kali lipat ukuran *block* algoritma DES dan memiliki *key* yang lebih panjang yaitu sepanjang 128 bit dimana algoritma DES yaitu 56 bit.

Berdasarkan perbandingan kedua grafik yang didapat diatas dapat diketahui bahwa algoritma AES memiliki performa yang lebih baik atas algoritma

DES karena algoritma AES mampu mengenkripsi lebih cepat data yang sama dengan yang diujikan pada algoritma DES walaupun dengan cara kerja yang lebih kompleks yang dapat dilihat pada grafik perbandingan penggunaan memori masing-masing algoritma dalam mengenkripsi data.

## 5.2 Perbandingan Berdasarkan Deskripsi Algoritma

| Faktor                   | DES      | AES                         |
|--------------------------|----------|-----------------------------|
| Panjang kunci            | 56 bit   | 128, 192, 256 bit           |
| Ukuran blok              | 64 bit   | 128, 192, 256 bit           |
| Jumlah Round             | 16       | 10/12/14                    |
| Jenis kunci              | Simetrik | Simetrik                    |
| Kemungkinan jumlah kunci | $2^{56}$ | $2^{128}, 2^{192}, 2^{256}$ |
| Dikembangkan tahun       | 1977     | 2000                        |

**Tabel 5.1 Perbandingan algoritma DES dan AES**

Berdasarkan tabel perbandingan diatas dapat diketahui bahwa dalam hal panjang kunci, ukuran blok dan kemungkinan jumlah kunci secara kuantitas algoritma AES lebih besar dibandingkan algoritma DES lalu dalam hal jumlah *round* secara kuantitas algoritma DES memiliki jumlah *round* yang lebih banyak dibandingkan algoritma AES.