

Advanced Encryption Standard (AES)

Yama Fredian Dwi Saputro

fds.yama@gmail.com

Lisensi Dokumen:

Copyright © 2003-2015 IlmuKomputer.Com

Seluruh dokumen di IlmuKomputer.Com dapat digunakan, dimodifikasi dan disebarkan secara bebas untuk tujuan bukan komersial (nonprofit), dengan syarat tidak mengubah atau merubah atribut penulis dan pernyataan copyright yang disertakan dalam setiap dokumen. Tidak diperbolehkan melakukan penulisan ulang, kecuali mendapatkan ijin terlebih dahulu dari IlmuKomputer.Com.

Pendahuluan

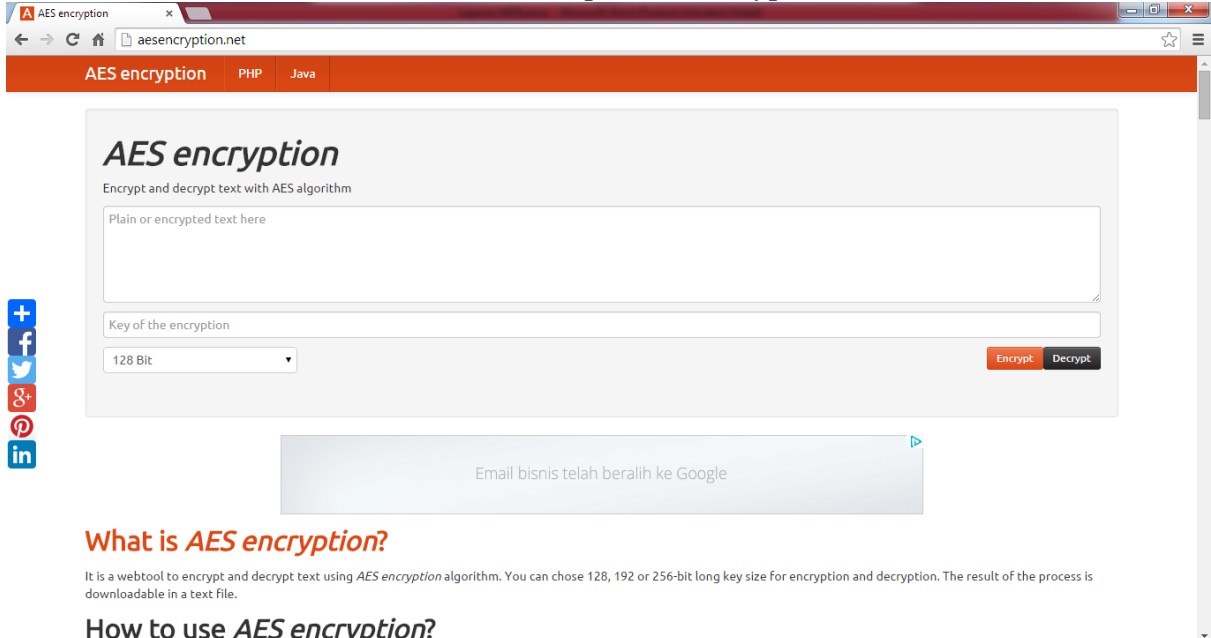
Advanced Encryption Standard atau AES merupakan algoritma kriptografi simetrik yang dapat digunakan untuk mengamankan data . Algoritma AES adalah blok chipertext simetrik yang dapat mengenkripsi dan mendekripsi informasi.

Enkripsi merubah data yang tidak dapat lagi dibaca disebut ciphertext; sebaliknya dekripsi adalah merubah ciphertext data menjadi bentuk semula yang kita kenal sebagai plaintext. Algoritma AES is menggunakan kunci kriptografi 128, 192, dan 256 bits untuk mengenkrip dan dekrip data pada blok 128 bits.

Algoritma AES merupakan penerus dari DES atau Data Encryption Standard yang dianggap sudah tidak aman lagi karena dengan perangkat keras khusus kuncinya bisa ditemukan. AES diumumkan oleh Institut Nasional Standar dan Teknologi (NIST) sebagai Standar Pemrosesan Informasi Federal (FIPS) publikasi 197 (FIPS 197) pada tanggal 26 November 2001 setelah proses standardisasi selama 5 tahun, di mana ada 15 desain enkripsi yang disajikan dan dievaluasi, sebelum Rijndael terpilih sebagai yang paling cocok. AES efektif menjadi standar pemerintah Federal pada tanggal 26 Mei 2002 setelah persetujuan dari Menteri Perdagangan. AES tersedia dalam berbagai paket enkripsi yang berbeda. AES merupakan standar yang pertama yang dapat diakses publik dan sandi-terbuka yang disetujui oleh NSA untuk informasi rahasia.

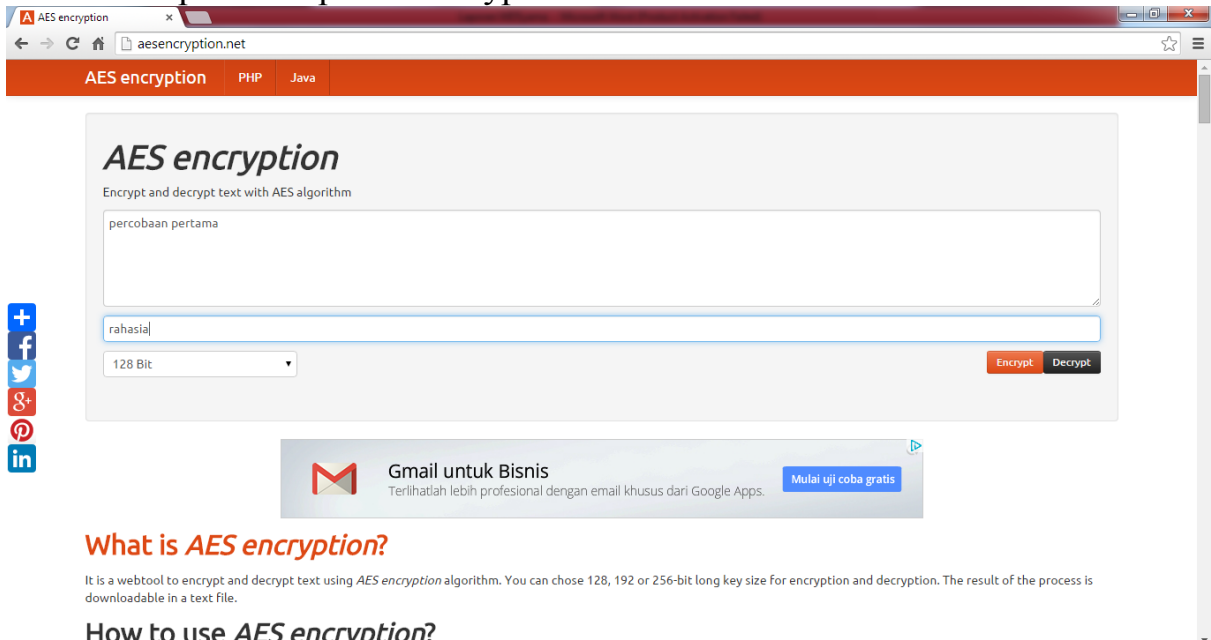
Langkah Kerja

1. Pertama-tama masuk ke situs <http://aesencryption.net/>



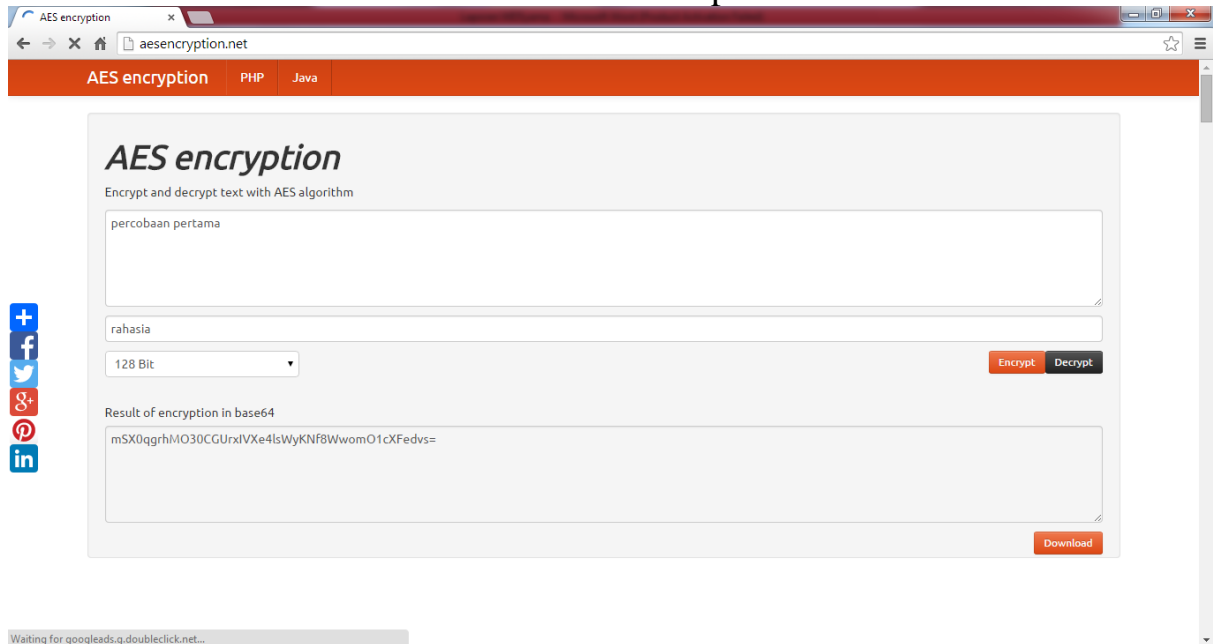
The screenshot shows the homepage of the AES encryption website. The browser address bar displays 'aesencryption.net'. The page features a navigation bar with 'AES encryption', 'PHP', and 'Java' links. The main content area is titled 'AES encryption' and includes the subtitle 'Encrypt and decrypt text with AES algorithm'. There is a large text input field labeled 'Plain or encrypted text here', a 'Key of the encryption' input field, and a dropdown menu set to '128 Bit'. 'Encrypt' and 'Decrypt' buttons are visible. A social media sidebar on the left contains icons for Facebook, Twitter, LinkedIn, and others. A banner at the bottom reads 'Email bisnis telah beralih ke Google'. Below the banner, there are sections titled 'What is AES encryption?' and 'How to use AES encryption?' with introductory text.

2. Tulis pesan yang ingin di enkripsi, masukkan password dan bit enkripsi. Lalu pilih “Encrypt”

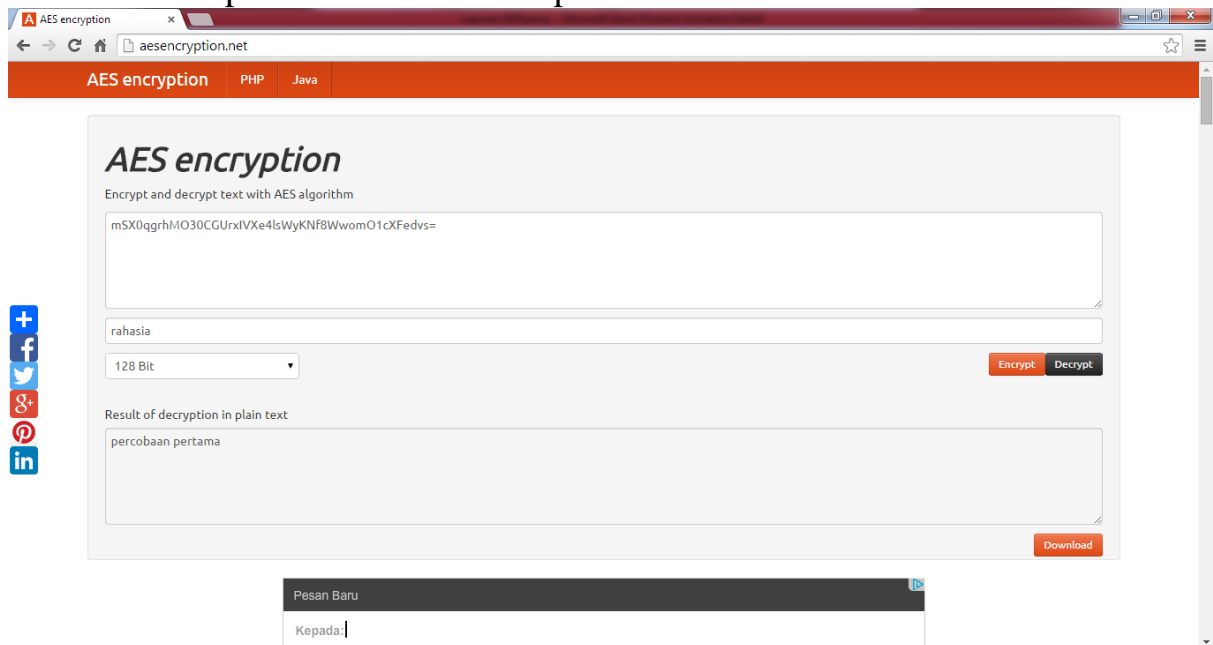


This screenshot shows the same AES encryption website interface, but with the input fields populated. The text input field contains 'percobaan pertama', the key input field contains 'rahasia', and the dropdown menu remains at '128 Bit'. The 'Encrypt' and 'Decrypt' buttons are still present. The social media sidebar and the 'Email bisnis telah beralih ke Google' banner are also visible. The 'What is AES encryption?' and 'How to use AES encryption?' sections are present at the bottom of the page.

3. Setelah itu akan muncul kode hasil enkripsi.

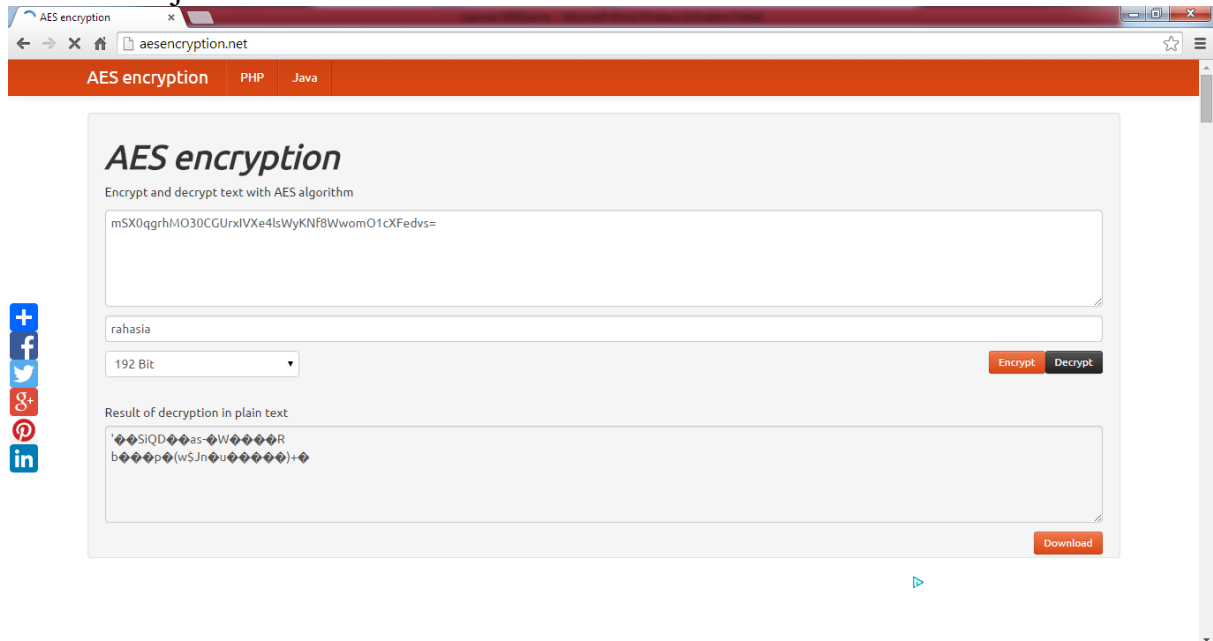


4. Untuk menerjemahkan kembali pesan yang telah dienkripsi masukkan kode hasil enkripsi, password dan bit enkripsi. Lalu pilih "Decrypt". Jika benar maka pesan yang ingin diterjemahkan akan muncul pada kotak hasil dekripsi.

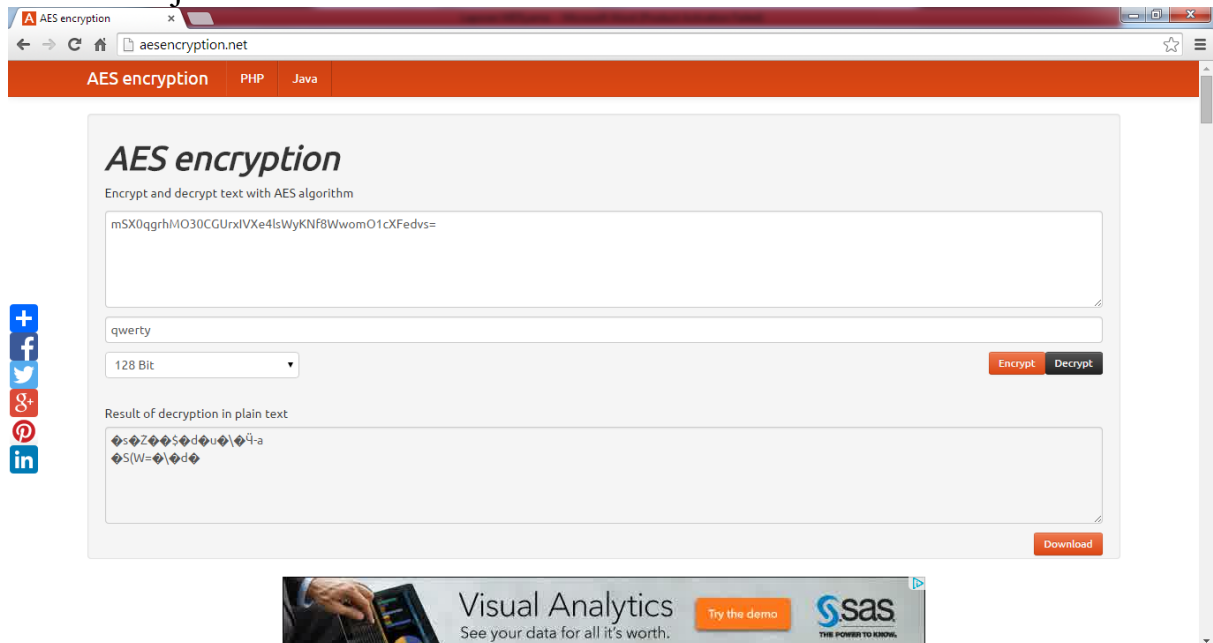


5. Jika bit enkripsi yang kita masukkan salah maka pesan akan gagal

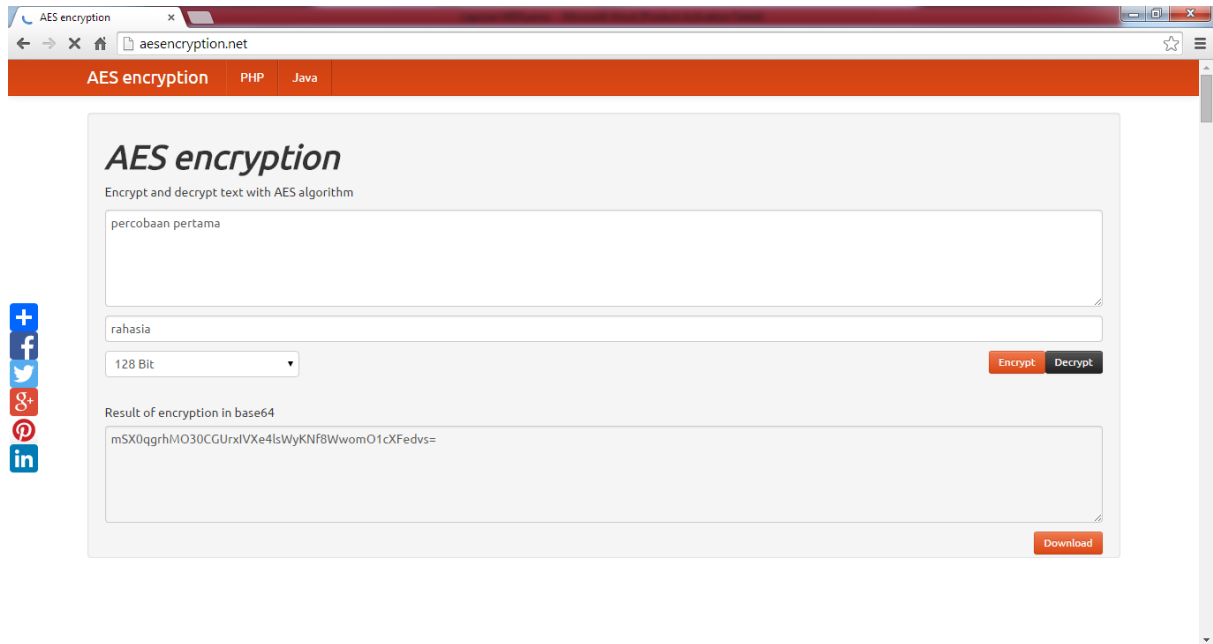
diterjemahkan.



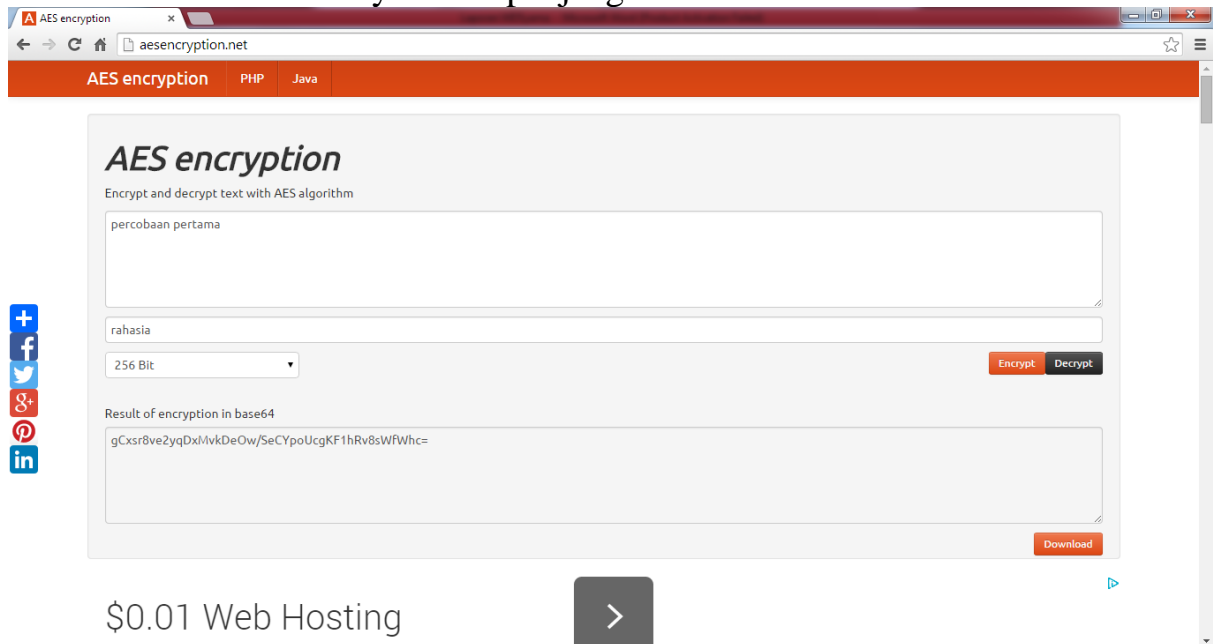
6. Jika password yang kita masukkan salah maka pesan akan gagal diterjemahkan.



7. Hasil kode enkripsi akan berbeda jika kita menggunakan bit enkripsi yang berbeda.

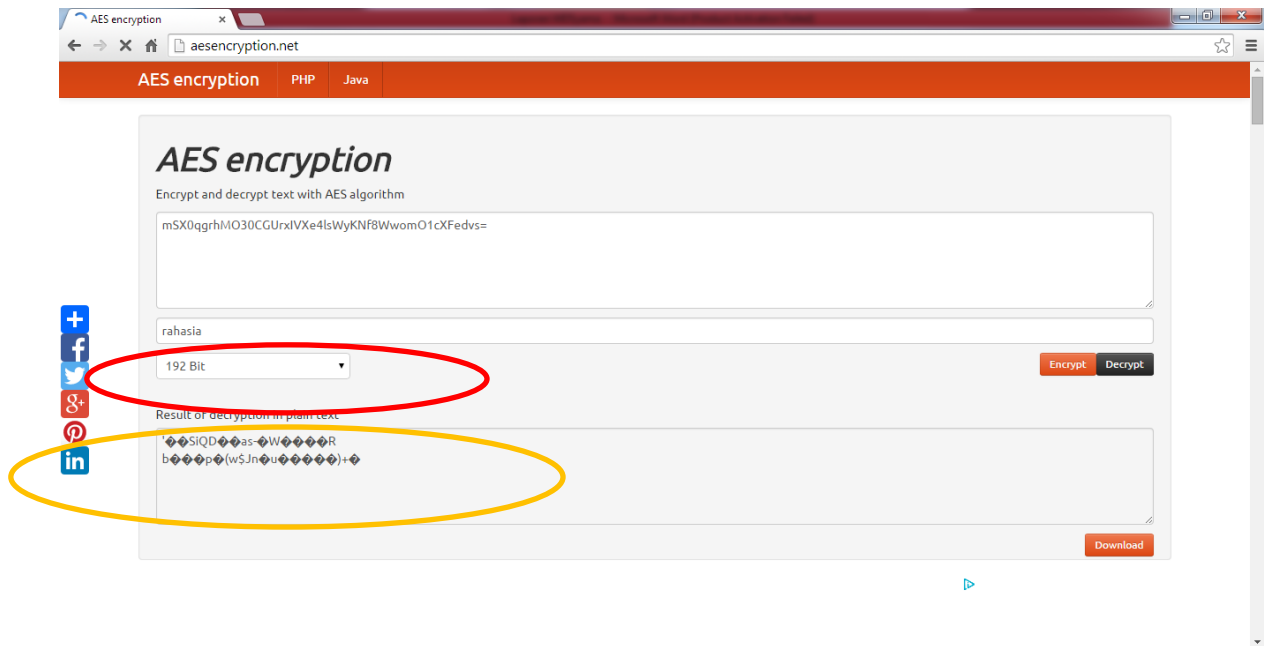


8. Semakin besar bit enkripsi yang digunakan maka hasil kode enkripsi akan semakin banyak atau panjang.

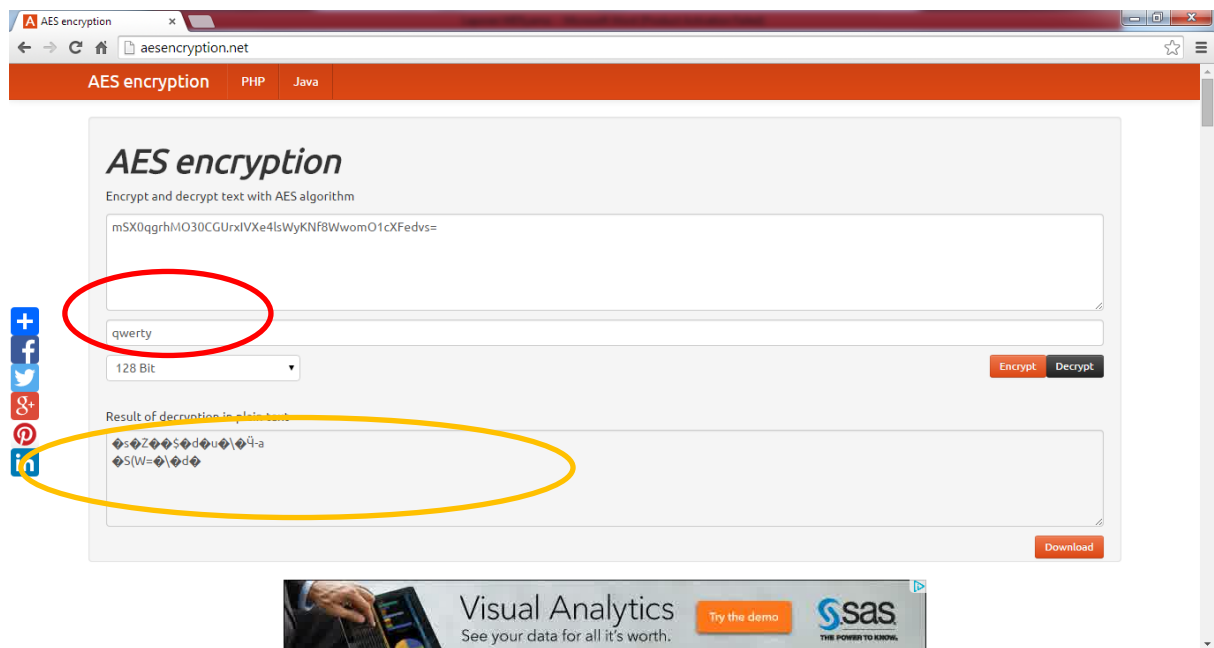


Analisa Data

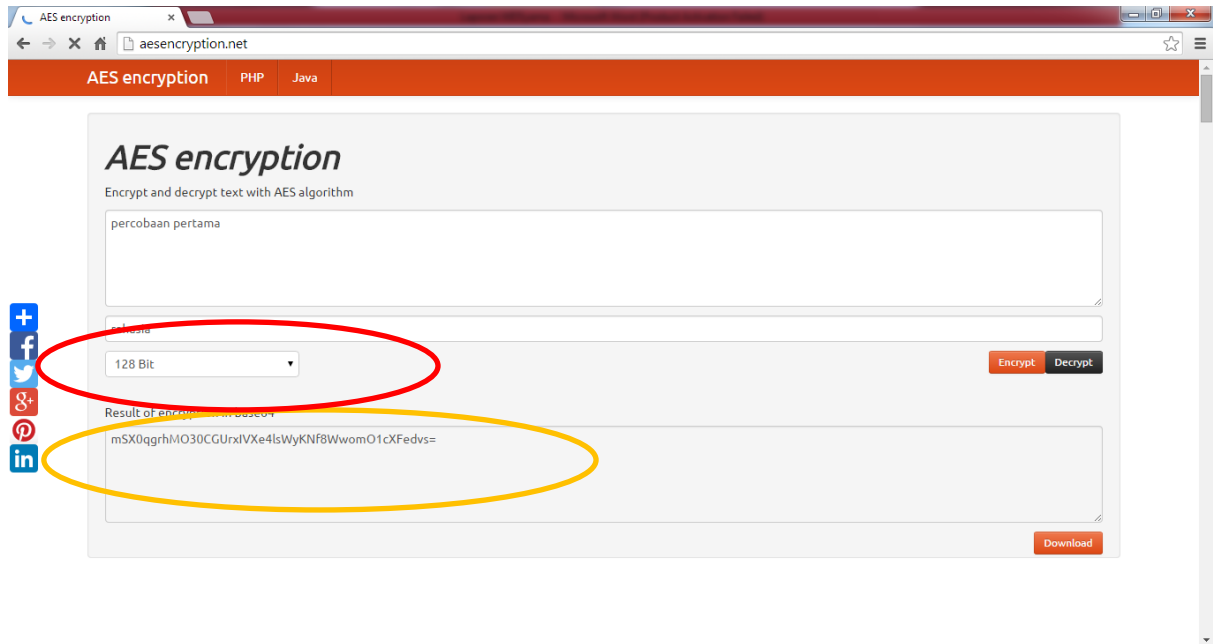
Berdasarkan data yang didapat pada saat praktikum terlihat bahwa jika bit enkripsi yang kita masukkan salah maka pesan akan gagal diterjemahkan.



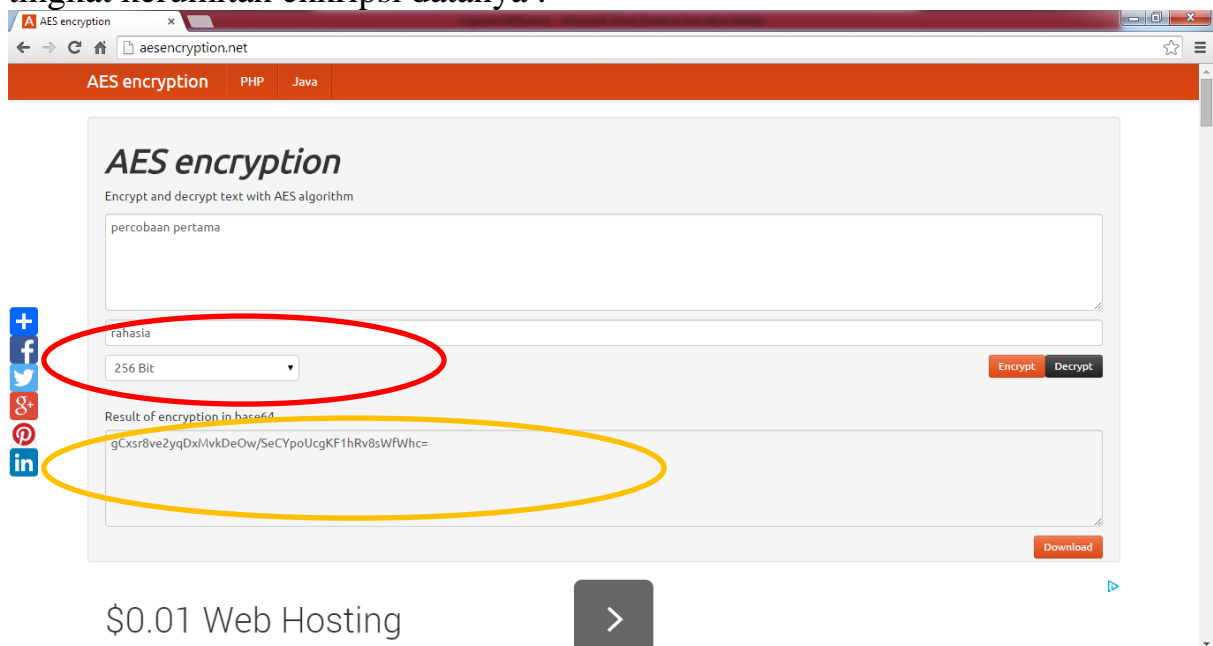
Jika password yang kita masukkan salah maka pesan juga akan gagal diterjemahkan.



Hasil kode enkripsi akan berbeda jika kita menggunakan bit enkripsi yang berbeda.



Semakin besar bit enkripsi yang digunakan maka hasil kode enkripsi akan semakin banyak atau panjang sehingga akan semakin bertambah pula tingkat kerumitan enkripsi datanya .



Kesimpulan

Algoritma AES masuk dalam aspek Authentication karena hanya orang yang benar yang dapat mengakses pesan dengan memiliki kunci enkripsi.

Biografi Penulis

Yama Fresdian Dwi Saputro. Menyelesaikan Program D4 Telekomunikasi di Politeknik Negeri Semarang.