Advanced Encryption Standard (AES)

Yama Fresdian Dwi Saputro
fds.yama@gmail.com

Pendahuluan

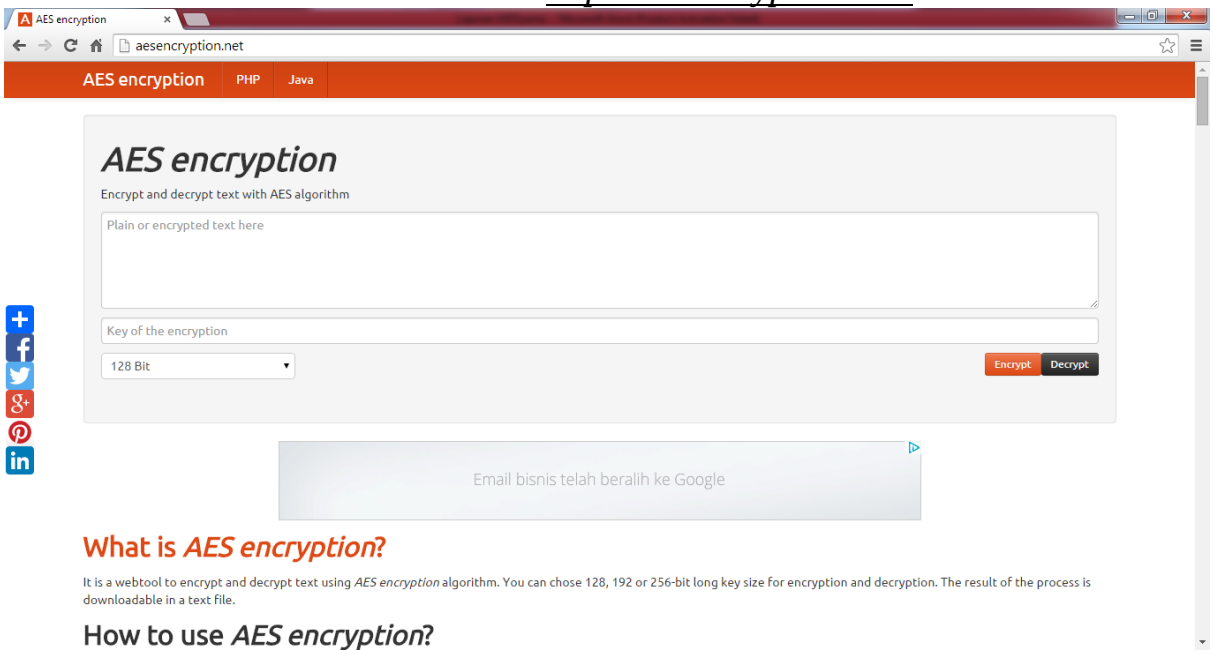
Advanced Encryption Standard atau AES merupakan algoritma kriptografi simetrik yang dapat digunkan untuk mengamakan data . Algoritma AES adalah blok chipertext simetrik yang dapat mengenkripsi dan mendekripsi informasi.

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 mengunakan kunci kriptografi 128, 192, dan 256 bits untuk mengenkrip dan dekrip data pada blok 128 bits.

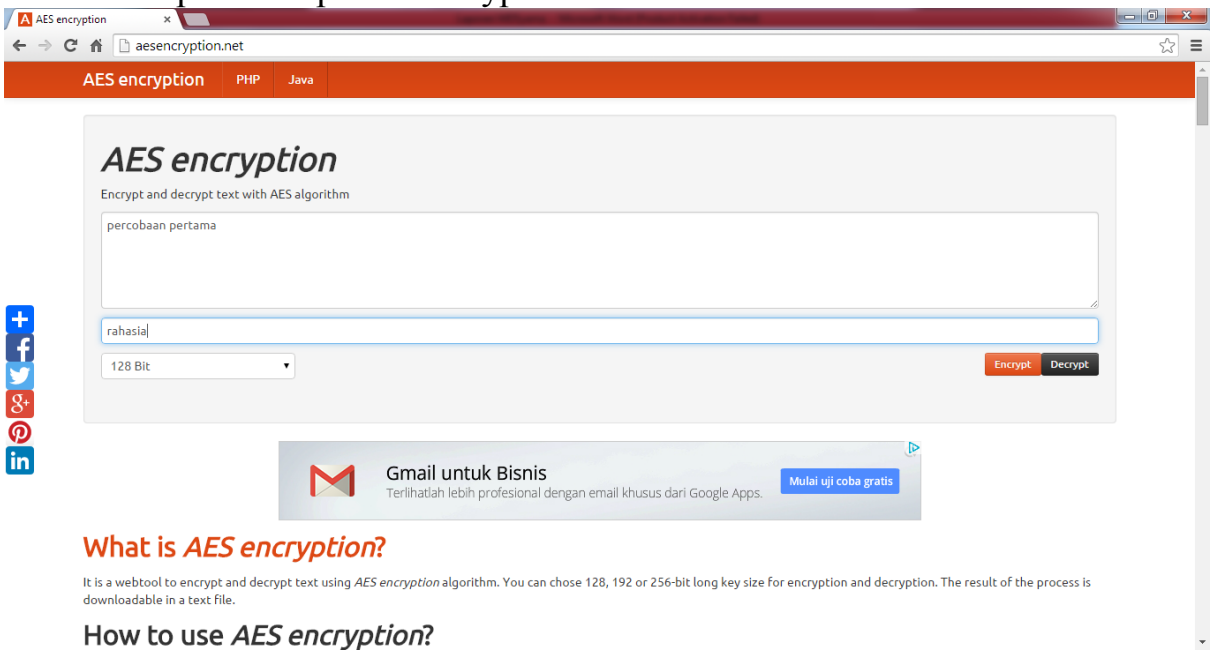
Algoritma AES merupakan penerus dari DES atau Data Encryption Standard yang dianggap sudah tidak aman lagi karena dengan perangkat keras khusus kuncinya bisa ditemukan. AES diumumkan oleh Institut Nasional Standar dan Teknologi (NIST) sebagai Standar Pemrosesan Informasi Federal (FIPS) publikasi 197 (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

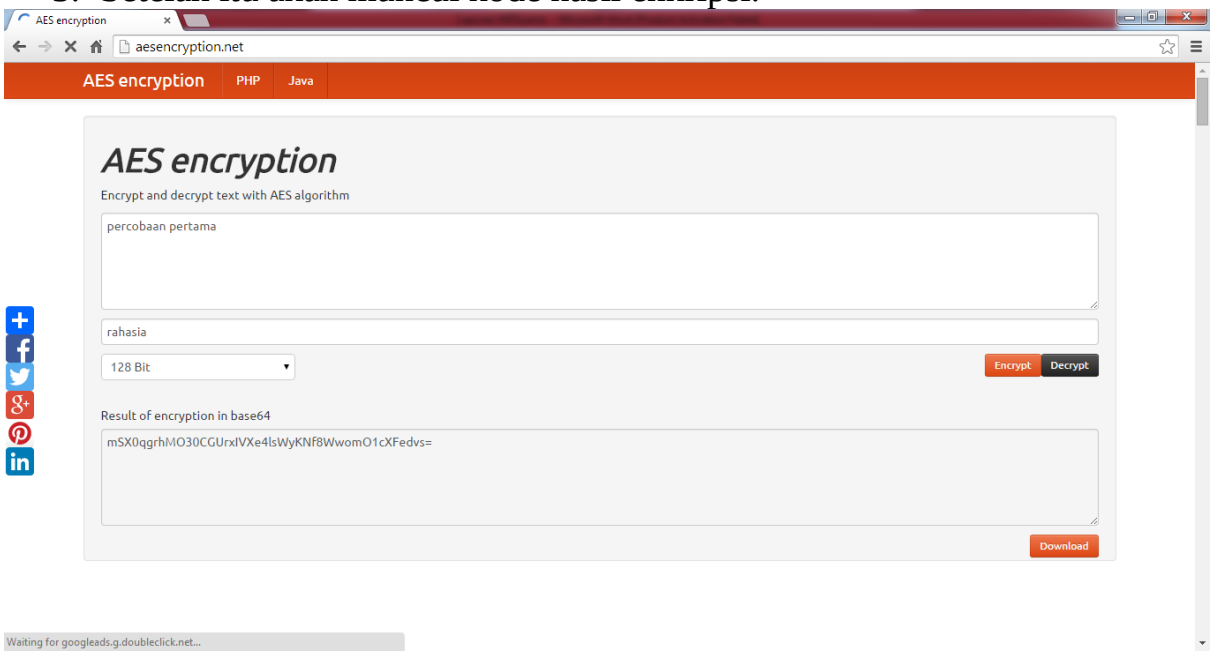
1. Pertama-tama masuk ke situs *http://aesencryption.net/*



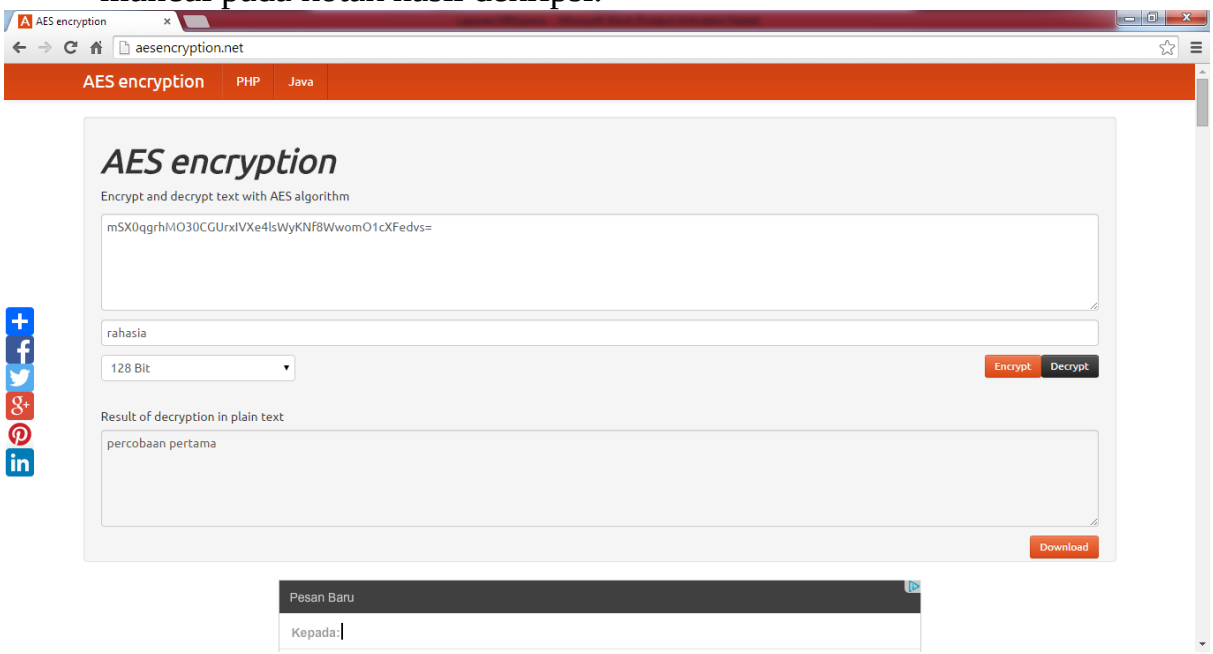
2. Tulis pesan yang ingin di enkripsi, masukkan password dan bit enkripsi. Lalu pilih "Encrypt"



3. Setelah itu akan muncul kode hasil enkripsi.

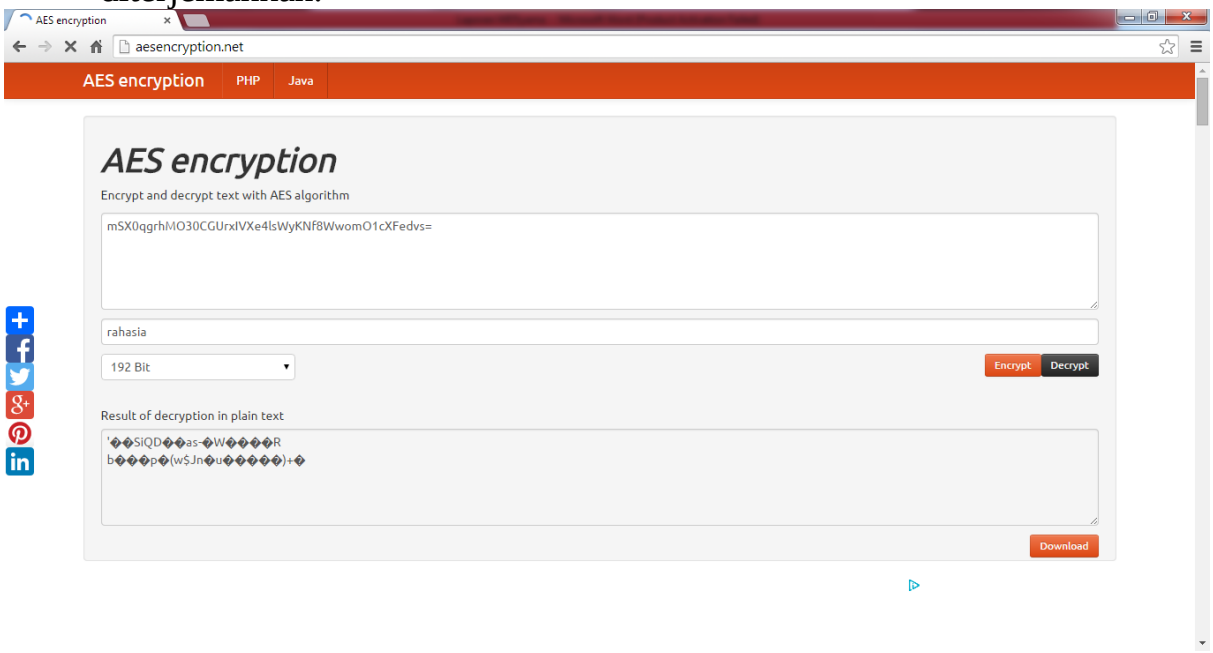


4. Untuk menerjemahkan kembali pesan yang telah dienkripsi masukkan kode hasil enkripsi, password dan bit enkripsi. Lalu pilih "*Decrypt*". Jika benar maka pesan yang ingin diterjemahkan akan muncul pada kotak hasil dekripsi.

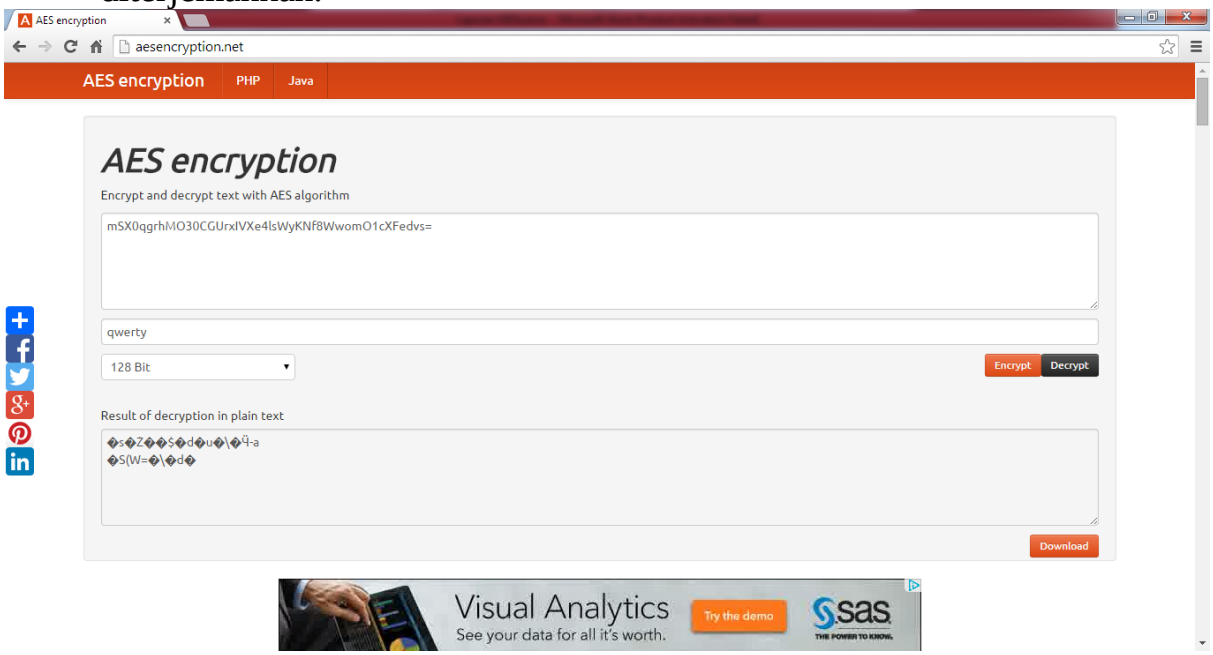


5. Jika bit enkripsi yang kita masukkan salah maka pesan akan gagal

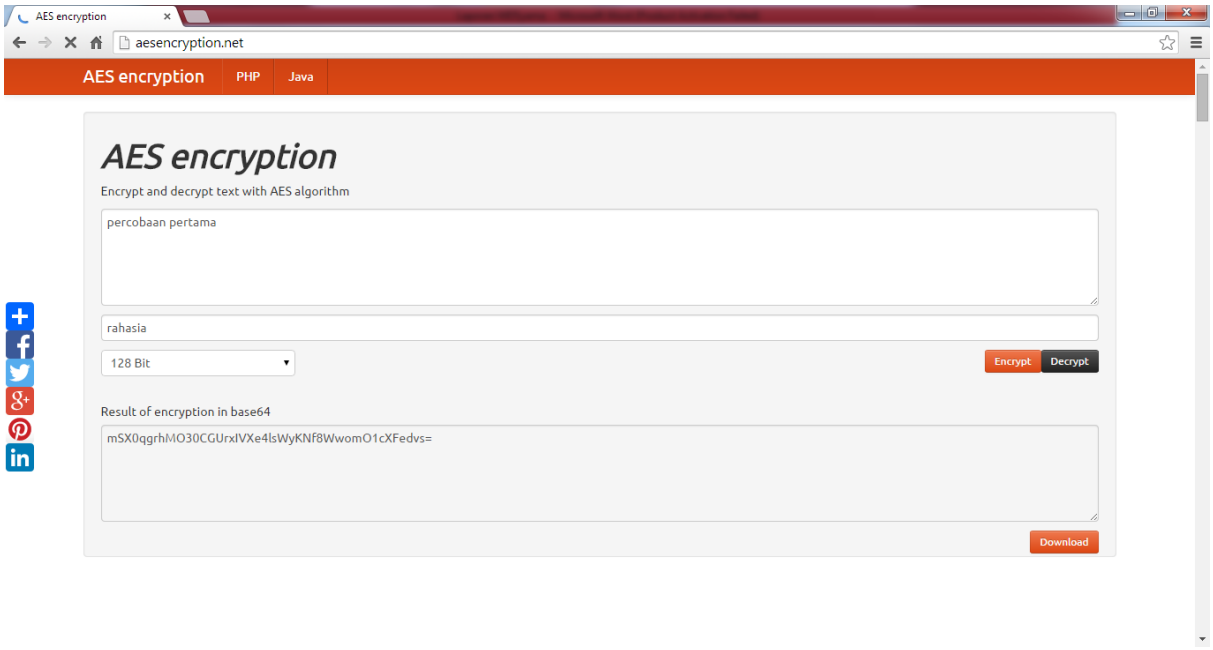
diterjemahkan.



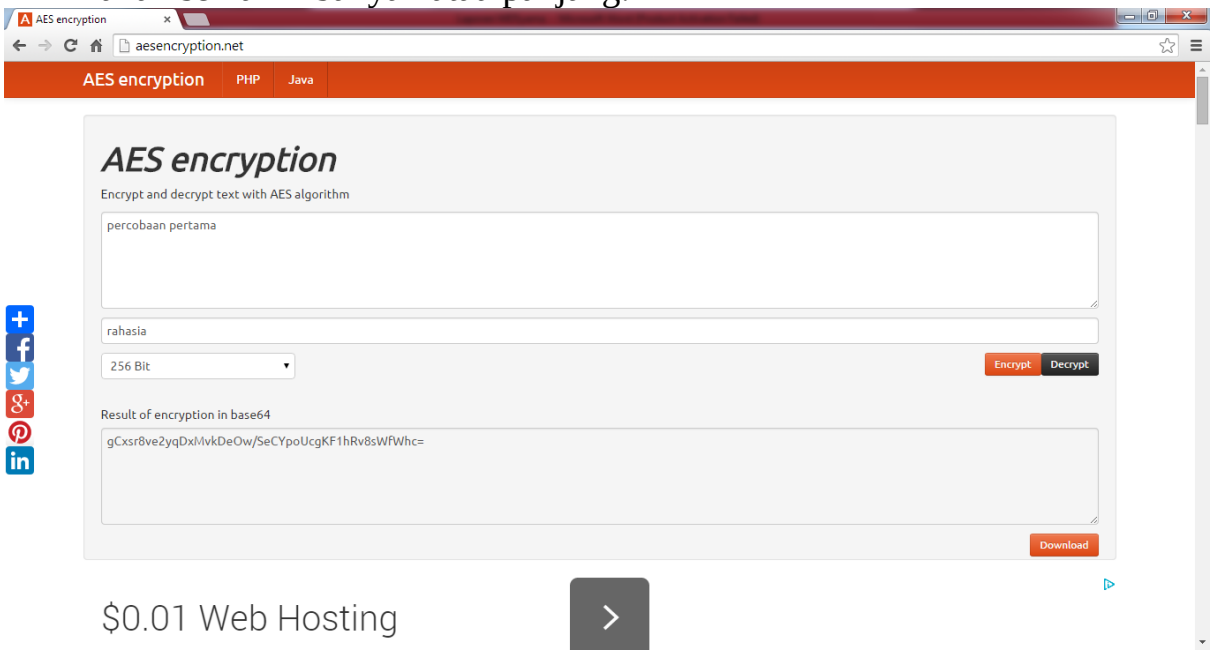
6. Jika password yang kita masukkan salah maka pesan akan gagal diterjemahkan.



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

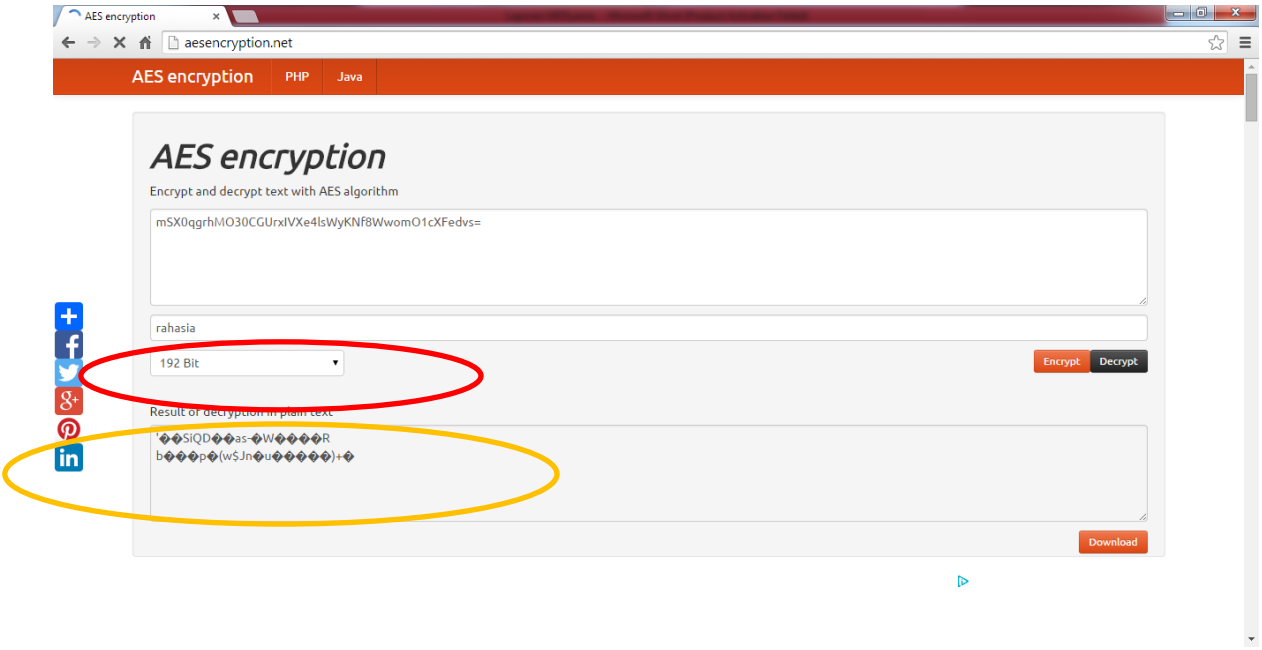


8. Semakin besar bit enkripsi yang digunakan maka hasil kode enkripsi akan semakin banyak atau panjang.

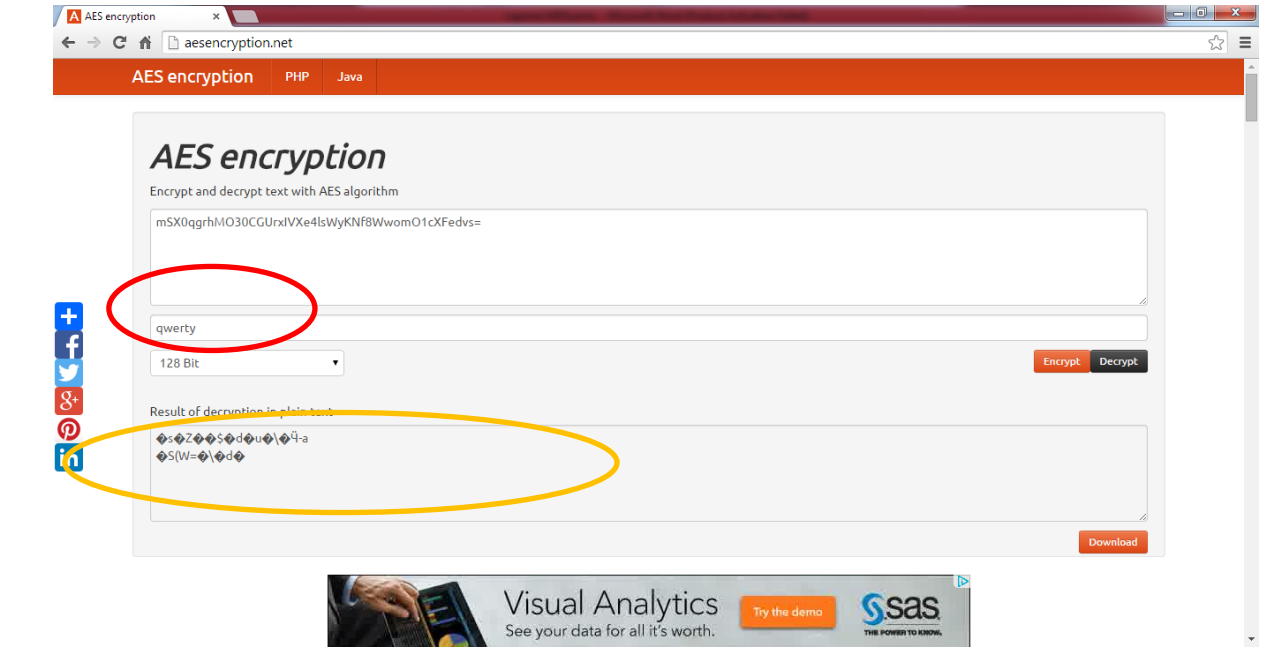


Analisa Data

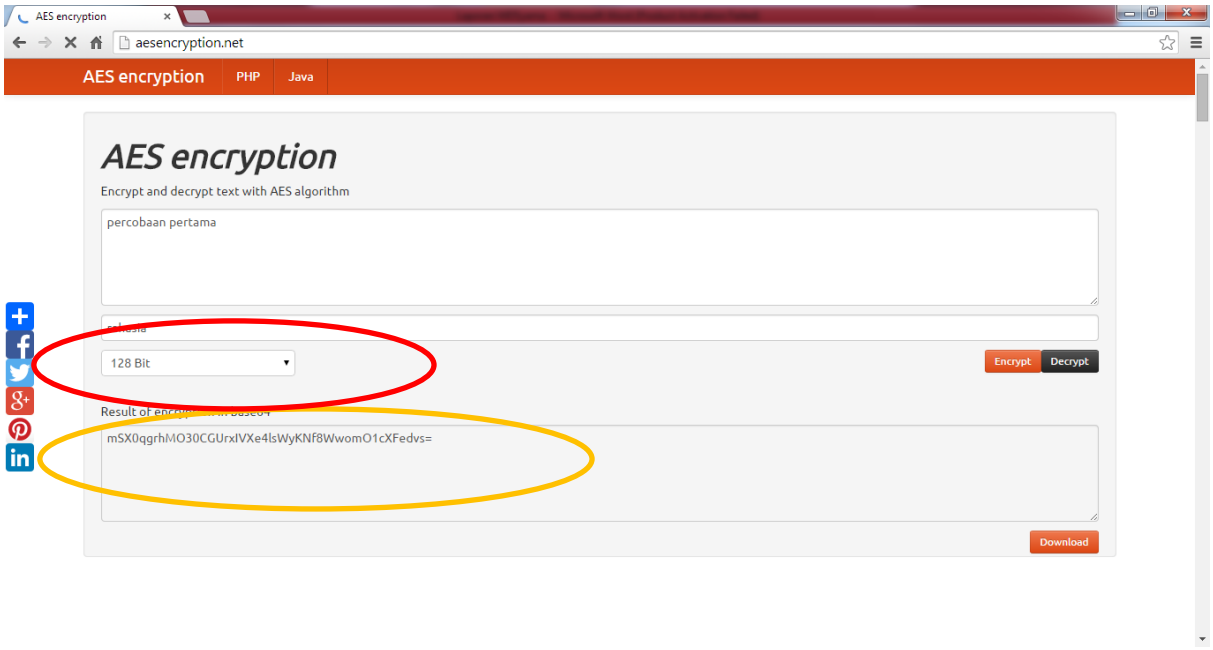
Berdasarkan data yang didapat pada saat praktikum terlihat bahwa jika bit enkripsi yang kita masukkan salah maka pesan akan gagal diterjemahkan.



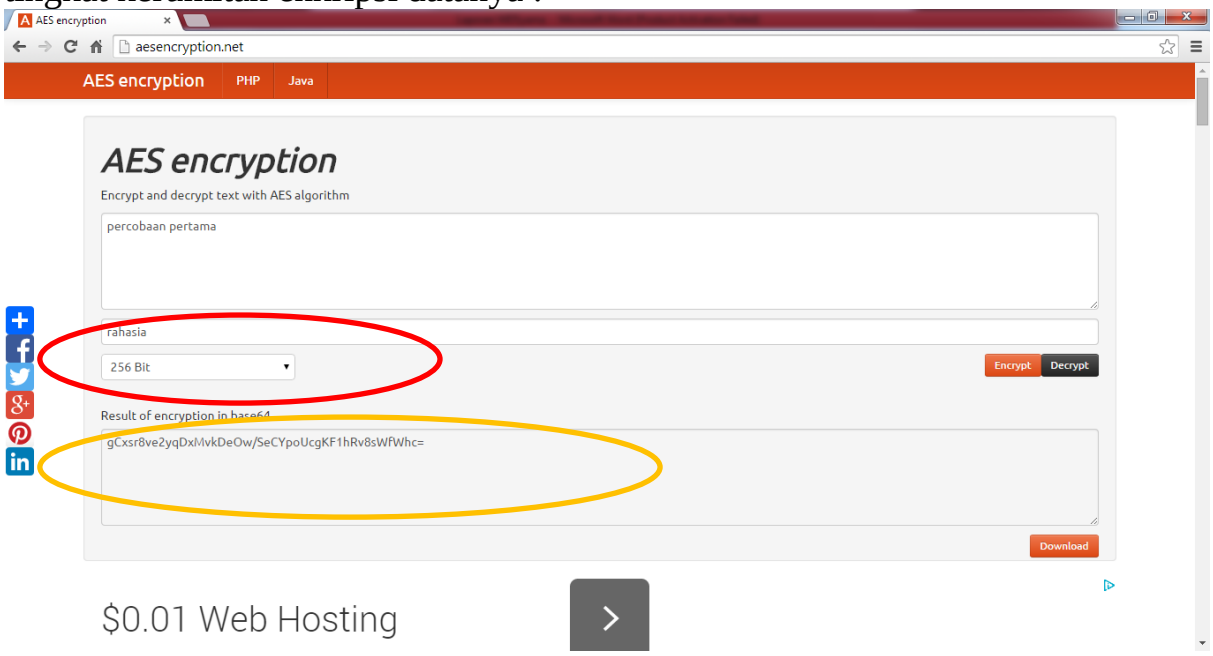
Jika password yang kita masukkan salah maka pesan juga akan gagal diterjemahkan.



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.