JOBSHEET 5

**Keamanan Sistem Informasi**

**Enkripsi & Decripsi**



Disusun oleh:

Nama: Muhammad Aprilianto Putra

No: 13

Kelas: IK-2A

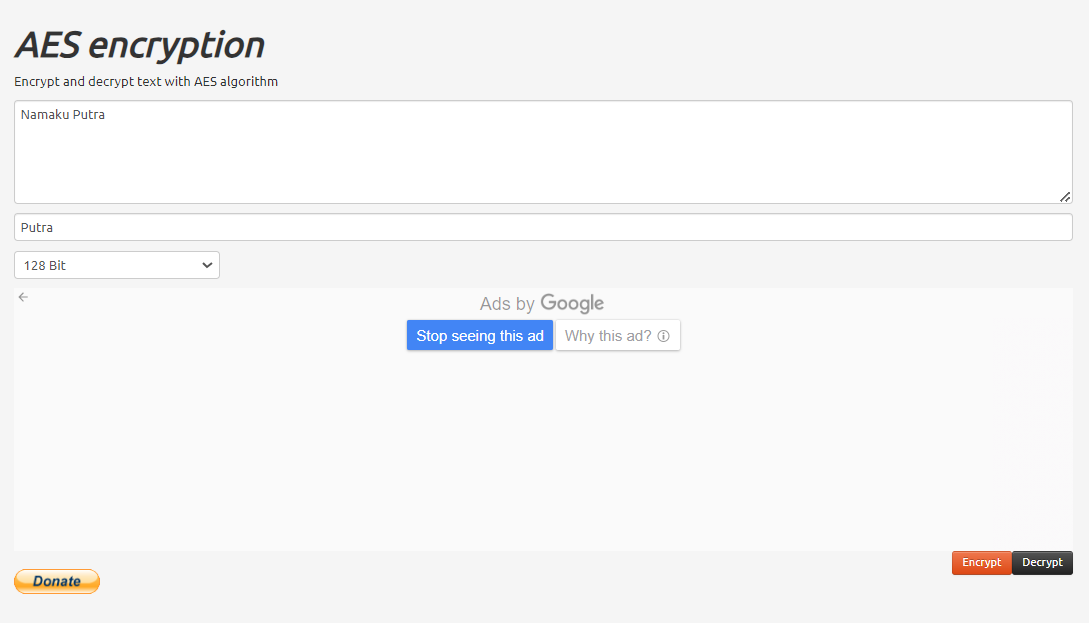
# Program Studi Teknik Informatika Jurusan Teknik Elektro

**POLITEKNIK NEGERI SEMARANG 2024**

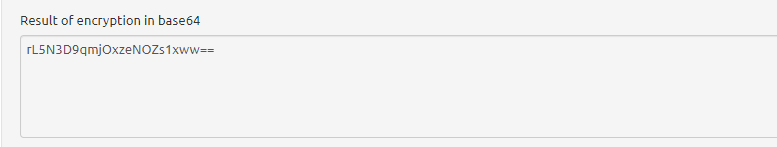
1. Di browser Web, cari encrypt decrypt AES online, . Dalam contoh menggunakan

alat yang tersedia dari: <http://aesencryption.net/>

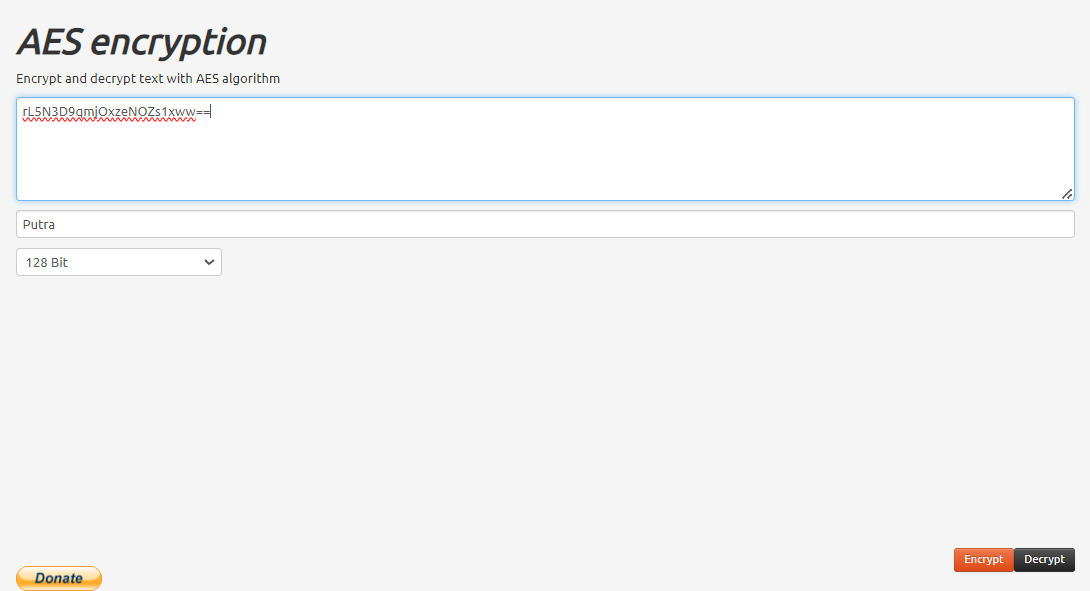
1. Masukan pesan yang akan dienkripsikan lalu inputkan key dan jumlah bitnya (128), lalu klik encrypt



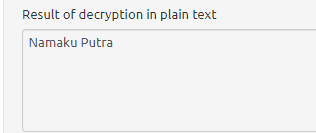
Hasil enkripsinya yaitu: rL5N3D9qmjOxzeNOZs1xww==



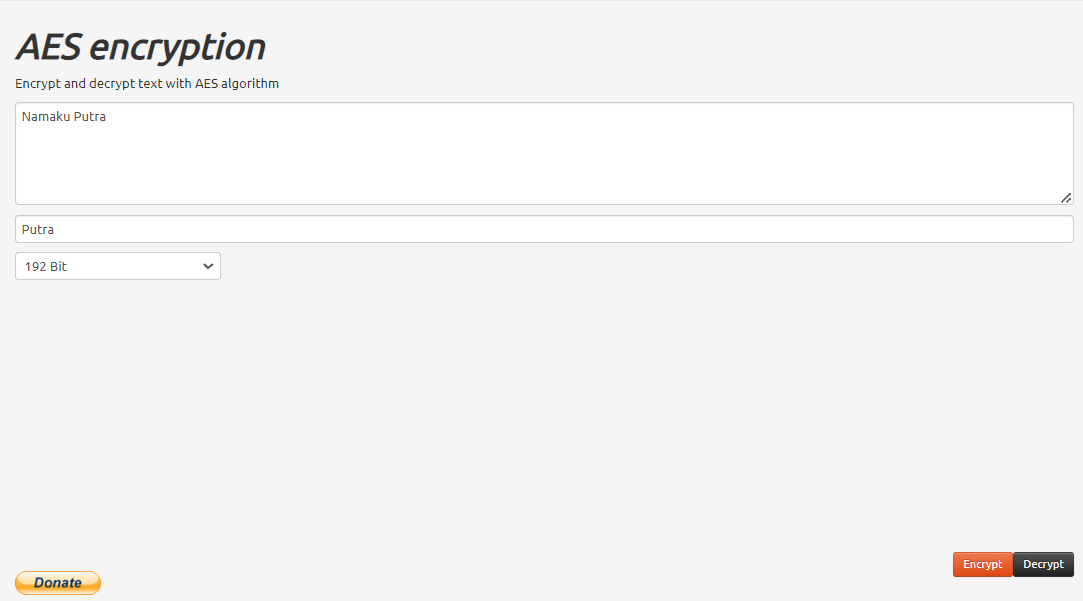
1. Copy hasil pesan enkripsinya, lalu inputkan key dan jumlah bitnya (128), lalu klik decrypt



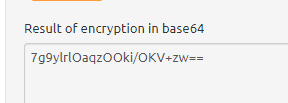
Hasil dekripsinya sebagai berikut:

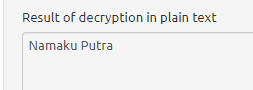
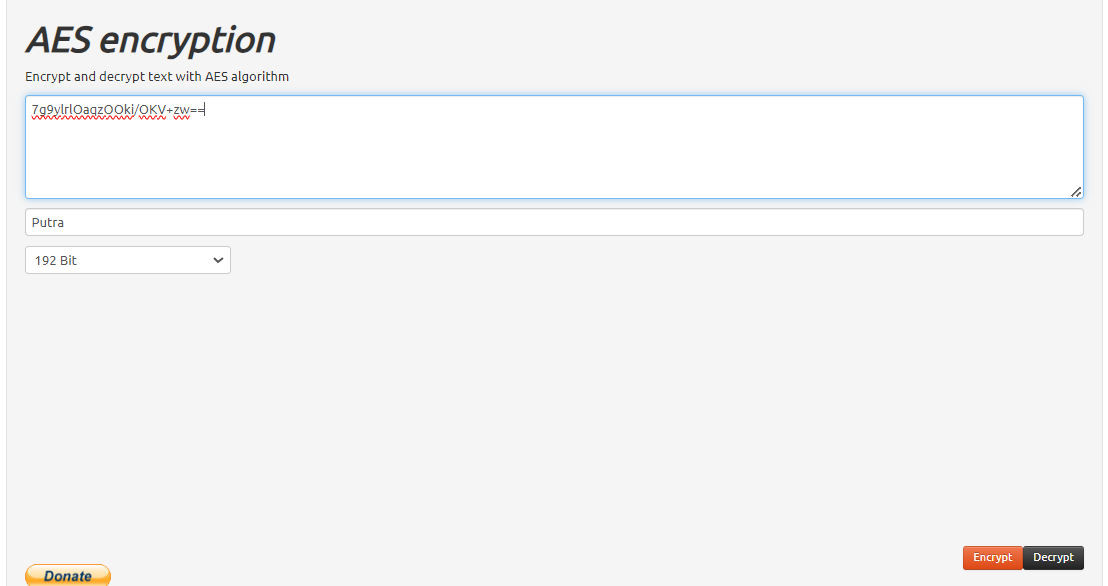


1. Coba kita bitnya menjadi 192 bit dengan pesan dan key yang sama lalu enkripsi:

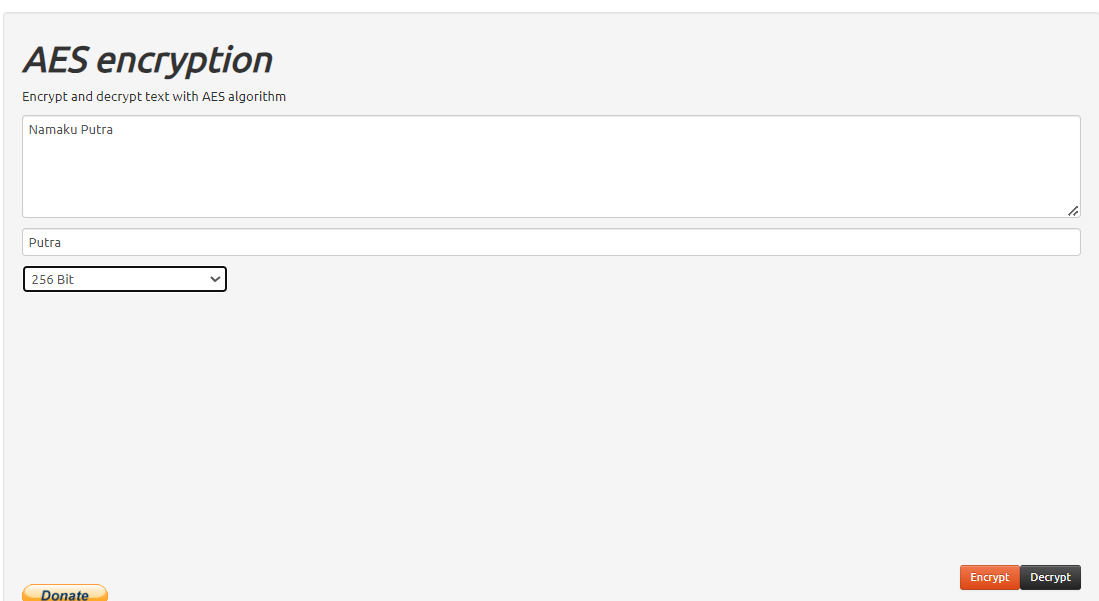


Hasil enkripsinya yaitu: 7g9ylrlOaqzOOki/OKV+zw==

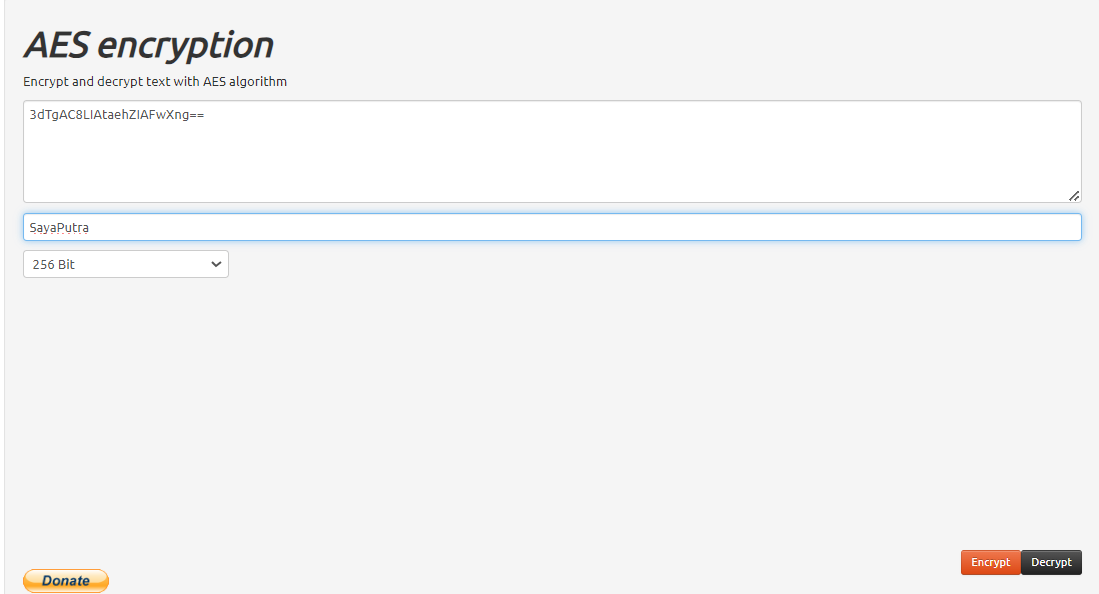


Coba kita dekripsi, maka hasilnya:  


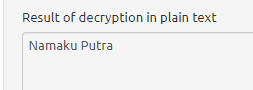
1. Coba kita bitnya menjadi 256 bit dengan pesan dan key yang sama lalu enkripsi:



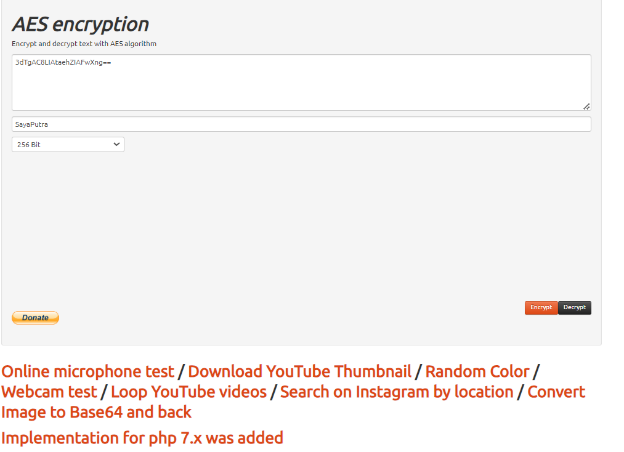
Hasil dari enkripsinya yaitu: 3dTgAC8LIAtaehZIAFwXng==, lalu kita dekripsi



Hasil dekripsi:

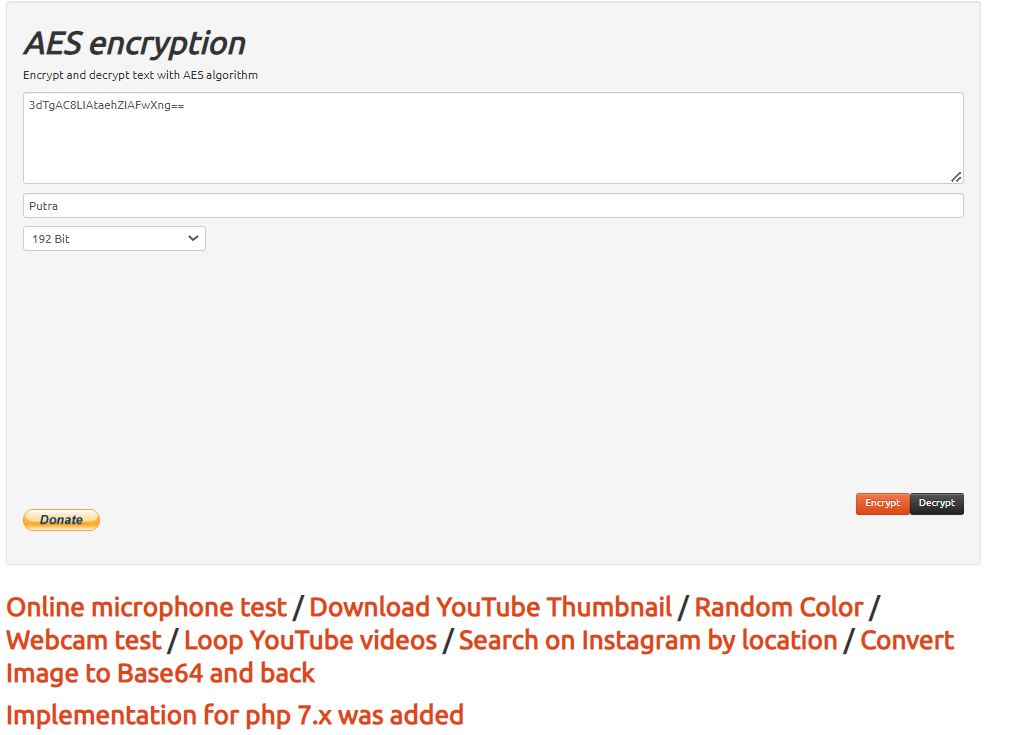


1. Coba kita inputkan key salah, dengan pengaturan sebelumnya, lalu dekripsikan pesan enkripsi sebelumnya:



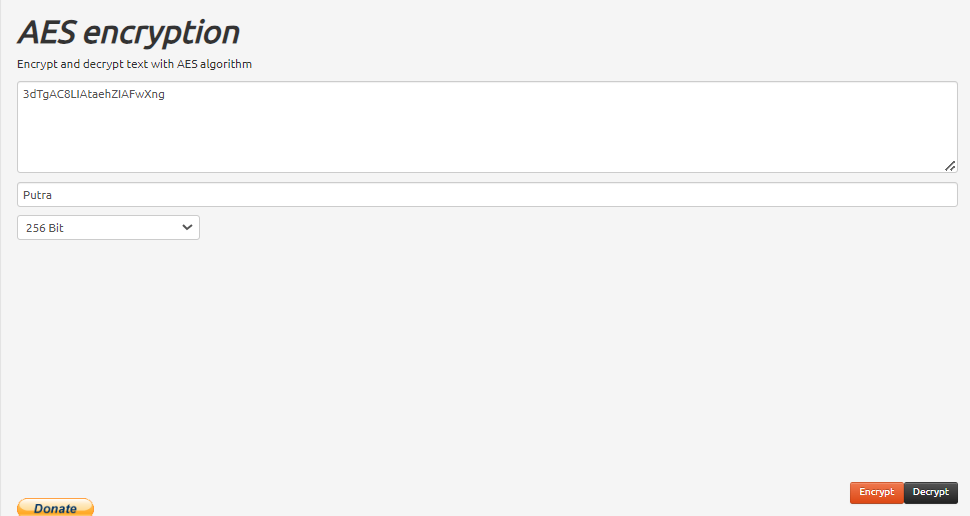
Maka hasilnya tidak menampilkan pesan apapun

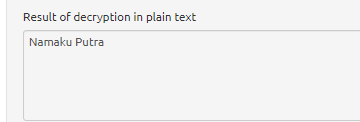
1. Coba kita inputkan jumlah bit yang berbeda yaitu 192bit (bit yang benar yaitu 256), lalu dekripsikan pesan enkripsi sebelumnya:



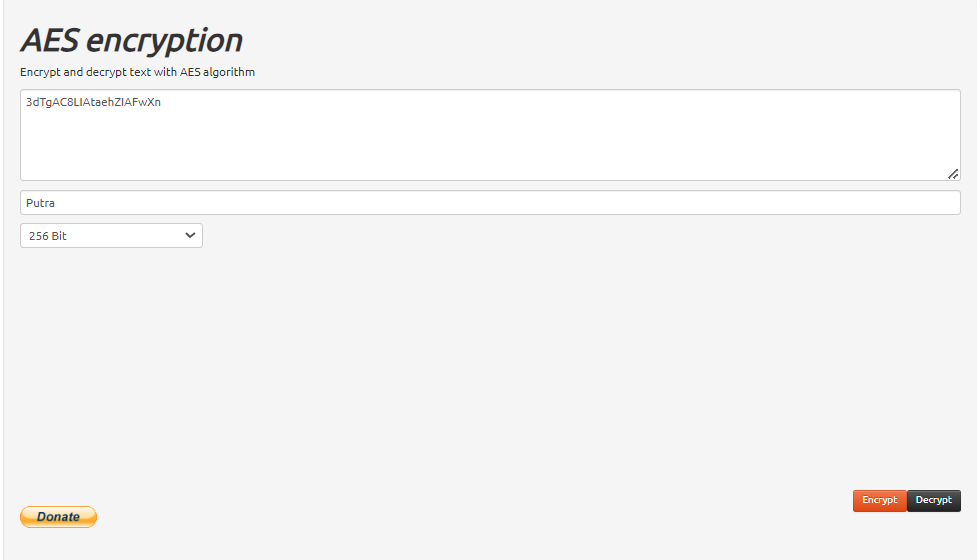
Maka hasilnya tidak menampilkan pesan apapun

1. Coba kita hapus 2 karakter pada pesan enkripsinya (pesan yang dihapus “==”):



Maka hasilnya yaitu pesan yang asli:  


1. Coba kita hapus satu karakter yaitu “g”:

  
Maka tidak menampilkan hasil apapun

Kesimpulan:

* Perbedaan utama antara ketiga ukuran kunci ini adalah panjang kunci yang digunakan dalam proses enkripsi dan dekripsi, yang pada gilirannya memengaruhi tingkat keamanan enkripsi. Semakin panjang kunci, semakin sulit untuk memecahkan enkripsi secara brute force (mencoba semua kemungkinan kunci secara berurutan).
* 128-bit: Ini adalah ukuran kunci yang paling umum digunakan dan disarankan untuk kebanyakan aplikasi kriptografi. Meskipun lebih sedikit dari 192-bit atau 256-bit, 128-bit masih memberikan tingkat keamanan yang sangat tinggi dan cukup untuk melindungi sebagian besar data dalam kebanyakan kasus.
* 192-bit: Ukuran kunci ini lebih panjang dari 128-bit namun lebih pendek dari 256-bit. Ini memberikan tingkat keamanan yang lebih tinggi dibandingkan dengan 128-bit, karena ruang kunci yang lebih besar, tetapi membutuhkan sedikit lebih banyak waktu untuk melakukan enkripsi dan dekripsi.
* 256-bit: Ini adalah ukuran kunci yang paling kuat dan memberikan tingkat keamanan tertinggi di antara ketiganya. Meskipun proses enkripsi dan dekripsi bisa menjadi lebih lambat dengan kunci 256-bit, ini seringkali dianggap sebagai pilihan terbaik untuk keamanan data yang sangat sensitif.
* Dalam kasus ini, karakter "==", yang merupakan padding, ditambahkan ke pesan terenkripsi untuk memastikan panjangnya sesuai dengan ukuran blok enkripsi. Ketika Anda menghapus karakter tersebut, pesan masih dapat dipulihkan karena algoritma dekripsi dapat mengenali padding dan menghilangkannya saat melakukan dekripsi.