|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **KERTAS KERJA UJIAN** | | | | |  |
| Semester : Ganji / **Genap** / Pendek\*) Tahun akademik : . . **.** | | | | |
|  |  |  |  |  |
|  |  |  |  |  |  |  |
| Nomor Induk Mahasiswa | | 41519120006 | | Nomor Ujian : |  | Paraf Mahasiswa |
| Nama |  | KARTIKA NIRWANA SILALAHI | | | |  |
| Fakultas / Program Studi | | ILMU KOMOUTER/TEKNIK INFORMATIKA S1 | | | | Paraf Pengawas |
| Mata Kuliah |  | KRIPTOGRAFI DAN STEGANOGRAFI | | | |  |
| Dosen |  | DRS. ACHMAD KODAR, MT.MKOM | | | | Nilai Ujian (00-100) |
| Waktu |  | Hari | Tanggal | Jam | Ruang |  |
| Pelaksanaan Ujian |  | SABTU | 11 JULI 2020 | 09.30-11.59 | E-310 |  |

Jawaban Pertanyaan

1. Perbedaan Kriptografi Klasik dan Modern

Dari segi penggunaan kunci, kriptografi klasik masih menggunakan kunci simetris dalam proses enkripsinya, sedang kriptografi modern sudah banyak menggunakan kunci asimetris. Kunci simetris adalah dimana kunci untuk enkripsi dan dekripsi menggunakan kunci yang sama, sedang kunci asimetris adalah dimana kunci untuk enkripsi dan dekripsi menggunakan kunci yang berbeda.  
  
Dari segi perkembangan, kriptografi modern terus mengalami perkembangan beriringan dengan berkembangnya ilmu matematika. Sedangkan kriptografi klasik, berkembang dengan penggabungan-penggabungan dengan teknik enkripsi lain yang saat ini banyak dilakukan oleh peniliti.

2. Bentuk bentuk Proses Chesar Cipher

Adapun langkah-langkah yang dilakukan untuk membentuk chiperteks dengan Caesar Cipher adalah :

Menentukan besarnya pergeseran karakter yang digunakan dalam membentuk cipherteks ke plainteks.

Menukarkan karakter pada plainteks menjadi cipherteks dengan berdasarkan pada pergeseran yang telah ditentukan sebelumnya.

Algoritma proses caesar cipher merupakan algoritma klasik yang memiliki langkah-langkah logis sebagai berikut :

1. Menghitung panjang karakter / huruf yang diinputkan dalam plaintext.

2. Tiap-tiap huruf diubah menjadi kode ASCII menggunakan proses looping.

3. Untuk melakukan pergeseran / proses enkripsi maka kode ASCII tersebut digeser dengan cara ditambah sebanyak pergeseran. Misal pergeseran 5 huruf maka kode ASCII ditambah dengan 5.

4. Jika ditemukan spasi (ASCII=32), maka tidak usah dilakukan penambahan. 5. Hasil pergeseran bilangan ASCII dikembalikan lagi menjadi huruf / karakter

3. Algoritma Kriptografi Hill Cipher

Hill Cipher merupakan penerapan aritmatika modulo pada kriptografi. Teknik kriptografi ini menggunakan sebuah matriks persegi sebagai kunci yang digunakan untuk melakukan enkripsi dan dekripsi. Dasar dari teknik Hill Cipher adalah aritmatika modulo terhadap matriks. Dalam penerapannya, Hill Cipher menggunakan teknik perkalian matriks dan teknik invers terhadap matriks. Kunci pada Hill Cipher adalah matriks n x n dengan n merupakan ukuran blok. Matriks K yang menjadi kunci ini harus merupakan matriks yang invertible, yaitu memiliki inverse K-1 sehingga :

Kunci harus memiliki invers karena matriks K-1 tersebut adalah kunci yang digunakan untuk melakukan dekripsi.

Algoritma Enkripsi Hill Cipher

Tahapan-tahapan algoritma enkripsi Hill Cipher sebagai berikut :

Korespondenkan abjad dengan numerik

A → 1, B → 2,…, Z → 26

Buat matriks kunci berukuran m x m

Matrik K merupakan matriks yang invertible yaitu memiliki multiplicative inverse K−1 sehingga K.K−1 =1

Plainteks P=p1p2…pn,diblok dengan ukuran sama dengan baris atau kolom matrik K

Matrik P di transpose

Kalikan Matrik K dengan Matrik P transpose dalam modulo 26

Kemudian ditransposekan

Ubah hasil langkah ke-7 kedalam abjad menggunakan koresponden abjad dengan numerik pada langkah 1 sehingga diperoleh cipherteks

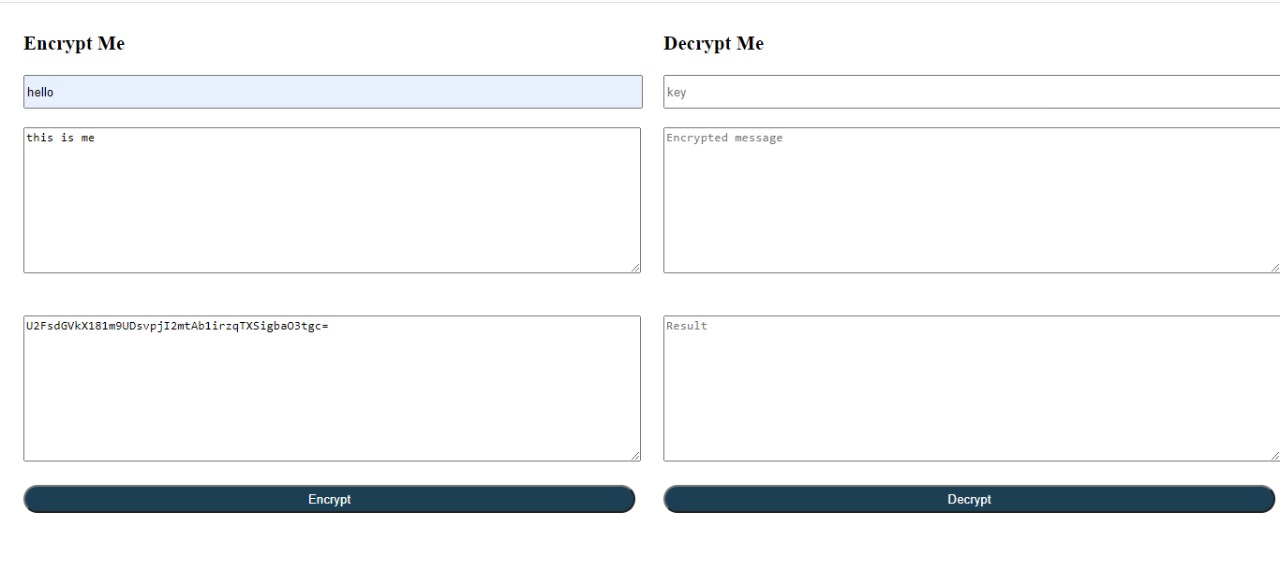
4. Aplikasi Kriptografi Modern yang dibuat

Advanced Encryption Standard (AES) merupakan algoritma cryptographic yang dapat digunakan untuk mengamankan data. Algoritma AES adalah blok chipertext simetrik yang dapat mengenkripsi (encipher) dan dekripsi (decipher) info rmasi. Enkripsi merubah data yang tidak dapat lagi dibaca disebut ciphertext; sebaliknya dekripsi adalah merubah ciphertext data menjadi bentuk semula yang kita kenal sebagai plaintext.

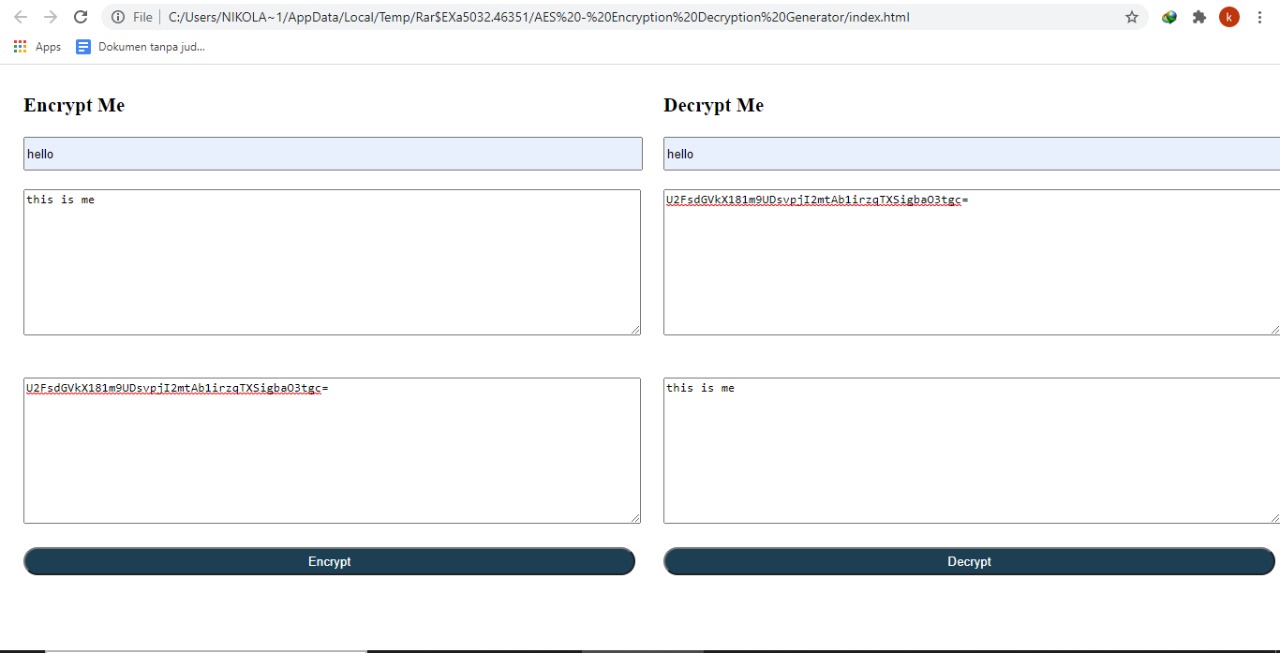
Pengelompokkan jenis AES adalah berdasarkan panjang kunci yang digunakan. Angka-angka di belakang kata AES menggambarkan panjang kunci yang digunakan pada tipa-tiap AES. Selain itu, hal yang membedakan dari masing-masing AES adalah banyaknya round yang dipakai.

Berikut Tampilan Awal AES – Encryption Descryption Generator

Pertama mencoba fungsi encrypt nya, misal dengan key = hello dan text = This is me. Tampilan seperti dibawah ini:



Selanjutnya mencoba fungsi decrypt nya, dengan key yang sama= hello dan text nya result dari encryption yang sebelumnya. Tampilan seperti dibawah ini:



Hasil descryption akan sama dengan text pada encryption sebelumnya. Untuk key bisa combinasi angka dan huruf.