Modul 3

A. Tujuan

1. Mampu menjelaskan definisi dan konsep Caesar Chiper
2. Mampu memahami konsep dasar Caesar Chiper

B. Dasar teori

1. Caesar Cipher

   Dalam kriptografi, sandi Caesar, juga dikenal sebagai sandi geser, sandi Caesar, kode Caesar atau pergeseran Caesar, adalah salah satu teknik enkripsi yang paling sederhana dan paling dikenal. Ini adalah jenis sandi substitusi di mana setiap huruf dalam teks biasa 'digeser' sejumlah tempat ke bawah alfabet. Misalnya, dengan pergeseran 1, A akan digantikan oleh B, B akan menjadi C, dan seterusnya. Metode ini pertama kali dibuat oleh Julius Caesar, yang tampaknya menggunakannya untuk komunikasi dengan jenderalnya.

2. Enkripsi dan Dekripsi

   - **Fungsi Enkripsi**

   $$E_n(x) = (x + n) \mod 26.$$

   - **Fungsi Dekripsi**

   $$D_n(x) = (x - n) \mod 26.$$

3. Contoh

   Kita akan melakukan proses enkripsi dan dekripsi menggunakan kata cryptography menggunakan kunci 3.

   Enkripsi

Plain Text	c	r	y	p	t	o	g	r	a	p	h	y
Alphabet Number + Key	2 + 3	17 + 3	24 + 3	15 + 3	19 + 3	14 + 3	6 + 3	17 + 3	0 + 3	15 + 3	7 + 3	24 + 3
Cipher Text	f	u	b	s	w	r	j	u	d	s	k	b

   Enkripsi dilakukan dengan menggeser alfabet sebanyak 3 karakter. Hasil dari enkripsi adalah “fubswrjudskb”

Dekripsi

Cipher Text	f	u	b	s	w	r	j	u	d	s	k	b
Alphabet Number - Key	5 - 3	20 - 3	1 - 3	18 - 3	22 - 3	17 - 3	9 - 3	20 - 3	3 - 3	18 - 3	10 - 3	1 - 3
Plain Text	c	r	y	p	t	o	g	r	a	p	h	y

Hasil dekripsi adalah “cryptography”

4. Keamanan

Caesar cipher bukanlah metode kriptografi yang aman karena hanya ada 26 kemungkinan kunci untuk dicoba, kita cukup mencoba setiap kemungkinan dan melihat mana yang menghasilkan sepotong teks yang dapat dibaca. Jika Anda mengetahui apa itu ciphertext, atau Anda dapat menebak sepotong, maka ini akan memungkinkan Anda untuk segera menemukan kuncinya.

Pendekatan yang lebih sistematis adalah mencocokkan distribusi frekuensi huruf. Dengan membuat grafik frekuensi huruf dalam ciphertext, dan dengan mengetahui distribusi yang diharapkan dari huruf-huruf tersebut dalam bahasa asli (plaintext), kita dapat dengan mudah melihat nilai pergeseran dan perpindahan karakter tertentu dari grafik ciphertext tersebut.

C. Program

Berikut adalah contoh hasil program Caesar chiper

plaintext : D3 Teknik Informatika PSDKU Madiun

ciphertext : G3 Whnqln Lqirupdwlnd SVGNX Pdglxq

plaintext : D3 Teknik Informatika PSDKU Madiun

D. TUGAS INDIVIDU

1. Membuat fungsi enkripsi dan dekripsi teks menggunakan caesar chiper (desain bebas, minimal dapat menampilkan plaintext dan ciphertext sesuai contoh di modul).
    - Bebas menggunakan bahasa pemrograman apa pun silahkan (Python, Java, PHP, dll).
    - Kunci pergeseran yang dipakai sesuai dengan nomor absen masing-masing mahasiswa. Misal nomor absen 5, menggunakan kunci pergeseran 5.
    - Tambahkan dengan **PENJELASAN PROGRAM** yang anda buat (terutama fungsi enkripsi dan dekripsinya) langsung di samping kode. Penjelasan ditulis pakai comment saja boleh.
2. Membuat enkripsi teks (nama lengkap kalian) di excel sebanyak 2x, enkripsi pertama menggunakan kunci pergeseran sesuai nomor absen. Selanjutnya hasil enkripsi pertama, kita enkripsi lagi menggunakan kunci dari kata “INFORMATIKA”. Contoh ada di file excel.
3. Pengumpulan Tugas Praktikum
    - Kedua file nomor 1 dan 2 digabung menjadi 1 memakai rar atau zip
    - **Untuk kelas TI E** Tugas Praktikum di kumpulkan di SPADA paling lambat tanggal **13 September 2021 jam 23.59**

      Untuk kelas TI D Tugas Praktikum di kumpulkan di SPADA paling lambat tanggal **14 September 2021 jam 23.59**
    - Format penamaan file SKD_namakelas_nim_nama