Modul 4

A. Tujuan

1. Mampu menjelaskan definisi dan konsep Vigenere Cipher
2. Mampu memahami konsep dasar Vigenere Cipher

B. Dasar teori

1. Vigenere Cipher

   Dalam kriptografi, sandi Vigenère adalah metode enkripsi teks alfabet dengan menggunakan serangkaian sandi Caesar yang berbeda berdasarkan huruf dari kata kunci. Skema cipher ini menggunakan string teks (katakanlah, sebuah kata) sebagai kunci, yang kemudian digunakan untuk melakukan sejumlah pergeseran pada plaintext.

   Sebagai contoh, mari kita asumsikan kuncinya adalah '**cipher**'. Setiap alfabet kunci dikonversi ke nilai numeriknya masing-masing: Dalam hal ini maka :

   c → 2, i → 8, p → 15, h → 7, e → 4, r → 17.

   Jadi, kuncinya adalah: 2 8 15 7 4 17.

   Kunci yang digunakan pada algoritma vigenere cipher harus memiliki jumlah karakter kurang dari atau sama dengan jumlah karakter (huruf) yang akan di enkripsikan.

2. Enkripsi dan Dekripsi

   Fungsi Matematika:

   - **Fungsi Enkripsi**

     Pi = (Ci-Ki) mod m, atau

     Ci = (Pi + Ki) – m, kalau hasil penjumlahan Pi dan Ki lebih dari m

   - **Fungsi Dekripsi**

     Pi = (Ci-Ki) mod m, atau

     Pi = (Ci – Ki) + m, kalau hasil pengurangan Ci dengan Ki kurang dari 0

     Ketarangan :

     Ci = nilai desimal karakter ciphertext ke-i

     Pi = nilai desimal karakter plaintext ke-i

     Ki = nilai desimal karakter kunci ke-i

     M = panjang alfabet yang digunakan

     Nilai desimal karakter: A=0 B=1 C=2 ... Z=25

3. Contoh

- **Fungsi Enkripsi**

  Pengirim dan penerima memutuskan sebuah kunci. Katakanlah 'cipher' adalah kuncinya. Representasi numerik dari kata ‘cipher’ adalah '2 8 15 7 4 17'

  Kemudian pengirim ingin mengenkripsi pesan, yaitu 'kriptografi'. Maka, dia akan mengatur plaintext dan kunci numerik sebagai berikut :

c	r	y	p	t	o	g	r	a	p	h	y
2	8	15	7	4	17	2	8	15	7	4	17

  Untuk melakukan enkripsi pada plaintext, geser tiap alfabet sesuai dengan nomor pasangan huruf nya. C->2 berarti huruf C di geser 2x, sehingga menjadi E. R-> 8 berarti huruf R digeser 8x menjadi Z, dan seterusnya. Proses keseluruhan enkripsi dapat dilihat pada tabel dibawah

c	r	y	p	t	o	g	r	a	p	h	y
2	8	15	7	4	17	2	8	15	7	4	17
e	z	n	w	x	f	i	z	p	w	l	p

  Ciphertext hasil enkripsi kata cryptography adalah “eznwxfizpwlp”

- **Fungsi Dekripsi**

  Untuk dekripsi, penerima menggunakan kunci yang sama dengan yang dipakai ketika proses enkripsi. Dekripsi dilakukan dengan menggeser ciphertext yang diterima dalam urutan terbalik untuk mendapatkan plaintext.

e	z	n	w	x	f	i	z	p	w	l	p
2	8	15	7	4	17	2	8	15	7	4	17
c	r	y	p	t	o	g	r	a	p	h	y

  Plaintext hasil dekripsi adalah “cryptography”

4. Keamanan

Vigenere Cipher dibuat dengan melakukan pengembangan pada algoritma Caesar Cipher standar. Vigenere Cipher dibuat dengan tujuan untuk mengurangi efektivitas kriptanalisis pada ciphertext dan membuat kriptosistem lebih kuat. Vigenere Cipher secara signifikan lebih aman daripada sandi Caesar biasa.

Vigenere Cipher biasanya digunakan untuk melindungi informasi politik dan militer yang sensitif. Algoritma ini disebut sebagai cipher yang sangat sulit dipecahkan karena kesulitan yang ditimbulkan pada kriptanalisis.

C. Program

Berikut adalah contoh hasil program Vigenere chiper

teks yang dienkripsi : SISTEM KEAMANAN DATA

Kunci : INFORMATIKA

ciphertext : AVXHVY KXIWAVNS RRFA

plaintext : SISTEM KEAMANAN DATA

D. TUGAS INDIVIDU

1. Membuat fungsi enkripsi dan dekripsi teks menggunakan vigenere chiper (desain bebas, minimal dapat menampilkan plaintext dan ciphertext sesuai contoh di modul).
   - Bebas menggunakan bahasa pemrograman apa pun silahkan (Python, Java, PHP, dll).
   - Kata yang akan di enkripsi adalah nama masing-masing. Contoh : Yusuf Fadlila Rachman
   - Kunci yang dipakai sesuai dengan kota tempat tinggal masing-masing mahasiswa. Contoh: Madiun.
   - Tambahkan dengan **PENJELASAN PROGRAM** yang anda buat (terutama fungsi enkripsi dan dekripsinya) langsung di samping kode. Penjelasan ditulis pakai comment saja boleh, atau di bagian readme Github.
2. Membuat enkripsi teks (nama lengkap kalian) di excel menggunakan *tabula recta*. Kata yang dienkripsi sesuai dengan nama lengkap masing-masing. Kunci yang digunakan sesuai dengan kota tempat tinggal masing-masing. Contoh ada di file excel.
3. Pengumpulan Tugas Praktikum
   - Upload file excel dan kode program di akun github masing-masing. Kemudian kumpulkan link github di SPADA. Contoh : https://github.com/fadilrahman46/IoT
   - **Untuk kelas TI E** paling lambat tanggal **20 September 2021 jam 23.59**
     Untuk kelas TI D paling lambat tanggal **21 September 2021 jam 23.59**
   - Format penamaan file SKD_namakelas_nim_nama