Anggota Kelompok :

1. Lisa Nurfauziyya (14/364139/PA/15913)
2. Jesy S. Amelia (14/365996/PA/16187)

**Homophonic Cipher**

Homophonic cipher ini didasarkan pada frekuensi karakter yang ada di plainttext.Ide cipher substitusi homofonik adalah menggantikan satu karakter pada plainteks menjadi satu atau lebih karakter pada cipherteks, one to many (satu-ke-banyak). Sehingga pada substitusi cipher ini, untuk satu plainttext yang sama dapat memiliki ciphertext yang berbeda.

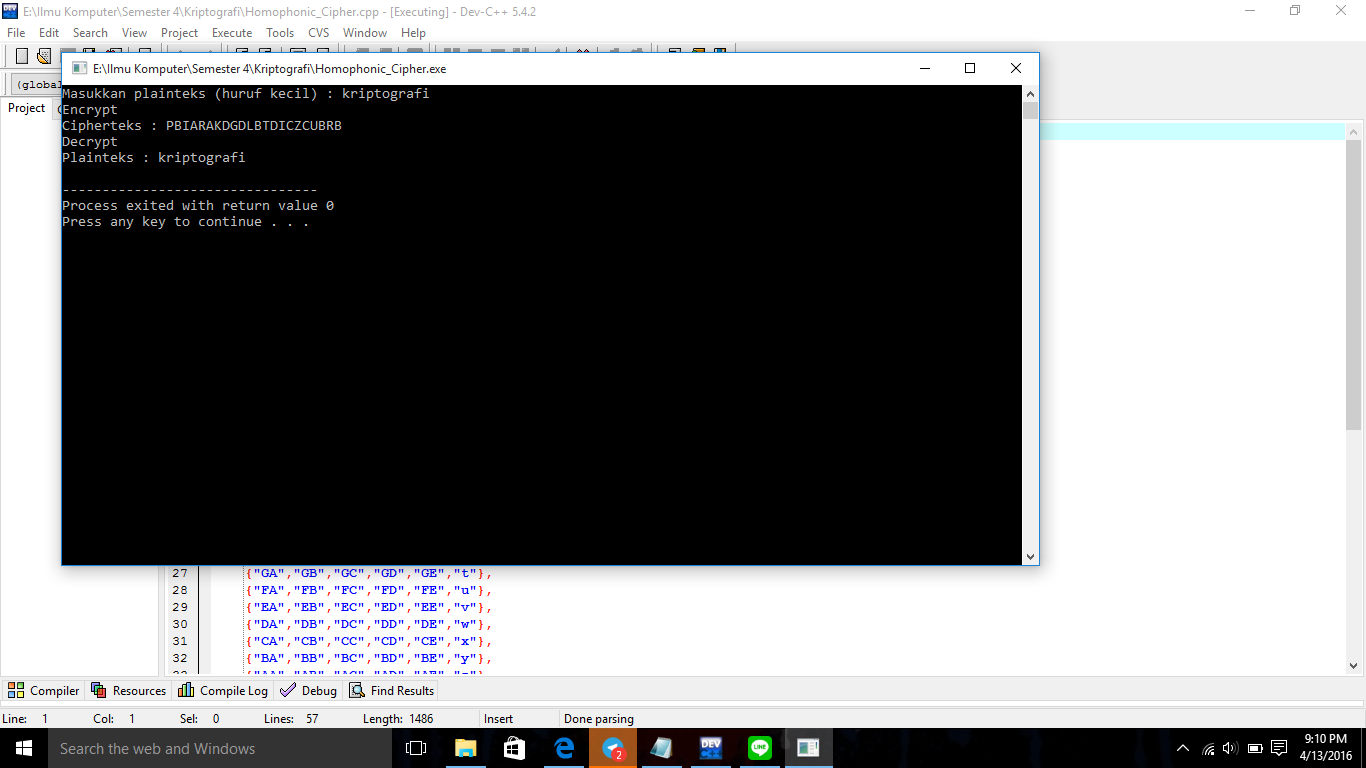
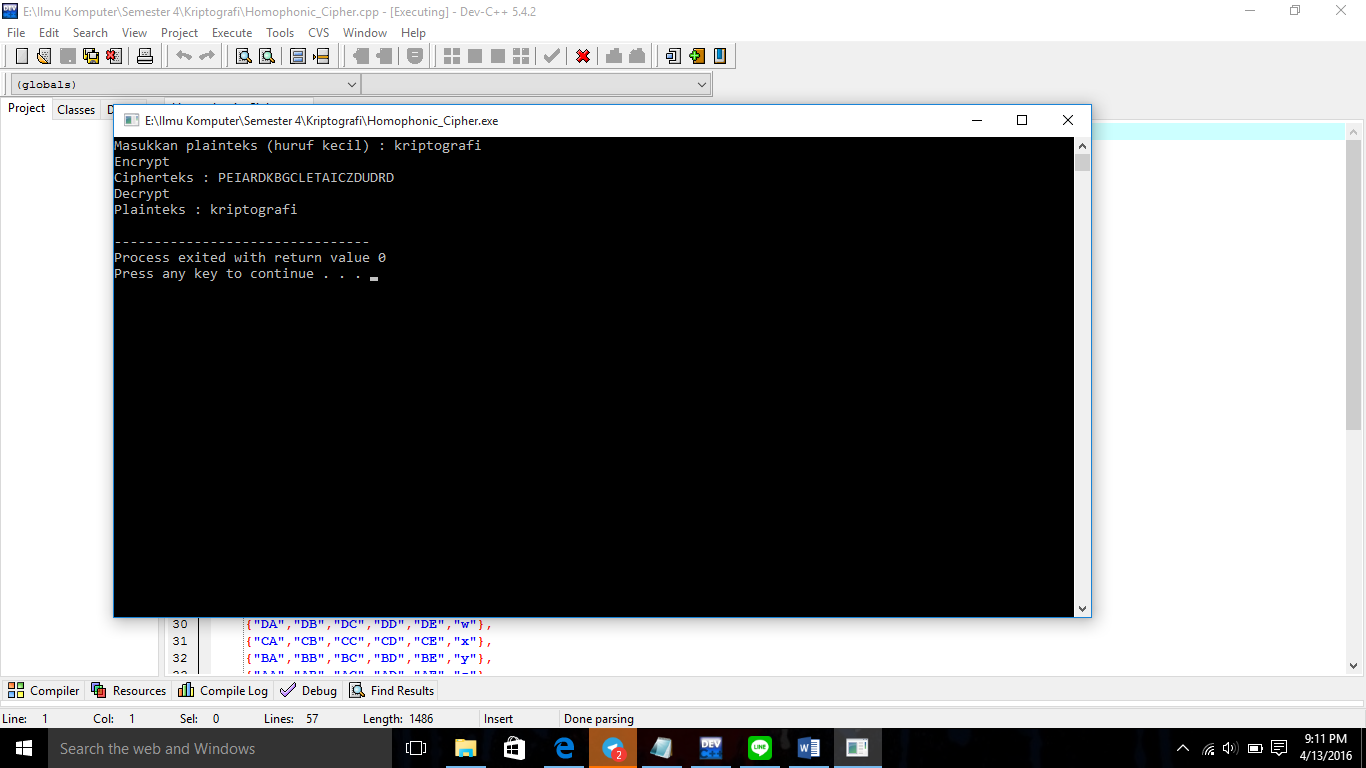
Pada implementasi yang dibuat, setiap plainttext yang ada di petakan menjadi 5 kemungkinan karakter cipher textnya (sesuai dengan ciri dari Homophonic Cipher, one to many).

contoh :

{"ZA","ZB","ZC","ZD","ZE","a"} dimana Huruf a dipetakan menjadi beberapa kemungkinan, diantaranya : "ZA","ZB","ZC","ZD","ZE" maka untuk memilih setiap kemungkinan ciphertext yang keluar dari input plainttext yang kita masukkan, dilakukan random pada kemungkinan ciphertext yang ada. Hal ini dapat menyebabkan plaintext yang sama kemungkinan memiliki ciphertext yang berbeda.

contoh :

dengan menggunakan plainteks yang sama yaitu “kriptografI”, cipherteks yang didapatkan berbeda, seperti yang ditunjukkan oleh gamabar berikut :



Jika seorang kripanalis ingin mengetahui/memecahkan kunci di kirimkan seorang sender kepada receiver menggunakan substitusi homofonic cipher,

maka jenis serangan berdasarkan informasi yang diketahui, adalah dengan "Known plainttext attact".

Know plainttext attact maksudnya adalah "seorang kripanalis harus mengetahui terlebih dahulu plainttext dan ciphertext nya untuk memperoleh kunci dari informasi tersebut.