Alternativ till GUI-del av Lab Kryptering

Vigenere-kryptot

Caesar-kryptot som har en enkel nyckel (antalet steg alfabetet skall rullas) kan knäckas med frekvens-analys. Vigenère-kryptot använder ett ord med flera bokstäver som nycklar, så att olika bokstäver i klartexten rullas olika många steg: A = 0, B = 1, C = 2, …
Man skriver nyckelordet (här ABC) ovanför klartexten, upprepat så många gånger som behövs (skiljetecken krypteras inte) och rullar varje bokstav som nyckeln ovanför anger:

```
ABCABCAB CAB CABCABCA  BCABC
KLARTEXT ATT KRYPTERA. PROVA!
KMCRUGXU CTU …
```

Om man *inte* känner nyckelns längd hjälper inte frekvensanalys. Men om man vet att nyckeln har *N* tecken så blir ju kryptot = *N* st caesar-krypton som således kan knäckas vart och ett med frekvensanalys: Det första består av tecken nr 1,*N*+1,2*N*+1, …,
nästa av 2, *N*+2,2*N*+2, …, osv.

1. Programmera en

```
function krypto = vigen(nyckel,klartext)
```

och en

```
function klartext = vigen_inv(nyckel,krypto)
```

Du kan anta att klartexten bara består av engelska versaler och skiljetecken. Dessa ska lämnas orörda vid krypteringen. På kurshemsidan finns texten (drygt en sida) `Digital_computers.txt` som är flytande engelska, versaler och gemena, skiljetecken, etc.

2. Använd den till att få en frekvensanalys som visar de fyra vanligaste bokstäverna.

3. Skriv också ett program som för en given text gör histogram för nyckellängd *N*.
Kryptera en längre engelsk text (flera hundra tecken) med en nyckel med fyra tecken, gör frekvensanalys på den och prova att rekonstruera nyckeln, visa att dekrypteringen ger klartexten.

4. Byt detta krypto med grann-gruppen och knäck deras krypto utan att tala om nyckeln!

Säker kommunikation med hemliga nycklar

Caesar-kryptot har en egenskap som gör det möjligt för två personer A och B som håller sina nycklar hemliga - också för varandra! - att kommunicera.
Låt meddelandet vara M. Caesar-rullning n steg ger krypterat meddelande $K = C_n(M)$.
Då är

$$M = C_{-n}(K)$$

och

$$C_k(C_n(M)) = C_{n+k}(M) = C_n(C_k(M)) \qquad (*)$$

A och B gör så här:
A sänder $K = C_a(M)$ till B. B kan inte läsa K, men krypterar K med sin nyckel b och skickar

$$C_b(C_a(M))$$

tillbaka till A. A applicerar nu sin dekryptering och sänder

$$C_{-a}(C_b(C_a(M)))$$

till B … som dekrypterar med sin nyckel,

$C_{-b}(C_{-a}(C_b(C_a(M))))$.

5. Visa att detta blir M! Illustrera genom att köra dina program med nyckellängd 1,
`vigen_inv(b,vigen_inv(a,vigen(b,vigen(a,klartext))))`

6. Visa, genom t ex att betrakta hur tecknet i position *k* i texten krypteras, att Vigenere-kryptot har egenskapen $C_{k1}(C_{k2}(M)) = C_{k2}(C_{k1}(M))$ där k1 och k2 är nycklarna (som kan vara olika långa). Visa därmed att A och B kan kommunicera med olika långa nycklar a och b,
`vigen_inv(b,vigen_inv(a,vigen(b,vigen(a,klartext))))=klartext`

7. (frivillig) I texten `Digital_computers.txt` finns ett meddelande gömt, en interjektion på god engelska. Vad är det?