LaborationsPM
Krypteringsmetoder och säkring av datasystem
Kursansvarig: Eric Järpe
Högskolan i Halmstad
Grupp 4

Laboration 1: Substitutionskrypton

I denna laboration är tanken att man bl a ska knäcka ett antal koder. De meddelanden som kodats är från början skrivna på svenska. Till hjälp i kodknäckandet kan man använda följande tabell över frekvenser av olika bokstäver i det svenska språket. Observera att de angivna frekvenserna är beräknade på ett allmänt urval av litteratur och avvikelserna i meddelanden kan varierar beroende på meddelandets längd och olika språkformer.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
9,3	1,3	1,3	4,5	9,9	2	3,3	2,1	5,1	0,7	3,2	5,2	3,5	8,8	4,1

P	Q	R	S	T	U	V	W	X	Y	Z	Å	Ä	Ö
1,7	0,01	8,3	6,3	8,7	1,8	2,4	0,03	0,1	0,6	0,02	1,6	2,1	1,5

Frekvenstabell över den procentuella förekomsten av de olika bokstäverna i ett urval av svensk litteratur. (Källa: Svenska Wikipedia.)

Laborationsuppgifter

1. I denna uppgift ska du använda det kodade meddelandet som finns på sidan `https://dixon.hh.se/erja/teach/itfc/intranet/lab1/gr4/uppg1.html`, som är länkad från kurshemsidan. Kopiera och klistra in i Word eller Notepad eller liknande. Denna text är ett meddelande som är kodat med ett s.k. *Caesarkrypto*. Din/er uppgift är helt enkelt att försöka knäcka koden! Svaret på uppgiften är meddelandet i klartext, men berätta också i ett par meningar om hur du/ni gjorde för att komma fram till detta svar.

2. I denna uppgift ska du använda det kodade meddelandet som finns på sidan `https://dixon.hh.se/erja/teach/itfc/intranet/lab1/gr4/uppg2.html`, som också är länkad från kurshemsidan. Kopiera och klistra in i Word eller Notepad eller liknande. Texten här är kodad med ett s.k. *substitutionskrypto*.
   (a) Hur kan man gå tillväga för att knäcka ett meddelande som är kodat med ett sådant krypto?
   (b) Vad blir meddelandet i klartext i fallet med texten i filen `uppg2.txt`?
   (c) Antag att man krypterade ett meddelande med ett substitutionskrypto och att man sedant tog den krypterade texten och krypterade den ånyo med ett annat substitutionskrypto. Skulle det då bli svårare att knäcka?

3. I ett *Vigenèrekrypto* använder man flera substitutionskrypton enligt ett visst mönster. Nu är meningen att du ska knäcka koden för det meddelande som finns på sidan `https://dixon.hh.se/erja/teach/itfc/intranet/lab1/gr4/uppg3.html`, som också är länkad från kurshemsidan. Kopiera och klistra in i Word eller Notepad eller liknande. Klartexten här är på engelska. En frekvenstabell för engleska språket finns länkad från kurshemsidan. I klartexten till detta meddelande har alla ordmellanrum, komman, punkter, bindestreck etc tagits bort. Det enda som behållits är bokstäverna a–z och siffrorna 0–9. Sedan har man krypterat med 3 substitiontionskrypton på alla dessa 36 tecken i ett rullande schema:
   - första tecknet med substitionskrypto 1
   - andra tecknet med substitionskrypto 2
   - tredje tecknet med substitionskrypto 3
   - fjärde tecknet med substitionskrypto 1

     $\vdots$
   - tecken nummer n med substitionskrypto $(n-1 \bmod 3)+1$

   Denna uppgift går ut på att knäcka koden och svaret är dels de 100 första tecknen i den klartexten, och dels eventuella datorprogram som använts för att åstadkomma knäckningen.

Rapporten

Laborationsrapporten ska innehålla

- Rubriken: *Rapport för Laboation 1.*
- Gruppens nummer.
- Namn på alla som är med i gruppen.
- Alla lösningsresonemang, delresultat, och svar på frågorna.

Lämpligen skriv rapporten i Mathematica eller Word. Kopiera och klistra in eventuella tabeller och övriga svar från Mathematica. Gör rapporten så liten och kompakt som möjligt, men så att alla svar och förklaringar finns med. Spara den sedan som ett pdf-dokument och skicka den med email till mig på `eric.jarpe@hh.se`.

Rapporten för laboration 1 ska vara inlämnad *senast* det sista inlämningsdatum som finns angivet på kurshemsidan, men man får givetvis gärna lämna in den tidigare.

LYCKA TILL!