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

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 meddelande i filen `gruppX_uppg1.crypt` (där `X` är numret på din grupp), som du fått som bilaga i ett email av mig. 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 i filen `gruppX_uppg2.crypt`, som du också fått som bilaga i ett email av mig. 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 `gruppX_uppg2.crypt`?
   (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 2 (eller flera) substitutionskrypton enligt ett visst mönster. Konstruera ett enkelt Vigenèrekrypto som växlar mellan 2 Caesarkrypton: det första där kryptoalfabetet är förskjutet m steg, det andra där kryptoalfabetet är förskjutet n steg, där m och n är de 2 tal som meddelats via email om denna uppgift.

   (a) Betrakta citatet

   > *Tala inte illa om din fiende men tänk!*
   >
   > Publilius Syrus, 100 e Kr

   Kryptera det mha Vigenèrekryptot i uppgift (d).

   (b) Skriv ett program i Mathematica som genomför krypteringen av det meddelande man ger det, dvs ett program som efterfrågar en klartext och som returnerar koden enligt Vigenèrekryptot ovan.

Rapporten

Laborationsrapporten ska innehålla

- Rubriken: *Rapport för Laboation 1.*
- 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 tabller och övriga svar från Mathematica. Rapporten så liten och kompakt som möjligt, men så att alla svar och förklaringar finns med. Skicka den sedan 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!