# 25. Enkel substitution – det allmänna fallet

I detta avsnitt skall ni forcera tre meddelanden som är krypterade med enkel substitution (ES-krypto). Kryptotexten är dock utformad på olika sätt. Klartext-orden är skrivna utan mellanrum, men det kan finnas något tecken för komma eller punkt. Till övningarna finns det i detta avsnitt tips och ledtrådar, särskilt för början av arbetet med de olika texterna.

**Övning 25A**

Här är en kryptotext som man har fått genom att kryptera en engelsk klartext med ES-krypto.

```
UYJRL  JSNLR  LVDGJ  LIYLD  FGHTB  RDFFY  XHJJL  FRDBO
FHVIS  IJHDG  ASIIY  UHYVS  JRKIJ  SBYUT  DMARD  SFDIB
DIDFF  HVEDM  LWWRL  VDGGK  FXFSG  SIOTY  CKSMA  WDGAS
TTBLQ  LTHXL  BHQLF  YLDFG  HEOLJ  JSIOH  KJHEJ  RLVDY
HERSG  UKTTY  SIOMH  KGSIW  WRLGJ  STTTS  QLBSI  JRLMK
XUHDF  BKIBL  FJRLG  JDSFG  WWRSG  LYLGV  RSMRV  LFLJR
LGDNL  DGRSG  NHJRL  FGVLF  LUFST  TSDIJ  OFLLI
```

Som ni har sett i avsnitt 24 är den engelska språkstatistiken olik den svenska. Den vanligaste bokstaven och det vanligaste trigrammet förekommer mycket oftare än de näst vanligaste. Som ni kommer att se, är det en fördel när man skall forcera ES-krypto.

Börja med att skriva kryptotexten på ett rutat arbetspapper som ni gjorde för texten i avsnitt 22, så att det blir plats för klartexten allteftersom den kommer fram.
Ta fram eller gör en kryptonyckelmall att fylla i när ni gjort ett antagande eller konstaterat en motsvarighet mellan en klartextbokstav och en kryptobokstav. Gör dessutom en monogramstatistik (pinnstatistik för enskilda bokstäver) för kryptotexten. Ni behöver inte plats för Å, Ä och Ö. De bokstäverna finns ju inte i engelska. Sedan är det dags att börja tänka…



 

Om ni behöver finns det ledtrådar på denna dels sista sida. Använd dig bara av en i taget och bara om ni har kört fast.

*Om ni behöver, se ledtråd 25A1 på sidan 7.*

*Om ni behöver, se ledtråd 25A2 på sidan 7.*

*Om ni behöver, se ledtråd 25A3 på sidan 7.*

Hittar ni något sannolikt ord?

*Om ni behöver, se ledtråd 25A4 på sidan 7.*

Sedan behöver ni nog inte fler tips för att klara av uppgift 25A.

**Övning 25B**

Detta är en övning i att forcera byggmästarkrypto. Repetera gärna avsnitt 7 i grundkursen om ni har glömt bort vad byggmästarkrypto är.

I den här övningen har vi bara använt 26 teckens nyckel. Vi har inte tagit med de vinklar som har två punkter. Då måste vi göra något för att kunna hantera våra svenska bokstäver 'å', 'ä' och 'ö'. Vi har här valt att helt enkelt ta bort punkterna över 'ä' och 'ö' samt ringen över 'å' innan vi krypterat texten. Så gör man ju när man skall tillverka Internet-adresser.

På nästa sida är kryptotexten som ni skall forcera. I stället för att kryptera ord-mellanrum har vi här gjort ett uppehåll i kryptotexten.
Varje tecken (en vinkel med eller utan punkt) i kryptotexten motsvarar en bokstav i klartexten, så det är alltså frågan om enkel substitution fast kryptotecknen ser ut på ett annat sätt. Det är enklare att hantera bokstäver i stället för vinklar. Därför kan ni provisoriskt ersätta vinklarna med bokstäver i stället. Ni kan till exempel använda den nyckel som finns i grundkursens övning 7A för den provisoriska ersättningen. Fast använd stora bokstäver eftersom det ännu inte är klartext.



 



 

Om ni gör det börjar kryptotexten så här: QIOOE LFBES IOLUU IIJMI SANGE ...

Nu börjar det egentliga forceringsarbetet. Gör först monogamstatistik som vanligt. Eftersom klartextbokstaven 'a' nu också kan betyda 'å' eller 'ä' förekommer den bokstaven nu oftare, ja till och med oftare än 'e'. Det vanligaste tecknet i kryptotexten borde därför motsvara 'a'.

Sedan kan ni göra upp en nyckelmall. Ta gärna den i övning 7A fast utan bokstäver i och fyll i 'a' där den bokstaven skall stå. Mot slutet av forceringsarbetet kan ni ha nytta av det om det finns ett särskilt mönster för bokstäverna i kryptonyckeln.

Vad gör ni härnäst? Vad kan ni få ut av en bigramstatistik av kryptotexten?

*Om ni behöver, se ledtråd 25B1 på sidan 7.*

Behöver ni fler tips?

*Om ni behöver, se ledtråd 25B2 på sidan 7.*

Nu behöver ni nog inte fler tips.

Ni ser att det kan bli en del problem med våra svenska bokstäver 'å', 'ä' och 'ö' när man ersätter dessa bokstäver med 'a' och 'o' rakt av. Ett alternativ är att ersätta dem med 'aa', 'ae' respektive 'oe', som vi gjorde i grundkursens avsnitt 12. Fast då blir monogramstatistiken ännu snedare och det blir ännu lättare att forcera kryptoton där man gör så. En bra forcör måste vara beredd på båda sätten att undvika våra svenska bokstäver.



 

**Övning 25C**

Här kommer en övning i att forcera ett sifferkrypto. Repetera gärna avsnitt 8 i grundkursen först om ni inte har sifferkrypto aktuellt. Varje sifferpar motsvarar en klartextbokstav, så det är alltså fråga om ES-krypto fastän kryptotexten består av sifferpar i stället för bokstäver. Här är kryptotexten.

07 05 38 08 45 38 20 40 29 09
38 07 35 15 15 20 40 17 38 36
16 15 05 15 20 25 15 00 39 20
19 20 40 30 37 20 38 49 05 39
45 37 20 38 15 38 46 07 07 09

38 19 20 40 19 38 30 37 09 40
19 20 49 15 45 37 09 38 20 40
49 20 28 28 20 38 19 20 15 20
17 15 30 37 20 40 49 16 35 20
15 15 18 30 37 09 40 19 20 49

16 35 38 49 17 36 40 19 09 38
49 30 18 07 05 38 08 45 38 20
40 09 15 15 28 46 49 09 30 18
20 40 05 39 17 38 36 16 15 05
15 20 25 15 20 40 00 19 46 38

20 07 15 20 38 49 46 15 15 20
38 29 09 40 30 18 35 40 18 39
20 19 09 15 15 26 16 16 38 46
15 15 09 49 15 09 15 30 49 15
30 17 20 38 00 49 35 18 05 15

15 49 05 39 09 28 28 15 30 19
26 15 09 40 09 15 15 37 20 15
09 37 30 28 17 09 29 09 40 17
05 39 39 20 38 09 15 15 29 09
40 36 15 15 09 09 37 00 00 00

Studera kryptotexten. Vilka siffror kan vara förstasiffror? Hur många är de? Samma frågor för andrasiffrorna. Hur många sifferpar kan det alltså finnas? Hur stämmer det med antalet bokstäver i alfabetet?



 

Först måste ni ha en monogramstatistik (pinnstatistik för de enskilda sifferparen). Ni kan göra den i en ruta som liknar en kryptonyckel som ni sett i avsnitt 8 i grundkursen.

| | 5 | 6 | 7 | 8 | 9 | 0 |
|---|---|---|---|---|---|---|
| 0 | | | | | | |
| 1 | | | | | | |
| 2 | | | | | | |
| 3 | | | | | | |
| 4 | | | | | | |

Skriv pinnarna i rutorna tätt, med var femte pinne liggande över de fyra föregående, så här:
𝍸 𝍸 𝍸 . . . . Då får de plats i rutorna och blir ändå lätta att räkna. Jämför sedan med monogramstatistiken för svenska språket i avsnitt 24. Vilket sifferpar är vanligast i kryptotexten? Vilken bokstav tror ni att det motsvarar?

*Behöver ni ett tips, se ledtråd 25C1 på sidan 7.*

Fortsätt därefter att identifiera de två vanligaste vokalerna.

*Behöver ni några sannolika ord, se tips 25C2 på sidan 7*

*Fler tips? Gå till tips 25C3 på sidan 7*



 

*Tips 25A1:*

Man kan anta att den vanligaste bokstaven i kryptotexten (vilken är det?) motsvarar den vanligaste bokstaven i engelska (se monogramstatistiken i avsnitt 24). Denna bokstav är även sista bokstav i det vanligaste trigrammet. Leta reda på det i texten. Det finns bara 31 ställen att leta bland. Nu har ni tre motsvarigheter mellan klartext- och kryptobokstäver. Fyll i dem på arbetspapperet och i kryptonyckelmallen.

*Tips 25A2:*

Nu är det bra med en bigramstatistik. Ni har sett att klartextbokstaven 'e' motsvarar kryptobokstaven L, som finns på 31 ställen i testen. Ta reda på de 31 bigram som börjar med L. Det vanligaste av dessa bigram motsvarar även det vanligaste engelska bigrammet som börjar på 'e'. Det hittar ni i den engelska bigramstatistiken i avsnitt 24. Nu har ni en bokstav till i nyckeln och ni kan fylla i den på arbetspapperet och i kryptonyckelmallen.

*Tips 25A3:*

Leta efter fler motsvarigheter med hjälp av bigramstatistiken som ni gjorde i tips 25A2 genom att jämföra med bigramstatistiken i avsnitt 24.

*Tips 25A4:*

Texten handlar om en känd person som var särskilt aktuell sommaren 2007, både i en bok och i en film. Hans namn finns med i texten.

*Tips 25B1:*

En annan möjlig väg är att göra en trigramstatistik, det vill säga skriva upp alla tretecken-kombinationer och ta reda på dem som förekommer fler än en gång i kryptotexten. Det tar en stund att göra det men det kan vara värt jobbet. Vanliga trigram i klartexten är 'och', 'han' och 'and'. Det ger några bokstäver till i nyckeln.

*Tips 25B2:*

Klartexten handlar om Mästerdetektiven Kalle Blomkvist och hans vänner, när de avslöjar juveltjuvarna.

*Tips 25C1:*

Det vanligaste sifferparet är 15 och då tror man kanske först att det motsvarar 'e' eller 'a', de vanligaste bokstäverna i svenska språket. Men i kryptotexten finns flera ställen där två stycken 15 förekommer efter varandra. Då är det nog ingen vokal. Antag därför i stället att 15 motsvarar någon av de vanligaste konsonanterna: 't', 'r' eller 'n'.

*Tips 25C2:*

Texten handlar om något som ni just nu håller på med.

*Tips 25C3:*

Texten handlar om kryptering, språkstatistik och forcering.