22. Enkel substitution (ES-krypto)

En svaghet med Caesar-krypto och med Vigenèrekrypto är att de använder alfabetets bokstäver i normal ordning. Enkel substitution (ES-krypto) använder oordnade alfabeten. Repetera gärna avsnitt 11 i grundkursen.

Ni börjar med ett exempel där ni följer – i flera led – hur forceringsarbetet fortskrider. Vi vet från början att det rör sig om enkel substitution. Här är kryptotexten:

```
PLEHG UJAAH ÅNTHG UÖEIG DFULN RUGMÖ
OLHHÖ UAZUO ZEKHU RZOOU URÖEU FZKUÖ
HHUÖE IGDFU RÖIGU EZKLH UYURÖ EIGEU
LNRUÖ HHURL EUFHJ IGDÖI GUGHH UAÖAA
GDUUM YUCZF HGUFT WEIÖU LFFUF ÖIGUR
LEUHY OOUÖE IGDFU
```

Först måste vi ha en pinnstatistik som visar hur vanliga de olika bokstäverna är i kryptotexten. Se tabellen till höger.

Sedan behöver ni ett arbetspapper med kryptotexten och plats för klartexten. Fortsätt att fylla i kryptotexten. Den är ju given på förhand. Sedan fyller ni i klartexten i rutorna på nästa sida allteftersom den växer fram under forceringsarbetet.

A	𝍸 I
B	
C	I
D	𝍸
E	𝍸 𝍸 II
F	𝍸 𝍸
G	𝍸 𝍸 IIII
H	𝍸 𝍸 𝍸 I
I	𝍸 IIII
J	II
K	III
L	𝍸 III
M	II
N	III
O	𝍸 I
P	I
Q	
R	𝍸 III
S	
T	II
U	𝍸 𝍸 𝍸 𝍸 𝍸 𝍸 II
V	
W	I
X	
Y	III
Z	𝍸 I
Å	I
Ä	
Ö	𝍸 𝍸 IIII

KRYPTO	P	L	E	H	G	U	J	A	A																
klar																									

KRYPTO																									
klar																									

KRYPTO																									
klar																									

KRYPTO																									
klar																									

KRYPTO																									
klar																									

KRYPTO																									
klar																									

KRYPTO																									
klar																									

Ni behöver också en kryptonyckelmall där ni fyller i kryptonyckeln allteftersom ni kommer på den:

Klartext																													
Krypto	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Å	Ä	Ö

Bokstaven U i kryptotexten förekommer väldigt många gånger, nästan 20 % av alla bokstäver i kryptotexten. Så ofta brukar inte en bokstav finnas i en svensk text. Antag att dess motsvarighet i klartexten har använts för att markera mellanrum mellan ord. Man kan förmoda att kryptören använt 'x' för detta. Då kan ni fylla i 'x' i klartextraderna under varje U i kryptotexten eller kanske helt enkelt stryka över alla U i kryptotexten Då ser ni hur långt varje klartextord är. Fyll dessutom i 'x' ovanför U i nyckelmallen. Det här är en bra början.

Det finns bara ett vanligt ord med bara en bokstav i svenskan och det är 'i'. I kryptotexten finns ett enbokstavigt ord, Y, och det har nog 'i' som motsvarighet. Fyll i alla 'i' på arbetspapperet och i nyckelmallen.

Nu ger ni er på alla ord med tre bokstäver. Leta efter de vanliga orden 'och', 'att', 'ett', 'hon' och 'han'. 'och' är ett vanligt ord som innehåller bokstäver, som inte är så vanliga. Då kan det inte motsvara RÖE eller RLE. Ö och L är för vanliga för det. GHH och ÖHH har andra och tredje bokstaven lika, så det kan det heller inte vara. Det som återstår är alltså LNR, som skall motsvara 'och'. Fyll i 'o', 'c' och 'h' på arbetspapperet och i nyckelmallen vid kryptobokstäverna LNR.

Nu hittar ni säkert 'han' och 'hon' och därmed kan ni fylla i den vanliga bokstaven 'n' på arbetspapperet samt i nyckelmallen. Tänk nu efter vilka trebokstavsord i kryptotexten som kan motsvara 'att', 'ett', 'hon' och 'han'. Fyll i arbetspapperet och nyckelmallen.

NU KOMMER NÅGOT MYCKET VIKTIGT! Gå noga, sakta och metodiskt igenom allt vad ni har gjort hittills när det gäller forcering av ES-krypto. Fundera på om det är något som är oklart och försök hitta en rimlig förklaring i så fall. Arbeta steg för steg och kolla att ni inte har missat någon iakttagelse eller gjort något fel. Det är väldigt lätt gjort, särskilt om man är ivrig och har bråttom.

Tänk också på att forceringsarbete kan vara besvärligt. Man gör antaganden som visar sig vara falska och man måste gå något eller några steg tillbaka och testa andra antaganden. Det riktigt roliga kommer när man har lyckats med en uppgift och kan känna den stora forceringsglädjen.

Ni har nog kommit på några bra sätt att ordna arbetet. Tidigare har ni sett att det är bra att alltid använda små bokstäver för klartext och stora för kryptotext. Här är ett tips till. Skriv alla bokstäver som ni är säkra på, med kulspets eller bläck och skriv varje bokstav som ni har gissat eller inte är helt säkra på med blyerts. Då är det lätt att sudda ut felaktigheter utan att de säkra delarna också försvinner.