19. Dubbelt Caesarkrypto

Caesar-krypto har två tydliga svagheter, som gör det lätt att forcera. Den ena är att det finns för få nycklar att välja mellan när man skall kryptera (se grundkursen, avsnitt 11). Den andra svagheten som vi har sett här i avsnitt 17 och 18 är att klartextens språkstatistik även finns lätt synlig i statistiken hos kryptotexten.

Vi skall nu införa ett krypto där kryptonyckeln är dubbelt så stor, dvs består av två tal mellan 1 och 28.

Vi börjar med ett exempel på en kryptotext.

Övning 19A

```
EDLUN SFXEK UKOLS ÅLZBT TÄÖXE QOGMR
PIIKW GMUUZ BNPVQ GSZJR MGWLA XTQSE
DQFRT KYNPT ÖXFMF TURJM FTJTU KSEEJ
GFSDT QBTNK OPVYU TVAFT TGNNÖ XVZFV
ÄVSES OFT
```

Gör pinnstatistik på denna text. Statistiken är påbörjad i tabellen till höger. Pinnarna för de tio första kryptobokstäverna är införda. Fortsätt med resten av kryptotexten

Den liknar inte någon statistik som ni sett förut. Låt oss gissa att varannan bokstav är krypterad med en Caesarnyckel och de övriga med en annan. Gör därför en statistik för bokstäverna med ordningsnummer 1, 3, 5, 7, … och en annan med bokstäverna med ordningsnummer 2, 4, 6, 8, … .

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

Statistikerna är påbörjade här. Pinnar för de tio första kryptobokstäverna är införda. Fortsätt med resten av kryptotexten.

Kryptobokstäver nr 1, 3, 5, …

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	

Kryptobokstäver nr 2, 4, 6, …

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	

Nu ser ni att det blev två Caesarkrypton som ni enkelt forcerar genom att se hur många steg som vardera texthalvan har förskjutits i förhållande till klartexten. Vad står det? Om ni vill kan ni använda två kryptomallar, en för varje nyckeltal. Kryptomallar finns sist i avsnitt 11 i grundkursen. Redigera klartexten d.v.s. skriv den som vanligt med stor bokstav, ordmellanrum och skiljetecken.

Svar: _____

_____

_____

_____

_____

_____

Övning 19B

Arbeta nu var för sig till att börja med. Välj en text, 100 - 150 tecken lång, och två tal mellan 1 och 28 som skall bli Caesar-nycklarna. Håll text och nycklar hemliga. Kryptera nu på samma sätt som i övning 19A, dvs använd nyckeltalen omväxlande för att Caesarkryptera klartextens bokstäver. Byt kryptotext med din kompis och forcera kompisens kryptotext. Gör inte uppgiften svårare än att du själv skulle ha kunnat klara av den.

