26. Enkel transposition

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	

Hittills har ni sett krypton som bygger på att en bokstav ersätts med en annan bokstav, ett annat tecken eller några siffror. Sådana krypton kallas ersättningskrypton eller substitutionskrypton. Enkel substitution (ES-krypto) är exempel på ett sådant. Nu skall ni få arbeta med en annan typ av krypton.

Övning 26A

```
HEEUJGXDD EDOMATTGE MDMRGDELR LESIHENOS
ILTKANSBX GAOERIJXX TNRNLSOAX MDMXAIRNX
```

Börja som vanligt med att göra en monogramstatistik. Använd mallen till höger här på sidan. Vad finner ni?

Monogramstatistiken är väldigt lik den för svensk klartext men ändå är det inte svenska. Den enda rimliga slutsatsen blir att det är ett meddelande på svenska vars bokstäver kastats om (bytt plats) till något obegripligt. Det kallas omkastningskrypto, eller med ett finare ord *transpositionskrypto*. Ni har hela klartexten framför er, det gäller bara att få bokstäverna i rätt ordning.

För att klara av denna övning räcker det med att fylla i kryptotexten kolumnvis i det här rutnätet. Det är påbörjat. Rutan kallar vi transpositionsrutan. Ni ser klartexten med detsamma när ni har fyllt i kryptotexten.

H	E	M					
E	D						
E	O						
U							
J							

Redigerad klartext: _____

_____

_____

Kryptören har skrivit in klartexten radvis (vågrätt) i rutan och sedan läst ut kryptotexten kolumnvis (lodrätt) från vänster till höger. En hel kolumn har blivit en grupp med bokstäver i kryptotexten.

Som ni ser blir den här enkla formen av transpositionskrypto alldeles för lättforcerad. Vi skall beskriva tre sätt att göra kryptot svårare att knäcka.

Det första sättet att förstärka kryptot är att läsa ut kryptotexten kolumnvis som i övning 26A men inte rakt av från vänster till höger utan i en ordning som kryptören och mottagaren kommer överens om och håller hemligt. Detta utgör alltså kryptonyckeln. Dessutom anger denna ordning automatiskt antalet kolumner som skall fyllas i. Först visar vi kryptering och dekryptering i övning 26B. Sedan arbetar ni själva med detta i övning 26C. Till sist tar ni itu med forcering, övning 26D.

Övning 26B

Ni skall kryptera klartexten: *Möt mig vid gamla bron kl. nitton. Kalle*
Kryptonyckeln (utläsningsordningen) är 1 3 2 6 5 4. Ni ser då också att det finns 6 kolumner i transpositionsrutan. Först fyller man i klartexten rad för rad i en transpositionsruta med sex kolumner. För ovanlighetens skull har vi gjort det mesta åt er. Det råkar bli 6 rader också.

1	3	2	6	5	4
m	ö	t	m	i	g
v	i	d	g	a	m
l	a	b	r	o	n
k	l	x	n	i	t
t	o	n	x	k	a
l	l	e	x		

Här blev det några smårutor över. Fyll i dem med 'x' tills vidare.

Det andra sättet att förstärka kryptot är att skriva kryptotexten i femgrupper så att man inte i onödan talar om för en forcör hur stor rutan är. Skriv kryptotexten färdigt här. Ni tar kolumnerna i den ordning som kryptonyckeln (siffrorna) anger.

MVLKT LTDBX NEÖIA_____

Kryptotexten består alltså av 7 stycken femgrupper och en ensam, sista kryptotextbokstav. Kontrollera det innan ni går vidare.

Leta upp de sist inskrivna X-en i kryptotexten. Ni ser nog att de kan vara till hjälp för en forcör när hon/han skall ta reda på i vilken ordning som kryptören har läst ut kryptotexten och hur stor rutan är.

Det är därför dags för det tredje sättet att förstärka kryptot: Fyll i de överblivna smårutorna med vanliga bokstäver, vilka som helst.

Stryk därför över de två sista x-en i rutan och skriv dit två andra bokstäver, vilka som helst. Ändra motsvarande kryptobokstäver i den kryptotext som ni skrivit. Det krypto som vi nu gjort tillsammans kallas *enkel transposition*.

Det sista steget i denna övning är att sätta sig in i hur man skulle dekryptera kryptotexten om det vore ”på riktigt”. Kryptotexten skall ju skrivas in lodrätt i transpositionsrutan (enligt kryptonyckelns ordning). Därför måste ni räkna ut hur många rader som denna skall innehålla. Kryptotexten består av 36 bokstäver, som skall fördelas på 6 kolumner. Antalet rader bör därför bli 36 delat med 6, det vill säga 6 rader. Vi gör en transpositionsruta med 6 rader och 6 kolumner och ovanför skriver vi dit kryptonyckeln (siffrorna som anger vilken ordning som vi skall fylla i kryptobokstäverna:

1	3	2	6	5	4
M		T			
V		D			
L		B			
K		X			
T		N			
L					

Fortsätt att skriva i kryptotextens bokstäver enligt kryptonyckelns ordning och kontrollera att ni får tillbaka klartexten om man läser radvis. Det är enkelt att se skräpbokstäverna på slutet och strunta i dem.

Nu är övning 26B färdig! Men repetera gärna de tre sätten att förstärka kryptot innan ni börjar med nästa övning.

Övning 26C

Detta är en övning där ni övar kryptering och dekryptering med enkel transposition. Ni krypterar var sin klartext. Sedan byter ni kryptotexter och kryptonyckel med varandra och dekrypterar den text som ni fått av kryptokompisen. Till sist diskuterar ni erfarenheter av arbetet.

Vill ni ha fler detaljer om hur ni skall göra, kan ni gå till tips 26C1 längst ner på sidan 6.

Till sist i denna övning skall ni diskutera erfarenheter med varandra. Var det något som var särskilt svårt? Gjorde ni något fel?

Det är väldigt vanligt när man håller på med krypto och inget att skämmas över! Tvärtom kan man lära något av de fel som man gör och man blir säkrare nästa gång.

Övning 26D

Nu skall ni lära er och öva forcering av enkel transposition. Då börjar vi som vanligt med en kryptotext uppdelad i femgrupper.

SEDLI GÄAVR MRNAU VHGNR XRSAE AINMT EITAR

Förutom ett X har denna kryptotext vanliga svenska bokstäver, till och med ett Ä, så vi antar att det rör sig om enkel transposition. Antalet bokstäver är 35. Och 35 är lika med 7 gånger 5. Så vi har möjligheterna att transpositionsrutan har fem kolumner och sju rader eller tvärtom.

Gör två transpositionsrutor på ett särskilt papper, en med 5 kolumner och en med 7 kolumner. Smårutorna bör vara 1 x 1 cm. Fyll i kryptotexten kolumnvis från vänster:

S	G	M				
E	Ä	R				
D	A	N				
L	V					
I	R					

S	A			
E	V			
D	R			
L	M			
I	R			
G				
Ä				

Försök avgöra vilken ruta som ser mest trolig ut.

Nu gäller det att ta reda på i vilken ordning kolumnerna skall stå för att ni skall kunna läsa klartexten radvis. Det görs enklare om ni klipper ut kolumnerna i transpositionsrutan för det troligaste alternativet.

Lägg nu kolumnremsorna i en ordning så att ni kan läsa klartext radvis. Det kan behövas några försök för det. Ni kan använda en bigramstatistik från avsnitt 24 eller kanske hitta ett sannolikt ord.

Om det inte går med den transpositionsruta ni valt, får ni pröva att göra samma sak med den andra.

Övning 26E

Nu är ni mogna att arbeta friare med enkel transposition. Ni kan utmana varandra i forcering.

Först arbetar ni var och en för sig. Bestäm var sin kryptonyckel för enkel transposition och hitta på var sin klartext som ni krypterar med nyckeln. Byt kryptotexter, skrivna i femgrupper, med varandra men lämna inte ut kryptonyckeln eller annat arbetspapper.

Forcera sedan din kryptokompis text. Gör inte uppgiften onödigt svår och i alla fall inte svårare än att du själv skulle kunna ha knäckt den. Var beredd att lämna tips om din kompis kört fast.

Prata sedan med varandra om hur ni tänkt när ni konstruerat uppgifterna och löst kompisens.

Tips 26C1:

Arbeta först var för sig. Var och en av er väljer en nyckel till enkel transposition, det vill säga hur många kolumner transpositionsrutan skall ha och i vilken ordning kryptotexten skall läsas ut i rutan. Hitta sedan på en klartext och skriv in den vågrätt rad för rad på ett rutat papper, (helst med encentimetersrutor) som vi gjort i övning 26B. Läs sedan ut kryptotexten lodrätt i den ordning som du har bestämt och skriv den i grupper om fem stora bokstäver.

Till din kryptokompis lämnar du sedan din kryptotext (alltså skriven i femgrupper) samt kryptonyckeln, det vill säga den ordning som använts för att läsa ut bokstäverna ur rutan. Du skal inte lämna klartexten eller den transpositionsruta som du själv har använt för krypteringsarbetet.

Sedan dekrypterar du den kryptotext som du fått av din kompis. Först måste du räkna ut hur många rader som transpositionsrutan skall ha (antalet bokstäver i kryptotexten delat med antalet kolumner). Sedan gör du upp en transpositionsruta som passar och skriver in kryptotexten i den. Det gör du i den ordning som kryptonyckeln anger. Du hittar då klartexten, skriven vågrätt i transpositionsrutan. Redigera klartexten, det vill säga skriv den med ordmellanrum och med stor bokstav, där det skall vara det, och sätt ut skiljetecken.

