11. Forcering av Caesarkrypto och enkel substitution – lärarsida

Att forcera Caesar-krypto är inte så svårt. Antalet möjliga nycklar är bara 28. En lämplig teknik för denna forcering presenteras i elevmaterialet nedan. Det kan vara bra att ha centimeterrutat papper till hands. Den sista sidan innehåller några tomma krypteringsnycklar.

Kommentarer, ledtrådar och facit:

Övning 11A: När eleverna har hittat klartextbörjan ”jag har...” blir det lätt så att de fortsätter att rulla kryptotexten åtminstone ner till klartextraden. Det är onödigt arbete. Det blir enklare om man först forcerar kryptonyckeln och sedan dekrypterar kryptotexten till klartext. Så bör vi göra även i denna kurs. Det sparar en hel del arbete. Därför kan det vara lämpligt att gå igenom hela detta exempel på tavlan. Eleverna kan sedan lösa nästa uppgift (nästan) helt själva eller två och två. Svar: Jag har hundra kronor i månaden.

Övning 11B: Svar: Hemligt språk är bra att kunna.

Övning 11C: Om eleven använder en Caesar-nyckel med omvänt alfabet, fungerar inte den forceringsmetod som behandlats. Då måste man först ”vända” kryptotexten genom att ersätta dess bokstäver så här: A->Ö, B->Ä, C->Å,..., Ä->B, Ö->A. Den mellantext man då får kan man forcera genom att rulla den på känt sätt.

Övning 11D: Eleverna börjar förmodligen genast att rulla några av de första bokstäverna i kryptotexten. Fem, sex bokstäver kan vara bra. Men klartext hittar de inte på en rad. Var är den då? Man kan tipsa om att leta på något annat sätt än rakt. Om inte det heller hjälper kan eleverna fundera på om det finns något ”sannolikt ord” i början av texten. Då hittar de nog ”hemlig...” och sedan kommer resten lätt fram. I detta exempel finns det ingen kryptonyckel att rekonstruera som underlättar dekrypteringsarbetet.
Svar: Hemligt meddelande om discot.

Enkel substitution (ES-krypto)

Det är ju synd att det är så lätt att forcera Caesar-krypto. Med ES-krypto tar vi ett steg mot ett mer svårknäckt krypto. Enkel substitution ställer än mer krav på noggrannhet hos eleverna.För att enklare kunna tillverka egna kryptonycklar finns i slutet av detta avsnitt mallar som man kan fylla med en kryptonyckels bokstäver.

Facit
Övning 11E: Svar: Lovdag i morgon.
Övning 11G: Svar: Kalle Blomkvist

Forcera Ceasarkrypto

Att forcera betyder att ta fram klartexten ur en kryptotext utan att känna till kryptonyckeln på förhand. Kryptotexten här är skriven i grupper om fem bokstäver. Då blir den enklare att hantera.

Övning 11A

Forcera det här kryptot:

Kryptotext: YPVWP DWGÖS DPZDA ÖADXÄ MÖPST Ö

Skriv några bokstäver till av kryptotexten överst i rutnätet här nedan. Skriv sedan lodrätt i alfabetsordning. Att skriva alfabetet lodrätt så här kallas att rulla kryptotexten.

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

Klartexten hittar du på en rad. Vilken? När du vet det, är det lätt att lista ut kryptonyckeln. Fyll i den.

Klartext	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
Krypto	P						V	W		Y																			

Nu behöver du inte rulla mera kryptotext. Det är bara att använda kryptonyckeln och dekryptera som du lärt dig i förra avsnittet.

Klartext: _____

_____

Redigerad klartext: _____

_____

Övning 11B

Här är en kryptotext till som hör till Caesarkrypto.

Kryptotext: KHPOL JWVSU ANBUE UDDWW NXQQD

Använd papper med rutor som är kvadrater med sidan 1 cm. Om du börjar allra överst på en A4-sida får du precis plats med de rullade alfabetena. Rulla några bokstäver i början av kryptotexten så att du kan ta reda på början av klartexten. Då kan du lista ut kryptonyckeln och det blir enkelt att dekryptera. Du kan använda en kryptonyckelmall.

Redigerad klartext: _____

_____

Övning 11C

Kryptera och låt en kompis forcera

Nu skall du göra en egen kryptonyckel till Caesar-kryptot och hitta på en egen klartext. Sedan krypterar du klartexten med nyckeln. Se till att din kryptokompis inte får se kryptonyckeln eller klartexten. Sedan lämnar du kryptot till kompisen så att hon/han får forcera fram klartexten. Forcera det krypto som du får av din kompis.

Forcering av ett okänt krypto

Övning 11D

Här är en kryptotext som hör till ett okänt krypto. Det kanske påminner om Caesarkrypto? Kan du lista ut vad det står? Det kan vara bra att ha ett tomt centimeterrutat papper.

Kryptotext: GCJHD AMEYW VVÄPÄ QQZWM QZITX

Redigerad klartext: _____

_____

ES-krypto

Det är synd att Caesarkrypto är så lätt att forcera. Det beror på att kryptobokstäverna kommer i alfabetsordning i kryptonyckeln. Titta på den första kryptonyckeln på den här sidan. Där kommer kryptobokstäverna i oordning. Om man använder en sådan nyckel när man krypterar säger man att man använder ES-krypto. Det är svårare att forcera än Caesar-krypto. ES står för Enkel Substitution.

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

Övning 11E

Här är en kryptotext som man gjort med denna nyckel. Vad står det? Kryptobokstäver är stora och klartextbokstäver små. Om du tänker på det blir det inte så lätt fel.

Kryptotext: AÖNCQ TRVÖÅ TÖY

Redigerad klartext: _____

_____

Som du märker tar det lång tid att dekryptera trots att kryptotexten är så kort. Det beror på att man måste leta efter kryptobokstäverna i kryptonyckeln. De står ju inte i alfabetsordning. Men du kan göra en särskild kryptonyckel för dekryptering. Den som står här nedanför hör till kryptonyckeln som du nyss använt. Den är påbörjad. Gör den färdig. Ta det lugnt! Annars blir det lätt fel.

Klartext	l	t	d	p	ä	x	b	h	s	ö	z	k	c	v	y														
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

Övning 11F

Hitta nu på en egen klartext, inte för lång, helst inte längre än 20 bokstäver. Kryptera den med nyckeln på förra sidan och byt krypto med din kryptokompis och dekryptera det meddelande som du får.

Nu ska du få veta hur man kan göra en nyckel till ES-krypto som blir lättare att komma ihåg och att använda.

ES-krypto med nyckelord

Nu skall vi göra en kryptonyckel till ES-krypto som är lätt att komma ihåg och som det är ganska lätt att hitta kryptobokstäverna i.

Först skall vi hitta på ett nyckelord. Det skall vara långt: Vi börjar med MÄSTERDETEKTIVEN. Nyckelordets bokstäver skriver vi in från vänster på platsen för kryptobokstäverna i en nyckelmall. Där skall bokstäverna vara olika så du måste hoppa över de bokstäver som vi redan skrivit in. Då ser det ut så här:

Klartext	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
Krypto	M	Ä	S	T	E	R	D	K	I	V	N																		

Resten av bokstäverna i alfabetet skriver du efter kodordet. Då blir det så här:

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

Alla bokstäver i alfabetet skall finnas med i raden för kryptobokstav.

Nyckelordet måste man hålla hemligt så att obehöriga inte får se det! Annars kan det hända att de kan lista ut vad du har skrivit.

Övning 11G

Dekryptera den här kryptotexten med kryptonyckeln som vi nyss gjort.

Kryptotext: NMAAE ÄAFBN QILO

Klartext: _____

_____

Övning 11H

Nu skall ni göra en egen kryptonyckel med hjälp av ett kodord. Arbeta först tillsammans med din kryptokompis. Hitta på ett långt kodord. Fyll i det i kryptonyckelmallen och hoppa över bokstäver som redan står där. Fortsätt med resten av bokstäverna i alfabetet. Alla bokstäverna i alfabetet måste vara med.

Klartext	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
Krypto																													

Sedan arbetar ni var för sig. Hitta på en lagom lång klartext och kryptera den med nyckeln som ni nyss gjort. Byt krypto med din kompis och dekryptera.

Klartextbokstav	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
Kryptobokstav																													

Klartextbokstav	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
Kryptobokstav																													

Klartextbokstav																													
Kryptobokstav	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

Klartextbokstav																													
Kryptobokstav	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

Internationella alfabetet

Klartextbokstav	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
Kryptobokstav																										