10. Caesarkrypto – lärarsida

Med detta och följande avsnitt blir det något svårare. Det finns också här fler övningar som man kan använda om man behöver det. Med Caesar-krypto skall texten i ett meddelande ersättas, bokstav för bokstav, genom att man som kryptobokstav tar den som ligger ett visst antal steg längre fram, t.ex. fyra, i alfabetet. Om den första klartextbokstaven är h blir den första kryptobokstaven L.

En kryptosnurra kan vara praktisk och intressant för eleverna. En sådan har tidigare presenterats i Nämnaren nr 4 år 2001.

För att enklare kunna tillverka egna kryptonycklar finns i slutet av detta avsnitt mallar som man kan fylla med en kryptonyckels bokstäver.

Det är viktigt att skilja på klartext- och kryptobokstäver. Därför använder vi små bokstäver i klartexter och STORA bokstäver i kryptotexter. När man krypterar kan man säga högt eller tyst: ”lilla t blir stora X, Lilla j blir stora N ...” När man dekrypterar säger man på motsvarande sätt: ”...stora Y blir lilla u, stora Z blir lilla v”.

På sidan 8 finns tomma kryptonyckelmallar som kan vara användbara i flera av uppgifterna.

Svar

Övning 10A: Svar: Vem är tjuven?

Övning 10B: Svar: Anders är inte tjuv.

Övning 10C: Svar: XNYZI RWXEP FBXIR
”tjuv” har hittills alltid blivit ”XNYZ”

Övning 10D: Svar: WCIÄJ KSÖIÅ YHÖSI S ”tjuv” blev nu ”IÄJK”

Övning 10F: Svar: ZJÖRF GRÖHG DPHRE EJD

Övning 10G: Svar: Kom inte till kojan i kväll!

Caesarkrypto

Detta krypto har använts för 2000 år sedan av den romerske kejsaren Julius Caesar.

När man krypterar med Caesar-krypto letar man upp en klartextbokstav i alfabetet och går sedan ett visst antal steg framåt. Den bokstav man då träffar på är kryptobokstaven.

Vi börjar med dekryptering

Övning 10A

Här är ett exempel på en kryptotext till ett Caesar-krypto:

Kryptotext: Z I Q C V X N Y Z I R ?

Skriv kryptotexten i rutor. Skriv alltid kryptotexten med STORA bokstäver. Översätt till klartext. Det kallas att dekryptera. Gå fyra steg tillbaka i alfabetet eller använd kryptonyckeln som står nedanför. Skriv alltid klartexten med små bokstäver.

Kryptotext	Z	I	Q	C	V	X	N	Y	Z	I	R
Klartext	v	e	m								

Skriv klartexten som vanlig svensk text. Det kallas att redigera klartexten efter dekryptering.

Redigerad klartext: Vem_____?

Kryptonyckel:

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	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	A	B	C	D

Övning 10B

Här är en övning till på dekryptering

Kryptotext: ERHIV WCVMR XIXNY Z

Kryptotext	E															
Klartext	a															

Redigerad klartext: And_____

Nu skall vi kryptera.

Att kryptera betyder att översätta från klartext (som man kan förstå) till kryptotext som man inte förstår. Skriv in klartexten i tabellen och kryptera. Gå fyra steg framåt i alfabetet eller använd kryptonyckeln som står på förra sidan. Skriv klartexten med små bokstäver och kryptotexten med stora bokstäver.

Övning 10C

Klartext: Tjuven stal båten.

Klartext	t	j														
Kryptotext	X	N														

Skriv kryptotexten med fem bokstäver i taget. Använd STORA bokstäver.

Kryptotext: XN_____.

Man säger att man skriver kryptotexten i femgrupper. Kolla resultatet med en kompis.

Byta nyckel

Om man alltid använder samma nyckel blir ett ord alltid likadant när man krypterar. Till exempel blev ordet tjuv alltid, ja vad då, med nyckeln på förra sidan:

_____.

Så blir det inte om man byter kryptonyckel. Vi tar den här nyckeln i stället.

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

Övning 10D

Kryptera den här klartexten: En tjuvaktig skata.

Klartext																
Kryptotext																

Vad blev klartextordet tjuv nu: _____. Kolla resultatet med en kompis.

Nu skall du göra en ny kryptonyckel, kryptera och dekryptera.

Övning 10E

Hitta på en egen Caesarnyckel tillsammans med din kryptokompis och skriv den i en kryptonyckelmall.

Hitta på en egen klartext och kryptera den med den kryptonyckel som ni har gjort. Byt krypto med kompisen och dekryptera det meddelande som du får.

Caesarkrypto med omvänt nyckelalfabet

Titta på den här nyckeln. Vad är det för speciellt med 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	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Ö	Ä	Å	Z	Y	X	W	V	U	T	S

Just det, här står kryptoalfabetet baklänges. Klartextbokstaven e motsvarar kryptobokstaven N och klartextbokstaven n motsvarar kryptobokstaven E. När man krypterar gör det alltså ingenting om man någon gång läser åt fel håll i nyckeln. Samma sak gäller när man dekrypterar. Det kan vara praktiskt ibland.

Börja med att kryptera.

Övning 10F

Klartext: Vi samlas klockan nio.

Förbered klartexten genom att skriva den glest. Skriv kryptotexten under. Använd nyckeln med det omvända nyckelalfabetet som står överst på denna sida.

Klartext: v i s a m l a s k l o c k a n n i o

Kryptotext: Z J _____

Kryptotext i femgrupper:

_____

Nu skall vi dekryptera.

Övning 10G

Vad står det här: H D F J E Ä N Ä J G G H D I R E J H Z T G G

Klartext: k o m _____

Redigerad klartext:

_____

Nu skall du göra en ny kryptonyckel, kryptera och dekryptera.

Övning 10H

Hitta på en egen Caesarnyckel med omvänt nyckelalfabet tillsammans med din kryptokompis och skriv den i en kryptonyckelmall.

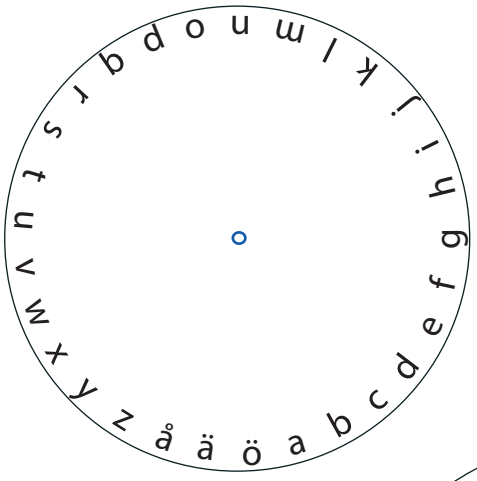
Hitta på en egen klartext och kryptera den med den kryptonyckel som ni har gjort. Byt krypto med kompisen och dekryptera det meddelande som du får.

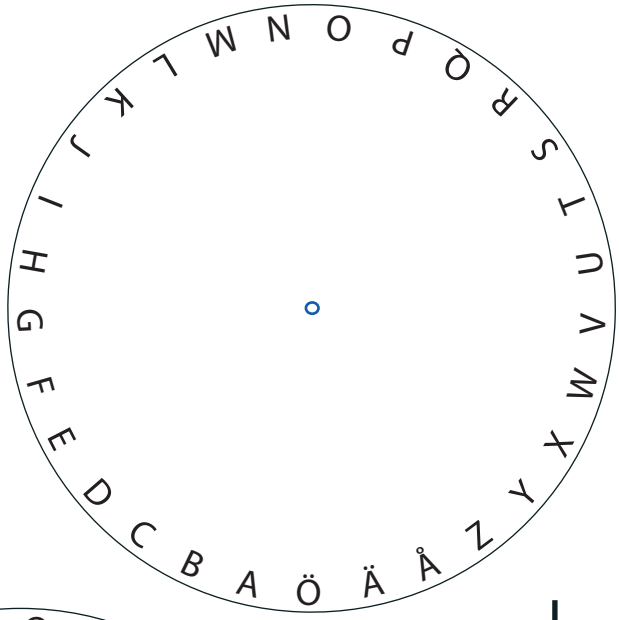
Gör en egen kryptosnurra

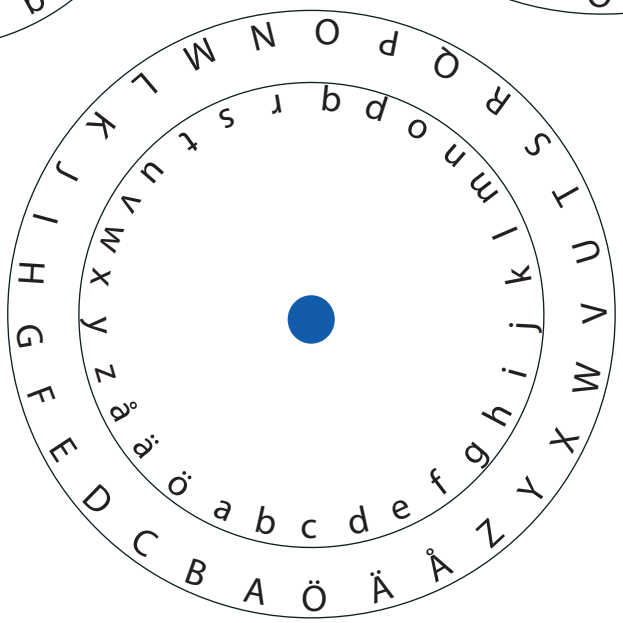
Du kan ha kryptonyckeln på två runda pappskivor som du sätter ihop med en pappersklämma i mitten. Du kan använda cirklarna på denna sida som mall.

Det kan vara praktiskt att använda Caesarnycklar med omvända alfabeten. Då blir det lättare att kryptera rätt.

För att ställa in en nyckel vrider du den ena skivan medan du håller den andra stilla. Bestäm hur skivorna skall stå. Du kan till exempel säga ”Vecka 27 ställer vi p mot Å på kryptoskivan”.







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																										