Nämnarens kryptoskola

1. Introduktion

Ett omfattande studiematerial som behandlar krypto – hemlig skrift finns nu utlagt på NCM:s webbsida. I denna första del följer en presentation av dess innehåll. De andra delarna finner du på ncm.gu.se/arkivN. De olika delarna i Kryptoskolan är skyddade av upphovsrättslagen, men får dock fritt kopieras för användning i undervisning eller för enskilt arbete och rekommenderas från årskurs 4 till gymnasiet.

Hur bevarar man en hemlighet? Och hur delar man med sig en hemlighet utan att den kommer fel person till del, ett problem som bekymrat och sysselsatt många människor i flera tusen år. I Havamal kan vi läsa: ”...det som tre veta det vet hela världen.” Givetvis är detta problem starkt knutet till skrivkonsten och så länge den har funnits har man brottats med detta problem. Det är i vissa fall en fråga om liv eller död. Om känslig information kommer fienden till del kan hans arbete/uppgift att tillintetgöra sin fiende underlättas.

Om man ristar in ett meddelande i huvudsvålen på en kurir som måste resa genom fiendeland – fungerar det? Kan man blanda ett hemligt meddelandes ord med andra till ett nytt som ser oskyldigt och ointressant ut? Ger fototekniken möjligheten att förminska en karta eller ett meddelande så att det undgår upptäckt? Finns det osynligt bläck som kan framkallas med uppvärmning eller bestrykning med lämpliga kemikalier? Eller med modernare teknik, kan man dölja ett skriftligt meddelande i ett fax eller på annat sätt digitaliserad bild? Hur går det till att dölja ett kortare meddelande bland den enorma mängd data som bildas, kommuniceras och lagras?

Alla dessa metoder har med varierande framgång prövats och använts i verkligheten. Nja, metoden att dölja en text i håret på en kurir, får vi nog ta med en nypa salt. De sätt att dölja ett meddelande som antytts ovan går in under begreppet *steganografi*. Men det här materialet skall vi ägna åt *kryptering*, dvs hur man döljer innehållet i ett meddelande genom att ersätta dess bokstäver med andra bokstäver, siffror eller andra tecken. Det skall ske på ett sådant sätt att den som inte är insatt i alla aspekter av förfarandet inte kan få reda på innehållet – i varje fall inte utan tidsödande arbete. Dock skall den behörige mottagaren, den för vilken meddelandet är avsett, givetvis enkelt kunna ta fram vad avsändaren menat.

Kokrorypoptotokokurorsos

Vad står det i rubriken till detta stycke? Den är skriven på rövarspråket, som blev bekant för den svenska läsekretsen, såväl unga som gamla, när Astrid Lindgrens böcker om Kalle Blomkvist kom ut. Men vad betyder det här:

ZAXLZ LXOZR XTZNX AZKXR ZEXTZ TXOZP XYZRX RZAXH

...eller det här:

KTLGOAT OIMKCNT MLILKÅA ?

Hur man tar reda på vad det står och hur man lär sig att *kryptera* och *dekryptera* (översätta en krypterad text tillbaka till den begripliga klartexten) på många olika sätt kan du lära dig och lära ut till andra med ett undervisningsmaterial på hemsidan.

Materialet tränar språkkänslan för elever från 10-årsåldern och uppåt. Barnen har då erövrat ett användbart skriftspråk och dessutom kommit till en ålder då hemligheter är spännande och viktiga. Det stärker elevernas förmåga till logiska resonemang och slutledningsförmåga. Materialet stimulerar deras kunskaper i svenska och blir en god tillämpning av alfabetet samt begreppen vokal och konsonant. Det premierar noggrannhet – annars blir det fel resultat – och det kan användas av ungdomarna när de vill hålla andra personer, barn såväl som vuxna, utanför sin sfär av hemligheter.

Undervisningsmaterial i elva avsnitt.

Undervisningsmaterialet är indelat i elva avsnitt. Det första avsnittet är en lärarhandledning med en översiktlig presentation av materialet, en kort historisk inledning samt en ordlista. Varje avsnitt innehåller kopieringsunderlag som är avsedda att lämnas till eleverna. Avsnitten inleds med fakta för läraren eller den som annars leder undervisningen. Där finns också detaljerade kommentarer och facit till uppgifterna. Man behöver givetvis inte använda hela materialet utan kan välja de avsnitt som är lämpliga med hänsyn till elevernas mognad och tillgänglig tid.

Huvuddelen av materialet är utprovat med några grupper om fyra till tolv elever i år 4 - 5 under ”elevens fria val”. De flesta eleverna har tyckt att hemlig skrift är väldigt spännande. Materialet kan givetvis inte bara användas av lärare i skolan utan även av föräldrar som vill ge sina barn något ovanligt och spännande att syssla med. Också de matematikklubbar som växer fram hittar många lämpliga uppgifter som kan engagera medlemmarna.

Kryptologi = matematik + språk

Kryptologi är läran om kryptering och *forcering*. Forcering betyder att man ur en till synes obegriplig kryptotext tar fram den sammanhörande begripliga klartexten utan att exakt veta hur det gått till att med kryptering förvandla klartexten till kryptotext. Som vetenskap innehåller kryptologin både matematik och språkkunskap. Låt oss som illustration till denna förening studera ett mycket enkelt krypto, nämligen Caesar-kryptot.

Texten i ett meddelande skall ersättas, bokstav för bokstav, genom att man som kryptobokstav tar den som ligger ett visst antal steg, säg tills vidare fyra, längre fram i alfabetet. Om den första klartextbokstaven är h blir den första kryptobokstaven L.

Det tal som styr krypteringen behöver inte vara just 4 utan vilket annat heltal som helst mellan 1 och 28; vi kallar det i det följande för kryptonyckeln och betecknar den N, $1 < N < 28$. Den som bestämmer nyckeln får överlämna den till den andra personen på ett säkert sätt t. ex. vid ett sammanträffande.

> Med en matematisk formel kan man beskriva krypteringsförfarandet så här:
> C = K + N (mod 29), där (mod 29) här betyder att vi subtraherar 29 om summan blir större eller lika med 29.

Det är bra att ha en översättningstabell mellan bokstäver och tal:

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28

Låt oss nu kryptera klartexten *Tjuven stal båten* med nyckeln N = 9 (mod 29). Fortsätt gärna att fylla i följande tabell.

Klartext	t	j	u	v	e	n	s	t	a	l	b	å	t	e	n
Klartext m. tal	19	9	20	21											
Addera nyckel	9	9	9	9											
Kryptotext m. tal	28	18	0	1											
Kryptotext	Ö	S	A	B											

Kryptots historia

Kryptots historia är mycket lång. Det visar bland annat det 2000 år gamla Caesar-kryptot som beskrivits ovan. Egentligen är väl krypteringskonsten en naturlig följd av skrivkonsten. Så snart man kan dokumentera sina tankar dyker också behovet upp att dölja dessa för obehöriga.

Det finns många intressanta händelser inom kryptots historia under århundradenas gång. Visste du till exempel att världens första mekaniska krypteringsapparat var svensk och konstruerad av en dotterson till Christofer Polhem?

Ett annat exempel: Under andra världskriget hyrde tyskarna telegrafledningar, bland annat mellan Berlin och ockupationsmakten i Oslo. Ledningarna avtappades i Sverige och en svensk matematiker lyckades knäcka kryptot. Det blev en mycket värdefull underrättelsekälla för Sverige, som på det sättet fick god kännedom om tyska truppers rörelser i Norge. Vi kunde bland annat med stor säkerhet avgöra att tyskarna inte planerade någon invasion av Sverige över gränsen i väster.

Och till sist: Kan man använda kvantfysikens märkliga egenskaper för att konstruera oforcerbara krypton? Eller för att forcera hittills oknäckta krypton? Det har man börjat att fundera på under den senaste tiden.

Ordförklaringar

*K*rypto – Hemligt språk. Krypto kan också betyda en viss metod för kryptering. I så fall heter det krypton i pluralis. I talspråk kan krypto också betyda kryptomeddelande.

*K*lartext – Text som kan förstås utan att man behöver använda en hemlig metod och/eller hemlig kryptonyckel.

*K*ryptera – Översätta en klartext till kryptotext med hjälp av krypto och kryptonyckel.

*K*ryptotext – Resultat av kryptering. En kryptotext kan man inte förstå utan att den först dekrypteras.

*D*ekryptera – Återföra en kryptotext till klartext med hjälp av ett krypto och oftast en hemlig kryptonyckel.

*K*ryptonyckel – Data som styr hur man krypterar och dekrypterar med ett visst krypto.

*S*teganografi – Metod för att dölja förekomsten av en text, t. ex. genom att använda osynligt bläck.

*F*orcering – Att ta fram klartexten som hör till en kryptotext utan att på förhand känna till den använda kryptonyckeln.

Nämnarens kryptoskola

2. Krypto – språk och matematik

Denna andra del av Kryptoskolan belyser kopplingar mellan språk och matematik. De andra delarna finner du på ncm.gu.se/arkivN. Kryptoskolan är ett studiematerial som är skyddat av upphovsrättslagen. Studiematerialet får dock fritt kopieras för användning i undervisning eller för enskilt arbete och rekommenderas från årskurs 4 till gymnasiet.

Med kryptering menar vi hur man döljer innehållet i ett meddelande genom att ersätta dess bokstäver med andra bokstäver på ett sådant sätt att den som inte är insatt i alla aspekter av förfarandet inte kan få reda på innehållet. Men givetvis skall den behörige mottagaren, den för vilken meddelandet är avsett, enkelt kunna ta fram vad avsändaren menat.

Med dekryptering avser vi den omvända processen, dvs att ur en given kryptotext, med full kännedom om hur avsändaren förfarit för att tillverka denna, ta fram den bakomliggande klartexten. Om den som gör detta inte exakt vet hur krypteringen har gått till talar vi om forcering.

Caesar-krypto

Det enklaste kryptot kallas Caesar-kryptot, benämnt efter den romerske härskaren med samma namn. Det går till så här:

Texten i ett meddelande skall ersättas, bokstav för bokstav, genom att man som kryptobokstav tar den som ligger ett visst antal steg längre fram i alfabetet, säg tills vidare tre steg, Om den första klartextbokstaven är *h* blir den första kryptobokstaven *K*.

Det tal som styr krypteringen behöver inte vara just tre utan vilket annat heltal som helst mellan 1 och 28; vi kallar detta tal för kryptonyckeln och betecknar den med N, $1 < N < 28$. Den som bestämmer nyckeln får överlämna den till den andra personen på ett säkert sätt t ex vid ett personligt möte.

Med en matematisk formel kan man beskriva krypteringsförfarandet så här:

$$C = K + N \pmod{29}$$

där (mod 29) här betyder att vi subtraherar 29 om summan blir större eller lika med 29. Talet 29 står för antalet bokstäver i det svenska alfabetet, *W* medräknat. Vi behöver en översättningstabell mellan bokstäver och tal:

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28

Låt oss nu kryptera klartexten *Tjuven stal båten* med kryptonyckeln N = 9. Kom ihåg att räkna (mod 29). Fortsätt att fylla i följande tabell:

Klartext	t	j	u	v	e	n	s	t	a	l	b	å	t	e	n
Klartext m. tal	19	9	20	21											
Addera nyckel	9	9	9	9											
Kryptotext m. tal	28	18	0	1											
Kryptotext	Ö	S	A	B											

Om man vill *dekryptera* en text, dvs återföra kryptotexten till klartext, utför man proceduren omvänt, alltså subtraheras kryptonyckeln från kryptotexten i talform bokstav för bokstav. Men det kan vara intressant att notera att inversen till addition med N (mod 29) kan utföras som addition med 29 - N (mod 29), eller i formler:

$K = C - N \pmod{29} = C + (29 - N) \pmod{29}$.

Använd denna metod för att dekryptera kryptotexten i föregående exempel. Dekrypteringsnyckeln blir 29 - 9 = 20.

Kryptotext	Ö	S	A	B											
Kryptotext m. tal	28	18	0	1											
Addera nyckel	20	20	20	20											
Klartext m. tal	19	9	20	21											
Klartext	t	j	u	v											

Om man i stället vill arbeta med det internationella 26-bokstavsalfabetet, alltså utan *å*, *ä* och *ö*, kan man använda metoderna ovan utan problem. Krypterings- respektive dekrypteringsformlerna blir då

$C = K + N \pmod{26}$

där $0 < C, K < 26$ och kryptonyckeln N uppfyller $0 < N < 26$ och

$K = C + (26 - N) \pmod{26}$.

Kryptering med multiplikation

Hur blir det om vi ersätter Caesar-kryptots addition med multiplikation? Låt oss undersöka det. Krypteringsformeln skulle i så fall se ut så här:

$C = N \times K \pmod{29}$
där $0 < C, K < 29$ och kryptonyckeln N uppfyller $2 < N < 29$.
(Fundera på varför vi undantar N = 1.)

Vi kan behöva subtrahera talet 29 några gånger så att resultatet hamnar i rätt intervall: från 0 till 28. En krypteringstabell ser ut så här för N = 4:

Klar	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
Klar m. tal	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Krypto m. tal	0	4	8	12	16	20	24	28	3	7	11	15	19	23	27	2	6	10	14	18	22	26	1	5	9	13	17	21	25
Krypto	A	E	I	M	Q	U	Y	Ö	D	H	L	P	T	X	Ä	C	G	K	O	S	W	Å	B	F	J	N	R	V	Z

Det här ser ju bra ut. Alla bokstäver förekommer i kryptoraden en och endast en gång. Det är tillräckligt för att vi skall kunna kryptera alla bokstäver och dekryptera entydigt. Detta kan man bevisa enkelt för alla nycklar, inte bara för N = 4. Om två klartextbokstäver K_1 och K_2 krypterade med nyckeln N skulle ge samma kryptobokstav skulle vi ha

$N \times K_1 = N \times K_2 \pmod{29}$ eller
$N \times (K_1 - K_2) = 0 \pmod{29}$, vilket är det samma som att
$N \times (K_1 - K_2) = m \times 29$ för något heltal m.

Eftersom 29 är ett primtal måste då någon av faktorerna i vänsterledet vara delbar med 29. Men så är inte fallet. Båda är ju högst 28 i absolutbelopp.

Låt oss gå över till dekryptering. Det omvända till multiplikation är ju division, men det verkar ju inte helt glasklart hur man skall beräkna C/N (mod 29). I fallet med Caesar-kryptot kunde vi ersätta subtraktion med addition; kan vi ersätta division med multiplikation? Vi försöker först med N =4.

$C = 4 \times K \pmod{29}$ och vi söker dekrypteringsnyckeln D, så att
$K = D \times C \pmod{29}$. Insättning ger
$K = D \times 4 \times K \pmod{29}$ och det skall gälla för alla K.

Detta kan vi uppnå om vi kan hitta ett heltal D så att

$D \times 4 = 1 \pmod{29}$ eller
$D \times 4 - 1 = m \times 29$ för något heltal m.

Den som är hemma i användningen av Euklides algoritm kan pröva med den. Annars går det bra att testa med några olika värden på m och se om *D* blir ett inte för stort heltal. Då finner man att m = 3 ger D = 22.

Om vi krypterar genom att multiplicera med 4, kan vi alltså sedan dekryptera med multiplikation med 22. Och så gäller det att subtrahera 29 tillräckligt många gånger så att resultatet håller sig inom intervallet från 0 till 28. Med samma teknik kan vi hitta den multiplikativa inversen till varje N (mod 29).

Men kan vi lika lätt använda ett sådant här multiplikationskrypto om vi begränsar oss till det internationella 26-bokstavsalfabetet? Vi kanske erinrar oss att för beviset om kryptots en-entydighet utnyttjades att 29 är ett primtal. Och talet 26 kan uppdelas $26 = 2 \times 13$. Låt oss se vad som händer om vi försöker med krypteringsformeln

$C = 4 \times K \pmod{26}$.

Motsvarande krypteringstabell skulle bli

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
Klar med tal	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Krypto m. tal	0	4	8	12	16	20	24	2	6	10	14	18	22	0	4	8	12	16	20	24	2	6	10	14	18	22
Kryptobokstav	A	E	I	M	Q	U	Y	C	G	K	O	S	W	A	E	I	M	Q	U	Y	C	G	K	O	S	W

Det här blir inget krypto. Funktionen är inte en-entydig. Exempelvis ger båda klartextbokstäverna *h* och *u* kryptobokstaven C. Det går inte att dekryptera, vilket inte är så förvånande. När vi multiplicerar med det jämna talet 4 så förblir produkten jämn hur många gånger vi än subtraherar det jämna talet 26.

Talet 13 kan vi inte heller ha som nyckel. Då får vi bara kryptobokstäverna *A* och *B*. Generellt får en kryptonyckel för multiplikationskryptot med 26-bokstavsalfabetet inte ha någon primfaktor som finns i 26, dvs 2 eller 13. Som möjlig kryptonyckel återstår det endast 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, och 25.

Enkel substitution

Låt oss gå ett steg till och definiera ett krypto där kryptotabellens alfabet för kryptobokstäver är slumpmässigt utplacerade. Kryptonyckeln består i den substitution/funktion som tabellen definierar. Här är ett exempel.

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

Låt oss kryptera texten *Ada och Kal badar* med denna nyckel.

Klartext	a	d	a	o	c	h	k	a	l	b	a	d	a	r
Kryptotext	Q	C	Q	Ö	M	H	L	Q	A	G	Q	C	Q	Å

Om man vill beskriva enkel substitution med en formel kommer man inte längre än till att skriva

$C = \mathcal{N}(K)$ för kryptering och $K = \mathcal{N}^{-1}(C)$ för dekryptering

Där $\mathcal{N}$ är funktionen som definieras av substitutionstabellen och $\mathcal{N}^{-1}$ dess invers.

Forcering

Kan den som snappat upp en kryptotext härleda den tillhörande klartexten utan att på förhand känna till den använda nyckeln? Eller med andra ord, hur lätt är det att knäcka de krypton som beskrivits ovan?

Caesar-kryptot har bara 28 olika nycklar. Det är bara att provdekryptera med dessa nycklar och den som ger läsbar klartext är den rätta. Hur detta arbete kan utföras praktiskt på ett enkelt sätt beskrivs i studiematerialet. Multiplikationskryptot har ännu färre nycklar, så det är inte svårare att knäcka.

Läsaren har nog redan märkt en annan svaghet i de multiplikationskrypton som vi behandlat hittills. Klartextbokstaven a blir alltid kryptobokstaven A oberoende av vilken nyckel som används. Det kan man undvika genom att använda två nyckeltal, N_1 och N_2 och krypteringsformeln $C = N_1 \times K + N_2 \pmod{29}$. Då blir det visserligen några fler nycklar att pröva, men forceringsarbetet blir endast obetydligt svårare.

Hur svårt är det att forcera enkel substitution? Låt oss först beräkna hur många nycklar som kryptot har. I substitutionstabellen som definierar kryptonyckeln kan vi placera ut kryptobokstaven *A* på 29 ställen. Då återstår 28 platser för *B*. Dessa två kan alltså sättas ut på 29×28 olika sätt. För *C* finns nu 27 platser och för de tre första $29 \times 28 \times 27$ sätt. Så fortsätter vi och finner att det finns $29 \times 28 \times 27 \times \ldots \times 2 \times 1 = 29!$ (29-fakultet) olika möjliga nycklar. Antalet möjliga nycklar är alltså ungefär 9×10^{30}, alltså en nia med trettio siffror efter sig.

Så många prövar man inte igenom i brådrasket. Men enkel substitution har en annan svaghet. Frekvensen hos klartextens bokstäver lyser igenom i kryptotexten. Det ser man tydligt i exemplet med Ada och Kal. I normalsvenskan är bokstaven *a* vanligast. I kryptotexten är Q vanligast. Man kan börja med att gissa att dessa bokstäver hör ihop. Och så fortsätter man med de övriga bokstäverna. Man brukar räkna med att en skicklig forcör klarar av att forcera enkel substitution om textlängden är 50 bokstäver eller fler.

För att konstruera svårforcerbara krypton behöver man alltså öka antalet möjliga nycklar tillräckligt mycket för att det inte skall gå att pröva igenom alla. Det måste dessutom gå till på ett sådant sätt att forcören inte kan ta några genvägar i sitt sökande efter den rätta nyckeln. För den som vill veta mer om de matematiska aspekterna av krypto rekommenderas Bruce Schneier: *Applied Cryptography, Second Edition*, John Wiley & Sons, 1996.

Nämnarens kryptoskola

3. Kryptots historia

I denna del av Kryptoskolan tar vi en titt på kryptots historia. Här finns några glimtar som kan vara intressanta för en större krets. De flesta uppgifterna i denna del kommer från tre böcker som är särskilt läsvärda om man är intresserad av kryptering. Dessa är Kahn: The Codebreakers [1], Bengt Beckman: Svenska kryptobedrifter [2] samt Simon Singh: Kodboken [3]. Innehållet i dessa böcker beskrivs närmare i slutet av denna del, där man även finner en ordlista.

De andra delarna finner du på ncm.gu.se/arkivN. Kryptoskolan är ett material som är skyddat av upphovsrättslagen. Studiematerialet får dock fritt kopieras för användning i undervisning eller för enskilt arbete och rekommenderas från årskurs 4 till gymnasiet.

Användning av hemlig skrift är mycket gammal. Konsten att kryptera var känd i det gamla Egypten och i Babylonien. Men låt oss börja i romarriket för cirka 2000 år sedan. Det är belagt att man då använde det krypto som nu går under benämningen Caesar-krypto.

Införandet av Caesar-krypto anses vara en stor förbättring av möjligheterna att sända hemliga meddelanden jämfört med den metod som användes i följande anekdot: Om man ville skicka ett meddelande från Rom till någon av provinserna utan att några fientligt sinnade personer kunde ta reda på innehållet rakade man av håret på en slav, ristade in texten i huvudsvålen och lät sedan håret växa ut. Slaven skickades iväg till den behörige mottagaren som rakade av slavens hår och som sedan kunde läsa meddelandet. Detta sätt att dölja ett meddelande är inte kryptering utan ett exempel på *steganografi*, dold skrift. Sanningshalten hos denna berättelse kan betvivlas.

Krypteringsprocessen för Caesar-krypto går till så här: Texten i ett meddelande skall ersättas, bokstav för bokstav, genom att man som kryptobokstav tar den som ligger ett visst antal steg längre fram i alfabetet, säg tills vidare tre. Om den första klartextbokstaven är *H* blir den första kryptobokstaven *K*.

Det tal som styr krypteringen behöver inte vara just tre, som romarna nöjde sig med, utan vilket annat heltal som helst mellan 1 och 28; vi kallar det i det följande för *kryptonyckeln* och betecknar den N, $1 \leqslant N \leqslant 28$ för det svenska alfabetet. Den som bestämmer kryptonyckeln får överlämna den till den andra personen på ett säkert sätt t ex vid ett sammanträffande. Med en matematisk formel kan man beskriva krypteringsförfarandet så här

$$C = K + N \pmod{29}, \qquad (1)$$

där (mod 29) här betyder att vi subtraherar 29 om summan blir större eller lika med 29.

Rökstenen

Foto: Bengt A Lundberg

Vid Rök kyrka i Östergötland står en märklig runsten, ristad på 800-talet. Denhar världens längsta runinskrift, över 800 runtecken. Huvudsakligen används runor ur alfabetet med sexton bokstäver, men det finns också tecken från den äldre runraden om tjugofyra bokstäver. Dessutom finns lönnrunor, dvs kryptotext som erhållits med tre eller fyra olika krypteringsmetoder.

Mest iögonfallande av lönnrunorna är runkorsen. Här har runristaren tänkt sig att runalfabetet är indelat i tre segment. Lönnrunan anger segment och ordningsnumret för tecknet i segmentet.

Med ett annat sätt att bilda lönnrunor används på rökstenen metoden att från en ”klartextruna” flytta sig ett steg fram i runalfabetet. Dit man då kommer blir motsvarande lönnruna. Men detta är ju Caesarkrypto med kryptonyckeln N = 1! Har runristaren på något sätt fått kännedom om detta krypto eller har han listat ut det själv? I vilket fall som helst måste det anses vara en stor bravad.

Bilden och uppgifterna om Rökstenen har jag hämtat ur en uppsats i Forskning och Framsteg nr 5, 1998, [5] där det också finns beskrivet både äldre och nyare tolkningar av runskriften, när den väl är dekrypterad, transkriberad och översatt till modern svenska. Se även [6].

Enkel substitution

Det stod snart klart att ett meddelande krypterat med Caesars metod är mycket lätt att forcera. Man behöver bara pröva igenom de 28 olika nyckelmöjligheterna och se efter vilken av de 28 olika ”klartexterna” som blir meningsfull. Ett något mer svårforcerat krypto får man om man ersätter kryptoalfabetet med en omordning, *permutation*, av bokstäverna i alfabetet, t ex så här:

Kryptonyckel $\mathcal{N}$:

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

$\mathcal{N}$ är här inte ett heltal utan substitutionen/funktionen som definieras av tabellen. När man krypterar letar man upp klartextbokstaven i den övre raden. Motsvarande kryptobokstav står i den undre raden, under klartextbokstaven. Sålunda blir klartextbokstaven *g* kryptobokstaven *T*. Krypteringsformeln blir

$$C = \mathcal{N}(K) \qquad (2)$$

Här är ett påbörjat exempel med nyckeln ovan:

Klartext	t	j	u	v	e	n	s	t	a	l	b	å	t	e	n
Kryptotext	B	U	X	N											

Vigenères krypto

Så småningom blev man uppmärksam på att även en enkel substitution är lätt att forcera om meddelandets längd inte är väldigt kort. Forceringen bygger på att olika bokstäver uppträder olika ofta (med olika frekvens) i vanlig text. Om bokstaven *a* förekommer i svensk text i tolv fall på hundra, gäller att motsvarande kryptobokstav, Q med nyckeln beskriven ovan, förekommer med samma frekvens i en kryptotext. Läs gärna mer om detta i *Kodboken* av Simon Singh [3].

En förbättring av Caesarkryptot brukar tillskrivas den franske diplomaten Blaise de Vigenère, född 1523, och kallas därför *Vigenèrekrypto*. Detta är enkelt att beskriva om vi går ut från krypteringsformeln (1) ovan. Med Vigenèrekrypto använder man olika tal N för varje bokstav som skall krypteras:

$$C_j = K_j + N_j \pmod{29} \qquad (3)$$

där C_j och K_j är siffermotsvarigheterna till klartextbokstav respektive kryptobokstav nr. j i respektive text. N_j är det tal som skall kryptera klartextbokstav nr j.

För att följden med talen N_j inte skall bli för svår att hantera, är den periodisk för Vigenèrekryptot. Dessutom kan de ha uttalbara motsvarigheter i alfabetet. Om nyckelordet är *BEDA* blir de första N-talen 1, 4, 3, 0, 1, 4, 3, 0, 1, 4, ... Låt oss kryptera vår favoritmening med denna nyckel.

Klartext	t	j	u	v	e	n	s	t	a	l	b	å	t	e	n
Klartext m. tal	19	9	20	21	4	13	18	19	0	11					
Addera nyckel	1	4	3	0	1	4	3	0	1	4					
Kryptotext m. tal	20	11	3	21	5	17	21	19	1	15					
Kryptotext	U	N	X	V	F	R	V	T	B	P					

Ett krypto som arbetar enligt formeln (3) kallas i denna uppsats linjärt. En annan typ av krypto får vi om vi i stället går ut ifrån formeln (2) för enkel substitution och använder olika substitutionsalfabeten $\mathcal{N}_j$ för bokstäverna som skall krypteras. Här blir det än mer nödvändigt att begränsa antalet olika $\mathcal{N}_j$ och sedan upprepa deras användning. Formeln blir

$$C_j = \mathcal{N}_j(K_j) \qquad (4)$$

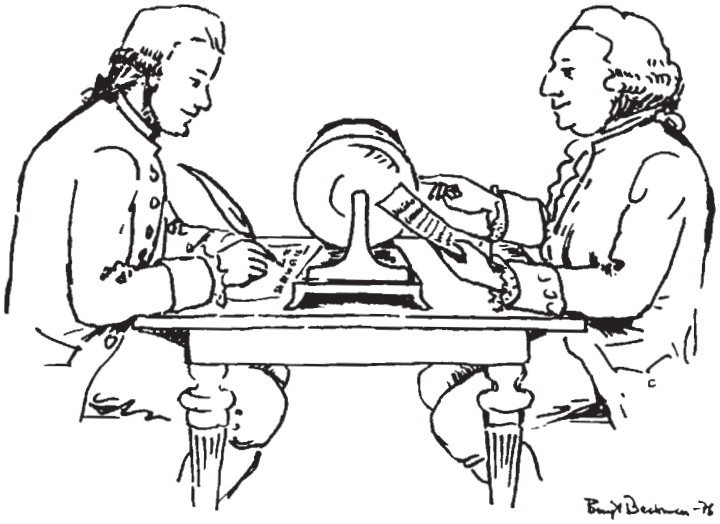
Ett sådant krypto kallas ibland *oordnad Vigenère* men här kallar vi det *olinjärt*.

Allteftersom forceringstekniken utvecklades blev det nödvändigt att göra kryptonycklarna mer omfattande, dvs öka perioden för N(j) respektive $\mathcal{N}$(j). Nycklarna blev svårare att hantera och krypterings- och dekrypteringsarbetet blev mer tidsödande. Antalet fel i arbetet ökade. Så småningom byggde man mekaniska apparater som utförde arbetet, sedan elektrifierades de. När elektroniken kom blev krypteringsapparaterna elektroniska och så småningom lät man datorer utföra krypteringen. Dock, under lång tid arbetade krypteringsapparater alltid (eller åtminstone nästan alltid) enligt en av de två principerna (3) eller (4).

Världens första krypteringsapparat

På 1400-talet uppfanns den s kchifferskivan, en mycket enkel mekanisering av Caesarnyckeln. Men om man inte räknar med den, så var världens första mer avancerade krypteringsapparat svensk. Den presenterades år 1786 i ett brev till Gustaf III. Uppfinnaren, tillika brevskrivaren, hette Fredrik Gripenstierna (1728-1804). Hans morfar är mera känd, Christofer Polhem.

De viktigaste delarna i Gripenstiernas krypteringsapparat är ett antal hjul, vartdera försett med alfabetet i ordning. På ena sidan av det bord där apparaten står, sitter den behörige ämbetsmannen och ställer in en klartextrad med en bokstav för varje hjul. På den andra sidan sitter den obehörige sekreteraren och skriver av motsvarande kryptotext; varje kryptotecken är ett tal mellan 0 och 99. Dessa tal står i oordning på baksidan av hjulen. Kryptot är alltså olinjärt. Teckningen, liksom uppgifterna i detta avsnitt, kommer från ”Svenska kryptobedrifter” av Bengt Beckman, [2] där det finns en utförlig beskrivning av Gripenstiernas krypteringsapparat och hur man skulle kunna tänka sig att fullständigt rekonstruera kryptot utgående från en kryptotext och *pålägg*, dvs från ett stycke av den motsvarande klartexten.



Första världskriget

När första världskriget bröt ut var man ganska väl förberedd när det gäller krypton – trodde man. Man använde handkrypton och krypteringsapparater samt även koder. En kod för kryptobehov består av förutom enskilda tecken vanligen förekommande ord och fraser samt deras krypterade motsvarigheter. En kod blev ofta en ganska stor bok. En fördel var att meddelandena blev kortare i krypterat skick. Nackdelen var att det blev oerhört viktigt att hålla koden hemlig. När den avslöjats, genom forcering eller stöld, gällde det att distribuera en ny till alla dem som man ville kommunicera med.

Men även på forceringssidan hade man gjort förberedelser. Särskilt i Frankrike hade man efter det förödmjukande Fransk-tyska kriget 1870-1871 byggt upp resurser för signalspaning och forcering av kryptomeddelanden. Även i andra länder fanns både kryptometoder och forceringsorgan. Marconis uppfinning av radion gav möjligheter för de krigförande men också tillfällen för den avlyssnande fienden. Behovet av krypto hade ökat.

Men de som konstruerat krypton hade långt ifrån alltid förutsett de geniala forcörernas möjligheter att knäcka deras krypton. På alla håll fick man fram värdefulla underrättelser genom forcering och dessa var långt ifrån oväsentliga för krigets förlopp. Störst betydelse hade nog forceringen av det s k Zimmermanntelegrammet. Detta var ett kodmeddelande från den tyske utrikesministern Arthur Zimmermann till Mexikos president där man dels aviserade det obegränsade ubåtskriget dels uppmanade Mexiko att anfalla USA, eventuellt med stöd av Japan. Telegrammet avlyssnades, forcerades i Storbritannien och delgavs USA. Där bidrog dessa underrättelser starkt till att man bröt sin neutralitet och inträdde i kriget.

Betydande delar av forceringsverksamhet i olika länder under andra världskriget dokumenterades 1931 av den svenske kryptologen Yves Gyldén: Chifferbyråernas insatser i världskriget till lands [7].

Mellankrigstiden

Erfarenheterna från världskriget togs till vara och man utnyttjade tekniken, särskilt möjligheten att använda elektromekaniska apparater. Det fanns ett särskilt behov av att åstadkomma långa följder av slumptal eller åtminstone följder av tal som liknande slumptal så mycket som möjligt. Redan på 1800-talet hade Vigenèrekryptot med kort nyckel visats vara osäkert. Men om man med teknikens hjälp kunde alstra långa följder av nyckeltal?

Ett sätt att åstadkomma långa slumpliknande tal eller matematiska transformationer var att använda flera lika stora hjul, vartdera med en indelning i delar, t ex 26 som antalet bokstäver i det internationella alfabetet. Hjulen monteras på en axel och fås att rotera efter varje krypteringssteg som ett räkneverk. Hjulet längs till höger flyttas ett steg för varje krypteringssteg, nästa hjul flyttas ett steg när det första gått ett varv osv. Om vi exempelvis använder fem hjul dröjer det 26^5 eller nästan 12 000 000 steg innan man kommer tillbaka till ursprungsläget. Det verkar vara betryggande mycket större än ett ganska stort skriftligt meddelande. Om man kan utnyttja hjulens möjligheter borde man kunna åstadkomma en stark kryptering, åtminstone vad gäller periodens längd.

I Tyskland konstruerades Enigma-kryptot efter denna princip. Vart och ett av hjulen, som kunde vara tre eller flera till antalet, hade två uppsättningar om 26 kontakter och mellan dessa 26 elektriska kopplingar som överförde en signal från en bokstav till en annan. Kryptot blev olinjärt.

Japanerna konstruerade ett krypto som i USA kallades Purple. Principen för Enigma var känd i Japan och man kan anta att kryptot var av liknande typ.

Ett annat sätt att med hjälp av hjul åstadkomma långa slumpliknande serier av tal är att använda hjul med olika långa indelningar som parvis inte skall ha några gemensamma faktorer och sedan låta alla hjulen flytta sig ett steg efter varje krypteringssteg. Hjullängderna 26, 25, 23, 21, 19 och 17 ger exempelvis totala perioden $26 \times 25 \times 23 \times 21 \times 19 \times 17$ eller drygt 100 000 000 steg, också det mycket större än ett långt meddelande.

I Tyskland tog man också fram andra typer av krypton. Ett kallades Geheimschreiber. Med fjärrskrift kunde man med långa avstånd elektriskt koppla ihop två elektromekaniska terminaler med tangentbord och utskriftsanordning. Man skrev sin text på den ena terminalen och med försumbar fördröjning skrevs texten ut på den apparat som man var uppkopplad med (den tidens

chat). Varje bokstav och typografiskt tecken kodades med en fembitskod. Men eftersom den överförda texten var lätt att avlyssna, gällde det att kryptera den, om ledningen var tillgänglig för obehöriga (läs annan stat). Geheimschreiber var därför försedd med ett inbyggt krypto, som var olinjärt och där periodlängden säkerställdes med hjul av olika längd.

I Sverige ledde den uppfinningsrike ingenjören Boris Hagelin konstruktionen av en familj av mekaniska krypteringsapparater. Franska staten beställde 5 000 st. men de kom inte till leverans. Kriget kom emellan. Hagelin lyckades dock mitt i brinnande krig ta sig till USA med en nermonterad apparat i bagaget. Amerikanerna blev intresserade och 140 000 exemplar tillverkades enligt konstruktörens anvisningar. Efter kriget startade Hagelin en firma i Schweiz, ett företag som fortsatte att utveckla och tillverka olika typer krypteringsapparater som såldes och säljs i ett stort antal länder. Hagelins krypteringsapparater arbetade med olika långa hjul och var väsentligen linjära.

Ett tredje sätt att åstadkomma långa sekvenser är att helt enkelt låta en god slumpmekanism lotta fram så många tal som motsvarar totallängden av alla meddelanden som man kan tänkas vilja sända till en viss mottagare och distribuera denna nyckelmängd i förväg med kurir till sändare och mottagare. Sedan gäller det också att aldrig använda ett tecken i nyckeln mer än en gång. Rätt hanterat är ett sådant engångskrypto oforcerbart. Varför slog dessa krypton aldrig igenom på bred front? Det visade sig att svårigheterna med att alstra nycklarna och distribuera dem till användarna i praktiken oftast var oöverstigliga. Det gällde att skicka mycket nyckelmassa på ett säkert sätt till varje par av enheter som behövde kommunicera med varandra. Användningen fick därför begränsas till ett fåtal användare som hade mycket hemliga meddelanden att utväxla. Även vid andra världskrigets början var man alltså väl försedd med för den tiden moderna krypteringsapparater. Men även på forceringssidan hade man tagit tillvara erfarenheterna från första världskriget.

Andra världskriget

Om man var väl förberedd kvalitativt när det gäller hantering och forcering av krypton, så var det betydligt sämre när det gäller kvantiteten. Vid och strax efter krigsutbrottet rekryterades många personer, män och kvinnor, till denna tjänst. I Sverige tog man kontakt med duktiga korsordslösare och publicerade också enkla kryptouppgifter. De som skickade in rätt lösning blev en god rekryteringsgrund. Forceringsorganisationerna lyckades väldigt väl i det underrättelsekrig som fördes med krypto, signalspaning och forcering – *kriget i etern* brukar det kallas. Här beskrivs tre av de mest omtalade fallen.

Enigmakryptot forcerades som resultat av ett lagarbete. Fransmännen hade fått tillgång en detaljerad beskrivning av en av de varianter som användes av tyskarna. Underlaget lämnades vidare till polackerna som gjorde stora framsteg när det gällde forceringen. Strax innan Polen anfölls av tyskarna flydde några polska forcörer till Storbritannien med tillräckligt underlag för att man där kunde fortsätta arbetet med att avslöja mycket av tyskarnas hemliga radiotrafik. Både i Storbritannien och i Frankrike hade man trott att Enigma var oforcerbar och man blev mycket förvånad när man fick höra om polackernas framgångar. Men hela tiden förbättrade tyskarna Enigma och nya modeller kom ut som med tiden blev allt svårare att forcera. Till sin tjänst tog britterna forceringsapparater som blev föregångare till dagens datorer. Av flera anledningar är det synd att

knappast någon dokumentation av dessa ”predatorer” finns kvar. Allt förstördes efter krigets slut. Det skulle dröja ända till 1970-talet innan det blev allmänt känt att engelsmännen lyckats knäcka ett av Tysklands viktigaste krypton.

I USA hade man lyckats knäcka Purple. Den prestationen utfördes av en grupp matematiker där William F. Friedman var den ledande. Friedman hade redan under första världskriget börjat arbeta med kryptologi och under mellankrigstiden fortsatte han att utveckla konsten och organisationen. Trots forceringsframgångarna kunde man inte få underrättelser som varnade för japanernas anfall av Pearl Harbor. Detta är en fråga som har analyserats i detalj flera gånger. Man kan nog sammanfatta resultaten som så att det helt enkelt inte fanns några meddelanden, forcerade eller i klartext, som tillräckligt tydligt angav anfallsplanerna. Det har inte kommit fram något stöd för antagandet att USA lät bli att varna flottbasen för att få anledning att inträda i kriget.

I Sverige var det till att börja med främst Yves Gyldén som stod bakom framgångarna. Den forcörsgrupp han ledde lyckades väl med att forcera olika länders koder. Men en annan forcör, som också till att börja med sysslade med att knäcka koder, blev det stora namnet inom svensk kryptologi, matematikern Arne Beurling. År 1940 skedde något mycket väsentligt för svensk underrättelsetjänst. För sin krypterade fjärrskrifttrafik med Geheimschreiber (på svenska G-skrivaren) behövde ockupationsstyrkan i Norge en teleledning till Berlin. Den gick över Sverige och tappades på alla meddelanden. Dessutom avlyssnades linjen mellan Berlin och tyska beskickningen i Stockholm. Det var en mycket stor bedrift av Beurling, när han utan förkunskap om G-skrivarens funktion, lyckades rekonstruera den och forcera en dags snappade meddelanden. Under flera år blev de forcerade G-skrivartelegrammen en mycket god underrättelsekälla. Bland annat kunde man få reda på att tyskarna inte skulle invadera Sverige, vilket innebar att vi inte behövde genomföra någon allmän mobilisering. Det sparade mycket pengar åt Sverige.

Fanns det då inga krypton som motstod forceringsförsöken? Jo, då. Som berättats ovan införde tyskarna under kriget alltmer sofistikerade Enigmamodeller. Alla kunde inte forceras. På samma sätt var det med G-skrivaren. Under krigets sista skeden kunde inte de nya modellerna forceras med någon större framgång.

Tre namn att minnas

I Storbritannien var logikern Alan M. Turing en av de tongivande vid forceringen av Enigma. Före kriget hade han varit en av pionjärerna för automatteorin. Han ställde sig frågan: ”Kan en automat, i en viss klass av generella teoretiska maskiner, (läs dator,) göra 'allting'?” Hans svar blev: Ingen automat kan göra allting, till exempel generellt avgöra om ett program till sist stannar eller inte. Efter kriget arbetade Turing med att utveckla det som vi i dag kallar dator. I SIGMA, band VI, sid 2203 - 2227 finns en lättläst uppsats av Alan Turing: ”Kan en maskin tänka?” [11]

Matematikern Claude E. Shannon arbetade under andra världskriget vid Bell Telephone Laboratories med två ämnen som visade sig vara beroende av varandra, nämligen informationsteori och kryptologi. Resultatet av denna forskning publicerades i två artiklar 1948 och 1949. ”A Mathematical Theory of Communication” [13] kom först. Där beskrev han hur mycket extra data, redundans, som måste läggas till för att ett meddelande skulle kunna avkodas efter att ha överförts på en brusig kanal. Det är ingen större överdrift att säga att Shannon

med denna uppsats blivit informationsteorins fader. Ett år senare kom ”Communication Theory of Secrecy Systems” [14]. Här kunde han matematiskt visa hur stor nyckel (hur mycket nyckelinformation) som krävs för att teoretiskt dölja en viss mängd klartext. Shannon gav en teoretisk förklaring till varför det är lätt att forcera enkel substitution och Vigenèrekryptot, varför man inte får använda en engångsnyckel två eller flera gånger samt att varje krypto med begränsad nyckel är teoretiskt forcerbart. Det sista påståendet innebär att det bara finns en kryptonyckel hörande till en kryptotext som inte är alltför kort. Så om man kan provdekryptera med alla tänkbara nycklar hittar man den enda och rätta klartexten bland alla provresultaten. En matematisk teori som visar när ett krypto är forcerbart med i praktiken tillgängliga resurser saknar dock fortfarande sin lösning.

Även Shannon har skrivit en populärvetenskaplig uppsats i SIGMA, band VI: ”En schackspelande maskin.” [12]

Det sista namnet jag vill framhålla i detta avsnitt är Arne Beurling. Som ovan beskrivits gjorde Beurling Sverige stora tjänster under andra världskriget bland annat genom att forcera tyskarnas G-skrivare. Han var en oerhört produktiv forskare inom matematisk analys. En av hans elever, Yngve Domar, som senare blev professor i matematik vid Uppsala universitet, tvekar inte att beteckna Beurling som ett geni (se [2]). Ett verkligt mattesnille, alltså. (Och tänk nuförtiden behöver man inte kunna så mycket mer än multiplikationstabellen för att kallas ”mattesnille” på en svensk skolgård!)

Mig veterligt har Beurling inte lämnat efter sig något populärvetenskapligt verk, men vill man veta mer om hans särpräglade personlighet, rekommenderas Bengt Beckmans bok [2]. Där finns också en detaljerad beskrivning av Beurlings metod för att forcera G-skrivaren.

DES - en standard för kryptering

År 1972 utlyste två amerikanska standardiseringsorgan en tävling om en krypteringsalgoritm, avsedd att användas för att skydda data som lagrades på en dator eller kommunicerades mellan två terminaler. IBM vann tävlingen och 1976 antogs algoritmen som USA-standard. Detaljerna hade publicerats något år tidigare tillsammans med en försäkran från IBM att garantera alla användare en avgiftsfri användarlicens. Det senare blev en av orsakerna till den stora framgång som algoritmen fick för IT-säkerheten under många år. Namnet blev Data Encryption Standard, DES.

DES innebar ett nytänkande på åtminstone tre sätt. För det första publicerades kryptoalgoritmen in i minsta detalj. Visserligen fanns det många godkända kryptopatent tidigare, men man hade åtminstone försökt dölja den exakta utformningen så gott det gick.

För det andra introducerades med DES ett blockkrypto. Algoritmen krypterar inte en bit, ett tecken eller en byte i taget utan ett block om 64 bitar. Härigenom kan man lätt tillverka speciell hårdvara som krypterar mycket snabbt. Men konstruktionen medger även att simuleringar i en standarddator kan göras ganska snabba.

För det tredje blev det startskottet till en enormt stor användning av krypto utanför den klassiska användarsfären, försvar och utrikesförvaltning. En bra redogörelse för DES finns i [4], ”Applied Cryptography” av Bruce Schneier.

Publicerade kryptonycklar - går det för sig?

Nyckelhantering – att tillverka, distribuera, hålla reda på, förvara, hantera och till sist förstöra kryptonycklar när de inte behövs längre har alltid varit ett stort problem. En anledning är förstås att kryptonycklar är hemliga. Obehöriga, varav främmande länders underrättelseorganisationer torde vara de mest resursstarka, är givetvis mycket intresserade av att få reda på vilka nycklar som använts för att kryptera meddelanden av värde för deras uppdragsgivare.

År 1976 lade två amerikanska matematiker fram ett helt nytt koncept för kryptering. Whitfield Diffie och Martin Hellman, presenterade vid ett symposium om informationsteori i Ronneby ”öppen nyckel-kryptering”. Hösten samma år kom deras resultat ut i tryck, ”New Directions in Cryptography” [15]. Grundidén innebär att man använder nycklar, som är uppdelade i två delar, en öppen, publicerbar nyckel används för kryptering och en hemlig för dekryptering.

Den som räknar med att få ett hemligt meddelande alstrar en dekrypteringsnyckel och håller den hemlig hos sig samt en tillhörande öppen krypteringsnyckel och publicerar denna i en allmänt tillgänglig katalog. Avsändaren krypterar meddelandet med den publika (öppna) nyckeln och skickar det till mottagaren, som tar fram sin privata (hemliga) nyckeldel och dekrypterar meddelandet.

Helt har man dock inte löst problemet med nyckeldistribution på detta sätt. Den som skall sända ett hemligt meddelande måste försäkra sig om att den öppna nyckel som han hämtar i den publicerade katalogen, verkligen tillhör den avsedde mottagaren så att han inte skickar hemligheter till någon annan. Sekretessproblemet har ersatts av ett autenticitetsproblem.

Tre amerikaner, de två datalogerna Ron Rivest och Adi Shamir samt matematikern Leonard Adleman, har uppfunnit det mest använda sättet för öppen nyckel-kryptering. Tillsammans konstruerade de det så kallade RSA-systemet efter initialerna i deras efternamn. Metoden bygger på att det i praktiken är svårt att uppdela stora tal i primfaktorer, om talet inte innehåller några små faktorer. Nämnaren nr 4, 2001, sid. 47 - 51 [8] innehåller en lättläst och enkel beskrivning av RSA-systemet.

Kvantfysiken i kryptologins tjänst

Två drömmar har alltid hägrat för kryptologerna, nämligen att uppfinna det oforcerbara kryptot och att forcera ett krypto som av många förklarats som praktiskt oforcerbart. Den första av dessa drömmar är som vi sett tidigare i denna uppsats förverkligad i och med engångskryptot, men vi önskar ett krypto som inte har engångskryptots ohanterliga nyckelhantering. På senare tid har man med utnyttjande av kvantfysikens förklaringar till vissa märkliga beteenden hos fotoner och elementarpartiklar kommit en bit på vägen mot dessa drömmars mål. Möjligheterna kallas kvantkryptering och kvantforcering. Båda finns beskrivna på ett så lättillgängligt sätt som förefaller vara möjligt i Kodboken [3]

Kvantkryptering

Ett kvantkrypto använder fotoner som är polariserade i olika riktningar på ett slumpartat sätt. Avsändaren av ett meddelande alstrar slumpmässigt polariserade fotoner och skickar dem till mottagaren som i sin tur använder slumpmässigt orienterade filter för att med viss sannolikhet ta reda på vad avsändaren sänt. Efter ett antal utbyten av fotonsekvenser och ”vanliga” data har avsändare och mottagare hos sig en identisk följd av bitar som kan användas för fortsatt kryptering och ingen avlyssnare på linjen kan ha fått del av dessa. Det är nämligen så att det inte går att avlyssna fotonsekvensen utan att förstöra den och det kan de behöriga användarna avgöra. Det finns också möjligheter att utväxla fotonsekvenser trots en avlyssnare och använda resultatet som ovan. Än så länge är kvantkryptoutvecklingen i sitt inledningsskede.

Man måste också övertyga sig om att de behöriga parterna verkligen kommunicerar med varandra och inte med någon obehörig. Vi har ett autenticeringsproblem att lösa dessutom.

Kvantforcering

Ett krypto som inte är ett (oforcerbart) engångskrypto kan enligt Shannon alltid forceras i teorin genom att man prövar att dekryptera en kryptotext med alla tänkbara nycklar och säger bingo! när ”klartexten” blir begriplig. För ett starkt krypto är detta antal är mycket stort. Låt oss anta i ett tänkt exempel att detta är 2^{100}, vi talar då om en 100 bitars nyckel. För en vanlig dator, som skall genomföra detta med en nyckel i taget, blir tidsåtgången orimligt stor. Men för en kvantdator kan det komma att bli möjligt.

En vanlig dator arbetar med bits, elektroniska vippor som kan inta värdet noll eller ett. En kvantdator använder i stället qubits (quantum bits) som samtidigt intar värdena noll och ett. Den utnyttjar elementarpartiklar som först givits ett visst värde för sitt spin, säg att de spinner medsols. Om man sedan skickar en svag energiimpuls till dem kan de komma i ett läge där det inte går att avgöra om de spinner med- eller motsols så länge vi inte försöker avläsa deras spinvärde. De spinner åt båda hållen samtidigt. Enligt kvantdatoridén kan man sedan ”räkna” (i vårt fall provdekryptera) med dessa qubits och skulle i princip kunna få alla möjliga ”klartexter” samtidigt!
I vårt fall med 100 bitars nyckel skulle ett register med 100 qubits räcka som utgångsvärde för de 2^{100} möjliga nycklarna.

Ännu finns endast mycket rudimentära tekniska realiseringar av kvantdatorer. Men om de blir verkliga och användbara i tillräckligt komplicerade fall, blir inga nuvarande krypton säkra - inte ens i praktiken.

Fyra böcker

År 1967 utkom en bok om kryptots historia från en tid långt före vår tideräkningsbörjan fram till våra dagar. Det är en riktig tegelsten. Själv har jag en förkortad version om 476 sidor. Författare och titel: David Kahn: The Codebreakers [1]. Tyngdpunkten ligger på tiden för de båda världskrigen och perioden däremellan. Upplägget är mer historiskt än matematiskt.

Den svenska kryptohistorien beskrivs på ett medryckande sätt i Bengt Beckman: Svenska kryptobedrifter [2]. Den innehåller bland annat en beskrivning av Gripenstiernas krypteringsapparat från 1700-talet (se ovan), Boris Hagelins mest kända krypteringsapparat samt en beskrivning av den svenska radiospaningen och forceringsverksamheten under första världskriget och mellankrigstiden. Men tyngdpunkten ligger på Arne Beurlings bravad att knäcka G-skrivaren och dess betydelse för svenskt försvar under andra världskriget. Både apparatens funktion och forceringsmetoden beskrivs detaljerat. Boken avslutas med en ordlista som förklarar de termer som vanligen används i Sverige inom kryptoområdet.

En detaljerad beskrivning av Enigma-kryptot och hur det forcerades före och under andra världskriget finns i Simon Singh: Kodboken [3]. Men boken innehåller också mycket annat av intresse, t.ex. ett kryptos betydelse för Maria Stuarts dödsdom och avrättning, Vigenères metod samt krypton hos Conan Doyle och Edgar Allan Poe. Singh beskriver också hur man löste gåtorna med hieroglyferna och Linear B. Amerikanerna använde under andra världskriget navajoindianer som på sitt stamspråk överförde radiomeddelanden mellan stridande enheter i Stilla-havsområdet. I boken beskrivs hur dessa indianer valdes ut och användes. Singh behandlar också modern kryptologi, bland annat DES, RSA och andra nutida kryptometoder, även kvantkryptering och kvantforcering.

En fjärde, mycket innehållsrik bok är Bruce Schneier: Applied Cryptography [4], också den en tegelsten, 760 sidor tjock. Den är övervägande matematisk till sin karaktär och innehåller ”allt” man kan tänkas behöva veta om kryptoprotokoll, kryptoteknik, kryptoalgoritmer och kryptopolitik. Den innehåller också källkod för nio kryptoalgoritmer, bland andra DES. Referenslistan upptar hela 1653 hänvisningar.

Ordförklaringar

Krypto – Hemlig skrift. Krypto kan också betyda en viss metod för kryptering.

Klartext – Text som kan förstås utan att man behöver använda en hemlig metod och/eller hemlig kryptonyckel.

Kryptera – Översätta en klartext till kryptotext med hjälp av krypto och kryptonyckel.

Kryptotext – Resultat av kryptering. En kryptotext kan man inte förstå utan att den först dekrypteras.

Dekryptera – Återföra en kryptotext till klartext med hjälp av ett krypto och oftast en hemlig kryptonyckel.

Kryptonyckel – Data som styr hur man krypterar och dekrypterar med ett visst krypto.

Steganografi – Metod för att dölja förekomsten av en text, t. ex. genom att använda osynligt bläck.

Substitutionskrypto – Krypto där man vid kryptering ersätter en bokstav eller ett tecken i klartexten med ett annat tecken eller par av tecken.

Transpositionskrypto – Krypto där man vid kryptering ändrar ordningsföljden för bokstäverna i klartexten.

Meddelande – består av namn (och eventuellt även adress) samt den text som man vill att mottagaren skall läsa.

Klartextmeddelande – Meddelande som består av namn m.m. och klartext.

Kryptomeddelande – Meddelande som består av namn m.m. och kryptotext.

Redigering – Åtgärder som görs på en text efter dekryptering för att stor bokstav, mellanslag och skiljetecken skall införas så att texten blir lätt att läsa för mottagaren.

Internationella alfabetet – ABCDEFGHIJKLMNOPQRSTUVWXYZ

Forcering – Att ta fram klartexten som hör till en kryptotext utan att på förhand känna till den använda kryptonyckeln.

Referenser

Huvudreferenser

[1] David Kahn: The Codebreakers, Weidenfeld and Nicolson, London, 1974.

[2] Bengt Beckman: Svenska kryptobedrifter, Albert Bonniers förlag, 1996, pocketutg. 2006.

[3] Simon Singh: Kodboken, Norstedts, 1999.

[4] Bruce Schneier: Applied Cryptography, Second Edition, John Wiley & Sons, 1996.

Rökstenen

[5] Gun Widmark: Varför Varin ristade, Forskning och Framsteg nr 5, 1998, sid. 16 - 22.

[6] Conny L A Petersson: Rökstenen, Varins besvärjelse, Noteria Förlag, Klockrike, 1991

Andra allmänna uppsatser

[7] Yves Gyldén: Chifferbyråernas insatser i världskriget till lands, Militärlitteraturföreningen förlag, 1931.

[8] Juliusz Brzezinski: Om kryptering, Nämnaren nr 4, 2001, sid. 47 - 51. (Artikeln behandlar huvudsakligen öppen-nyckelkryptering, särskilt RSA-kryptot. I artikeln anges felaktigt att Arne Beurling knäckte Enigma-kryptot.)

[9] Johan Håstad: Ett datornät utan chiffer är som en stad med olåsta dörrar, Forskning och Framsteg nr 8, 1995, sid. 22 - 27.

Tidiga uppsatser om datorer och informationsteori

[10] John von Neumann: En allmän och logisk teori för automater, SIGMA vol. VI, sid 2174 - 2202, Forum, 1960.

[11] Allan M. Turing: Kan en maskin tänka? SIGMA vol. VI, sid 2203 - 2227, Forum 1960.

[12] Claude Shannon: En schackspelande maskin, SIGMA vol. VI, sid 2228 - 2236, Forum 1960.

[13] Claude Shannon: A Mathematical Theory of Communication, Bell System Technical Journal, vol. 27, nr 4, 1948, sid. 379 - 423, 623 - 656.

[14] Claude Shannon: Communication Theory of Secrecy Systems, Bell System Technical Journal, vol. 28, nr 4, 1949, sid. 656 - 715.

Öppen nyckel-kryptering

[15] Whitfield Diffie and Martin Hellman: New Directions in Cryptography, IEEE Transactions on Information Theory, vol IT-22, nr 6, Nov 1976, sid. 644 - 654.

Nämnarens kryptoskola

4. Lärarhandledning

Denna lärarhandledning ger en översiktlig beskrivning av Kryptoskolan, lästips och ordförklaringar. De andra delarna finner du på ncm.gu.se/arkivN. Kryptoskolan är ett material som är skyddat av upphovsrättslagen. Studiematerialet får dock fritt kopieras för användning i undervisning eller för enskilt arbete och rekommenderas från årskurs 4 till gymnasiet.

Kommer du ihåg hur det var i elva-, tolvårsåldern? Du hade erövrat ett skriftspråk som öppnade dörren till en helt ny värld och du hade många hemligheter gemensamma med dina närmaste kamrater, hemligheter som ni kunde gömma undan nyfikna utanför kretsen av de mest betrodda och kanske även undan föräldrar och andra vuxna. Hjälpmedlet var krypto - eller ni kanske kallade det chiffer.

Med detta undervisningsmaterial kan du i minnet återuppleva den tiden, men framför allt vidarebefordra kunskaper om krypto till dina elever. På köpet får du ett material som på ett spännande sätt övar eleverna i att hantera svenska språket. Det stärker elevernas förmåga till logiska resonemang och slutledningsförmåga. Noggrannhet premieras, den som försöker slarva igenom övningsuppgifterna lyckas sämre.

Det handlar alltså om *kryptering*, då man översätter en begriplig klartext till en förhoppningsvis obegriplig kryptotext, samt om *dekryptering* då man återför kryptotexten till läsbar klartext.

Det mesta av undervisningsmaterialet är utprovat tillsammans med elever i årskurs 4 och 5, men det kan även användas av äldre elever. En del av övningarna är lätta om man är noggrann. De riktigt svåra utmaningarna kan vara lämpliga att diskutera gemensamt.

Materialet är indelat i tio avsnitt utöver denna lärarhandledning. I de sju första avsnitten lär man sig använda olika sätt att kryptera. Två avsnitt ägnas åt några andra kryptobesläktade egenskaper hos svenska språket. Det sista avsnittet innehåller ett ”examensarbete” samt förslag till ”elevens kryptobok”. I kryptomaterialet finns även en text om ämnesintegrationen mellan matematik och språk.

Översiktlig beskrivning av undervisningsmaterialet

I det här materialet får eleverna lära sig olika sätt att kryptera. För varje krypto som införs ges ett antal exempel både på kryptering (då man översätter en begriplig klartext till en förhoppningsvis obegriplig kryptotext) samt på dekryptering där det omvända visas. För varje krypto uppmanas eleven att hitta på en egen klartext, kryptera den och lämna den till en kamrat för dekryptering.

Varje avsnitt börjar med en sida avsedd för läraren. Där finns kommentarer, ledtrådar och facit till övningarna i avsnittet. Därefter följer ett elevunderlag, vars sidor man kan kopiera och lämna till eleverna.

För varje krypto som introduceras arbetar man lämpligen omväxlande parvis och enskilt på följande sätt: Läraren börjar med att presentera kryptometoden. Sedan övar sig eleverna med dekryptering och kryptering enligt materialet. Då arbetar de tillsammans två och två. Sedan hittar var och en på en klartext, krypterar den och lämnar den till sin kompis, som dekrypterar den kryptotext han/hon fått.

Rövarspråket är ett exempel på talkrypto (hemligt pratspråk) som verkar förbryllande för dem som inte satt sig in i hur det fungerar. Många elever kommer dock (tyvärr?) att finna att deras föräldrar eller far- och morföräldrar behärskar det från den tiden då Kalle Blomkvist och hans kamrater var som mest i ropet. Oftast används vårt svenska alfabet om 29 bokstäver, alltså även med bokstaven W, när vi lär oss skriftkrypto.

Lodrätt-vågrätt-kryptot är en enkel variant av omkastningskrypto, vilket innebär att textens tecken skrivs i en annan ordning än de förekommer i klartexten. I anslutning till detta först beskrivna krypto införs begreppen klartext, kryptotext, kryptera och dekryptera.

Även hålkrypto (som också kallas rasterkrypto) är ett omkastningskrypto. Man använder en skiva av tunn kartong eller tjockt papper med hål genom vilka man skriver klartexten i en kvadrat på ett underliggande papper. Genom att vrida skivan ett kvarts varv tre gånger kan man skriva flera bokstäver i samma kvadrat på papperet. När man tar bort skivan ser man kryptotexten bestående av klartextbokstäverna framträda i blandad ordning. Hålkrypto är alltså också ett transpositionskrypto. Materialet innehåller en mall som man kan använda om man vill använda tillverka flera mallar/raster. Begreppet kryptonyckel införs.

Byggmästarkryptot, som även kallas frimurarchiffer, är ett sätt att ersätta bokstäverna i en text med tecken som varken är bokstäver eller siffror. En kryptotext ser därför avskräckande ut för att eventuellt hindra den obehörige som vill komma åt innehållet.

Sifferkryptot visar hur man kan ersätta en texts bokstäver med två siffror. När man krypterar med en kod översätter man uttryck, hela ord eller stavelser till en kodgrupp. I materialet är en kodgrupp två tecken, en bokstav och en siffra. Ett klartextord etc. översätts till en kodgrupp på samma sätt som man krypterar en klartextbokstav till två siffror med sifferkrypto.

Morsealfabetet är inget krypto. Vem som helst, som har lärt sig det, kan ju tolka vad som står om man snappar upp ett morsemeddelande. Men man skickade ofta kryptomeddelanden med morse. Därför kan det vara intressant att få veta litet om det.

Caesar-kryptot är ett autentiskt krypto, använt i det gamla romarriket. Där ersätts en klartextbokstav med en annan som kommer ett visst antal steg framåt i alfabetet. I anslutning till detta krypto blir begreppet kryptonyckel mera betydelsefullt, när det gäller att göra krypton som blir motståndskraftiga mot forcering. Trots möjligheten att införa olika nycklar inom ramen för ett krypto är Caesar-kryptot inte alls starkt. Det visar avsnittet som behandlar forcering av

detta krypto. Den svåra extrauppgiften visar att man kan använda den vanliga forceringsmetoden för Caesar-krypto på andra typer av krypton.

Med ES-KRYPTO (Enkel Substitution) visas hur man kan kryptera genom att ersätta bokstäverna i en text på ett mer komplicerat sätt än i Caesar-krypto. Tyvärr blir då kryptonyckeln svår att komma ihåg i det generella fallet. I samma avsnitt visas hur man kan konstruera nycklar till ES-krypto på ett enkelt sätt. Kryptonyckeln bildas ur ett lösenord som är lätt att memorera. Därefter visas hur man kan göra för att undvika bokstäverna Å, Ä och Ö i kryptotext .

Under rubriken EXTRA UTMANINGAR presenteras några uppgifter som visar vad skriftspråket ”tål” av uppblandning, omkastning och utelämnande av bokstäver. Man kan räkna med att endast få elever klarar av dem utan hjälp. Men de är mycket lämpliga att diskutera i grupp under ledning av en pedagog. I avsnitten ”Kommentarer, ledtrådar och facit” finns tips som man kan ge för att leda eleverna på rätt spår mot en lösning av uppgifterna.

Till sist finns ett förslag till en mer omfattande övningsuppgift, ett ”examensarbete” samt tips för hur man kan samla allt material som en elev gjort till en KRYPTOBOK.

Lästips

Böcker för barn

Johan Stensson: Här får du veta någonting om hemlig skrift, Albert Bonniers förlag, 1970.

Eileen O'Brien & Diana Riddel: Hemlig skrift, Berghs Bokförlag AB, 1998. (I boken får man bland beskrivningar av många krypteringssätt identifiera sig med Agent A när hon avslöjar Agent X genom att forcera dennes krypterade meddelanden.)

Heidi Jergovsky: Hemliga språk - Koder, chiffer och hemliga tecken, Bonnier Carlsen, 2002.

Ur Nämnaren

Ronnie Ryding: UPPSLAGET Gör en krypteringssnurra, Nämnaren nr 4, 2001, sid 32 - 33.

Tomas Fridström: Kryptering - utmaning för 12-åringar, Nämnaren nr 4, 2003, sid 34 - 36.

Lotta Wedman: Kryptering på gymnasiet, Nämnaren nr 2, 2005, sid 40 - 43.

Juliusz Brzezinski: Om kryptering, Nämnaren nr 4, 2001, sid. 47 - 51.

Ordförklaringar

*K*rypto - Hemlig skrift. Krypto kan också betyda en viss metod för kryptering. I talspråk kan krypto också betyda kryptomeddelande.

*K*lartext - Text som kan förstås utan att man behöver använda en hemlig metod och/eller hemlig kryptonyckel.

*K*ryptera - Översätta en klartext till kryptotext med hjälp av krypto och kryptonyckel.

*K*ryptotext - Resultat av kryptering. En kryptotext kan man inte förstå utan att den först dekrypteras.

*D*ekryptera - Återföra en kryptotext till klartext med hjälp av ett krypto och oftast en hemlig kryptonyckel.

*K*ryptonyckel - Data som styr hur man krypterar och dekrypterar med ett visst krypto.

*S*ubstitutionskrypto - Krypto där man vid kryptering ersätter en bokstav eller ett tecken i klartexten med ett annat tecken eller par av tecken.

*T*ranspositionskrypto - Krypto där man vid kryptering ändrar ordningsföljden för bokstäverna i klartexten.

*M*eddelande - består av mottagarens namn (och eventuellt även adress) samt den text som man vill att han/hon skall läsa.

*K*lartextmeddelande - Meddelande som består av namn m.m. och klartext.

*K*ryptomeddelande - Meddelande som består av namn m.m. och kryptotext.

*R*edigering - Åtgärder som görs på en text efter dekryptering för att stor bokstav, mellanslag och skiljetecken skall införas så att texten blir lätt att läsa för mottagaren.

*I*nternationella 26-bokstavsalfabetet - ABCDEFGHIJKLMNOPQRSTUVWXYZ

*F*orcering - Att ta fram klartexten som hör till en kryptotext utan att på förhand känna till den använda kryptonyckeln.

5. Rövarspråket – lärarsida

Det är lätt att tala rövarspråket. Man bara dubbelskriver varje konsonant och sätter bokstaven O emellan. De första exemplen går man lämpligen igenom med klassen/gruppen på tavlan. Då syns principen tydligt. Allt eftersom eleverna blir säkrare går man över till att prata rövarspråket. Många elever blir så entusiastiska att de övar på egen hand mellan lektionerna och snabbt blir mycket duktiga. Man kan öva rövarspråket några minuter varje kryptolektion.

Kommentarer, ledtrådar och facit

Övning 5A: Svar: KOKOMOM INONTOTE HOHITOT

Övning 5B: Det underlätta tolkningen om man gör ett lodrätt streck mellan de bokstavsgrupper som skall bli en klartextbokstav: HOH|A|NON HOH|A|ROR E|NON HOH|U|NON|DOD !
Svar: Han har en hund!

Övning 5C: Svar: Jag heter Magnus. Vad heter du? / Jag heter.....

Övning 5E: Samma som rövarspråket men med bokstaven E i stället för O mellan de dubbelskrivna konsonanterna. Svar: Jag tycker om honung.

Övning 5F: Man kan leta efter bokstäver och bokstavsgrupper som förekommer ofta. Är de kanske onödiga? Den som ”krypterat” har lagt till OD efter varje konsonant. Stryk dem. Det som är kvar blir klartexten. Svar: Min bästa vän heter Nasse.

Övning 5G: Leta också här efter bokstäver som förekommer ofta. Det står BO före varje konsonant. Stryk dem. Svar: Christoffer Robin.

Övning 5H: Samma som rövarspråket men varje ord är skrivet baklänges. Om man först tar bort alla dubbelskrivna bokstäver med deras O emellan blir det: REGIT RATTUKS DITLLA.
Man ser nog snart att det sista ordet är bakvänt. Om man då prövar att vända alla orden får man svaret.
Svar: Tiger skuttar alltid. (”Alltid skuttar Tiger” kan också godkännas.)

Övning 5I: Här ser man att det finns för många T för att vara vanlig klartext. Man ser också att de förekommer parvis. Stryk alla T. Då ser man svaret. Den som ”krypterat” har satt ett T före och ett T efter varje vokal.
Svar: Uggla är vis och kan skriva.

Övning 5J: Svar: Nalle Puh

Rövarspråket

Om du vill prata med en kompis och inte vill att någon annan skall förstå vad du säger, kan ni använda rövarspråket.

Gör så här: Dubblera alla konsonanter och sätt ett O emellan.
Låt vokalerna vara som de är.

Här är ett exempel. Klart språk: Akta dig!

A är en vokal så den låter vi vara: A
K är en konsonant så den blir KOK
T är också en konsonant så den blir TOT
A låter vi också vara. A

Det första ordet Akta blir alltså A KOK TOT A.

Det andra ordet dig blir på samma sätt DOD I GOG.

Akta dig! blir alltså på rövarspråket AKOKTOTA DODIGOG !

Övning 5A

Klart språk: Kom inte hit!

På rövarspråket: _____

Kolla resultatet med en kompis.

Övning 5B

Vad står det här? HOHANON HOHAROR ENON HOHUNONDOD .

Klart språk: _____

Övning 5C

På rövarspråket: JOJAGOG HOHETOTEROR MOMAGOGNONUSOS.
VOVADOD HOHETOTEROR DODU ?

Klart språk: _____

_____

Svara på rövarspråket:

JOJAGOG HOHETOTEROR _____

Övning 5D

Arbeta två och två. Prata rövarspråk med varandra. Till en början kan det vara bra att skriva ner meningen på rövarspråk på ett papper och lämna det till kompisen.

Utmaningar

Övning 5E

Den här kryptotexten påminner om rövarspråket. Vad står det?

Krypto: JEJAGEG TETYCECKEKERER OMEM HEHONENUNENGEG

Klartext: _____

_____

På nästa sida kommer fler texter som liknar rövarspråket. Försök att forcera dem. Forcera betyder att översätta till klartext utan att veta hur kryptören har gjort. Kryptören är den som har krypterat.

Övning 5F

Krypto: MODINOD BODÄSODTODA VODÄNOD HODETODEROD NODASODSODE

Klartext: _____

_____

Övning 5G

Krypto: BOCBOHBORIBOSBOTOBOFBOFEBOR BOROBOBIBON

Klartext: _____

_____

Övning 5H

Krypto: ROREGOGITOT RORATOTTOTUKOKSOS DODITOTLOLLOLA

Klartext: _____

_____

Övning 5I

Krypto: TUTGGLTAT TÄTR VTITS TOTCH KTATN SKRTITVTAT

Klartext: _____

_____

Övning 5J

Klartexterna på denna sida kommer från en bok som handlar om en liten björn.

Vad heter björnen? _____

6. Omkastningskrypto – lärarsida

I ett omkastningskrypto krypterar man genom att skriva klartextens bokstäver i en annan ordning än den som klartexten har. I detta material visar vi två typer av omkastningskrypto, Lodrätt-vågrätt-krypto och Hålkrypto.

Lodrätt-vågrätt-krypto

Skriv in kryptotexten vågrätt i en rektangel och läs ut klartexten lodrätt.

Övning 6A: Svar: Vi kan inte träffas idag.

Övning 6B: Svar: Bokstaven X har använts i stället för punkt och för att fylla ut tomma rutor. Klartexten läses av från höger till vänster. Klartexten blir: ”Hemligt meddelande. Ladan har brunnit.”

Övning 6C: Svar: LRTÅGOM OIXRÅMI TNHIUTG TLONTIX AÅNTXLM ÄSFEKLY

Övning 6D: Det är viktigt att eleverna verkligen räknar ut hur många rader som behövs när de skall kryptera. Om de tar till för få rader är det lockande att skriva överskjutande bokstäver så att det blir omöjligt att dekryptera. Om raderna blir för många, måste de fylla ut med onödigt många X och det ser inte så bra ut.

Övning 6E: Här skall klartexten läsas ut från vänster till höger men man tar varannan kolumn. Svar: Vi får pizza till lunch idag.

Övning 6F: Att kryptotexten är skriven i grupper om fem bokstäver (femgrupper) är bara ett praktiskt sätt att hantera den. Det sättet används i många autentiska sammanhang. För att forcera kryptotexten måste eleverna först pröva några olika alternativ för antalet kolumner. Man kan tipsa dem om att pröva antalen 5, 6, 7 och 8. Det blir då fyra olika bokstavsområden i rutnätet. Snart finner eleverna att de inte hittar klartexten någonstans om de skall läsa den på det sätt de lärt sig. Om de inte hittar texten tipsar man dem att leta efter texten på något annat sätt. Snart hittar de klartexten skriven nedifrån och upp från höger till vänster i området med sju kolumner.. Svar: Nyckeln är borta. Hur skall jag komma in?

Hålkrypto

Man lägger ett speciellt raster med hål över en kvadrat och skriver in klartextens bokstäver genom hålen i rastret, vrider rastret ett kvarts varv och fortsätter att skriva in. Kryptotexten läses som vanligt, rad för rad, i kvadraten med bokstäverna. Det mest hållbara rastret får man om man kopierar mallen på tunn kartong och sedan skär ut hålen med en vass kniv. Tyvärr tar det ganska mycket tid om man skall förse alla i en större elevgrupp med ett eget raster. Alternativet blir att kopiera mallarna på tjockt papper och låta eleverna klippa ut hålen med en liten sax. Sidan 10 är ett tomt rutat papper som passar för hålkryptot.

Övning 6G: Svar: Fest hos Emma på lördag för kryptoklubben.

Övning 6H: Svar: IXDDLD REÄTUI ÄSKCRK AKGENI INNDTF EÖXTXX

Lodrätt-vågrätt-krypto

Vad står det här: KTLGOAT OIMKCNT MLILKÅA ?

Det är en kryptotext. Bara den som har lärt sig krypto kan ta reda på vad det står. Nu skall vi lära oss hur det går till.

Skriv bokstäverna i kryptotexten i rutor:

K	T	L	G	O	A	T
O	I	M	K	C	N	T
M	L	I	L	K	Å	A

Läs som de lodräta orden i ett korsord, kolumn för kolumn:

KOMTILLMIGKLOCKANÅTTA
Skrivet på vanligt sätt: Kom till mig klockan åtta.

Detta kan man förstå. Det kallas klartext. Att översätta från kryptotext (som man inte förstår) till klartext (som man förstår) kallas att dekryptera.

Övning 6A.

Kryptotext: ASFTNAV GIFRTNI XDAÄEIK .

Den här gången skall vi läsa klartexten från höger till vänster, kolumn för kolumn. Man kan skriva siffror ovanför rutorna för att komma ihåg hur man skall läsa av:

7	6	5	4	3	2	1
A				N	A	V
G					N	I
						K

Siffrorna 7 6 5 4 3 2 1 kallas kryptonyckeln.

Fyll i resten av kryptotexten i rutorna. Läs klartexten och skriv den här:

Klartext: VIKAN _____

Skriv på vanligt sätt.

Klartext: Vi kan _____

Vi har använt bokstaven X för att fylla ut tomma rutor på slutet.

Övning 6B

Kryptotext: NRDDDGH IBAEETE TRNXLMM XUHLAEL XNAANDI

Fyll i kryptotexten på ett rutat papper med 1 cm rutor. Läs klartexten.

Klartext, från rutorna (stora bokstäver): _____

_____

Klartext, skriven på vanligt sätt: _____

_____

Bokstaven X är använd på två sätt. Vilka? Från vilket håll läser du? Skriv siffror ovanför rutorna (kryptonyckeln).

Nu skall du översätta en klartext till kryptotext. Det kallas att kryptera.

Klartext är en text som man kan förstå. Kryptotext är en text som man inte förstår.

Övning 6C

Klartext: Lotta är inlåst. Hon får inte gå ut. Kom till mig. My

Först måste vi ta reda på hur många rader vi behöver till rutorna. Räkna till sju i klartexten. Det måste vi göra sex gånger. Vi behöver alltså sex rader. Fyll i rutorna där klartexten skall vara. Skriv X i stället för punkt. Fyll ut med X om det blir rutor över.

1	2	3	4	5	6	7
L	R					
O	I					
T						
T						
A						
Ä						

Läs kryptotexten rad för rad. Skriv den med sju stora bokstäver i taget här:

_____ _____

_____ _____

_____ _____

_____

Kolla resultatet med en kompis. Nu har du krypterat en text med Lodrätt-vågrätt-krypto.

Nu skall du kryptera ett meddelande och lämna kryptot till en kompis.

Övning 6D

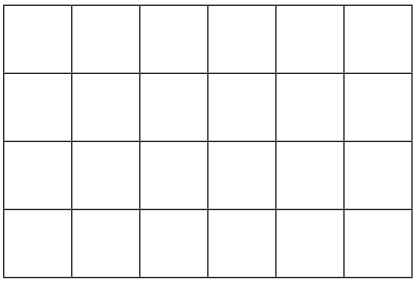
Hitta på en egen klartext, inte för lång. Kryptera den med lodrätt-vågrätt krypto och lämna den till en kompis som får dekryptera den, det vill säga ta reda på klartexten

Utmaningar

Man kan göra Lodrätt-vågrätt-krypto på andra sätt. Vad står det här?

Övning 6E

Kryptotext: VLRNZD ILPCAA FLIHTG ÅUZIIX
Kryptonyckel: 1 4 2 5 3 6



Redigerad klartext: _____

_____

Övning 6F

Här är en kryptotext skriven i grupper om fem bokstäver. Du tror att det är ett krypto som påminner om Lodrätt-vågrätt-krypto. Men du vet inte hur många kolumner som har använts. Det behöver inte vara fem kolumner. Du vet inte heller hur man skall läsa ut klartexten i rutorna. Men du är en duktig forcör, det betyder en person som kan ta reda på klartexten utan att veta hur den som krypterat har gjort.

XAGAH BEXMA KARKX MJSTÄ CNOLR RNYIK LUOLN

Använd ett kladdpapper med rutor om 1 cm sida och gör olika försök.

Klartexten är:_____

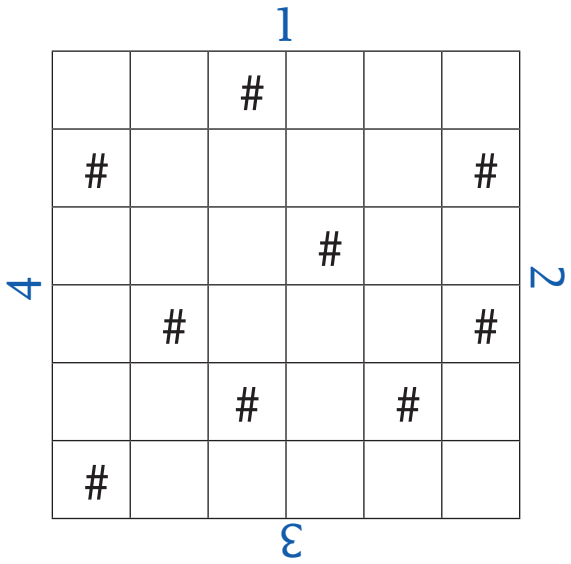
_____

_____

Hålkrypto

Nu skall du få lära dig att skriva bokstäverna på ett listigt sätt. Du skriver dem i en speciell ordning. Det blir väldigt svårt att ta reda på klartexten för den som inte lärt sig krypto.

Klipp ut en mall efter ritningen här nedan. Det blir lätt att använda den om rutorna inuti mallen är precis 1 cm i sida. Klipp sedan hål i de rutor som är markerade med #.



		#			
#					#
			#		
	#				#
		#		#	
#					

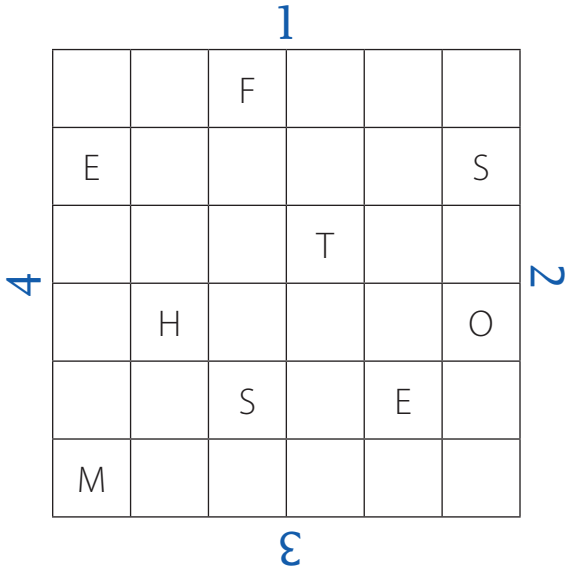
Övning 6G

Skriv kryptotexten i rutorna här nere.

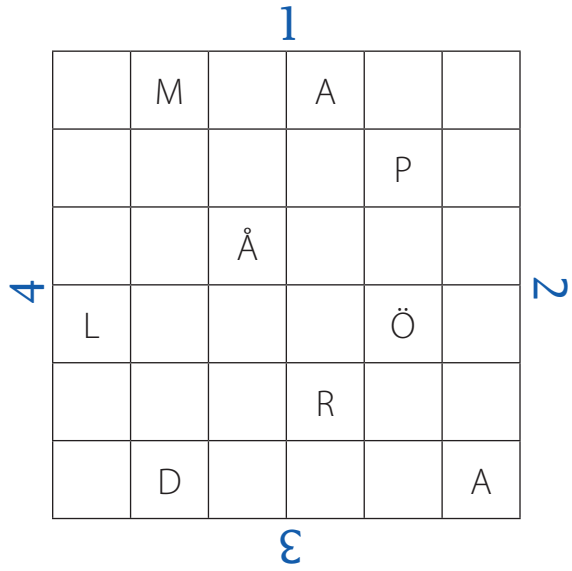
OMFAKG EFLÖPS RUÅTKB
LHRBÖO YESREP MDNTXA

O	M	F	A	K	G
E	F	L			

Lägg mallen över rutorna med kryptotexten. Då ser det ut så här



Kontrollera att dessa bokstäver stämmer med det som står efter Klartext (FESTHOS).
Vrid mallen över rutorna så att tvåan kommer överst. Då ser det ut så här



Skriv nu dessa bokstäver efter de förra. Vrid mallen så att trean står överst. Fortsätt att skriva klartext. Vrid mallen så att fyran står överst. Skriv resten av klartexten.

Klartext: FESTHOS_____

Skriv nu klartexten som vanlig svenska med stor bokstav, mellanrum mellan orden och punkt/utropstecken/frågetecken i slutet av varje mening. Det kallas att redigera klartexten.

Redigerad klartext:_____

_____

_____

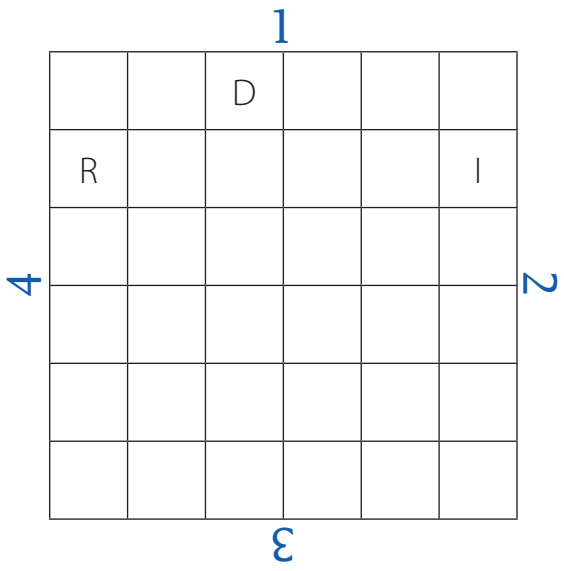
Mallen är hålkryptots kryptonyckel. Se till att bara de som skall läsa klartexten kan få tag på den. Annars kan andra läsa hemligheterna.

Nu skall du kryptera en klartext med hålkrypto.

Övning 6H

Klartext: Drick inte! Du kan dö. Det är gift i läsken.

Lägg mallen över rutorna med ettan uppåt. Skriv klartextens första nio bokstäver genom hålen (påbörjat). Skriv X i stället för punkt och utropstecken. Vrid mallen så att tvåan och sedan trean och till sist fyran kommer uppåt och skriv varje gång nio klartextbokstäver i rutorna.



Skriv kryptotexten här: _____

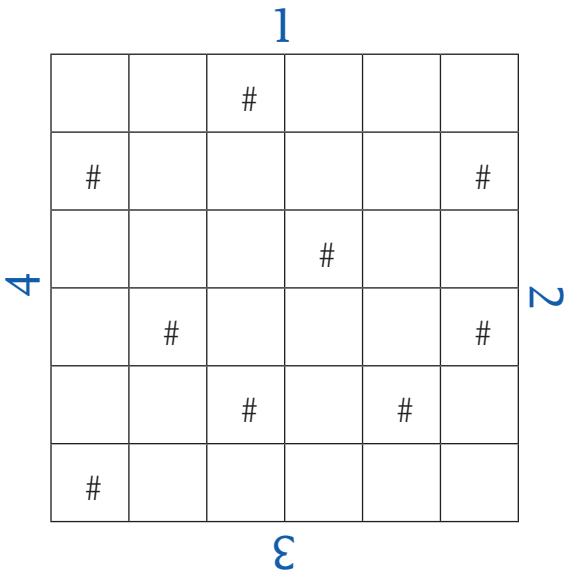
_____

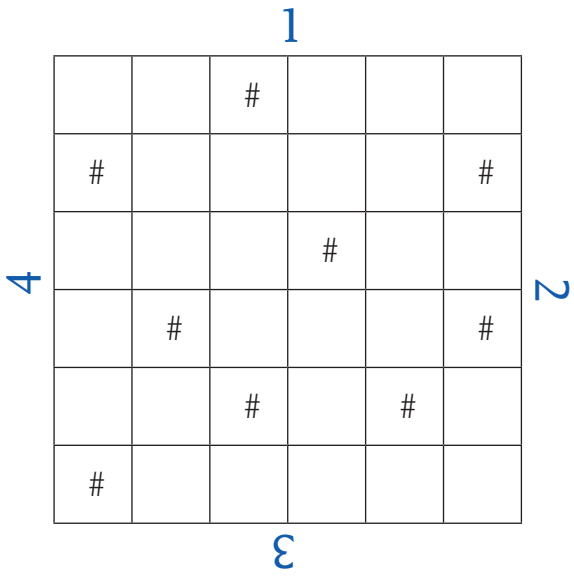
_____

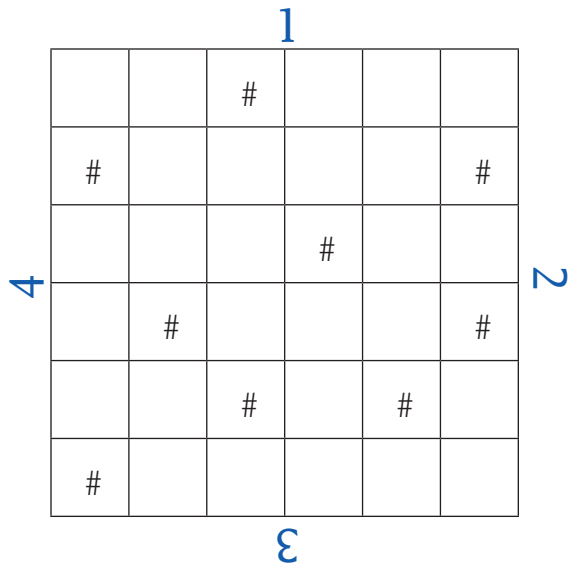
Kolla resultatet med en kompis.

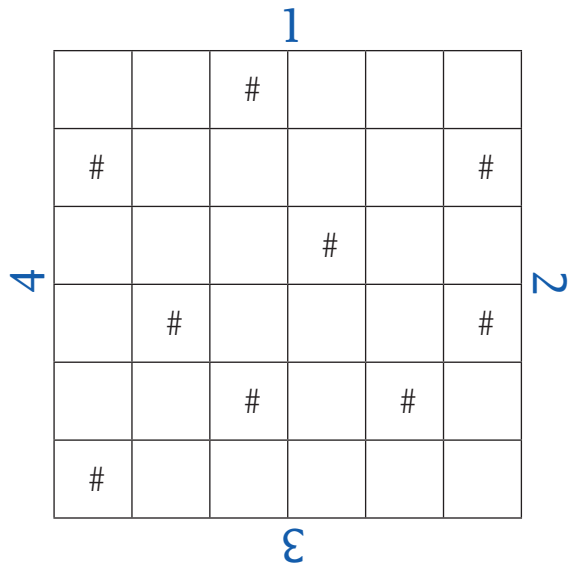
Övning 6I

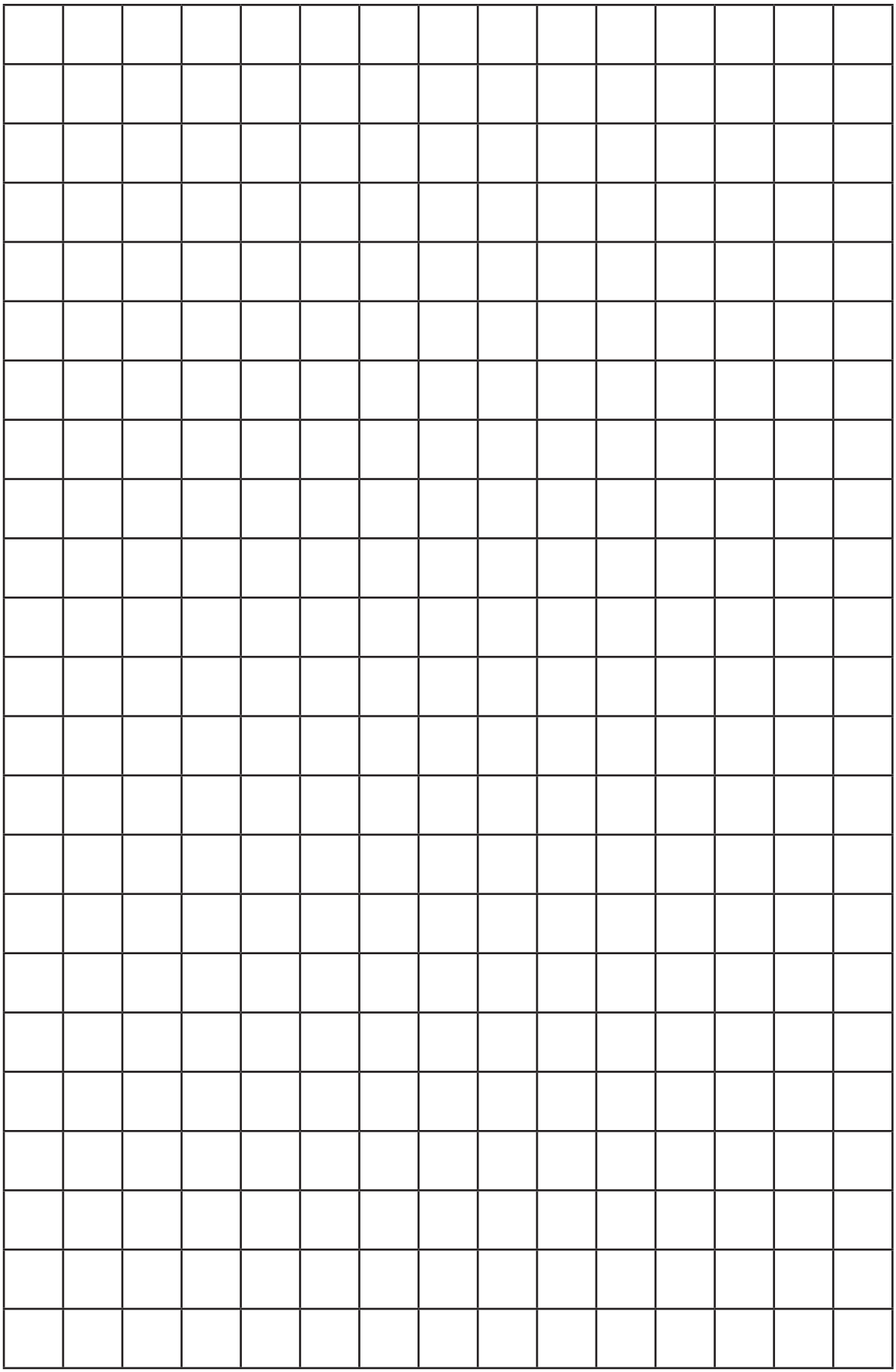
Gör en egen kryptotext för ett meddelande till en kompis. Skriv klartexten genom hålen i mallen på ett rutat papper som du gjort förut. Om klartexten är längre än 36 bokstäver behöver du flera rutor.











7. Byggmästarkrypto – lärarsida

Svar och kommentarer

Övning 7A: Svar: Boken om My är bra.
Övning 7B: Svar: Ge mig nyckeln!

Övning 7C: Svar: 

Övning 7E: Svar: 

Övning 7F: Svar: Var är ringen?
Övning 7G: Tekniken är ”att läsa klartexten på två eller tre rader”. Den som ”krypterat” har använt den första formen av byggmästarkrypto men inte skrivit ut de prickar i kryptotecknen som behövs ibland. Ett första tips är att dekryptera som vanligt och skriva ”klartexten” på den första hjälplinjen under kryptotexten. På den andra hjälplinjen skriver man den ”klartext” som man får om man antar att den finns en prick i varje kryptotecken. Till sist kan man behöva skriva det man får om man antar att det skall finnas tre prickar i den vinkel som utgör det tionde kryptotecknet. Då ser det ut så här:

h	e	d	c	i	g	a	b	c	u	b	b	e	e
q	n	m	l	r	p	j	k	l	y	k	k	n	n
									ö				

Klartexten hittar man genom att leta i de två/tre raderna. Ett tips kan vara att börja leta efter ett ord som brukar finnas i många texter, nämligen ordet ”hemlig”. Svar: Hemliga klubben

Övning 7H: Man bör ha löst uppgift 7G innan man ger sig på det här. Samma teknik, att läsa klartexten på (här) tre rader använder man här. Den som ”krypterat” har använt den andra formen av byggmästarkrypto men inte satt ut de prickar som gör kryptotexten tolkningsbar. Först ”dekrypterar” man och antar att det inte skall vara några prickar alls. Då får man en ”klartext” som börjar så här: g a p d ...Sedan gör man samma sak under antagandet att det alltid skall vara en prick i varje tecken. Och så samma procedur för två prickar. Då ser det ut så här:

g	a	p	d	t	d	p	x	g	a	t	a	g	a	m	p	ä
h	b	r	e	u	e	r	y	h	b	u	b	h	b	n	r	ö
i	c	s	f	v	f	s	å	i	c	v	c	i	c	o	s	.!?

Sedan läser man klartexten genom att ta en bokstav från en lämplig rad.
Svar: Har du frågat chans?

Byggmästarkrypto

Med Byggmästarkrypto byter du ut bokstäverna i en klartext mot tecken som varken är bokstäver eller siffror.

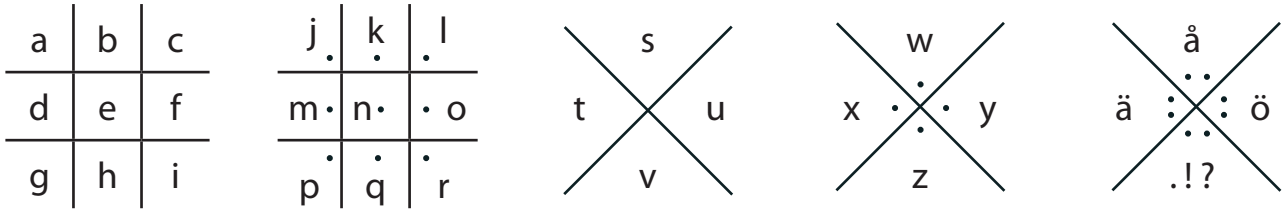
Övning 7A

Så här kan en kryptotext se ut:

Klartext: b o _____

_____

För att ta reda på vad kryptotexten betyder behöver du en kryptonyckel till byggmästarkryptot. Den ser ut så här:



Ett kryptotecken består av de streck som står närmast bokstaven i nyckeln. Ibland måste man lägga till en eller två punkter vid strecken.

Fortsätt att fylla i klartexten ovan. Skriv klartexten med stor begynnelsebokstav, mellanrum mellan orden och skiljetecken. Skriv den på nästa rad. Detta kallas att redigera klartexten.

Redigerad klartext: Bo_____

_____

Övning 7B

Dekryptera det här: 

Klartext: _____

Nu skall du kryptera med byggmästarkrypto.

Övning 7C

Klartext: Var är yxan?

Förbered kryptering genom att skriva texten med mellanrum mellan bokstäverna.

Förberedd klartext: v a r ä _____

_____

Kryptotext: 

Övning 7D

Skriv en egen klartext på ett särskilt papper. Kryptera med byggmästarkrypto. Byt kryptotext med en kompis. Dekryptera.

Byggmästarkrypto – utmaningar

Man kan göra byggmästarkrypto på olika sätt.
Så här kan en kryptonyckel se ut:

Kryptonyckel:

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

Detta byggmästarkrypto använder man på samma sätt som det förra. Som du ser får inte alla bokstäver plats i nyckeln. Om man måste kryptera en bokstav som inte finns med får man hitta på något. Kanske skriva ss i stället för z.

Övning 7E

Klartext: Kryptoskola

Föreberedd klartext: k r y p t o s k o l a

Kryptotext:  _____

Övning 7F

Vad står det här?

Kryptotext: 

Klartext: v a _____

Redigerad klartext: _____

_____

Övning 7G

Här är några tecken som påminner om byggmästarkrypto. Men vad står det? Det ser ut som om det fattas något.

_____

_____

_____

Redigerad klartext: _____

_____

Övning 7H

Och vad står det här?

_____

_____

_____

Redigerad klartext: _____

_____

8. Sifferkrypto – lärarsida

För att använda sifferkrypto använder man en rektangel om 5 gånger 6 bokstäver. Siffror från 0 till 5 ovanför och 5 till 9 till vänster om rektangeln anger hur man översätter klartextens bokstäver till två siffror. Vi använder samma sifferpar för punkt, frågetecken och utropstecken. Efter dekryptering går det lätt att ur sammanhanget bestämma vilket tecken som avses.

Kommentarer, ledtrådar och facit

Övning 8A: Svar: Båten är borta!

Övning 8B: Svar: 65 50 53 50 71 51 75 62 71 71 54 75 95

Övning 8C: --

Övning 8D:
Svar: Vi har hittat båten.
Den som har krypterat har inte brytt sig om att hålla reda på vilken siffra som skall stå först av de två.

Övning 8E: --

Övning 8F: Här är det samma siffror (1, 2, 3, 4, 5) som avgör vilken rad och kolumn som anger bokstaven. Då måste man vara noga med att ange rätt siffra först.
Svar: Lotta fyller år idag.

Övning 8G: --

Övning 8H: För att klara av denna utmaning blir det lättare om man har gjort övningarna 8D och 8F innan. Den som har ”krypterat” har slumpmässigt växlat mellan att skriva radsiffran först och att skriva kolumnsiffran först. Man kan tipsa eleven så här. Dekryptera först och gissa att det är radsiffran som står först. Då börjar ”klartexten” så här: h e m h r g a .. .. .. Dekryptera sedan och gissa att det är kolumnsiffran som står först: l v m l i g a .. .. ..
Skriv sedan dessa ”klartexter” ovanför varandra på de ritade hjälplinjerna. Då ser det ut så här:

h	e	m	h	r	g	a	e	u	g	v	n	u	i	s	d	ä	i	i	a	d
l	v	m	l	i	g	a	v	ä	g	e	s	ä	r	n	p	u	r	r	a	p

Den riktiga klartexten hittar man om man läser omväxlande på dessa rader.
Svar: Hemliga vägen är spärrad.

Sifferkrypto

Med sifferkrypto ersätter du varje bokstav i en klartext med två siffror. Du använder ett sådant här rutnät:

	0	1	2	3	4	5
5	A	B	C	D	E	F
6	G	H	I	J	K	L
7	M	N	O	P	Q	R
8	S	T	U	V	W	X
9	Y	Z	Å	Ä	Ö	.!?

Den första siffran bestämmer raden, andra siffran bestämmer kolumnen.

Övning 8A

Dekryptera den här kryptotexten:

Kryptotext: 51 92 81 54 71 93 75 51 72 75 81 50 95

Klartext: b å t e n_____

Skriv klartexten som på vanlig svenska med stor bokstav i början av en mening, mellanrum mellan orden och punkt/utropstecken/frågetecken i slutet av varje mening. Det kallas att redigera klartexten.

Redigerad klartext: Båten _____

Övning 8B

Nu skall du kryptera den här klartexten:

Klartext: Ladan brinner!

Förbered först klartexten så att den består av små bokstäver.

Gör mellanrum mellan bokstäverna så att siffrorna i kryptotexten får plats under klartextbokstäverna. Kryptera.

Förberedd klartext: l a d_____

Kryptotext: 65 50 53 _____

Övning 8C

Hitta på en egen klartext, kryptera den med sifferkrypto och lämna kryptot till en kompis som får dekryptera den.

Övning 8D

Vad är detta? Är det någon som bara skojat?

Kryptotext: 38 62 61 05 57 16 26 81 18 50 18 15 92 81 45 71 59

Klartext: _____

Redigerad klartext: _____

_____

Hur blev det så här? Svara här:

Den som har krypterat _____

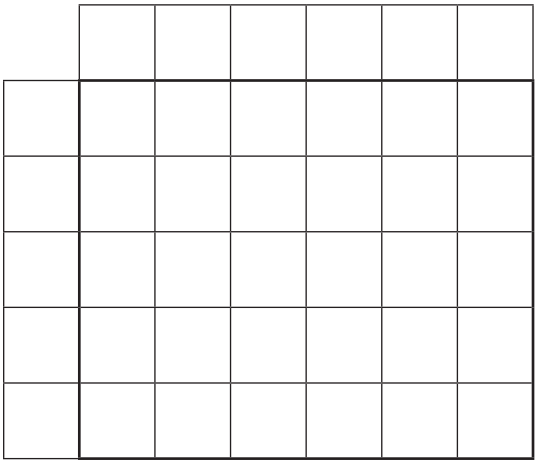
_____

_____

Rutmönstret med siffror och bokstäver som vi har använt för att kryptera och dekryptera kallar vi kryptonyckeln till sifferkryptot. Du kan göra andra sifferkrypton om du skriver siffrorna och bokstäverna i en annan ordning i ett sådant rutmönster. Du får då en annan kryptonyckel, men vi kallar det fortfarande sifferkrypto.

Övning 8E

Hitta på en egen kryptonyckel till sifferkrypto och skriv in den i rutmönstret:



Hitta på en egen klartext. Kryptera den med kryptonyckeln som du nyss har gjort. Byt kryptonyckel och krypto med en kompis och dekryptera.

Man kan skriva kryptonyckeln till sifferkrypto med samma siffror för första och andra siffran, så här:

Kryptonyckel:

Andra siffran

Första siffran	0	1	2	3	4	5
1	A	B	C	D	E	F
2	G	H	I	J	K	L
3	M	N	O	P	Q	R
4	S	T	U	V	W	X
5	Y	Z	Å	Ä	Ö	.!?

Då måste man hålla reda på vilken siffra som skall skrivas först.

Övning 8F

Vad står det här?

Kryptotext: 25 32 41 41 10 15 50 25 25 14 35 52 35 22 13 10 20 55

Klartext: I o _____

Redigerad klartext: _____

Övning 8G

Skriv en egen klartext på ett särskilt papper, kryptera den med sifferkrypto. Använd nyckeln på förra sidan. Byt kryptot med en kompis och dekryptera.

Utmaning

Övning 8H

Annika hittade ett papper med bokstäver och siffror på. Så här såg det ut:

	0	1	2	3	4
0	A	B	C	D	E
1	F	G	H	I	J
2	K	L	M	N	O
3	P	R	S	T	U
4	V	Y	Å	Ä	Ö

12 04 22 12 31 11 00

04 34 11 40 23 34 13

32 03 43 13 13 00 03

Annika som är bra på krypto tror att det är ett sifferkrypto men hon kan inte ta fram klartexten. Kan du hjälpa henne?

_____

_____

_____

Klartext: _____

Nämnarens kryptoskola

9. Kryptokoder och morsealfabetet – lärarsida

När man krypterar med en kod översätter man hela ord eller uttryck med en kodgrupp. I det här avsnittet skall vi använda kodgrupper som består av en bokstav och en siffra. Tabellen som talar om hur man skall översätta uttrycket kallas kodnyckeln. Kodmeddelanden blir korta, men man måste veta ungefär vad det är för klartexter som man skall kryptera. Annars blir det svårt att göra kodnyckeln.

Elevmaterialet innehåller två olika kodnycklar för olika intresseinriktningar. Det finns också en övning där eleverna kan göra en egen kodnyckel. Detta kanske lämpar sig bättre som uppgift till en grupp elever.

Kommentarer och facit

Övning 9A: Här står ordet HAR i klartext mitt bland kodgrupperna. Så kan man göra om det inte är något som avslöjar någon hemlighet.
Svar: Sofie har födelsedag på söndag. Ring mig i morgon.

Övning 9B: Svar: Till alla i hemliga klubben. C2 F3 G4 E3

Övning 9C: --

Övning 9D: Svar: Till Viktor. Cykelklubben har träning på lördag klockan 10.

Övning 9E: Svar: Till alla i cykelklubben. A5 Q2 G1 H4 G2 I5 O5 C2 G1

Övning 9F: --

Övning 9G: --

Övning 9H: --

Telegrafi – morsealfabetet

Morsealfabetet är inget krypto. Vem som helst som har lärt sig det kan tolka vad som står om man snappar upp ett morsemeddelande. Men man skickade ofta kryptomeddelanden med telegrafi och använde då morsealfabetet. Därför kan det vara intressant att få veta litet om det.

Övning 9I: Svar: Ylva, som läses Da di da da, di da di dit, di di di da, di da.

Koder

När man krypterar med en kod översätter man hela ord eller uttryck med en kodgrupp. I den här kursen skall vi använda kodgrupper som består av en bokstav och en siffra, till exempel C2. Här är en kodnyckel. Där kan man se hur översättningen går till.

	1	2	3	4
A	Emma	Viktoria	Johanna	Helena
B	Isabella	Hanna	Sofie	Ida
C	födelsedag	fest	present	tårta
D	glass	godis	saft	läsk
E	i dag	i morgon	på lördag	på söndag
F	stallet	fotbollsplanen	hemma hos	i skolan
G	kom till	kom inte till	ring	mig

Ett kodmeddelande kan se ut så här:

Övning 9A

Till Johanna. B3 har C1 E4 G3 G4 E2. Vad står det?

Klartext:_____

_____

_____

Kodmeddelanden blir korta. Men man måste veta ungefär vad det är för klartexter som man skall kryptera. Annars blir det svårt att göra kodnyckeln.

Övning 9B

Nu skall du kryptera det här meddelandet:

Till alla i hemliga klubben. Fest hemma hos mig på lördag.

Kodmeddelande: Till alla i hemliga klubben. C2 _____

_____

Kontrollera resultatet med en kompis.

Övning 9C

Nu skall du hitta på ett eget meddelande med ord som finns i kodnyckeln. Kryptera det och byt kodmeddelande med en kompis.

Ibland vill man också kunna kryptera sådana ord som man inte tog med när man gjorde upp kodnyckeln. Då kan det vara bra att ha alfabetets bokstäver i kodnyckeln. Det kan också vara bra att ha siffrorna där. En sådan kodnyckel kan till exempel se ut som på nästa sida:

	1	2	3	4	5
A	Felix	Viktor	Johan	Filip	Daniel
B	Anton	Joakim	Gustav	Simon	Fredrik
C	i går	i dag	i morgon	på lördag	på söndag
D	klockan	kom till	kom inte till	ring	mig
E	0	1	2	3	4
F	5	6	7	8	9
G	. ! ?	a	b	c	d
H	e	f	g	h	i
I	j	k	l	m	n
J	o	p	q	r	s
K	t	u	v	w	x
L	y	z	å	ä	ö
M	cykel	klubben	ambulans	bak	bromsar
N	bår	fram	handskar	helikopter	hjul
O	hjälm	hjärnskakning	hopp	idealspår	komma tvåa
P	körstil	laga	platå	punktering	reka banan
Q	reparera	skadad	skivbroms	terrängbanan	träning
R	tävling	utväxling	vinna	växlar	V-broms

Övning 9D

Ett kodmeddelande kan se ut så här:

Till Viktor. M1 M2 H4 G2 J4 Q5 C4 D1 E2 E1 G1 Vad står det?

Till Viktor. Klartext: Cykelklubben _____

_____

Övning 9E
Kryptera det här meddelandet:

Till alla i cykelklubben. Daniel skadad. Han kom tvåa idag.

Kodmeddelande: Till alla i cykelklubben. A5 _____

_____

Kontrollera resultatet med en kompis.

Övning 9F
Nu skall du hitta på ett eget meddelande med ord som finns i kodnyckeln. Kryptera det och byt kodmeddelande med en kompis.

Grupparbete

Övning 9G
Nu skall ni göra en egen kodnyckel. Tänk er att ni har en klubb, som ... Ja, vad håller ni på med? Ibland kanske ni vill skicka meddelanden till varandra, meddelanden som andra personer inte skall få läsa. Gör en kodnyckel som är lämplig för detta. Gör en kladd på ett särskilt papper. Renskriv kodnyckeln på ett annat papper.

Övning 9H
Gör ett kodmeddelande med kodnyckeln som ni har gjort och lämna till någon annan i gruppen. Dekryptera det meddelande som du får.

Telegrafi - morsealfabetet

För att skicka ett meddelande från en avsändare till en mottagare använde man särskilt förr i tiden det så kallade morsealfabetet. En bokstav består då av långa och korta signaler:

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** ▬ ▬ ▬ ▬	

En lång signal skall vara tre gånger så lång som en kort. Mellanrummet mellan signalerna i ett tecken skall vara lika långt som en kort. När man läser ett morsetecken kallar man en lång för da. En kort kallas di. Men om en kort signal kommer sist i ett tecken säger man dit (med kort i).

Exempel: ▬ ▬ ▬ ▬ ▬ ▬ ▬ ▬ ▬ betyder Arne

och läses di da, di da dit, da dit, dit.

Övning 9I

Vad står det här:

Svar:_____Läses: _____

Övning 9J

Skriv ditt namn med morsetecken:

Hur läser man det: _____

_____

Övning 9K

Skriv ett ord med morsetecken här:

och låt en kompis tolka det.

Skriv svaret här:_____

_____

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.

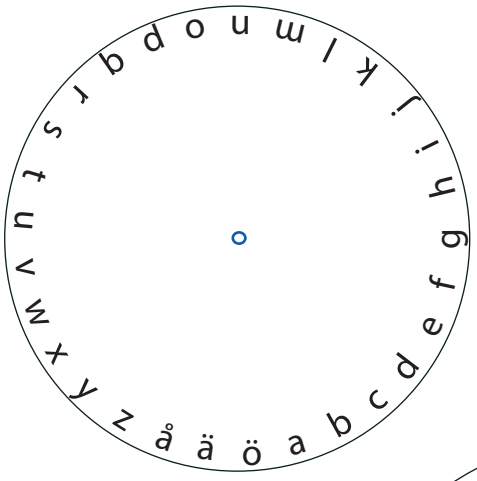
Hitta på en egen klartext och kryptera den med den kryptonyckel som ni har gjort. Byt krypto med kompisen och dekryptera det meddelande som du får.

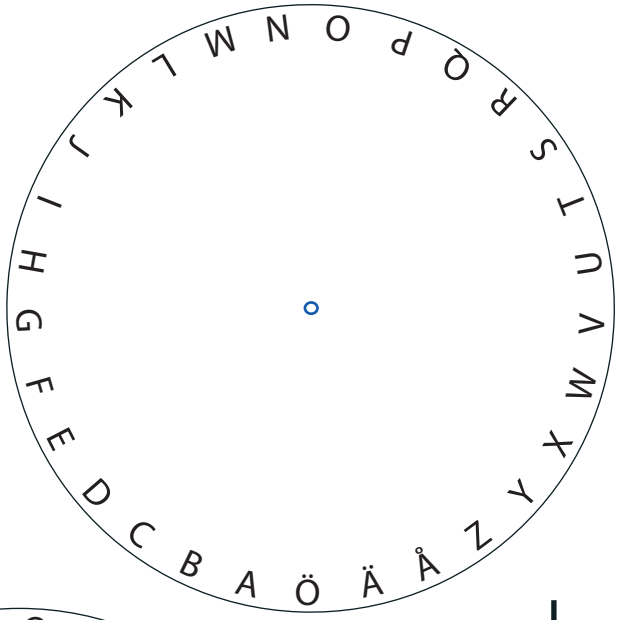
Gör en egen kryptosnurra

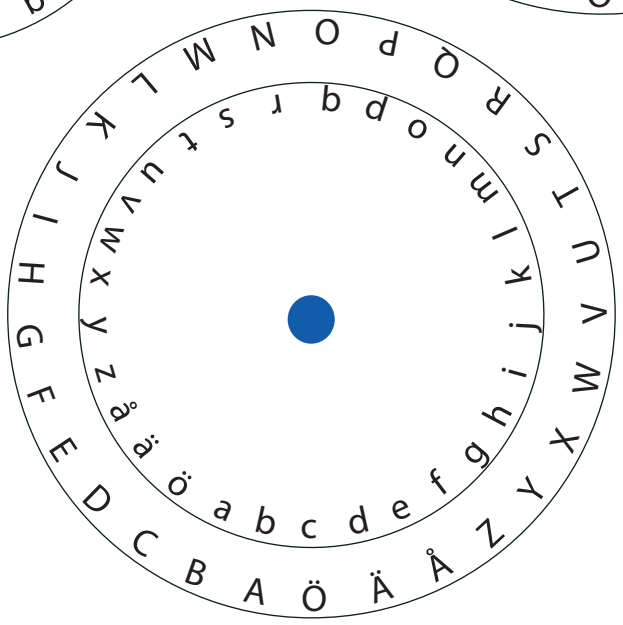
Du kan ha kryptonyckeln på två runda pappskivor som du sätter ihop med en pappersklämma i mitten. Du kan använda cirklarna på denna sida som mall.

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																										

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																										

Nämnarens kryptoskola

12. Kryptotext utan ÅÄÖ – lärarsida

I bland kan bokstäverna Å, Ä och Ö ställa till problem när man skall skicka ett krypto-meddelande. Det kan t. ex. hända om man vill skicka meddelandet över Internet till någon som bor utomlands. Alfabetet ABCDEFGHIJKLMNOPQRSTUVWXYZ (utan ÅÄÖ) kallas det internationella alfabetet.

I det här avsnittet får eleverna lära sig hur man kan koda texter, skrivna med vårt 29-bokstavsalfabet, så att resultatet får bokstäver ur det korta alfabetet. Dessutom finns utmaningar i att tolka meningar där man misslyckats med en sådan kodning.

Kommentarer, ledtrådar och facit

Övning 12A: Svar: Häxan är på ön.

Övning 12B: Svar: b y k s o r n a x a e r x f o e r x l a a n g a

Övning 12C: Svar: FCOWS VREBE IVBJS IVBPE ERKE

Övning 12D: Här har ä blivit #, å blivit % och ö har blivit £.
Svar: Det är lätt att svara på din fråga. Övergångsstället är vitmålat.

Övning 12E: Alla svenska bokstäver (å, ä och ö) har blivit ? . När man kommit på det kan man prova de tre alternativen, om man inte ser med detsamma vad det skall stå, till exempel bår, bär eller bör för det första ordet.
Svar: Du bör hålla ålen bakom ögonen så att den inte förstörs.

Övning 12F: Här har å, ä, ö blivit ers. När man har kommit på det, kan man använda samma teknik som i övning 12E.
Svar: Lägg gäddan på bänken och ös båten före kvällen!

Övning 12G: Alla å, ä och ö har försvunnit helt.
Svar: Det växer en rönn på ön i ån.

Övning 12H: Här har alla å, ä, ö blivit € . Dessutom har det efterföljande tecknet försvunnit. Det som kommit bort i det första ordet är ”åt” och i det andra ordet ”å och mellanslag”.
Svar: Vi har skickat åtta foton som vi tog i Peking och på några andra ställen. Låt oss få reda på när de kommit fram. Hjärtliga hälsningar från Åke och Örjan.

Övning 12I: Här ser man vad en kinesisk ordbehandling kan ställa till med.
å har blivit å
ä har blivit ä
ö har blivit ö
Svar: Det är konstigt att skriva ä med ae, å med aa och ö med oe. Jag hoppas att ni kan förstå vad jag menar. Varma hälsningar.

Kryptotext utan ÅÄÖ

Ibland kan bokstäverna Å, Ä och Ö ställa till problem när man skall skicka ett meddelande. Det kan hända om man vill skicka meddelandet över Internet till någon som bor utomlands. Alfabetet ABCDEFGHIJKLMNOPQRSTUVWXYZ (utan ÅÄÖ) kallas det internationella alfabetet.

Då är det bäst att översätta å, ä och ö till någonting annat innan man krypterar. Vi bestämmer oss också för att använda bokstaven x som mellanrum mellan ord eller meningar. Då måste vi också ersätta bokstaven x i klartexten med någonting annat. Vi översätter

å till aa	ä till ae	ö till oe	x till ks

Övning 12A

En klartext, förberedd för kryptering, kan se ut så här:

Förberedd klartext: h a e k s a n x a e r x p a a x o e n .

Vad står det? Skriv svaret här: _____

_____

Nu skall du förbereda en klartext på det här sättet och kryptera den med Caesarkrypto så att det inte blir några å, ä eller ö i kryptotexten. Använd x som ordmellanrum.

Övning 12B

Klartext: Byxorna är för långa.

Förberedd klartext: b y k s o _____

_____

Nu finns inga å, ä eller ö i klartexten. Då kan du kryptera med den här kryptonyckeln. Tänk på att hålla reda på små och stora bokstäver!

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

Övning 12C

Skriv kryptotexten med fem stora bokstäver i taget.

Kryptotext: F C O W S _____ _____ _____ _____

Kolla resultatet med en kompis.

Text utan åäö - några utmaningar

Här är några texter där å, ä och ö har blivit något helt annat. Vad står det?

Övning 12D

Det #r l#tt att svara p% din fr%ga. £verg%ngsst#llet #r vitm%lat.

Svar: _____

_____

Övning 12E

Du b?r h?lla ?len bakom ?gonen s? att den inte f?rst?rs.

Svar: _____

_____

Övning 12F

Lersgg gersddan pers bersnken och erss bersten fersre kversllen!

Svar: _____

_____

Övning 12G

Det vxer en rnn p n i n.

Svar: _____

_____

Och här är två Internetmeddelanden från Kina. I det första har de svenska bokstäverna kommit bort och ersatts av €. Dessutom har ett tecken till försvunnit.

Övning 12H

Vi har skickat €ta foton som vi tog i Peking och p€n€ra andra st€len. L€ oss f€reda p€n€ de kommit fram. Hj€tliga h€sningar fr€ €e och €jan.

Svar: _____

_____

_____

Övning 12I

Det är konstigt att skriva ä med ae, å med aa och ö med oe. Jag hoppas att ni kan förstå vad jag menar. Varma hälsningar.

Svar: _____

_____

_____

_____

13. Extra utmaningar – lärarsida

Extra utmaningar nr 1

Här har författaren dolt texten genom att blanda i extra bokstäver. Det påminner något om rövarspråket.

Övning 13A: Ett tips kan vara att försöka hitta bokstäver som inte förekommer på ett normalt sätt i en text. Eleven hittar då kanske A, B, C, D, E, ... på varannan plats i texten. Om man stryker dem så ser man klartexten. Alternativt kan man tipsa om att leta efter ett sannolikt ord, t. ex. HEMLIG. Då ser man också hur kryptören gjort. Svar: Hemligt meddelande.

Övning 13B: Efter ett tag ser nog eleven att orden är skrivna baklänges och uppdelade i femgrupper. Sista gruppen är utfylld med XXXX.
Svar: På det fjärde gäller det. På det femte smäller det.

Övning 13C: Ett första tips kan vara att leta efter konstiga bokstäver. Eleven ser många X och Z. Om man stryker dem återstår: ALLORTNAKRETTO-PYRRAH. Läs baklänges.
Svar: Harry Potter kan trolla.

Extra utmaningar nr 2

Dessa övningar visar att det finns överflödig information i vårt sätt att bilda ord. Vi kan få fram betydelsen även om bokstäverna är omkastade eller delvis saknas.

Övning 13E: Svar: Emil i Lönneberga hette en pojke som bodde i Lönneberga.

Övning 13 F: Man kan tipsa om att denna mening kommer från samma bok som i föregående exempel. Ju mer förhandsinformation man har om en text desto enklare blir forceringen.
Svar: Emil hade en lillasyster som hette Ida.

Övning 13G: Svar: Barnens dag i Bullerbyn

Övning 13H: Den här övningen är mycket svårare än 13G eftersom konsonanterna bär mycket mer information om innehållet än vokalerna. Men det underlättar om man vet eller gissar att texten kommer från samma bok.
Svar: Vi ska göra barnens dag åt Kerstin.

Övning 13I: Svar: Dyk, Ronja, skrek Birk!

Övning 13J: Tips: Jämför med övning 13I.
Svar: Ronja tittade på Birk.

Övning 13K: Svar: Astrid Lindgren

Övning 13L: Svar: Tja! Läget? God dag! Hur mår du?

Extra utmaningar nr 1

Övning 13A
Vad står det här:

AHBEC MDLEI FGGTH MIEJD KDLEM LNAON PDQER

Svar:_____

_____

Övning 13B
Vad står det här:

TEDRE LLÄMS ETMEF TEDÅP XTEDR ELLÄG EDRÄJ FTEDÅ PXXXX

Svar: _____

_____

_____

Övning 13C
Vad står det här:

ZAXLZ LXOZR XTZNX AZKXR ZEXTZ TXOZP XYZRX RZAXH

Svar:_____

_____

Övning 13D
Hitta på ett annat sätt att gömma en text: Skriv här:

_____

_____

_____

_____

Lämna till en kompis och se om det går att lista ut vad du menar.

Extra utmaningar nr 2

Även om man blandar om bokstäverna i orden i en text kan man ofta se vad det står ändå. Vad står det här? Skriv rätt text på raden under:

Övning 13E
Emli i Lönnebrega ttehe ne pokje smo debod i Bergalennö.

Rätt text: _____

_____

Övning 13F
Här är bokstäverna blandade ännu mera. Men du kan säkert lista ut vad det skall stå.

Elim deha ne sysllaliter mos tehet Dai

Rätt text:_____

_____

Även om man tar bort några bokstäver i en text kan man ibland läsa vad det står ändå. Här är några exempel.

Övning 13G
Här har vi tagit bort vokalerna:

B__r n__n s d__g __ B__l l__r b__n Vad står det? Fyll i det som fattas.

Om man tar bort konsonanterna blir det mycket svårare:

Övning 13H

__i __ __a __ ö__a __a__ __e__ __ __a __ å__ __e__ __ __i __.

Och här är två exempel från en annan bok.

Övning 13I

Utan vokaler: D__k, R__n j a, s k r__k B__ r k!

Övning 13J

Utan konsonanter: __ o__ __ a __i__ __a __e __å __i__ __.

Övning 13K

Vem har förresten skrivit böckerna som texterna är tagna ifrån?

_____

Ibland kan man se vad det står utan en enda bokstav: Vad säger ungdomar till varandra ibland när de träffas - och vad säger äldre?

Övning 13L

__ __ __ ! __ __ __ __ __ ?

__ __ __ __ __ __ ! __ __ __ __ __ __ __ __ ?

14. Examensarbete

Kanske finns det några elever i en kryptokurs som är snabba och mogna för en mer omfattande arbetsuppgift. Ett förslag till en sådan uppgift finns nedan. Den kan givetvis anpassas efter förhållandena och tillgång av tid.

Kryptobok

Om en grupp eller klass elever har följt en kryptokurs kan det vara intressant för dem att samla resultatet, alla ifyllda kopieringsunderlag, alla rutiga och randiga arbetspapper som eleven använt. Man kan göra ett häfte, ”kryptobok” av detta. Ett förslag till försättsblad finns sist i detta avsnitt.

Här kan man för hand eller med dator fylla i skolans namn, termin och läsår samt klass.

Exempel på examensarbete

Arbeta två och två, först tillsammans:

Bestäm ett krypto som ni vill använda. Kryptotexten skall bestå av bokstäver i internationella alfabetet ABCDEFGHIJKLMNOPQRSTUVWXYZ eller siffror. Ni får gärna hitta på något eget.

Tillverka en nyckel till det krypto ni valt.

Sedan arbetar ni var för sig med att skriva en klartext, 50 - 100 bokstäver lång. Om det behövs, förbered den så att den går att kryptera.

Kryptera texten.

Skriv kryptotexten i grupper om fem bokstäver (eller siffror).

Gör ett kryptomeddelande av kryptotexten genom att sätta dit namn (och eventuellt adress) på den som skall ha meddelandet (din kompis).

Byt kryptomeddelanden med varandra.

Dekryptera kryptotexten i meddelandet som du fått av din kompis.

Redigera meddelandet så att det blir lätt att läsa (stor bokstav i början av en mening, mellanrum mellan orden och punkt/utropstecken/frågetecken i slutet av varje mening).

Utvärdera arbetet tillsammans genom att beskriva hur det gick. Skriv vad som var lätt och vad som var svårt. Ta gärna reda på vad andra skrivit om krypto och jämför med era erfarenheter.

Lycka till!

Krypto – hemlig skrift

av _____

klass _____

15. Inledning

Avsnitten från och med nummer 15 är en fortsättning av Nämnarens kryptoskola som sedan december 2006 finns tillgänglig på NCMs webplats. Vi förutsätter att den som vill arbeta med fördjupningskursen har tillgodogjort sig grundkursen, som omfattar avsnitten 4 - 14. Man bör särskilt känna sig förtrogen med avsnitten 10 och 11. Vi som har utformat denna del av kryptoskolan heter Bengt Beckman och Stig-Arne Ekhall. Språkstatistiken har tagits fram av Jesper Ekhall.

I fördjupningskursen behandlar vi nästan endast forcering. Det betyder att från en kryptotext ta reda på den klartext som man har använt för att med kryptering åstadkomma kryptotexten utan att veta hur krypteringen har gått till i detalj. Det viktigaste hjälpmedlet är klartextens statistiska struktur, till exempel hur ofta en viss bokstav och bokstavskombinationer normalt förekommer i löpande text på det språk som klartexterna är avfattade på. Oftast gäller det svenska språket, men vi uppmanar forcörerna att även pröva engelska eller eventuellt annat språk som man behärskar.

Vi tänker oss att de som arbetar med fördjupningskursen är något äldre än de som ägnade sig åt grundkursen. Eleverna går nog i grundskolans högstadium eller på gymnasiet. Vi tror att de själva hämtar ner avsnitten från NCMs webplats och därför finns här i de olika avsnitten inte någon lärarsida med inledning, tips och svar till övningsuppgifter.

Bäst lär man sig krypto om man är två personer som samarbetar. Dessutom är det roligare än att vara ensam. Man kan utmana sin kryptokompis med kryptotexter och se efter om han/hon kan forcera dem. Liksom i grundkursen föreslår vi därför i första hand att två elever arbetar tillsammans med materialet, som är utformat med det som förutsättning. Men det går också bra att tillgodogöra sig kursens innehåll om man är ensam i studiearbetet.

Uppgifterna i fördjupningskursen tar längre tid att genomföra än uppgifterna i grundkursen. Ibland kan de nog vara tålamodsprövande. Fast om man tänker på hur ungdomar i dag kan sitta i timmar vid datorn med spel och andra aktiviteter, så blir det uppenbart att de även kan ägna en hel del tid också för att lära sig de första grunderna i forcörens spännande arbete. Den som kan datorprogrammering uppmanas att själv göra program som hjälpmedel för arbetet med kryptering, dekryptering och forcering.

Bengt Beckman *Stig-Arne Ekhall*

16. Språkstatistik

I grundkursen lärde ni er hur olika krypton är beskaffade. Ni fick lära er att kryptera och dekryptera på olika sätt. I slutet av kursen fick ni nosa på kunskap hur man forcerar, knäcker krypton utan kunskap om hur de är gjorda. I denna del av kursen fortsätter ni att lära er forcering.

Ett nödvändigt hjälpmedel är språkstatistik. Man måste först av allt veta hur vanlig en viss bokstav är i klartexten. Därför börjar ni med att göra en enkel pinnstatistik. Skriv först alfabetets bokstäver lodrätt på ett rutat eller linjerat papper. Sedan tar ni fram en svensk text från en tidning eller en bok. Börja var som helst i texten, gå igenom texten bokstav för bokstav, hoppa över mellanslagen och sätt en ”pinne” efter respektive bokstav. Sluta efter 80 bokstäver. Strunta i om ni slutar mitt i ett ord eller inte.

Antagligen kommer er statistiska uppställning att se ut ungefär som i tabellen till höger:

Det skall finnas 80 stycken ”pinnar”, en pinne för varje bokstav i den valda texten. I exemplet som vi visat här, ser ni också att det finns sju ’a’, ett ’b’ och så vidare och att det inte finns någon bokstav som har förekommit fler än 7 gånger.

Bokstäverna q, w, x, y och z är ovanliga i svenska språket. Därför är det nog tomt, ”nollor”, även i er språkstatistik. Vilka andra iakttagelser gör ni?

a	𝍸 II
b	I
c	I
d	IIII
e	𝍸 II
f	I
g	II
h	II
i	𝍸
j	
k	IIII
l	𝍸
m	III
n	𝍸 I
o	𝍸
p	II
q	
r	𝍸
s	𝍸 I
t	𝍸 II
u	I
v	III
w	
x	
y	
z	
å	I
ä	I
ö	I

Övning 16A

Gör fyra statistiker på avsnitt om 80 tecken svensk text och jämför resultaten.

Om man gör språkstatistik på en stor mängd svensk text finner man att bokstaven 'e' är vanligast, sedan kommer 'a' och därefter 'r' 'n' 't' 's' 'i' 'l' 'd' och 'o' i ordning. Ni såg i övning 16A att detta inte alltid stämmer för korta textavsnitt. I avsnitt 24 finns olika språkstatistiker för svenska och engelska. De är nödvändiga hjälpmedel när ni skall fördjupa er ännu mer.

Tänk på att använda små bokstäver för klartexter. För kryptotexter används stora bokstäver. Ni såg i avsnitten 10 och 11 i grundkursen att det är praktiskt att skilja klartext från kryptotext på detta sätt.

Övning 16B

Vad är det för märkligt med klartextstatistiken tilll höger här på sidan? Hur kan det ha det blivit så?

a	𝍸
b	/
c	/
d	////
e	𝍸
f	/
g	//
h	//
i	////
j	
k	///
l	////
m	//
n	𝍸
o	////
p	//
q	
r	////
s	////
t	𝍸/
u	/
v	//
w	
x	𝍸𝍸𝍸//
y	
z	
å	
ä	/
ö	/

17. Caesarkrypto och språkstatistik

I detta avsnitt får ni se hur en statistik över bokstäverna i en kryptotext ser ut som kommer av Caesar-krypto och hur den liknar statistiken för klartext. Ni får också se hur man kan utnyttja detta för att få fram kryptonyckeln som man har använt. På så sätt har ni fått ett nytt sätt att forcera Caesar-krypto.

Till höger är slutet av statistiken för en 80 teckens kryptotext som hör till ett Caesarkrypto. När man krypterar med Caesarkrypto ersätter man varje klartextbokstav med den bokstav som kommer ett visst antal steg längre fram i alfabetet. Det antal steg som man använder kallas kryptonyckeln för kryptot och det skall vara oförändrat för ett helt meddelande. Det borde betyda att språkstatistiken med dess toppar och nollor har förskjutits lika många steg neråt, d.v.s. framåt i alfabetet som kryptonyckeln anger. (Och den del som ramlar över kanten efter 'ö' finns överst i statistiken från och med 'a'.)

R	////
S	///
T	
U	~~////~~ //
V	~~////~~
W	~~////~~ ///
X	/
Y	//
Z	
Å	
Ä	
Ö	

I exemplet ovan kan man se att det finns en lucka med fyra nollor vid ZÅÄÖ. Kan det motsvara klartextens wxyz ? Det stämmer med de tre topparna UVW som kan motsvara rst i klartexten och i så fall med T som motsvarighet till nollan 'q'. Om ni vill se kryptonyckeln mycket tydligt kan ni använda en kryptonyckelmall.

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																	T	U	V	W			Z	Å	Ä	Ö			

T kommer tre steg efter klartextbokstaven 'q' och så vidare. Det verkar mycket troligt att nyckeln till denna kryptotext är 3. Fyll i resten av kryptonyckeln.

Övning 17A och 17B

Ni kan nu gå tillbaka till grundkursens övningar 11A och 11B. Kryptotexterna är kortare än 80 tecken, men ni kan göra pinnstatistik på kryptotexterna och se om ni kan få fram kryptonyckeln med dem. Ta var sin övning och jämför era erfarenheter.

Övning 17C

Arbeta först var för sig. Leta upp var sin text, 50 - 80 bokstäver lång. Bestäm var sin kryptonyckel (ett tal mellan 1 och 28) och håll text och nyckel hemliga för kompisen. Caesar-kryptera och byt kryptotext med varandra. Gör pinnstatistik på kompisens kryptotext och bestäm vilken kryptonyckel som använts. Dekryptera texten. Byt erfarenheter med varandra.

Övning 17D

Forcera den här kryptotexten. Den är skriven med fem bokstäver i taget för att det skall vara enklare att hantera den. Gör pinnstatistik. Det är en fördel att vara två personer även här. En läser bokstäverna och en sätter pinnarna i statistikrutorna. Studera statistiken. Hur är kryptot gjort? Dekryptera Vad står det?

ZYJVB LBLYJ JQYZZ YRÖPZ YKOQS LENJY LÖJKQ YZYJJ PEÅSY
RÖRXÖ ÄYJKO QKSLU HUJKÄ ÖSRBP WYKFF

18. Engelska och andra språk

Övning 18A

Ta fram en engelsk bok eller tidning och gör pinnstatistik på några avsnitt om 80 bokstäver. Det blir bara 26 rader i statistiken. Engelskan har ju inte 'å', 'ä' eller 'ö'. Jämför med de svenska statistikerna. Vad finns det för likheter? Vilka "nollor" finns? Andra olikheter? Förklara dem med exempel från engelska ord. Om man gör statistik på en stor mängd engelsk text finner man att bokstaven 'e' är vanligast, precis som i svenska. Sedan följer i ordning 't' 'a' 'i' 'n' 'o' 's' 'r', men som i svenska språket kan det vara en annan ordning om man behandlar korta textavsnitt.

Övning 18B

Utmana varandra på att forcera engelskt Caesar-krypto. Välj var sin engelsk text om 50 - 80 tecken och en Caesar-nyckel, d.v.s. ett tal mellan 1 och 25 och håll kryptotext och nyckel hemlig. Kryptera och byt sedan kryptotext med varandra. Forcera din kompis text genom att göra pinnstatistik och jämföra med de klartext-statistiker som ni gjort. Vilken blir förskjutningen? Kryptonyckeln? Dekryptera. Berätta för varandra hur ni tänkt.

Har ni något annat språk gemensamt? Gör då samma sak för det språket. Ni kan behöva göra en statistik på ett större material, kanske 500 tecken, för att få en bra grund för iakttagelser.

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.

20. Vigenères krypto

Ni såg i föregående avsnitt att det blir svårare att forcera kryptot med två nyckeltal än med ett. Då kan vi förstås fortsätta och använda fler nyckeltal och använda dem om och om igen. Ett sådant krypto kallas Vigenère-krypto efter den franske diplomaten *Blaise de Vigenère*, född år 1523.

I flera hundra år ansåg man att Vigenère-kryptot var oforcerbart, men som ni säkert anar var det inte så. Ni skall få lära er hur man knäcker Vigenères krypto. Men först skall vi gå igenom hur man krypterar och dekrypterar med Vigenère-krypto på två olika sätt. Det första sättet använder Vigenère-rutan:

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

Övning 20A

Man behöver ett nyckelord. Låt oss ta POTTER. Klartexten *Kryptera är som att trolla* krypterar man så här:

k	r	y	p	t	e	r	a	ä	r	s	o	m	a	t	t	t	r	o	l	l	a
P	*O*	*T*	*T*	*E*	*R*	*P*	*O*	*T*	*T*	*E*	*R*	*P*	*O*								
Z	C	O	F	X																	

Klartextbokstaven bestämmer kolumnen och nyckelbokstaven bestämmer raden där man skall ta kryptobokstaven i Vigenèrerutan. Kryptera färdigt i tabellen ovan och skriv kryptotexten i grupper om fem stora bokstäver här:

Z C O F X

Övning 20B

Dekryptera kryptotexten ZWWJS SOLÖB ZLIIV LENYÖ YJZKW YOA
Nyckeln är HOKUS. Arbeta i den här tabellen:

Z	W	W	J	S	S	O	L	Ö	B	Z	L	I	I													
H	*O*	*K*	*U*	*S*	*H*	*O*	*K*	*U*	*S*	*H*	*O*															
s	i	m	s	a																						

Nyckelbokstaven bestämmer en rad i Vigenèrerutan. Där söker ni upp kryptobokstaven och avläser klartextbokstaven i klartextraden upptill.

Skriv den redigerade klartexten här:

Men det finns ett annat sätt att ordna arbetet när man krypterar och dekrypterar med Vigenèrekrypto. Först tänker vi oss att vi använder fyra nyckeltal, 1, 4, 3 och 20. Att kryptera med ett visst nyckeltal innebär ju att man går just det antal steg fram i alfabetet. Om vi först översätter bokstäverna i alfabetet till tal blir kryptering det samma som att addera nyckeltalet till klartexttalet. Så här kan man göra:

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28

Och så här blir krypteringen av klartexten *Tjuven stal båten*. Tänk på att ni måste subtrahera 29 om kryptobokstaven motsvarar ett tal som är större än 28

Övning 20C

Klartext	t	j	u	v	e	n	s	t	a	l	b	å	t	e	n
Klartext m. tal	19	9	20	21	4	13	18	19	0	11					
Addera nyckel	1	4	3	20	1	4	3	20	1	4					
Mellantext m. tal	20	13	23	41	5	17	21	39	1	15					
Subtrahera 29				-29				-29							
Kryptotext m. tal	20	13	23	12	5	17	21	10	1	15					
Kryptotext	U	N	X	M	F	R	V	K	B	P					

Och när man dekrypterar skall man subtrahera nyckeltalen från kryptotexttalen. Blir det negativt skall man addera 29. Gör färdigt krypteringen i rutorna ovan.

Övning 20D

Här är kryptotexten WMOBF RERUX RÅISQ som skall dekrypteras med samma nyckeltal som i övning 20C.

Kryptotext	W	M	O	B	F	R	E	R	U	X	R	Å	I	S	Q
Kryptotext m. tal	22	12	14	1	5	17									
Subbtrah. nyckel	1	4	3	20	1										
Mellantext m. tal	21	8	11	-19											
Addera 29				+29											
Klartext m tal	21	8	11	10											
Klartext	v	i	l	k											

Det kan bli lättare att hantera negativa tal och tal större än 28 om ni använder en omvandlingstabell som visar hur samma bokstav kan motsvara olika tal:

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57
0	-28	-27	-26	-25	-24	-23	-22	-21	-20	-19	-18	-17	-16	-15	-14	-13	-12	-11	-10	-9	-8	-7	-6	-5	-4	-3	-2	-1

Kryptera och dekryptera färdigt exemplet ovan. Vilken blir klartexten efter dekrypteringen?

Svar: _____

Det kan vara svårt att komma ihåg flera nyckeltal till Vigenèrekryptot. Och man vill inte gärna ha nyckeltalen nedskrivna någon längre tid. Ett papper försvinner ju så lätt. Men man kan använda ett nyckelord och sedan översätta ordets bokstäver till tal efter tabellen som finns på förra sidan. I övningarna 20C och 20D motsvarar talen 1, 4, 3 och 20 ”ordet” BEDU som är uttalbart men inte så lätt att gissa.

Övning 20E

Vilket nyckelord motsvarar 6, 8, 17, 14? Svar:_____

Övning 20F

Nu skall ni forcera en text som är krypterad med Vigenèrekrypto. Fyra nyckeltal har använts:

CQÄTU RÖLBS CUOCR RTÄXN JMTEO UNRJE ELMFK NHÖYL UHÅGG
NDOHQ NFFQN DFRFA SDÅDB LRTFQ ZASJE NEDBS AJDET ÖYLBH
NKUSN GFKCE SOBOU NXOMK SÖSCR SYENN ORQEU MKGSÖ CPÄQR
FUDBM AQQAS DÅFPS NVUQI CLDYL FQCÅY MRJJM TEOSV NHHÅT
FRKMZ BXEGR ÄMFMO OSSXA TSNDD HTASQ RTURD UNO

Arbeta tillsammans med denna uppgift. När ni gör de fyra pinnstatistikerna, en för varje nyckeltal, kan det vara svårt att hålla reda på vilket nyckeltal som hör till vilken bokstav. Arbetet blir säkrare om ni först skriver om texten på ett rutat papper med fyra bokstäver i varje rad; här är början. De bokstäver som står i första kolumnen hör till det första nyckeltalet osv.

	C	Q	Ä	T							
	U	R	Ö	L							
	B	S	C	U							

Vad blir klartexten? Motsvarar de fyra nyckeltalen ett uttalbart nyckelord?

Övning 20G

Nu kan du utmana din kryptokompis på forcering av Vigenèrekrypto. Arbeta först var för sig. Välj var sitt nyckelord och håll det hemligt. Ta inte ett för långt ord, tre bokstäver kan vara lagom. Översätt nyckelordets bokstäver till nyckeltal. Välj sedan var sin text, cirka 150 tecken lång, och kryptera den med nyckeltalen eller använd Vigenère-rutan. Håll klartexten hemlig. Byt sedan kryptotext med din kompis och forcera texten som du fått.

Det blir omväxling i arbetet om ni tar klartexter på något annat språk, till exempel engelska.

21. Sannolikt ord

Som ni har sett kan det ta ganska lång tid att forcera en text som är krypterad med Vigenèrekrypto om man inte vet något om klartexten mer än att den är skriven på ett särskilt språk. Men om man känner till att det finns ett speciellt ord i texten och helst vet att det förekommer på en särskild plats där, då blir det mycket lättare.

Övning 21A

Här är en kryptotext och ni vet att alla klartexter brukar börja med ordet hemlig och att man brukar använda Vigenèrekrypto. Hur många nyckeltal har använts och vad står det?

OEAÖD NTAQO LIÄJW SLYCN RAÖÖÖ

Börja med att översätta det ”sannolika ordets” bokstäver till tal. Sedan kan ni arbeta i den här uppställningen eller göra hela forceringsarbetet på ett särskilt rutat papper. En kryptobokstav kommer så många steg efter klartextbokstaven som nyckeltalet anger. Alltså är nyckeltalet kryptobokstaven minus klartextbokstaven.

Kryptotext i bokstavsform	O	E	A	Ö	D	N	T	A							
Kryptotext i talform	14	4	0	28											
Klartext i talform	7	4	12												
Nyckeltal = krypto – klar	7	0	-12												
+29			+29												
Nyckeltal, icke negativa	7	0	17												
Nyckelbokstäver	*H*														

Om ni bara vill använda bokstäver så går det också bra. Då tar ni fram Vigenèrerutan och får fram nyckelbokstaven ur klartextbokstaven i övre raden och kryptobokstaven i rutan.

Svar: Nyckelord:_____ Klartext:_____

Övning 21B

Här är en annan kryptotext och du vet att kryptören brukar fylla i klartexten med 'x' på slutet så att även sista kryptogruppen består av fem bokstäver. I denna övning slutar klartexten med tre 'x' det vill säga 'xxx'. Man har använt Vigenère-krypto med fyra kryptotal. Vilken är klartexten? Bildar nyckeltalen ett uttalbart nyckelord?

ZUÅPW WTZGW IYXVÖ RSGCF

Svar: Nyckelord:_____Klartext: _____

Övning 21C

Utmana din kryptokompis att forcera Vigenèrekrypto med sannolikt ord. Kom först överens om att klartexterna skall börja med något visst ord, t.ex. 'kompis'. Gör sedan var sin klartext, högst 50 tecken lång, och bestäm var sitt nyckelord, tre eller fyra bokstäver långt. Håll klartexten och nyckeln hemlig. Översätt eventuellt nyckelordet till nyckeltal och kryptera med Vigenèrekrypto. Byt sedan kryptotext med din kompis och forcera den du får.

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.

23. ES-krypto – fortsättning

Om ni har gjort rätt, bör arbetspapperet med texterna och nyckelmallen nu se ut ungefär så här:

KRYPTO	P	L	E	H	G	■	J	A	A	H	Å	N	T	H	G	■	Ö	E	I	G	D	F	■	L	N
klar		o	n	t	e					t		c		t	e		a	n		e				o	c

KRYPTO	R	■	G	M	Ö	O	L	H	H	Ö	■	A	Z	■	O	Z	E	K	H	■	R	Z	O	O	■
klar	h		e		a		o	t	t	a							n		t		h				

KRYPTO	■	R	Ö	E	■	F	Z	K	■	Ö	H	H	■	Ö	E	I	G	D	F	■	R	Ö	I	G	■
klar		h	a	n						a	t	t		a	n		e				h	a		e	

KRYPTO	E	Z	K	L	H	■	Y	■	R	Ö	E	I	G	E	■	L	N	R	■	Ö	H	H	■	R	L
klar	n			o	t		i		h	a	n		e	n		o	c	h		a	t	t		h	o

KRYPTO	E	■	F	H	J	I	G	D	Ö	I	G	■	G	H	H	■	A	Ö	A	A	G	D	■	■	M
klar	n			t			e		a		e		e	t	t			a			e				

KRYPTO	Y	■	C	Z	F	H	G	■	F	T	W	E	I	Ö	■	L	F	F	■	F	Ö	I	G	■	R
klar	i					t	e					n		a		o					a		e		h

KRYPTO	L	E	■	H	Y	O	O	■	Ö	E	I	G	D	F	■										
klar	o	n		t	i				a	n		e													

Klartext					n		e	t				o		c				h			x				i				a
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 23A

Nu kan ni säkert avsluta forceringen genom att gissa/lista ut de återstående bokstäverna och fylla i dem. Redigera sedan klartexten, dvs skriv den med stor bokstav i början av varje mening och sätt ut skiljetecken (punkt, komma, frågetecken, utropstecken).

Skriv den redigerade klartexten här:

Fyll också i kryptobokstäverna i en nyckelmall:

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	Ö																												

Vad har kryptören använt som nyckelord för att lätt kunna komma ihåg hela kryptonyckeln?

Svar: _____

24. Språkstatistik – fortsättning

Som ni såg i de föregående avsnitten, underlättade det väldigt mycket att veta var klartextens ord börjar och slutar och därmed hur långa de är. Man måste förutsätta att kryptören också vet det och helt enkelt utesluter ordmellanrum och skriver meningarna i en enda lång rad. Möjligen finns det något som talar om när en mening börjar och slutar, men det ger inte forcören mycket hjälp. I fortsättningen antar vi därför att ordmellanrum inte används vid kryptering.

Men även med orden utpekade behövde ni mer än enkel pinnstatistik för språkets bokstäver för att knäcka kryptot. Ni behövde t ex veta några vanliga korta ord för att göra insteg. I det här avsnittet skall vi presentera mer språkstatistik och visa hur den kan användas för forcering.

I detta avsnitt finns data som anger hur ofta enskilda bokstäver samt kombinationer av två och tre bokstäver förekommer i svenska och engelska.

Det material som ligger till grund för de svenska statistikerna består av cirka 60 000 tecken modern tidningstext. De olika texterna har tagits från olika ämnesområden så att de resulterande statistikerna skall bli så neutrala som möjligt.

Motsvarande engelska material är ungefär lika stort som det svenska och har utvalts på samma sätt.

Monogramstatistik anger hur ofta enskilda bokstäver förekommer i en viss textmassa. Vi har helt uteslutit siffror, mellanslag och skiljetecken. Stora bokstäver har räknats som små.

Bigramstatistik anger hur ofta två bokstäver efter varandra förekommer i materialet. Textmassan har behandlats som en enda lång följd av bokstäver. Alla andra tecken har uteslutits.

Trigramstatistik anger hur ofta olika trebokstavskombinationer förekommer i textmassan. De har beräknats på samma sätt som bigramstatistik. De tal som anger hur ofta en bokstav eller bokstavskombination förekommer är procenttal.

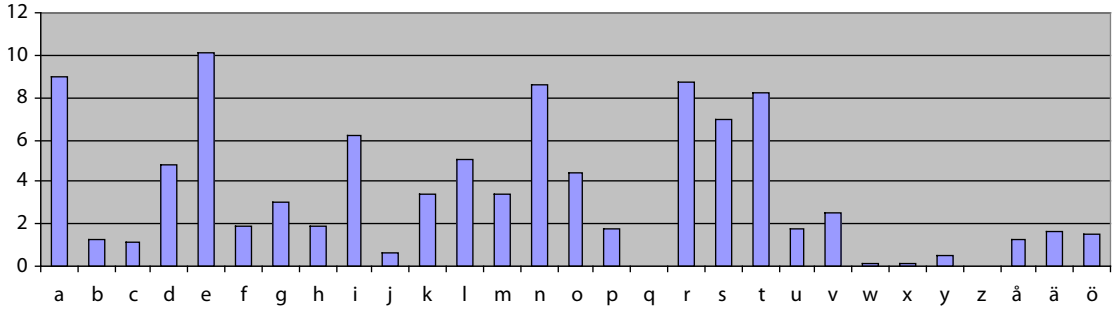
Monogramstatistik – svenska

I bokstavsordning

a	9,0
b	1,3
c	1,2
d	4,8
e	10,1
f	1,9
g	3,0
h	1,9
i	6,2
j	0,6
k	3,4
l	5,0
m	3,4
n	8,6
o	4,4
p	1,8
q	0,0
r	8,7
s	6,9
t	8,2
u	1,8
v	2,5
w	0,1
x	0,1
y	0,5
z	0,0
å	1,3
ä	1,7
ö	1,5

I ordning efter förekomst

e	10,1
a	9,0
r	8,7
n	8,6
t	8,2
s	6,9
i	6,2
l	5,0
d	4,8
o	4,4
m	3,4
k	3,4
g	3,0
v	2,5
h	1,9
f	1,9
p	1,8
u	1,8
ä	1,7
ö	1,5
å	1,3
b	1,3
c	1,2
j	0,6
y	0,5
x	0,1
w	0,1
z	0,0
q	0,0



Bigramstatistik – svenska

(Bigram som förekommer mer sällan än i 0,25 % av fallen har en tom ruta.)

Andra bokstav

Första bokstav	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
a				0.6			0.4				0.3	0.6	0.5	1.7				1.5	0.6	1.1		0.6							
b					0.4																								
c								0.7			0.3																		
d	0.5				2.2													0.3	0.3										
e				0.6		0.3						0.6	0.3	2.5				2.2	0.7	1.2									
f																													0.7
g	0.5				0.8																								
h	0.5																												
i				0.4			0.6				0.4	0.6		1.3	0.3				0.9	0.4									
j																													
k	0.8				0.4										0.5					0.3									
l	0.7			0.3	0.5				0.7			0.9							0.3										
m	0.5				0.7				0.3				0.3																
n	1.0			1.2	0.5		0.8		0.7					0.4	0.4				0.9	0.6									
o			0.8									0.3	0.9	0.6				0.7											
p																0.3		0.3									0.3		
q																													
r	1.1			0.4	1.1				1.1		0.4		0.3	0.4	0.5				0.7	0.4									
s	0.5				0.4				0.5		0.8				0.6				0.4	1.5		0.3							
t	1.0				1.3				1.2						0.5			0.5	0.6	1.1									
u														0.4						0.3									
v	0.6				0.5				0.5																				
w																													
x																													
y																													
z																													
å														0.3															
ä														0.3				0.6											
ö																		0.8											

De 32 vanligaste bigrammen i svenska språket med sina procenttal:

en	2,5	et	1,2	ta	1,0	oc	0,8
er	2,2	nd	1,2	na	1,0	ng	0,8
de	2,2	ti	1,2	is	0,9	ör	0,8
an	1,7	ra	1,1	ll	0,9	ge	0,8
st	1,5	re	1,1	ns	0,9	rs	0,7
ar	1,5	at	1,1	om	0,9	li	0,7
in	1,3	tt	1,1	sk	0,8	me	0,7
te	1,3	ri	1,1	ka	0,8	es	0,7

Trigramstatistik – svenska

Det vanligaste trigrammet i svenska språket är 'för', tätt följt av 'och', 'nde' och 'and'. Vart och ett av dessa förekommer i en stor textmassa med frekvensen 0,6 %. De 60 vanligaste trigrammen i ordning efter hur vanliga de är:

för	des	men
och	var	ion
nde	med	han
and	ist	lan
ing	nin	und
ter	ers	sto
den	isk	ern
att	eri	ger
ade	ste	lle
gen	ten	ris
som	rna	örs
ens	are	ett
ill	lig	nga
det	ans	ent
ska	ena	upp
sta	ren	eno
til	ati	sam
era	nge	nte
rin	ver	man
der	rde	sen

Dessa trigram har en eller två vokaler. Det vanligaste trigrammet med bara konsonanter är 'str' som kommer på plats 61.

Här kommer en övning som ni kan göra med hjälp av trigramstatistiken och lite logiskt tänkande.

Övning 24A

De sex vanligaste trigrammen i svenska språket har krypterats med enkel substitution. Resultatet har blivit: TÄX, EUÅ, AZB, YIB, UÅZ, CUD i någon ordning. Vilka kryptogrupper betyder vad?

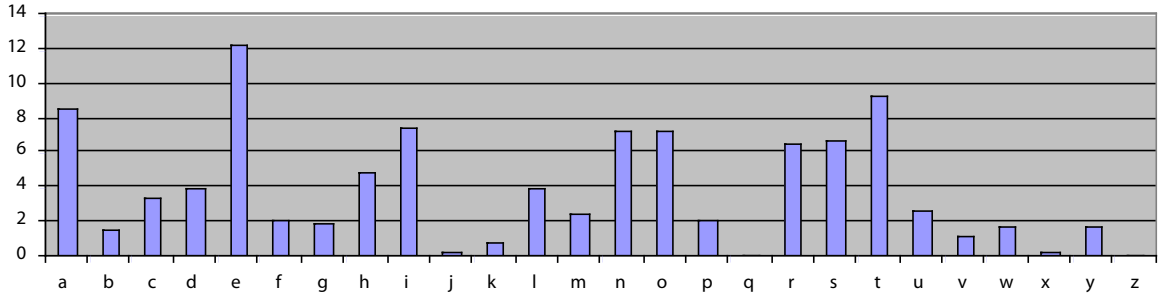
Monogramstatistik – engelska

I bokstavsordning

a	8,7
b	1,5
c	3,3
d	3,9
e	12,3
f	2,1
g	1,9
h	4,8
i	7,5
j	0,2
k	0,7
l	4,0
m	2,5
n	7,3
o	7,2
p	2,0
q	0,1
r	6,5
s	6,8
t	9,3
u	2,6
v	1,2
w	1,7
x	0,2
y	1,7
z	0,1

I ordning efter förekomst

e	12,3
t	9,3
a	8,7
i	7,5
n	7,3
o	7,2
s	6,8
r	6,5
h	4,8
l	4,0
d	3,9
c	3,3
u	2,6
m	2,5
f	2,1
p	2,0
g	1,9
w	1,7
y	1,7
b	1,5
v	1,2
k	0,7
x	0,2
j	0,2
q	0,1
z	0,1



Övning 24B

Jämför med svensk monogramstatistik. Vilka likheter och skillnader hittar ni?

Bigramstatistik – engelska

(Bigram som förekommer mer sällan än i 0,25 % av fallen har en tom ruta.)

första bokstav \ andra bokstav	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
a			0.3	0.3					0.5			0.9	0.3	1.5				1.0	0.8	1.2					0.3	
b					0.4																					
c	0.5				0.6			0.3							0.6					0.3						
d	0.4				0.7				0.5						0.3					0.4						
e	1.1		0.7	1.1	0.4	0.3			0.4			0.4	0.5	1.3	0.3	0.3		1.9	1.3	0.7			0.3			
f															0.4					0.3						
g					0.3																					
h	1.0				2.2				0.5						0.4											
i			0.5	0.4	0.3							0.4		1.9	0.6			0.3	1.0	0.9						
j																										
k					0.3																					
l	0.6				0.6				0.6			0.4			0.3										0.3	
m	0.4				0.7				0.3						0.3											
n	0.7		0.5	0.9	0.6		0.8		0.4						0.4				0.5	1.3						
o						0.7						0.4	0.4	1.5				1.0	0.3	0.4	0.6		0.3			
p	0.3				0.4										0.3			0.3								
q																										
r	0.6				1.4				0.7						0.7				0.5	0.5						
s	0.7		0.3		0.8			0.3	0.7						0.5				0.5	1.3	0.3					
t	0.8				0.9			2.8	1.1						1.0			0.4	0.4	0.5						
u														0.3				0.4	0.3	0.3						
v					0.7																					
w	0.3				0.3			0.3	0.3																	
x																										
y																										
z																										

De 32 vanligaste bigrammen i engelska språket är med sina procenttal:

th	2,8	es	1,3	to	1,0	as	0,8
he	2,2	nt	1,3	is	1,0	se	0,8
in	1,9	en	1,3	ar	1,0	ng	0,8
er	1,9	at	1,2	ha	1,0	ta	0,8
on	1,5	ed	1,1	nd	0,9	de	0,7
an	1,5	ea	1,1	te	0,9	ec	0,7
re	1,4	ti	1,1	al	0,9	sa	0,7
st	1,3	or	1,0	it	0,9	et	0,7

Övning 24C

Jämför engelsk och svensk bigramstatistik. Vilka likheter och skillnader hittar ni?

Trigramstatistik – engelska

Det i särklass vanligaste trigrammet i engelska är 'the' som förekommer i 1,8 % av alla trigram. Det näst vanligaste är 'ing' som har procenttalet 0,6. Sedan följer i tur och ordning 'ent', 'and', 'ion', 'tha' och 'tio', som har sannolikheter från 0,6 till 0,4.

De 36 vanligaste trigrammen i engelska är, ordnande efter sina procenttal:

the	int	ear	nce
ing	ter	ers	men
ent	ere	eth	res
and	her	ons	ont
ion	est	sin	rea
tha	for	dth	are
tio	ati	sta	eco
nth	ver	con	sth
hat	tth	ist	ith

Övning 24D

Några av de vanligaste trigrammen är egna ord. Vilka är det? De andra trigrammen ingår som delar i ord eller bildar övergång mellan två ord som kommer efter varandra. För vart och ett av dessa trigram, försök att finna ord som innehåller just det trigram som ni gått ut ifrån. Exempel: 'ter' ingår i 'winter'. Vem av er hittar riktiga engelska ord till flest trigram på fem minuter?

25. Enkel substitution – det allmänna fallet

I detta avsnitt skall ni forcera tre meddelanden som är krypterade med enkel substitution (ES-krypto). Kryptotexten är dock utformad på olika sätt. Klartext-orden är skrivna utan mellanrum, men det kan finnas något tecken för komma eller punkt. Till övningarna finns det i detta avsnitt tips och ledtrådar, särskilt för början av arbetet med de olika texterna.

Övning 25A

Här är en kryptotext som man har fått genom att kryptera en engelsk klartext med ES-krypto.

```
UYJRL  JSNLR  LVDGJ  LIYLD  FGHTB  RDFFY  XHJJL  FRDBO
FHVIS  IJHDG  ASIIY  UHYVS  JRKIJ  SBYUT  DMARD  SFDIB
DIDFF  HVEDM  LWWRL  VDGGK  FXFSG  SIOTY  CKSMA  WDGAS
TTBLQ  LTHXL  BHQLF  YLDFG  HEOLJ  JSIOH  KJHEJ  RLVDY
HERSG  UKTTY  SIOMH  KGSIW  WRLGJ  STTTS  QLBSI  JRLMK
XUHDF  BKIBL  FJRLG  JDSFG  WWRSG  LYLGV  RSMRV  LFLJR
LGDNL  DGRSG  NHJRL  FGVLF  LUFST  TSDIJ  OFLLI
```

Som ni har sett i avsnitt 24 är den engelska språkstatistiken olik den svenska. Den vanligaste bokstaven och det vanligaste trigrammet förekommer mycket oftare än de näst vanligaste. Som ni kommer att se, är det en fördel när man skall forcera ES-krypto.

Börja med att skriva kryptotexten på ett rutat arbetspapper som ni gjorde för texten i avsnitt 22, så att det blir plats för klartexten allteftersom den kommer fram.
Ta fram eller gör en kryptonyckelmall att fylla i när ni gjort ett antagande eller konstaterat en motsvarighet mellan en klartextbokstav och en kryptobokstav. Gör dessutom en monogramstatistik (pinnstatistik för enskilda bokstäver) för kryptotexten. Ni behöver inte plats för Å, Ä och Ö. De bokstäverna finns ju inte i engelska. Sedan är det dags att börja tänka…

Om ni behöver finns det ledtrådar på denna dels sista sida. Använd dig bara av en i taget och bara om ni har kört fast.

Om ni behöver, se ledtråd 25A1 på sidan 7.

Om ni behöver, se ledtråd 25A2 på sidan 7.

Om ni behöver, se ledtråd 25A3 på sidan 7.

Hittar ni något sannolikt ord?

Om ni behöver, se ledtråd 25A4 på sidan 7.

Sedan behöver ni nog inte fler tips för att klara av uppgift 25A.

Övning 25B

Detta är en övning i att forcera byggmästarkrypto. Repetera gärna avsnitt 7 i grundkursen om ni har glömt bort vad byggmästarkrypto är.

I den här övningen har vi bara använt 26 teckens nyckel. Vi har inte tagit med de vinklar som har två punkter. Då måste vi göra något för att kunna hantera våra svenska bokstäver 'å', 'ä' och 'ö'. Vi har här valt att helt enkelt ta bort punkterna över 'ä' och 'ö' samt ringen över 'å' innan vi krypterat texten. Så gör man ju när man skall tillverka Internet-adresser.

På nästa sida är kryptotexten som ni skall forcera. I stället för att kryptera ord-mellanrum har vi här gjort ett uppehåll i kryptotexten.
Varje tecken (en vinkel med eller utan punkt) i kryptotexten motsvarar en bokstav i klartexten, så det är alltså frågan om enkel substitution fast kryptotecknen ser ut på ett annat sätt. Det är enklare att hantera bokstäver i stället för vinklar. Därför kan ni provisoriskt ersätta vinklarna med bokstäver i stället. Ni kan till exempel använda den nyckel som finns i grundkursens övning 7A för den provisoriska ersättningen. Fast använd stora bokstäver eftersom det ännu inte är klartext.

Om ni gör det börjar kryptotexten så här: QIOOE LFBES IOLUU IIJMI SANGE ...

Nu börjar det egentliga forceringsarbetet. Gör först monogamstatistik som vanligt. Eftersom klartextbokstaven 'a' nu också kan betyda 'å' eller 'ä' förekommer den bokstaven nu oftare, ja till och med oftare än 'e'. Det vanligaste tecknet i kryptotexten borde därför motsvara 'a'.

Sedan kan ni göra upp en nyckelmall. Ta gärna den i övning 7A fast utan bokstäver i och fyll i 'a' där den bokstaven skall stå. Mot slutet av forceringsarbetet kan ni ha nytta av det om det finns ett särskilt mönster för bokstäverna i kryptonyckeln.

Vad gör ni härnäst? Vad kan ni få ut av en bigramstatistik av kryptotexten?

Om ni behöver, se ledtråd 25B1 på sidan 7.

Behöver ni fler tips?

Om ni behöver, se ledtråd 25B2 på sidan 7.

Nu behöver ni nog inte fler tips.

Ni ser att det kan bli en del problem med våra svenska bokstäver 'å', 'ä' och 'ö' när man ersätter dessa bokstäver med 'a' och 'o' rakt av. Ett alternativ är att ersätta dem med 'aa', 'ae' respektive 'oe', som vi gjorde i grundkursens avsnitt 12. Fast då blir monogramstatistiken ännu snedare och det blir ännu lättare att forcera kryptoton där man gör så. En bra forcör måste vara beredd på båda sätten att undvika våra svenska bokstäver.

Övning 25C

Här kommer en övning i att forcera ett sifferkrypto. Repetera gärna avsnitt 8 i grundkursen först om ni inte har sifferkrypto aktuellt. Varje sifferpar motsvarar en klartextbokstav, så det är alltså fråga om ES-krypto fastän kryptotexten består av sifferpar i stället för bokstäver. Här är kryptotexten.

07 05 38 08 45 38 20 40 29 09
38 07 35 15 15 20 40 17 38 36
16 15 05 15 20 25 15 00 39 20
19 20 40 30 37 20 38 49 05 39
45 37 20 38 15 38 46 07 07 09

38 19 20 40 19 38 30 37 09 40
19 20 49 15 45 37 09 38 20 40
49 20 28 28 20 38 19 20 15 20
17 15 30 37 20 40 49 16 35 20
15 15 18 30 37 09 40 19 20 49

16 35 38 49 17 36 40 19 09 38
49 30 18 07 05 38 08 45 38 20
40 09 15 15 28 46 49 09 30 18
20 40 05 39 17 38 36 16 15 05
15 20 25 15 20 40 00 19 46 38

20 07 15 20 38 49 46 15 15 20
38 29 09 40 30 18 35 40 18 39
20 19 09 15 15 26 16 16 38 46
15 15 09 49 15 09 15 30 49 15
30 17 20 38 00 49 35 18 05 15

15 49 05 39 09 28 28 15 30 19
26 15 09 40 09 15 15 37 20 15
09 37 30 28 17 09 29 09 40 17
05 39 39 20 38 09 15 15 29 09
40 36 15 15 09 09 37 00 00 00

Studera kryptotexten. Vilka siffror kan vara förstasiffror? Hur många är de? Samma frågor för andrasiffrorna. Hur många sifferpar kan det alltså finnas? Hur stämmer det med antalet bokstäver i alfabetet?

Först måste ni ha en monogramstatistik (pinnstatistik för de enskilda sifferparen). Ni kan göra den i en ruta som liknar en kryptonyckel som ni sett i avsnitt 8 i grundkursen.

	5	6	7	8	9	0
0						
1						
2						
3						
4						

Skriv pinnarna i rutorna tätt, med var femte pinne liggande över de fyra föregående, så här:
𝍸 𝍸 𝍸 . . . . Då får de plats i rutorna och blir ändå lätta att räkna. Jämför sedan med monogramstatistiken för svenska språket i avsnitt 24. Vilket sifferpar är vanligast i kryptotexten? Vilken bokstav tror ni att det motsvarar?

Behöver ni ett tips, se ledtråd 25C1 på sidan 7.

Fortsätt därefter att identifiera de två vanligaste vokalerna.

Behöver ni några sannolika ord, se tips 25C2 på sidan 7

Fler tips? Gå till tips 25C3 på sidan 7

Tips 25A1:

Man kan anta att den vanligaste bokstaven i kryptotexten (vilken är det?) motsvarar den vanligaste bokstaven i engelska (se monogramstatistiken i avsnitt 24). Denna bokstav är även sista bokstav i det vanligaste trigrammet. Leta reda på det i texten. Det finns bara 31 ställen att leta bland. Nu har ni tre motsvarigheter mellan klartext- och kryptobokstäver. Fyll i dem på arbetspapperet och i kryptonyckelmallen.

Tips 25A2:

Nu är det bra med en bigramstatistik. Ni har sett att klartextbokstaven 'e' motsvarar kryptobokstaven L, som finns på 31 ställen i testen. Ta reda på de 31 bigram som börjar med L. Det vanligaste av dessa bigram motsvarar även det vanligaste engelska bigrammet som börjar på 'e'. Det hittar ni i den engelska bigramstatistiken i avsnitt 24. Nu har ni en bokstav till i nyckeln och ni kan fylla i den på arbetspapperet och i kryptonyckelmallen.

Tips 25A3:

Leta efter fler motsvarigheter med hjälp av bigramstatistiken som ni gjorde i tips 25A2 genom att jämföra med bigramstatistiken i avsnitt 24.

Tips 25A4:

Texten handlar om en känd person som var särskilt aktuell sommaren 2007, både i en bok och i en film. Hans namn finns med i texten.

Tips 25B1:

En annan möjlig väg är att göra en trigramstatistik, det vill säga skriva upp alla tretecken-kombinationer och ta reda på dem som förekommer fler än en gång i kryptotexten. Det tar en stund att göra det men det kan vara värt jobbet. Vanliga trigram i klartexten är 'och', 'han' och 'and'. Det ger några bokstäver till i nyckeln.

Tips 25B2:

Klartexten handlar om Mästerdetektiven Kalle Blomkvist och hans vänner, när de avslöjar juveltjuvarna.

Tips 25C1:

Det vanligaste sifferparet är 15 och då tror man kanske först att det motsvarar 'e' eller 'a', de vanligaste bokstäverna i svenska språket. Men i kryptotexten finns flera ställen där två stycken 15 förekommer efter varandra. Då är det nog ingen vokal. Antag därför i stället att 15 motsvarar någon av de vanligaste konsonanterna: 't', 'r' eller 'n'.

Tips 25C2:

Texten handlar om något som ni just nu håller på med.

Tips 25C3:

Texten handlar om kryptering, språkstatistik och forcering.

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.

27. Examensarbete

I detta avsnitt finns fyra övningar utan ledtrådar. Det blir ert ”examensarbete”. Om ni har klarat av de flesta av övningarna hittills, klarar ni också av examensarbetet om ni är noggranna och har tålamod om ni gör något felaktigt antagande. Sådant händer den bäste forcör. Det ingår i yrket.

För varje övning skall ni bestämma språk, kryptometod, klartext och krypto-nyckel.

Svaren skall vara fullständiga, så långt det går, och alla klartexter skall vara redigerade. Ni svarar själva för rättning och ”betygsättning”. Ni kan välja att samarbeta eller att tävla med varandra.

Övning 27A

RGLSÖ LEFKM LRZOO EFALX HOGOE WOVVC ETEFI QELNG CÖQEL
OLÅRR MLTEF TLIQM FTENO ÖQMLE FNEBB ELTEO EAOIQ EFNHZ
EOODI QMFTE NHZLN AXFTM LNIDR GLSÖL EFMOO BÅNMI DEFGC
ALXHO GOEWO EFVVT ÅLERO ELNÅO OELKM FIDZF DCETM OOPHH
LÅOOM NOMOI NOIAE LNZDG OONGC MBBOI TPOMF MOOQE OMQIB
AMKMF AGCCE LMOOK MFXOO MMQVV

Övning 27B

EHSSC VWMMP SGEPS XNWZP HZYLX ASNYT PJHIF PYMWJ HSYQM
EPOWS ANYYP ZOWSP QMGNQ NMENY YPZNZ MEPEL MGHQF PYLXA
SNYTP GWORW LSQPZ WMGHZ QJPSP YEPSX NWZPG EHTSN YXNTE
MEHKP VLMNM PIQPJ EPSPN ZMEPO WSPQM GEHSS CQQRH SJHQM
ESWAA NZTNZ MEPQW OMPKP ZNZTH NSGAL MNMEH YZWMA LSZPY
JENMP HZYEW MHQEP FZPJN MJWLI YGNOK WIYPX WSMEH YQMHS
MPYOW SMEPF NIIGG

Övning 27C

AKÄEF ORECX ESEIC KMMTH LVSKO LÄDOR LITTR BTRVÖ

Övning 27D

OVLWS ATLMP BNOLH OXQKV AVTDP KDPBE XKLÖF ÄUALH OGPYS
WHPYR OSSCZ BDFDE ÄFLYR ÖDPBR HGZYQ INYTW UAAZQ UUYOI
RJJWT KDPXÄ CEXAO BLWPK HONSX KLLZQ PÖÖLR NEÖAQ KMXLE
ATSLR RAOPW VARTX SHUJP ÖIRFZ KDAVY VLPOI ÖÄRLH IRSPQ
WAFOB RÖÖOI ROYVE VLPÖS ZAFBM ATLSE XHJYK ORTMY ÖKPYÄ

