

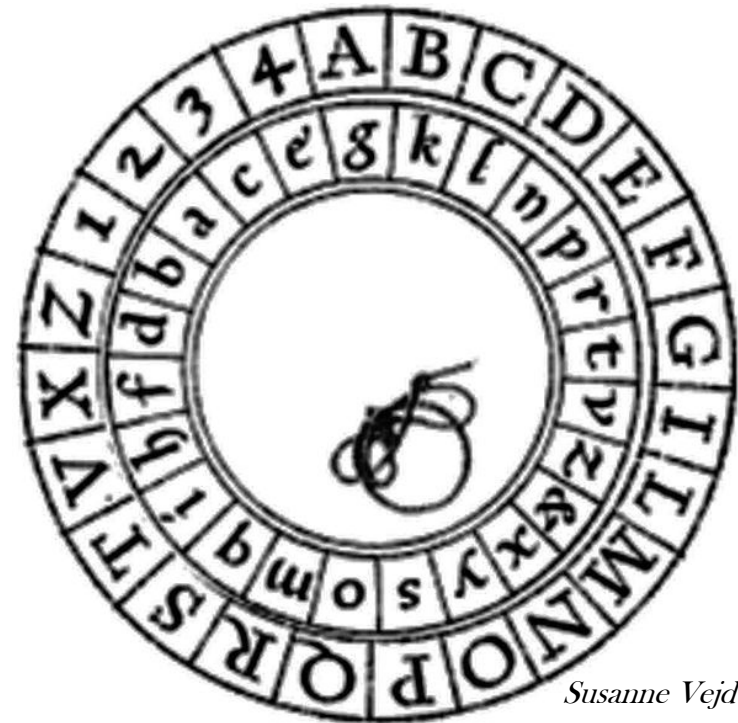
En liten pamflett om
Chiffer
hemliga meddelanden
och
konstgjorda språk
på lajv.

*Kopiera så mycket du vill! Du kan ladda ner
pamfletten och andra material från
susanne.vejdemo.se/lajv/chiffer/*

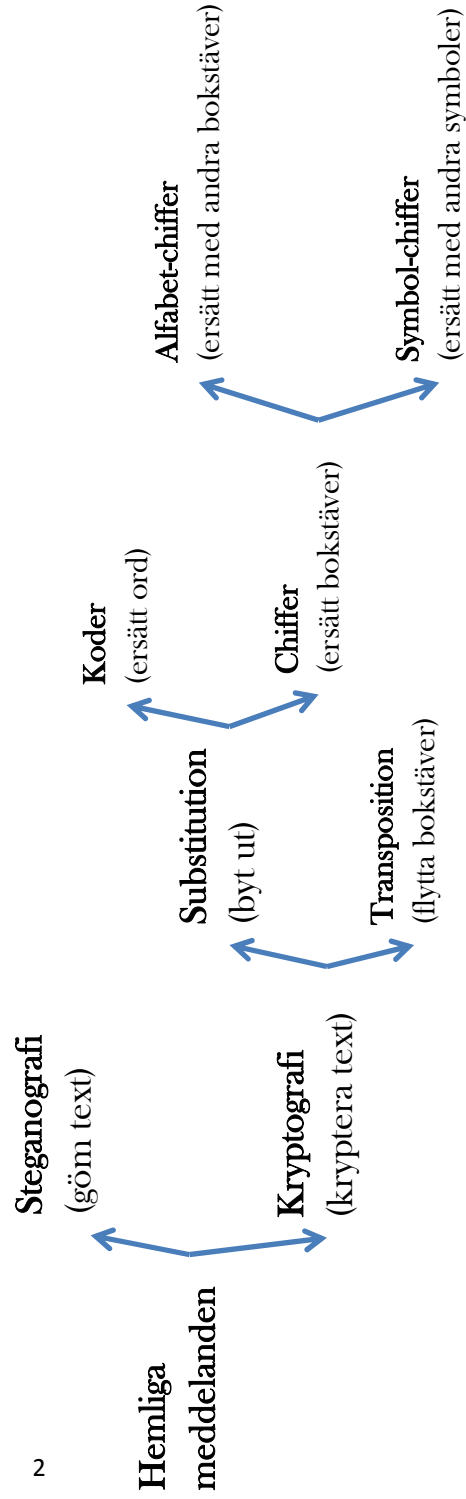
*Hör av dig om du hittar felstavningar eller
felchiffreeringar i materialet!*

*Varma hälsningar,
– Susanne
[susanne @ vejdemo . se](mailto:susanne@vejdemo.se)*

Chiffer
hemliga meddelanden
och
konstgjorda skriftspråk
på lajv



*Susanne Vejdemo
[susanne @ vejdemo . se](mailto:susanne@vejdemo.se)*



◆ Hemliga meddelanden

Den här pamfletten handlar om praktiska sätt att föra fram hemliga meddelanden på lajv. Vill du läsa mer utförligt om chiffrens roll i världs-historien rekommenderar jag att du börjar med Simon Singhs *The Code Book*, Doubleday, 1999).

Pamfletten kommer att avhandla

Steganografi – konsten att gömma meddelanden, och olika typer av

Kryptografi – hur man krypterar meddelanden genom exempelvis

Transposition – hur man flyttar bokstäver på regelbundna sätt genom alfabetet, eller

Substitution – hur man byter ut bokstäver genom

Koder – där man byter ut hela ord, eller

Chiffer – där man byter ut bokstäver genom:

Alfabet-chiffer – byt ut andra bokstäver, eller

◆ **Symbol-chiffer** – byt ut mot andra symboler.

Chiffer på lajv

Chiffer (och koder) kan vara ett fantastiskt inslag på alla typer av lajv. Det är roligt att både få skriva och avkoda chiffer som man redan har lösningen till—och det är fantastiskt att få knäcka en kod eller hitta ett gömt meddelande. Hur mycket mer spännande är det inte när en oförsiktig budbärare kan låta polisen skriva av brevet med maffiabossens instruktioner, eller när mötesplatsen för schamanens ritual måste hittas på ett till synes helt blankt papper. Föreställ er fogdens skräckslagna min när hon skalar sitt morgonägg och hittar en dödskalle skriven på insidan – eller den försmådde sonens glädje när han inser att det finns ett hemligt budskap gömt innuti mammans testamente. Vad sägs om ett uppsnappat kort kodat budskap som antas ange fiendens anfallsrutt för morgondagen, och en febril nattlig aktivitet kring stabsbordet när man försöker tyda det innan gryningen.

Chiffer kan göra typiska ”**avslöja informationen**”-intriger mycket roligare. Inte nog med att det fins rykten om att Drottningen har ihop det med Markisinnan – det finns också en borttappad (givetvis chifferad) dagbokssida... Kanske ett *brädgårdschiffer*?

Chiffer kan **öka trovärdigheten** när världsomvälvande hemligheter ska kunna avslöjas. Känns det märkligt att sheriffen har statskupp-planerna gömd i sin resväska? Inte om hon tror att ingen kan avslöja det finurliga *bokchiffret* dokumenten är skrivna på. Om hon bara visste att en avhoppare skulle kunna visa upp bevisen för Prinsen – om bara den rätta kodboken hittades....

Chiffer kan vara **kulturbyggande rekvisita**. Trollspelarna arbetar hela tiden för att få andra att verkliga gå upp i illusionen att de inte har latexbitar i ansiktet – coola skräder, håruppsättningar och ett eget skriftspråk (kanske ett *stavelsebaserat skriftspråk*?) hjälper till.

Chiffer kan **göra McGuffins användbara**. Varför letar vi så ofta efter

magiska artefakter? Ofta för att en McGuffin (en pryl som mest finns till för att letas efter) blir ännu roligare om den faktiskt kan användas till något också. En kodnyckel till ett chiffer är ett icke-magiskt alternativ. Alla Neconomiconjägarna känner till Upsaliensis-manuskriptet—men för att tyda det måste man ha *substitutionschiffernyckeln* i Gröna Boken. Jakten kan börja!

Chiffer kan användas för att **spela upp** visa personer. Ge de alviska alkemisterna off-information om hur man löser, exempelvis, ett *Vigenère-chiffer* och varna dem för att det kommer. När det väl dyker upp behöver de bara kodordet—och sen kan de till allas häpnad lösa chiffret framför de förbluffade människornas ögon.

Till sist så är det många av oss som tycker att chiffer är roliga bara för att de är chiffer! Bygg dock inte intriger som antar att alla deltagare känner på det sättet.

Lösbara problem med chiffer på lajv

”Det finns ingen tid alls.” Vissa tycker det är roligt att sitta och lösa chiffer, men många inte. Vi är ju på lajv för att interagera med andra människor — och det finns så mycket annat att göra!

==> Arrangörer bör försöka se till att det finns lugna tidsperioder där man kan lösa chiffret om det är ett hektiskt lajv. 3-timmarspauser när folk kan äta, vila och knäcka kod, exempelvis.

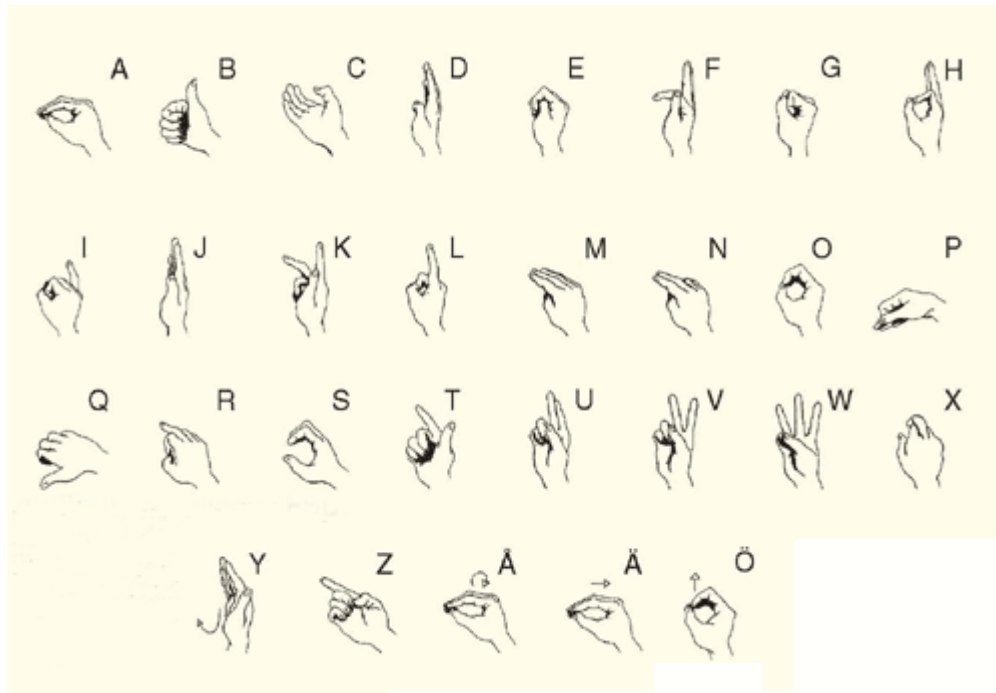
”Det tar för lång tid.” Att lösa chiffer i lugn och ro vid köksbordet är en helt annan sak än att lösa chiffer blöt och kall på lajvområdet—det tar längre tid.

==> Gör en bedömning av tidsåtgången därhemma och trippla den.

”Det är illusionsbrytande.” Chifferlösning kan bryta illusionen vi försöker bryta upp—karaktärer som ska vara bra på att lösa chiffer kan ha spelare som inte är lika bra.

==> Nyckelchiffer hotar inte att avslöja kunskapskillnaden mellan

Svenskt handalfabet



karaktärer och spelare lika mycket. Utmaningen förvandlas till artefakt- eller hemlighetsletande. Eller så kan man tipsa vissa spelare innan. Ge dem den här pamfletten, exempelvis.

Det tar för kort tid. Lösningen ska komma vid en viss tidpunkt på lajvet—men gör vi det för lätt så går det för fort och arrangörernas planering fungerar inte.

==>Gör ett flerstegschiffer och lämna ut ledtrådar pö om pö.

Exempelvis kan man ha ett ceasarchiffer där alla konsonanter skiftas två konsonanter åt höger, alla vokaler två vokaler åt vänster och sedan ska meddelandet läsas baklänges. Dela ut dessa tre lösningsbitar en efter en.

Varning för vissa chiffer

Visst vore det coolt om smugglarna kommunicerade med varandra genom tjuvlyktor (där man kan täppa för eller släppa fram ljuskällan) eller steampunktelegrafisten faktiskt avkodade ett inkommande knatter. Och vi vill alla se pirater, eller flottofficerare, som skickar meddelande med semaforflaggor! Men — chiffer där informationen kommer i en enda ström, och inte är nedskrivna, är väldigt svår att tolka även för de som haft lite träning i det innan. Räkna inte med att någon kan lära sig på plats. Det är väldigt, väldigt lätt att tappa bort var någonstans man är i avkodningen. Satsa på nedskrivna chiffer, eller ljud- eller bildinspelade kortare meddelanden som kan spelas upp när som helst, om och om igen, för lajvbruk.

Alla exempel ovan kan ju göras som en förberedd scen, förstås, där avkodaren redan vet signalen.

Nedskrivna chiffer på papper har ju också andra problem - de kan exempelvis bli blöta. Se till att du som arrangör har en backupplan om det händer. Chiffer kan även brännas in på trä eller läder, ristas in i mjuk metall eller skrivas på en biten siden som sen sys in i ett plagg— eller varför inte lamineras, om din genre tillåter det.

Stenografi

Stenografi är konsten att gömma meddelanden. Vi kommer ta upp några lajvvänliga varianter här, även om vi förstås ser fram emot galnare sätt på framtida lajv. Det är lätt att gömma en liten, liten pappersbit—men poängen med chiffer på lajv är ju (oftast) att de ska kunna hittas. Det sägs att Demaratus lät tatuera in ett meddelande i skalpen på en budbärare, väntade tills håret växte ut, och sedan kunde mottagen se meddelandet genom att raka av håret igen. Hur häftigt som helst—men lite svårt att hitta—om man inte har fått ett tips, förstås...

Osynligt bläck

Osynligt bläck är otroligt enkelt att göra—mitt tips är att använda mjölk eller citronsaft. Doppa sen en spets i vätskan och skriv ditt meddelande på pappret. Låt det torka. Värm pappret varligt med ett ljus (eller stoppa in det i ugnen). Låter det för enkelt—prova själv!

Både mjölk och citronsaft kan lämna en liten spegling på det annars blanka pappret—det finns två enkla sätt att motverka det.

Det första är att skriva ett annat meddelande ovanpå det blanka pappret.

Det andra är att skrynkla ihop pappret, och sen räta ut det igen. Då syns plötsligt ingenting. De två metoderna kan också med fördel kombineras.

Skriva på kokta ägg

Gör en lösning med en del alun (köpes på apoteket) och två delar vinäger. Koka ett ägg så det blir hårdkokt (viktigt!). Sen doppar du en spets i lösningen och skriver på ägget. Vänta en halvtimme—och skala sedan ägget!

Eftersom alun finns i många olika varianter så rekommenderar jag att du testat det här på ett ägg innan du använder just den lösningen du blandat ihop på själva lajvet.

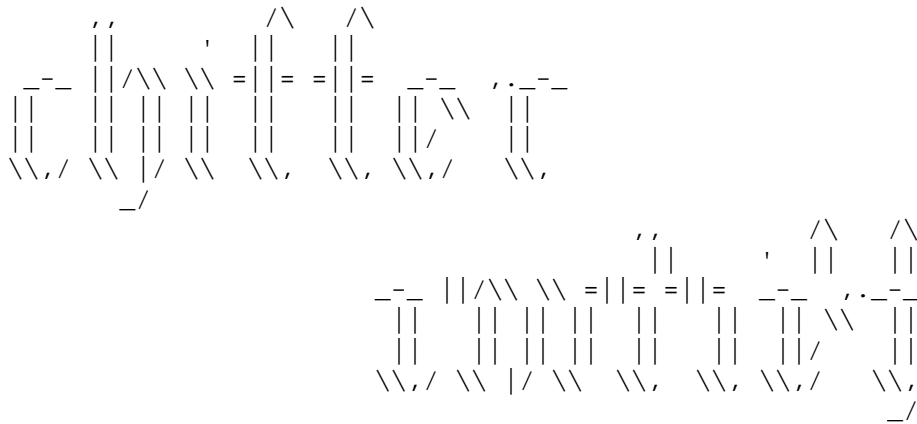
International Morse Code

1. A dash is equal to three dots.
2. The space between parts of the same letter is equal to one dot.
3. The space between two letters is equal to three dots.
4. The space between two words is equal to seven dots.

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



in meddelandet på en dator. Utmärkt för exempelvis lajv med hemliga sällskap. I exemplet nedan döljs meddelandet genom att det vänsterställs (kan göras enkelt i ex. Word):



Göm under något som kommer att tas bort

Ett kort meddelande kan med fördel läggas under tårtan—tårtan kommer ätas upp bit för bit och meddelandet framträdas. Botten på brödkorgar är ett annat hett tips. Tänk hur förvånade inkvisitionen blir av det hemliga tipset om nunnornas förehavanden som dyker upp under den till kyrkan donerade sockerkakan...

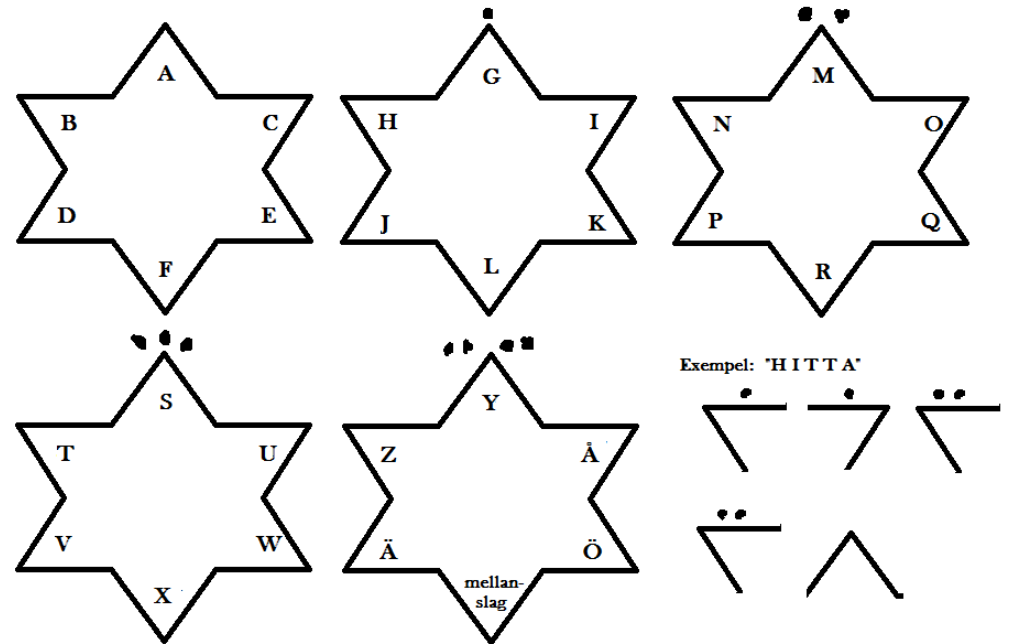
Göm innuti mat

Bevakningen på kolar-Johan som lett strejken var stenhård—men rättegångsdagens morgon fick han in en hel limpa bröd och en vattenflaska. Med stiletten inbakad i limpan och den hemliga mötesplatsen inbränd på läderbiten gömd i vattenflaskan kunde han sen lätt fly och möta upp med sina bröder och systrar i Kampen.

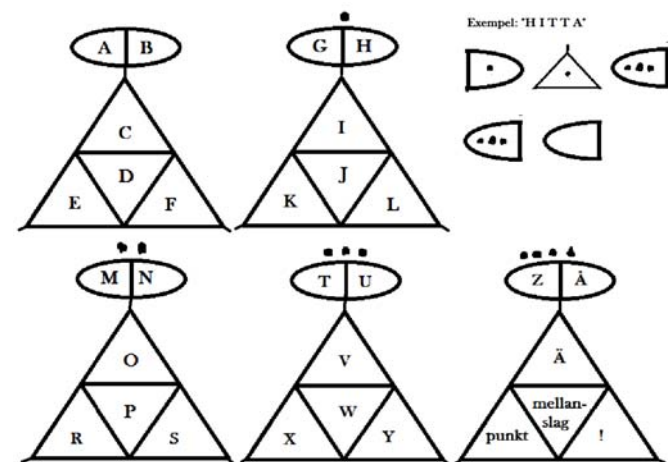
Så meddelande med krasse

I Lagens Långa Näsa (Alfredsson, 1983) berättas om en man som sår gräsfrön på det stora fältet precis innan asfalten hälldes på för den nya landningsbanan. Inom några år hade landningsbanan spruckit och

På samma sätt kan alfabetet gömmas i massa olika symmetriska konstruktioner. Vad sägs om en sexuddig stjärna?



Eller kanske kan illuminatisällskapet använda en uppdelad pyramid och ett öga?



Strukturbaserade symboliska chiffer

Strukturbaserade chiffer innehåller delar av både transposition och substitutions-chiffer. Bokstäverna ersätts med symboler—men det finns ett mönster i hur symbolerna ser ut.

Brädgårdschiffer

Brädgårdschiffer är en gammal scoutklassiker—det finns en hel del överlapp mellan scouter och lajvare, så du kan nog vara säker på att åtminstone någon av dina deltagare kommer att kunna lösa det off.

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

Bokstäverna ersätts med den visuella strukturen de är placerade i. Nu borde du kunna läsa ut meddelandet nedan:



Men varför begränsa sig till fyrkantiga strukturer? Du kan göra ditt chiffer som ett brädgårdschiffer på sniskan:

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

texten ”polisen suger” framträtt tydligt för alla piloter som skulle landa eller lyfta. Nu kanske det är lite väl ambitiöst för ett lajv—men jag kan rekommendera att leka med krasse. Krassefrön kan köpas i välsorterade matbutiker, och har växt upp på bara några dagar. De kan sås i form av enkla meddelanden (MORD, ALEX, HJÄLP) i blomrabatter—eller på blött hushållspapper på en bricka.

Skriv på insidan av en lampskärm

Genom att skriva med tjocka drag på insidan av en lite mörkare lampskärm borde texten projiceras upp på väggen när rummet är mörkt och lampan tänd. Detta beror dock mycket på ljusförhållandena och materialiet i lampskärmen—så fundera ett tag innan du försöker med den här tekniken.

Mikrofiche och mikropunkter

Förr i tiden kunde man på universitet få tag på microfichemaskiner som reducerade hela a4-ark till små, små prickar på ett genomskinligt papper. Det här var en populär teknik under Kalla Kriget för spioner—genom att göra texter så små att de kunde döljas i punkter på dokument var det lätt att föra ut text. Som arrangör kan du höra dig för om det finns några som fortfarande har microfiche-maskiner eller liknande apparater. Dina spelare kan läsa meddelandet genom att hitta en microfiche-läsare—i Stockholm finns de på de flesta universitetsbibliotek och Kungliga Biblioteket, bland annat.

Skriv ut i font tre med en riktigt bra fotoskrivare

En annan variant är att skriva ut i fontstorlek 2 eller 3 med en riktigt, riktigt bra fotoskrivare (kanske DPI 1500?). Texten kan maskeras som en del av en linje, exempelvis—eller en del av ett foto. Den kan avkodas med ett förstoringsglas.

Dölj i ett religiöst mässande

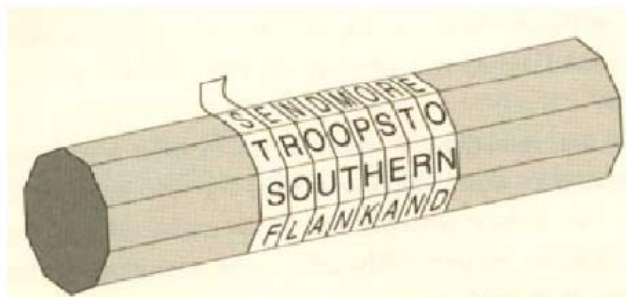
Det finns en gammal scoutsketch där tre personer ombeds att bedja till sina gudar Tafoo, Lajam och Wha. Var och en mässar ett av namnen, och de tre personerna mässar en efter en, alltid i samma mening. I början ska de mäsas sakta, och sen fortare och fortare. Efter ett tag framträder ett nytt meddelande i mässningen—Tafoo Lajam och Wha blir Wha-taFoo-lAjAm, dvs. What a Fool I Am.

Samma sak skulle kunna göras i en mässning på lajv. Cthulu-anhängarna blir tillsagda att mäsas "Iias", "Ankh" och "Tamar" - döm om deras förvåning, och deras människoooffers stora glädje, när budskapet "Sankta Maria" dyker upp istället.

Nå: en teknik som bara kan användas vid vissa speciella tillfällen – men håll med om att den är rolig.

Stavchiffer

Stavchiffer är en gammal grekisk klassiker, lika enkel som det är briljant. Vira en remsa av papper, tyg eller läder runt en stav (se figur). Skriv ditt meddelande i stavens riktning. Ta bort remsan, och fyll i det tomma utrymmet mellan bokstäverna med slumpmässiga bokstäver (du kan till och med låta dem forma vissa ord, för att förvirra). Chiffret löses genom att remsan viras runt en stav med exakt samma omkrets. Plötsligt får jakten på den magiska staven en ny innebörd. Eller är det kanske Brujah-primogens baseballträ som är lösningen?



Piktografiska skriftsystem

I piktografiska skriftsystem motsvaras (grovt förenklat) varje ord av en symbol—en bild. Kinesiska är det mest välkända exemplet på detta. I figuren nedan kan man se hur den kinesiska skriften har utvecklats. De sk. Orakel-benen härstammar från 1200 f.kr.

Oracle Bone Script	Seal Script	Clerical Script	Semi-Cursive Script	Cursive Script	Regular Script (Traditional)	Regular Script (Simplified)	Pinyin	Meaning
							ri	Sun
							yuè	Moon
							shān	Mountain
							shuǐ	Water
							yǔ	Rain

http://en.wikipedia.org/wiki/Chinese_character_classification (120121)

Piktografiska skriftsystem skulle göra sig utmärkt på lajv, för orcher, troll eller andar som försöker kommunicera med människor. Varför inte använda sig av orakelben-skriften? Eller hitta på en helt egen?

Ett välanvänt piktografiskt system (långt mindre utvecklat än kinesiskan) är Bliss-symboler. De används ofta av mentalt handikappade för att kommunicera och har visat sig mycket effektiva. Ett exempel på Bliss-symboler ses nedan.



Bliss-symboler för "jag vill gå på bio". Från http://en.wikipedia.org/wiki/File:Bliss_cinema.png (120121)

en av symbolerna i Hangul:

"For instance, the consonant Ǝ [tʰ] is composed of three strokes, each one meaningful: the top stroke indicates Ǝ is a plosive, like Ɔ ' , Ƨ g, Ƣ d, Ƨ j, which have the same stroke (the last is an affricate, a plosive-fricative sequence); the middle stroke indicates that Ǝ is aspirated, like Ƨ h, Ƨ k, Ƨ ch, which also have this stroke; and the curved bottom stroke indicates that Ǝ is alveolar, like Ƣ n, Ƣ d, and Ƣ l. " (http://en.wikipedia.org/wiki/Hangul_120121)

I Tolkiens Tengwar så används exempelvis en dubblering av en rundel till att indikera skillnaden mellan tonande och tonlösa ljud.

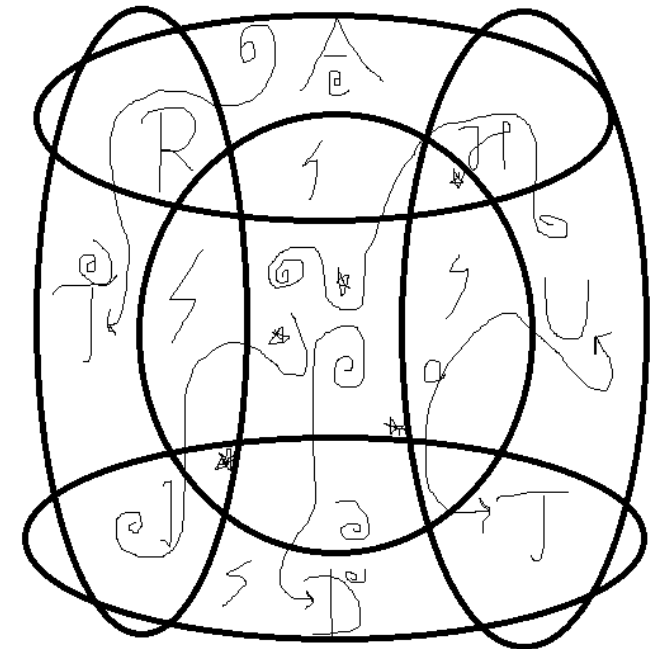
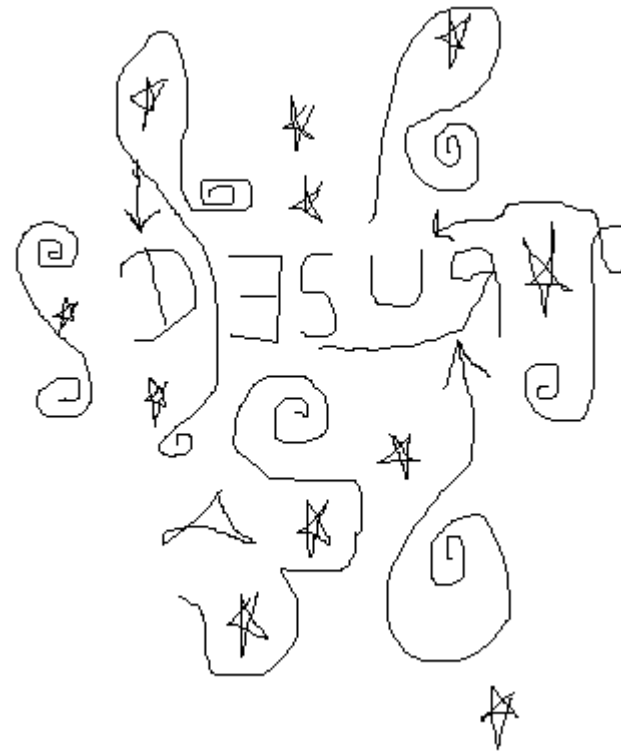
Ɔ — p

Ɔ — b

Ɔ — f

Ɔ — v

http://en.wikipedia.org/wiki/File:Tengwar_alphabet.png (120121)



Abstrakt ”konst”

Den här chiffrertekniken är så bra, att jag nästan lämnade den ute ur pamfletten... Den går ut på att du skapar något som ser ut lite som ett abstrakt konstverk med mycket och vilseledande information—men så snart man vet hemligheten är det lätt att dechiffrera. I figuren (min fina skapelse i paint) ser du en radda med bokstäver—de kan folk få försöka avkoda som ett substitutions- eller transpositionschiffer så mycket de vill. Nyckeln ligger nämligen i stjärnorna under bokstäverna. Den högsta stjärnan visar på meddelandets första tecken, den näst högsta stjärnan på meddelandets andra tecken. Gott om pilar och symboler villar bort betraktaren. I nästa figur ses samma teknik användas, men här står bokstäverna i en cirkel. Den första bokstävemarkeras med stjärnan längst ut. Stjärnan nästa längst ut markerar den andra bokstävemarkeringen i meddelandet. Någon med lite mer konstnärlig begåvning än jag skulle kunna göra en vacker schamantrumma med ett meddelande, exempelvis. Eller en abstrakt oljemålning — en gåva från den försvunna Malkaväldsten, kanske, som kan hängas upp på Elysiumet...

Fonetiska skriftspråk

Alla lingvisters favoritskriftspråk är Hangul—det koreanska skriftspråket som på ordet av kung Sejong den Store skapades av en grupp lingvister på 1440-talet.

Fonetiska skriftspråk tar hänsyn till språkljudens mindre beståndsdelar. Ett exempel är att ljudet för ”b” och ”p” egentligen uttalas på precis samma sätt i själva munnen. Prova. Den enda skillnaden är att b är ”tonande” - om du håller handen på struphuvudet och säger ”sab” så känner du att det vibrerar på sista ljudet. Gör samma sak, men säg ”sap” så märker du att det inte vibrerar. På så sätt skulle du kunna använda samma symbol för ”b” och ”p”-ljuden, med bara en liten markering för om det ska utläsas som tonande (”b”) eller tonlöst (”p”). ”d” och ”t” är också i princip samma ljud (fast det första är tonande och det andra tonlöst), och samma gäller ”g” och ”k” och ”f” och ”v”.

Men låt oss gå ett steg till—vad sägs om att ”s” och ”t” egentligen är typ samma ljud? Båda är tonlösa (säg ”las” och ”lat” - ingen vibration på struphuvudet), och uttalas med tungan på samma ställe. Skillnaden är i hur de uttalas—”s” är en sk. frikativ, och uttalas med massa friktion, ett slags väsande, medan ”t” är en sk. plosiv, och uttalas med en kort explosion av luft. Så du skulle kunna skapa en enda symbol både för ”t”, ”d” och ”s” - och sen använda små markörer för att visa om de är tonande/tonlösa samt på vilket sätt de uttalas.

Om du är en språknörd som jag, så tycker du det här är fantastiskt fascinerande, och kan läsa mer om det på nätet. (Exempelvis så har Karl Erland Gadelii fina anteckningar från en grundkurs i lingvistik han höll 2006 här: http://www.ling.gu.se/~jonas/teaching/elementa/FonEL_kit_ht06.pdf). Är du inte det så finns det många andra skriftspråkstyper att fokusera på.

Både Hangul och Tolkiens Tengwar använder sig av sådan här fonetisk kunskap om hur språkljud är uppbyggda. För att citera Wikipedia om

Stavelsebaserade skriftsystem

Redan på dagis lär svenskar sig att skilja ut stavelser: "Han-na" och "Susan" har två stavelser, "A-lex-and-er" har fyra. Vissa skriftsystem har olika symboler för hela stavelser. I japanska, exempelvis så ser さ och た helt annorlunda ut, trots att de uttas "sa" respektive "ta".

Stavelsebaserade skriftsystem lämpar sig bäst för språk som inte tillåter att så många konsonanter följer direkt på varandra (som "and" i "Alexander") och inte heller tillåter att stavelser slutar på en konsonant (som "san" i Susan"). Så det skulle vara lite väl komplicerat att för lajvbruk bygga ett stavelsebaserat skriftsystem för just svenska. Men håll med om att det är vackert!

ん	わ	ら	や	ま	は	な	た	さ	か	あ	-
N	WA	RA	YA	MA	HA	NA	TA	SA	KA	A	
お	り		み	ひ	に	ち	し	き	い		-
WI	RI		MI	HI	NI	CHI	SHI	KI	I		
	る	ゆ	む	ふ	ぬ	つ	す	く	う		-
	RU	YU	MU	FU	NU	TSU	SU	KU	U		
あ	れ		め	へ	ね	て	せ	け	え		-
WE	RE		ME	HE	NE	TE	SE	KE	E		
を	ろ	よ	も	ほ	の	と	そ	こ	お		-
WO	RO	YO	MO	HO	NO	TO	SO	KO	O		

Japanskans hiragana-alfabet—ett av tre inhemska alfabet. Dessutom använder man sig av arabiska siffror (1,2,3) och romerska bokstäver (som våra). Alla systemen blandas med varandra. Från http://en.wikipedia.org/wiki/File:Table_hiragana.svg (120121)

Kryptografi – transpositions- och substitutionschiffer.

Nu ska vi prata om transposition och substitutionschiffer. De flesta rena substitutionschiffer kan inte lösas på lajv utan någon form av nyckel—de är helt enkelt för svåra. Undantagen är visuella symbolchiffer som exempelvis brädgårdschiffer. Transpositionschiffer kan, förstås, lösas med att man hittar en kodnyckel—men kodnyckeln kan också kluras ut om man har tillräckligt med tid.

Transpositionschiffer

Transpositionschiffer innebär att man flyttar bokstävernas egentliga värde inom alfabetet. De kan varieras in i det oändliga, så vi kommer bara ta upp två här: ceasarchiffer och Vigenèrechiffer.

Ett exempel på en transposition är om alla bokstäver antar värdet av bokstaven till vänster—dvs "B" står egentligen för "A". Om du som arrangör vill att deltagarna ska få klura ut chiffren så rekommenderar jag ett enkelt ceasarchiffer. En variant är att off lära deltagarna om hur Vigenèrechiffer fungerar, så får de försöka lösa det när de väl hittat kodordet. Det tål att sägas igen: ett enkelt ceasarchiffer (transponering av alla bokstäver tre steg, exempelvis) kan lösas av en person med lite erfarenhet på kanske en halvtimme: man måste ju nämligen prova alla varianter. Ett Vigenèrechiffer kommer vara orealistiskt att lösa utan någon form av kunskap att det är ett Vigenèrechiffer—lösaren kommer helt enkelt anta att det är ett ceasarchiffer, och ägna alldeles för lång tid åt att försöka lösa det.

De följande chiffren kommer att illustreras med bokstavsruutnätet på nästa sida.

Ceasarchiffer

Ceasarchiffer innebär att man förskjuter alla bokstäver ett visst antal steg. Titta i bokstavsruutnätet och välj hur många steg åt vänster du vill förskjuta. Väljer du två, så tittar du på rad 2: "h" blir chiffererat till "j", "i"

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

blir "k", "t" blir "v". "hitta" blir alltså "jkvvc". Man kan också förskjuta bakåt. Vill du förskjuta bakåt tre steg tittar du på rad -3 (aka. rad 25). "hitta" blir då: dfppz.

Abjad och Abugida

Abjad och Abugida är termer för konsonantskrifter: skriftspråk som huvudsakligen eller enbart består av konsonanter. Om vokaler markeras (det görs sällan eller inte alls i abjad, men ofta i abugida), så görs det med små, små markeringar vid konsonanterna. Exempel på konsonantskrifter är arabiska och hebreiska, eller Ge'ez (Etopien) och South Arabian (Yemen). Fndr p m d nt kn frst knsntls txt md lt trng

أ	ب	ج	د	هـ	و	ز	ح	ط	ي	ك	ل	م	ن	س	ع	ف	ص	ق	ر	ش	ت	ث	خ	ذ	ض	ظ	غ
gh	z	d	dh	kh	th	t	sh	r	q	s	f	'	s	n	m	l	k	y	t	h	z	w	h	d	j	b	'

Arabiska, från http://en.wikipedia.org/wiki/Arabic_alphabet (120121)

translit.	h	l	h	m	ś (SA s ²)	r	s (SA s ¹)	k	b	t	h	n
Ge'ez	ሀ	ለ	ሐ	መ	ሠ	ረ	ሰ	ቀ	በ	ተ	ኀ	ነ
South Arabian	𐩧	𐩨	𐩩	𐩪	𐩫	𐩬	𐩭	𐩮	𐩯	𐩰	𐩱	𐩲

translit.	'	k	w	'	z (SA d)	y	d	g	t	s	d	f
Ge'ez	አ	ከ	ወ	ዐ	ዘ	የ	ደ	ገ	ጠ	ጸ	ፀ	ፈ
South Arabian	𐩣	𐩤	𐩥	𐩦	𐩧	𐩨	𐩩	𐩪	𐩫	𐩬	𐩭	𐩮

Ge'ez och South Arabian, från http://en.wikipedia.org/wiki/Ge%27ez_script (120121)

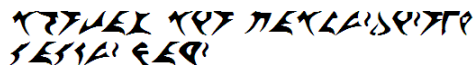
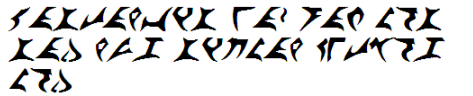
Konsonantskriftsystem går ju fortare att skriva än alfabeten med vokaler. Men de kanske trots det är lite för komplicerade för lajvbruk.

Olika typer av skriftspråk

Innan du kan börja bygga ditt eget skriftspråk så är det nyttigt att veta lite om några vanliga typer. Jag kommer att ta upp fonemiska skriftspråk, fonetiska skriftspråk, stavelsebaserade ("syllabiska") skriftspråk och piktografiska skriftspråk. Många av världens riktiga skriftspråk kombinerar flera av dessa olika system.

Fonemiska skriftspråk

Svenskan och engelskan använder ett fonemiskt alfabet ofta kallat "romerskt alfabet". Kyrilliskan (som ryskan på föregående sida) är också ett fonemiskt alfabet. För att uttrycka det med en grov förenkling så innebär ett fonemiskt alfabet att de minsta betydelseskapande ljuden i språket får ett eget tecken. I orden "bär", "där", "här", "lär" är "b", "d", "h" och "l" ansvariga för att slutresultatet blir helt olika i de olika orden. De får därför egna tecken. Nedan finns exempel på två fonemiska skriftspråk—kyrilliska och det konstgjorda språket Klingon. Det har gjorts flera fonemiska lajvskriftspråk, exempelvis till Kastariavärlden.

A a	А а	Р р	Р р	
Б б	Б б	С с	С с	
В в	В в	Т т	Т т	
Г г	Г г	У у	У у	
Д д	Д д	Ф ф	Ф ф	Transliteration: bortaS blr jablu'DI'reH QaQqu' nay'. qaStaHvIS wa' ram loS SaD Hugh SijlaH qetbogh loD.
Е е	Е е	Х х	Х х	
Ж ж	Ж ж	Ц ц	Ц ц	Translation: Revenge is a dish best served cold Four thousand throats can be cut in one night by a running man.
З з	З з	Ч ч	Ч ч	
И и	И и	Ш ш	Ш ш	
Й й	Й й	Щ щ	Щ щ	
К к	К к	Ъ ъ	Ъ ъ	
Л л	Л л	Ы ы	Ы ы	
М м	М м	Ь ь	Ь ь	
Н н	Н н	Э э	Э э	
О о	О о	Ю ю	Ю ю	
П п	П п	Я я	Я я	

En mer avancerad variant är att förskjuta den första bokstaven två steg åt vänster, den andra bokstaven två steg åt höger, den tredje bokstaven två steg åt vänster etc. Ytterligare en variant är att skjuta alla vokaler en vokal till höger och alla konsonanter en konsonant till höger. De mer avancerade varianterna kommer att kräva lång tid att lösa, och jag rekommenderar dem inte för lajv. Det är krävande nog att lösa ett vanligt ceasarchiffer.

Ceasarchiffer med kodord

Istället för att säga att man förskjuter ett visst antal steg, kan man förskjuta med ett kodord. Om man har ordet "drottning" som kodord börjar man att ta bort alla dubletter av bokstäver: "drotmig" Sen sätter man kodordet först i förskjutningen, som i figuren, och fyller på med resten av alfabetet—minus bokstäverna "d", "r", "o", "t", "n", "i" och "g".

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

Vigenèrechiffer

Vigenèrechiffer är riktigt svårt att knäcka även med substitutionsmetoden, även om det går. Räkna absolut inte med att någon kan göra det med papper och penna under själva lajvet.

Vigenèrechiffer måste använda ett bokstavnätverk som det på föregående sida. Börja med att bestämma ett kodord—exempelvis KUNG. Skriv KUNGGUNGGUNGG etc ovanför meddelandet du vill chiffrera, i det här fallet "uppror":

K	U	N	G	K	U
U	P	P	R	O	R

"u" i "uppror" kodas enligt rad "k": "u" blir alltså "b".

"p" i "uppror" kodas enligt rad "u": "p" blir alltså "g".

”p” i ”uppror” kodas enligt rad ”n”: ”p” blir alltså ”ö”.

”r” i ”uppror” kodas enligt rad ”g”: ”r” blir alltså ”x”.

”o” i ”uppror” kodas enligt rad ”k”: ”o” blir alltså ”u”.

”r” i ”uppror” kodas enligt rad ”u”: ”r” blir alltså ”i”.

Det roliga med Vigenèrechiffer är att när man väl kan tekniken och har kodordet kan man göra mycket häftiga ”uppvisningslösningar” på lajvet, genom att bara avkoda med hjälp av bokstavsnetet. Hur mycket bättre blir inte steampunkkalkemistens skrivbord med ett snyggt bokstavsnet ovanpå de tunga böckerna?

Substitutionschiffer

Koder

Den formella definitionen på en kod, till skillnad från ett chiffer, är att man i koden byter ut hela ord mot andra ord. Det är rimligt att en militärstab på ett lajv skulle kunna skicka sina meddelanden i vad som verkar vara klartext—men där man bytt ut ”kanon” mot ”sjukvårdare”, ”anfall” mot ”läsa bön” och ”fånge” mot ”vilopaus”. *”Flytta sjukvårdarna in bland främsta ledet, och läs morgonbönen vid första gryningsljuset. Ta inga vilopausar under dagen.”*

”Riktiga” chiffer

Chiffer kommer från franskans *chifre* (ursprungligen ”noll”, senare ”siffra”). Ett chiffer handlar alltså om att man byter ut en symbol mot en annan symbol. Här kommer vi avhandla alfabetchiffer (byt ut en bokstav mot en annan bokstav eller siffra) och symbolchiffer (byt ut en bokstav mot en annan symbol).

Alfabetchiffer

Alfabetchiffer innebär att originaltextens bokstäver byts ut slumpvis mot andra bokstäver. ”A” skulle kunna bytas ut mot ”L” och ”B” mot

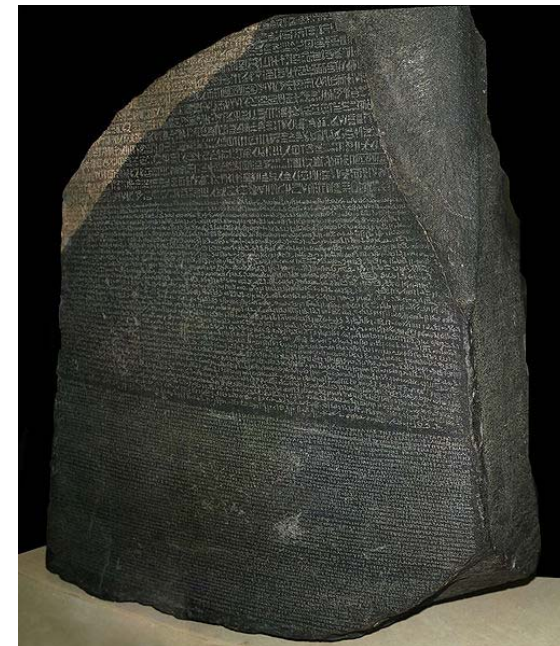
Konstgjorda skriftspråk

Konstgjorda skriftspråk är en sorts symbolchiffer. De är inte bara roliga att göra—de kan också fungera som kulturstärkande för främmande kulturer i ditt lajv. Räkna inte med att någon faktiskt klarar av att knäcka ett okänt skriftspråk under lajvet OM du inte ger en så kallad parallelltext. En parallelltext är samma text skriven på två språk. Om jag förstår att nedanstående två ord är samma, kan jag sen börja nysta upp andra ord. (I just det här fallet kommer man få lite problem med я- symbolen i kyrilliskan)

Вікіпедія

Wikipedia

Den mest berömda parallelltexten är utan tvekan Rosetta-stenen, som nu finns på British Museum. Eftersom samma text är skriven på den tre gånger, kunde man börja dechiffrera de egyptiska hieroglyferna.



http://en.wikipedia.org/wiki/File:Rosetta_Stone.JPG (120121)

Bokchiffer

Bokchiffer är ett mycket svårt substitutionschiffer att knäcka utan att ha tillgång till nyckeln—och i nyckeln i det här fallet är en bok. Mottagaren har exakt samma utgåva av boken—skiljer sig utgåvan, så kan det inte användas.

Jag väljer Dan Anderssons Samlade Dikter, utgiven av Wahlström&Widstrand 1989 på Aktietrykkeriet i Trondhejm.

Jag vill skriva budskapet ”ser du?”. Alltså hittar jag en sida som innehåller bokstaven ”s”. Jag noterar sidnumret, radnumret och symbolnumret (och ignorerar mellanslag): 40-1-8 (sida 40, rad 1, symbolnummer 8). På samma sätt hittar jag en annan plats i boken där bokstäverna ”e”, ”r”, ”d” och ”u” är, och kanske också ett ”?”.

En lättare variant är att bara skriva ett sidnummer—välj en sida vars första bokstav råkar vara den du söker. I Anderssons bok skulle sidan 50 kunna representera ”s” exempelvis. Sid 37, nedan, skulle vara ”o”.

Bokchiffer är roliga på lajv, eftersom det kan vara roligt att jaga efter en bok som en McGuffin. Men deltagarna måste få lite ledning i vilken av alla varianter av chifferering som används, om de ska kunna lista ut knepet. Att bara satsa på en sida=en bokstav är nog det realistiska — undvik mer komplicerade varianter.



Symbolchiffer

Symbolchiffer är när bokstäver byts ut mot symboler. Detta kan ske helt slumpvist, som i Drottning Marys chiffer, eller enligt ett visst mönster, som i brädgårdschiffren. Återigen så avråder jag från slumpvisa chiffer—de kan lösas, men knappast under ett kort lajv.

Drottning Marys chiffer

Drottning Mary (Mary Queen of Scots) blev avrättad för att hennes chiffer, och därigenom hennes komplott, löstes. Drottning Marys chiffer är till viss del ett symbolchiffer, till viss del ett alfabetchiffer och till viss del en kod (eftersom vissa ord byts ut mot en symbol).

En rolig sak med det här chiffret är att det är ytterst google-bart. Det innebär att lajvare i ett nutidslajv kan få ett chiffererat meddelande som de inte kan knäcka (för att de inte har tiden—det gick ju uppenbarligen att knäcka) men senare kan få informationsbiten att det är Queen Mary's Cipher. Lite googling senare så är meddelandet knäckt.