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:
> $C = K + N \pmod{29}$, 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.

