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.

