

## Kryptering

Kryptering är en metod för att förvandla information till oläslig rappakalja. Genom komplicerade matematiska algoritmer går det att skapa krypterade meddelanden som är extremt svåra att knäcka. Det här är en viktig del av informationsflödet på internet. Mycket av det som görs, till exempel betalningar, skulle inte kunna göras utan kryptering. Det finns alltid information som inte ska finnas fritt tillgänglig för alla. För att sådan information ska hållas hemlig behövs kryptering. Det handlar inte endast om företags- eller bankhemligheter utan också om helt vardagliga saker i vår digitala värld. Kryptering är viktigt då man handskas med all sorts digital information. Kryptering är viktig då man skapar spel för datorer. Till exempel så skulle inte spelet Pokémon Go fungera rätt om spelet inte skulle ha skyddats med kryptering. Utan kryptering skulle vem som helst kunna flytta figurerna dit man vill ha dem och hela spelets mening skulle försvinna

Kryptering är troligtvis lika gammalt som skriftspråket självt. Man vet att kryptering användes redan under Julius Caesar tid. När ett brev skulle skickas med hemlig information krypterade man informationen. Julius Caesars algoritm var att förskjuta alfabetet  $n$  steg, och nyckeln var  $n$ . Om texten exempelvis är "kolobi" och  $n$  är tio blir det krypterade meddelandet "uzvzls" eftersom de bokstäverna är tio steg framåt i alfabetet. Detta kallas då för C-10 (nyckel minus 10). Mottagaren flyttar bokstäverna tio steg bakåt för att dekryptera kryptot. Systemet var mycket enkelt och lätt att dekryptera, förutsatt att man visste algoritmen.

Övningen är ett sätt att börja prata säkerhet på nätet samtidigt som eleverna får möjlighet att använda bokstäver på ett spännande sätt.

På sista sidan finns en "snurra". Låt eleverna klistra två ex av snurran på tjockt papper. Sen ska ett ex av hela snurran klippas ut och ett ex

av den inre snurrcirkeln. Fäst ihop delarna med en påsnit. Färglägg gärna bokstaven A på båda snurrorna. Detta gör det enklare att se hur många steg snurran förflyttas.



Eleverna kan skriva sina krypterade namn eller meddelanden till varandra. Elever kan tolka meddelanden som läraren skrivit.

*Viktigt är att bestämma vilken av snurrsskivorna som är ursprungsbokstav resp kod-bokstav samt hur många steg snurran förflyttats.*

