Möjligheternas dag 2024
Årskurs 4-6
Tema: Kryptering

Skapad av Malin Bernelf

Varför kryptering?

Att arbeta med kryptering är något som lockar många elever. Det är spännande att försöka ta reda på vad som står i ett hemligt meddelande och det är kul att kunna skicka egna hemliga meddelanden.

Vad kan man öva sig på när man arbetar med kryptering?

Eleven övar på flera saker. Det tydligaste är kanske beräkningar, och beroende på vilket kryptosystem man använder så övar man på olika typer av beräkningar. Samtidigt övar eleven på att skriva för hand och att skriva både gemener och versaler. Om man ger elever uppgifter som kräver att de funderar lite på hur de ska lösas så övar man också problemlösning och resonemang. Vill man jobba med kryptering på engelska så använder man 26 bokstäver i alfabetet istället för de 28 som används i svensk kryptering. Då ersätts j med i, men v och w krypteras individuellt. Att låta eleverna få utlopp för sin kreativitet och skapa egna sätt att kryptera kan vara mycket kreativt.

Etik kring kryptering

Under möjligheternas dag pratade vi med eleverna om att man inte ska använda hemliga meddelanden för att få någon att känna sig utanför, och att hemligheter alltid ska vara snälla. T.ex. så berättar vi inte vad vi köpt till någon i födelsedagspresent i förväg för då förlorar vi överraskningsmomentet.
Kryptering används i samhället för att skydda information i olika sammanhang, t.ex. när vi betalar med bankkort på nätet, men kryptering kan också användas för olaglig aktivitet. Ett exempel på det är olika krypterade chattar som används för kommunikation i olagliga sammanhang. Beroende på ålder och mognad kan detta också tas upp med eleverna som ett exempel på att kryptering kan missbrukas.

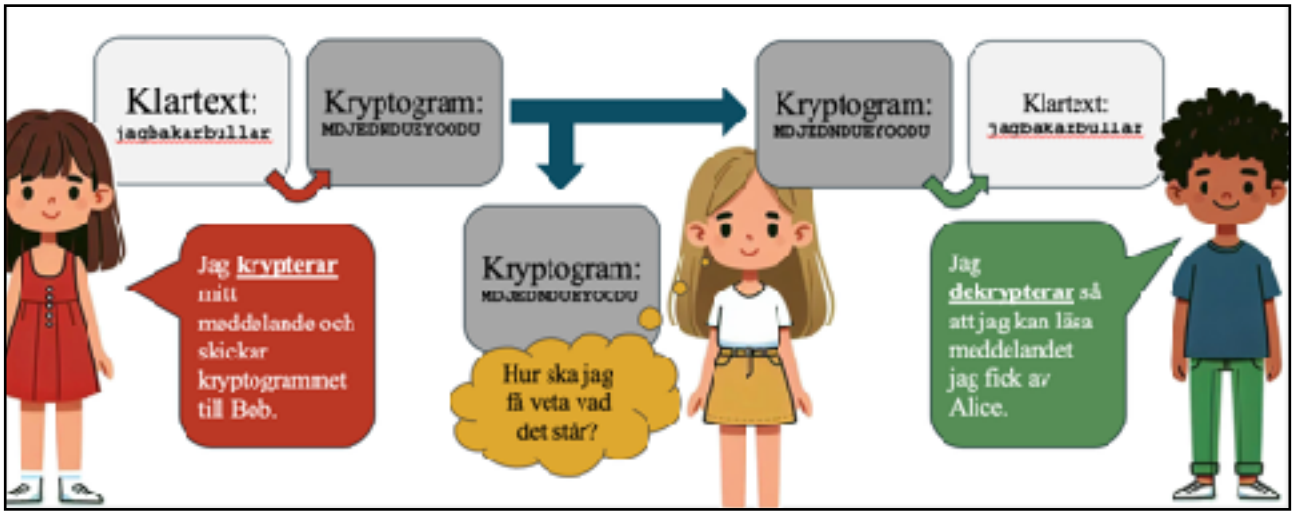
Grundläggande begrepp

Klartext - texten vi vill skicka som hemligt meddelande. När vi skriver om klartexten för att kunna kryptera den tar vi bort allt utom bokstäverna.
Nyckel - det är den information som vi behöver för att kunna kryptera och dekryptera.
Kryptogram - det vi får när vi gjort texten hemlig.
Kryptera - det vi gör när vi skapar kryptogrammet.
Dekryptera - det vi gör när vi omvandlar kryptogrammet till klartext så att det går att läsa.
Kryptoanalys - att undersöka kryptogram för att försöka ta reda på klartexten
Forcera - att lyckas omvandla ett kryptogram till läsbar text utan att ha tillgång till nyckeln.
Kryptosystem - den metod man använder för att kryptera och dekryptera.

Viktigt att veta är att klartexten skrivs med gemener och kryptogrammet med versaler.

Vilka är Alice, Bob och Eve?

Inom kryptering används ofta Alice och Bob i olika exempel. Det är alltid Alice som skickar meddelande till Bob. (Vi skickar från A till B.) Eve är den som vill komma åt kryptogrammet och ta reda på vad det står där. Eve heter som hon gör på grund av engelskans ord för att tjuvlyssna (eavesdropping).



Att omvandla bokstäver till tal

Det behöver vi göra för att kunna kryptera om vårt kryptosystem kräver beräkningar av något slag. Då använder vi tabellen nedan. Av olika skäl har vi i svenska alfabetet då valt bort w och om det dyker upp i klartexten får vi kryptera det som om det vore ett v.

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

Att räkna i kryptering

När vi gör beräkningar i kryptering så behöver vi använda något som kallas moduloräkning. Man kan ta klockan som ett exempel på moduloräkning. När vi kommer till 12 så är vi tillbaka på 0. När vi räknar med modulo 28, vilket vi gör eftersom vårt valda alfabet har 28 bokstäver, så är 28 detsamma som 0. Vi använder moduloräkning i exemplet som finns i presentationen, men jag använder inte ordet moduloräkning med eleverna. Vill man lära sig mer så är det däremot enklast att söka på moduloräkning så hittar man gott om material på nätet.

Kryptosystem

Det finns många olika kryptosystem och de klassiska kryptosystemen kräver inte datorberäkningar, men de är också ganska enkla att forcera. Avancerade kryptosystem som t.ex. RSA kräver datorberäkningar och passar för äldre elever.

Bland de klassiska kryptosystemen är förskjutningskrypto kanske det mest kända, men det finns också andra spännande kryptosystem som t.ex. Vigenère-krypto och affint krypto. Det finns också flera olika kryptosystem som bygger på att man flyttar runt bokstäverna i klartexten på olika sätt och det finns också kryptosystem som använder andra symboler än bokstäver och siffror.

Exempel

I den presentation som är en bilaga till detta dokument finns beskrivet hur Alice och Bob använder sig av förskjutningskrypto för att kommunicera utan att Eve ska få veta vad de skriver, både med hjälp av beräkningar och med hjälp av kryptosnurra.
Eve funderar på hur många olika nycklar det finns, och för förskjutningskrypto finns det 27 nycklar. Att det inte finns 28 beror på att om vi förskjuter 28 steg är vi tillbaka där vi började och kryptogrammet blir den läsbara klartexten - alltså en dålig nyckel. Förskjuter vi t.ex. 30 steg är det samma sak som att förskjuta 2 steg och därför är det inte intressant för oss att välja andra förskjutningar än 1-27 eftersom alla andra nycklar kommer att motsvara en av nycklarna 1-27.
Uppgifter finns tillgängliga i ett separat dokument. Sist i detta dokument finns lösningsförslag och facit.

Stödjande struktur

När man ska kryptera och dekryptera är det viktigt att hålla ordning på vad man gör. I presentationen använder jag en tabell likt den nedan och det brukar vara en bra hjälp.

Klartext										
Kodad klartext										
Beräkning										
Kodat kryptogram										
Kryptogram										

Att skapa egna kryptosystem

Att låta eleverna skapa egna kryptosystem brukar vara engagerande för de flesta elever. Låt eleverna skapa fritt men hjälp dem gärna genom att ställa kontrollfrågor som får dem att reflektera över om deras kryptosystem fungerar bra. Exempel på frågor är

1. När du krypterar en bokstav med ditt kryptosystem, får du då alltid samma bokstav som kryptogram?
2. Hur gör du när du dekrypterar?
3. Är det svårt att dekryptera om man känner till nyckeln?
4. Hur många olika nycklar finns det?

Att jobba vidare

För den som vill jobba mer med kryptering så tipsar jag om Nämnarens kryptoskola. Du hittar den på Nationellt Centrum för Matematik: https://ncm.gu.se/krypto/