TOMAS FRIDSTRÖM

Kryptering – utmaning för 12-åringar

Här berättas om en lektionsserie kring kryptering, som en sjätteklass varit med om. Lärarna ville se om 12-åringar kunde ta till sig relativt avancerad matematik. Resultatet förvånade alla inblandade, utom eleverna.

Under två veckor av höstterminen 2002 arbetade eleverna i en av skolans sjätteklasser med kryptering under totalt 8 matematiklektioner. Klassen är, tycker vi, en helt vanlig sjätteklass med normal spridning av kunskaper och färdigheter. Flera elever hade fortfarande stora problem med multiplikationstabellen.

Fyra olika metoder

Första lektionen handlade om krypteringens historia, dess användning under andra världskriget och i dagens datorer. Syftet med introduktionen var att få eleverna att relatera de kommande ganska teoretiska lektionerna till händelser utanför skolans.

Under fyra lektioner gick vi sedan igenom fyra olika krypteringsalgoritmer. Av dessa var två av substitutionstyp och två av transpositionstyp. Eleverna lärde sig se skillnad på de två huvudtyperna, som dock för enkelhets skull kallades ersättningskrypto och omkastningskrypto. De kryptон som vi lärde ut var alla enkla, och vi kallade dem sifferkrypto, Ceasarkrypto, brädgårdskrypto/scoutkrypto och stavkrypto. Varje lektion följde samma enkla mönster: en teorigenomgång, sedan några exempel på tavlan och till sist övning genom att eleverna skickade egna meddelanden och krypteringsnycklar mellan varandra. Till stavkryptot använde vi långa papperslängder som eleverna lindade kring runda stavar. De andra kryptona krävde inga särskilda hjälpmedel.

Tomas Fridström är civilingenjör och lärare i matematik, no och teknik på Söraskolan i Österåker

Sifferkrypto

Sifferkryptot vi använde bytte helt enkelt ut varje bokstav A ... Ö mot en siffra 1 ... 28. Siffrorna kunde inte vara omkastade men väl förskjutna, tex A=7, B=8 osv. Detta ger en mycket enkel krypteringsnyckel som helt enkelt är antalet steg som siffrorna förskjutits. Eleverna skickade varandra lappar med krypterad text och en siffra 1 ... 28 som var ”nyckel”. En enkel text som

”Jag äter” kan då t ex krypteras som:

10 1 7 27 20 5 18 Nyckel = 1

Eller

13 3 9 1 22 7 20 Nyckel = 3

Bokstavskrypto

Bokstavskryptot bytte på ett liknande sätt ut varje bokstav A ... Ö mot en annan bokstav A ... Ö. Nyckeln var hur många steg krypteringen ändrar bokstäverna. Tex om nyckeln = 2 byts A mot C, B mot D osv. ”Jag äter” blir då:

L C I A V G T Nyckel = 2

Brädgårdskrypto

Brädgårdskryptot behöver ingen nyckel eftersom det endast är en enkel omkasning av ordningen. Vi skrev hemliga meddelanden genom att numrera alla bokstäverna i originalmeddelandet, och först skriva alla de udda bokstäverna i ordning och sedan alla de jämna. ”Jag äter” blir

J G T R A Ä E

Stavkrypto

Stavkryptot gjorde vi mer intressant och kanske roligare genom att arbeta med långa papperslängder som eleverna lindade kring runda stavar. Först när papperslappen lindats kring en stav med rätt diameter så går det att läsa meddelandet. ”Nyckeln” här är alltså stavdiametern.

Vi provade inga svårare algoritmer än dessa fyra. Nästa steg hade nog annars varit ett mer komplicerat utbyteskrypto där man byter varje bokstav, A ... Ö mot ett tal, 1 ... 28, men inte i ordning som vi gjorde ovan.

Vi hade gått framåt snabbt i undervisningen. Fram till denna punkt kunde dock all kryptering och de-kryptering göras ”mekaniskt”, dvs genom användning av enkla regler. Alla elever kunde därför hänga med.

Kodknäckning

Lektion sex och sju var betydligt mer avancerade, vi tänkte nämligen lära ut enkel kodknäckning! Eleverna skulle få prova på att knäcka krypterade meddelanden utan att få reda på vilken nyckel eller ens vilken av de fyra krypteringsmetoderna som använts.

Det vi planerade för dessa två lektioner var förstås mycket mer avancerat än den matematik vi normalt arbetar med. Vi hade innan försöket diskuterat kollegor emellan om det var lämpligt att ta med kodknäckningen eller inte i försöket. Argumentet för var att det gav en fin ”knorr” på avsnittet som de avancerade eleverna kunde ta till sig. Argumentet emot var att endast ett fåtal i klassen, om ens någon, skulle kunna klara av det.

Då de första fem lektionerna gått bra och alla elever deltagit med stort intresse bestämdes att vi skulle försöka. Eleverna fick lära sig att arbeta i fyra steg:

- Först en allmän analys för att bestämma krypteringsmetoden.
  Är det bara siffror i meddelandet?
  Är det ovanliga eller vanliga bokstäver som dominerar? Etc.
- Sedan analys av första ordet, som ju ofta är ordet ”Hej” el dyl.
- Därefter analys av dubbelsymboler, som i svenskan ofta står för ”tt”.
- Till sist, om inget annat hjälper, frekvensanalys av hela meddelandet för att kunna jämföra meddelandets vanligaste tecken med svenska alfabetets vanligaste bokstäver E,A,N m fl.

Förvånade lärare

Till allas – utom elevernas – förvåning upplevdes inget av detta som svårt eller märkvärdigt, inte ens frekvensanalysen. De flesta eleverna arbetade timme sju med att knäcka kodmeddelanden som stod skrivna på tavlan. De flesta klarade av att läsa någon eller flera meddelanden. Eller var det i själva verket så att ett fåtal knäckte koder och de övriga tog hjälp av dem? Det skulle provet under den avslutande lektionen avgöra!

Enastående provresultat

Provet bestod av en teorifråga, två meddelanden att kryptera där vi bestämde metod och nyckel, samt ett kodat meddelande som eleverna skulle knäcka. Detta meddelande var:

22 14 21 4 23 23 4 21 16 4 17
16 8 7 16 4 10 8 17 8 15 15 8
21 12 17 23 8 ?

Klarar läsarna att knäcka detta?
(Svar finns på Anslagstavlan)

Vi rättade med stigande förvåning: 24 elever av 26 hade knäckt krypteringen! Nästan alla klarade de övriga frågorna. 90% av de fel vi fann var små slarvfel vid krypteringen. Max poäng på provet var 9. Medianresultatet räknades ut till 8,5!

Efteråt

Veckan efter var matematiklektionerna tillbaka i den vanliga lunken. De elever som just excellerat i lärande tragglade nu med grunderna. Vi försökte få dem att förstå att de just lärt sig något som de flesta vuxna skulle ha väldigt svårt att lära, men det ville inte eleverna acceptera. När vi pratade om terminen upplevde eleverna de två krypteringsveckorna som mycket enklare än de övriga veckorna.

Nyttan som eleverna kan ha av kryptering och kodknäckning är kanske begränsad. Men vi hade alla roligt och fick ett bra avbrott ifrån de vanliga lektionerna. En slutsats att dra av försöket är att även 12-åringar är kapabla till avancerat matematiskt tänkande. Speciellt om de inte upplever det de gör som matematik.

DPL 20

Dialoger om problemlösning ger denna gång ett tillfälle att arbeta med kryptering.

83 Julkrypto

OCLONTROU TRANJVHPO
DOUJNT NKKN KCUNTR
RO THJVHFV FPA IXK
PMG
RVV FPVV OÅVV BT