15. Inledning

Avsnitten från och med nummer 15 är en fortsättning av Nämnarens kryptoskola som sedan december 2006 finns tillgänglig på NCMs webplats. Vi förutsätter att den som vill arbeta med fördjupningskursen har tillgodogjort sig grundkursen, som omfattar avsnitten 4 - 14. Man bör särskilt känna sig förtrogen med avsnitten 10 och 11. Vi som har utformat denna del av kryptoskolan heter Bengt Beckman och Stig-Arne Ekhall. Språkstatistiken har tagits fram av Jesper Ekhall.

I fördjupningskursen behandlar vi nästan endast forcering. Det betyder att från en kryptotext ta reda på den klartext som man har använt för att med kryptering åstadkomma kryptotexten utan att veta hur krypteringen har gått till i detalj. Det viktigaste hjälpmedlet är klartextens statistiska struktur, till exempel hur ofta en viss bokstav och bokstavskombinationer normalt förekommer i löpande text på det språk som klartexterna är avfattade på. Oftast gäller det svenska språket, men vi uppmanar forcörerna att även pröva engelska eller eventuellt annat språk som man behärskar.

Vi tänker oss att de som arbetar med fördjupningskursen är något äldre än de som ägnade sig åt grundkursen. Eleverna går nog i grundskolans högstadium eller på gymnasiet. Vi tror att de själva hämtar ner avsnitten från NCMs webplats och därför finns här i de olika avsnitten inte någon lärarsida med inledning, tips och svar till övningsuppgifter.

Bäst lär man sig krypto om man är två personer som samarbetar. Dessutom är det roligare än att vara ensam. Man kan utmana sin kryptokompis med kryptotexter och se efter om han/hon kan forcera dem. Liksom i grundkursen föreslår vi därför i första hand att två elever arbetar tillsammans med materialet, som är utformat med det som förutsättning. Men det går också bra att tillgodogöra sig kursens innehåll om man är ensam i studiearbetet.

Uppgifterna i fördjupningskursen tar längre tid att genomföra än uppgifterna i grundkursen. Ibland kan de nog vara tålamodsprövande. Fast om man tänker på hur ungdomar i dag kan sitta i timmar vid datorn med spel och andra aktiviteter, så blir det uppenbart att de även kan ägna en hel del tid också för att lära sig de första grunderna i forcörens spännande arbete. Den som kan datorprogrammering uppmanas att själv göra program som hjälpmedel för arbetet med kryptering, dekryptering och forcering.

Bengt Beckman *Stig-Arne Ekhall*

© Nämnaren, Bengt Beckman & Stig-Arne Ekhall