MAN 060 – Elementär talteori
Sommaren 2007

Kappsäckskrypto

En ganska enkel men charmerande tillämpning på kongruensräkning är så kallad kappsäckskryptering, en krypteringsmetod som baseras på kappsäcksproblemet. Metoden föreslogs möttes till en början med entusiasm och förväntning men visade sig senare inte hålla måttet; Shamir publicerade 1982 en algoritm som snabbt löser de speciella kappsäcksproblem som uppstår i kappsäckskrypto.

Kappsäcksproblemet

Själva kappsäcksproblemet, eller i varje fall en variant av det, kan formuleras så: vi har en uppsättning föremål, alla med given vikt i hela kilogram. Några av föremålen packas ned i en kappsäck som sedan vägs. Problemet är att givet kappsäckens vikt avgöra vilka av föremålen som blivit nedpackade.
En matematisk formulering är: givet positiva heltal $a_1, a_2, a_3, \ldots a_n$ och S, bestäm en följd $x_1, x_2, x_3, \ldots x_n$, där varje $x_i = 1$ eller $= -1$, sådan att $\sum_{i=1}^{n} x_i a_i = S$.
Det allmänna kappsäcksproblemet är svårt i den meningen att det i dag inte finns någon algoritm som är väsentligen snabbare än att pröva alla möjliga följder $x_1, x_2, x_3, \ldots x_n$. Dessa är 2^n till antalet varför redan en kappsäck med 100 föremål bereder ett problem som i praktiken är hopplöst.

Det finns emellertid lättlösta specialfall av kappsäcksproblemet: Om nämligen följden $\{a_i\}_{i=1}^{n}$ är ***superväxande***, det vill säga $a_j > \sum_{i=1}^{j-1} a_i$ för alla j, $2 \le j \le n$, kan man lösa problemet så här:

Steg 1: om $a_n < S$, sätt $x_n = 1$
Steg 2: om $a_{n-1} < S - x_n a_n$, sätt $x_{n-1} = 1$
Steg 3: om $a_{n-2} < S - x_{n-1} a_{n-1} - x_n a_n$, sätt $x_{n-2} = 1$
Och så vidare.

Allra enklast är att välja $a_i = 2^i$ i vilket fall kappsäcksproblemet övergår i problemet att skriva S på binär form (fast baklänges). Om till exempel $S = 23$ blir talen $x_1, x_2, x_3, \ldots x_n$ lika med 1,1,1,0,1.

Kappsäckskrypto

Idén med kappsäckskryptot är att med hjälp av kongruensräkning överföra ett enkelt kappsäcksproblem, det vill säga med en superväxande följd, till ett svårt (allmänt).

Klartexten representeras av en binär sträng $\{x_i\}_{i=1}^{N}$ som delas in i block av längd $=n$.

Välj en superväxande följd $\{a_i\}_{i=1}^{n}$ där $a_j > \sum_{i=1}^{j-1} a_i$ för alla j, $2 \le j \le n$. Välj dessutom ett tal m med $m > 2a_n$ och ett tal w med $(w,m)=1$. Låt $b_i = wa_i$ för varje i och bilda, för varje block av klartexten, $S = \sum_{i=1}^{n} x_i b_i$. S skickas som kryptotext och för att rekonstruera klartexten krävs att man löser ett antal svåra kappsäcksproblem.

Den som känner w och m kan emellertid beräkna $\tilde{w}$ där $w\tilde{w} \equiv 1 \pmod{m}$ och därefter multiplicera den givna ekvationen $S = \sum_{i=1}^{n} x_i b_i$ med $\tilde{w}$ och erhålla $S\tilde{w} = \sum_{i=1}^{n} x_i \tilde{w} b_i$ där högerledet är kongruent med $\sum_{i=1}^{n} x_i a_i$ modulo m eftersom $\tilde{w}b_i = \tilde{w}wa_i \equiv 1a_i \pmod{m}$. Genom att reducera $S\tilde{w}$ modulo m till den minsta resten som vi kan kalla S_0 får vi ett nytt kappsäcksproblem $S_0 = \sum_{i=1}^{n} x_i a_i$ där likhet gäller eftersom $\sum_{i=1}^{n} a_i < m$. Detta kappsäcksproblem är enkelt eftersom $\{a_i\}_{i=1}^{n}$ är superväxande.