3/2 2002

$RSA-kryptosystemet$

Kryptering är studiet av sk kryptosystem för säker kommunikation. Avsändaren, S, transformerar, *krypterar*, meddelandet innan hon sänder iväg det så att förhoppningsvis endast godkända mottagare, M, kan rekonstruera, *dechiffrera*, det. Här skall jag beskriva det så kallade RSA-kryptosytemet (efter Rivest, Shamir och Adleman som utvecklade det). I detta system gör varje deltagare en krypteringsnyckel offentlig och en dechiffreringsnyckel hemlig. Sändaren behöver bara kolla upp mottagarens krypteringsnyckel i den offentliga tabellen och kryptera efter den. M dechiffrerar sedan med hjälp av sin hemliga nyckel. Alla ord representeras i RSA med siffror. T ex SEND MONEY blir

$$20061505011416150626$$

S är 20:e siffran i alfabetet, E den 6:e och så lägger man till en nolla för att alltid få tvåsiffriga tal osv. Blanktecken utelämnas vanligtvis.

Här följer hur det går till mer i detalj. Alla M väjer först två primtal, vanligtvis med ca 100 siffror vardera. Kalla dem p och q. Sedan beräknar M $z = p \cdot q$ och $\phi = (p-1) \cdot (q-1)$. Sedan väljs ett heltal n sådant att $\gcd(n, \phi) = 1$. Man väljer oftast n som ett primtal. Sedan gör M de två talen

$$z, n$$

offentliga. Slutligen beräknar M det UNIKA talet s, $0 < s < \phi$, som uppfyller $n \cdot s \bmod \phi = 1$. Talet s hålls hemligt och används för dechiffreringen. Om nu S vill sända iväg heltalet $a, 0 \leq a \leq z-1$, till M med nycklarna z och n så beräknar hon $c = a^n \bmod z$ och skickar c. M dechiffrerar genom att beräkna $c^s \bmod z$ SOM VISAR SIG VARA LIKA MED a !!!!!!!!

Övning. Gå igenom proceduren ovan genom att välja två mindre primtal p och q.

Om det skall vara säkert så skall p och q vara minst 100-siffriga och för att förenkla räkningarna mod z för stora tal så är följande samband användbart

$$a \cdot b \bmod z = (a \bmod z) \cdot (b \bmod z) \bmod z.$$

Visa! Att krypteringen-dechiffreringen verkligen fungerar beror på följande sats som vi inte bevisar här

$$a^u \bmod z = a$$

för alla $0 \leq a < z$ och $u \bmod \phi = 1$. Med hjälp av dessa två samband får vi

$$c^s \bmod z = (a^n \bmod z)^s \bmod z = (a^n)^s \bmod z = a^{ns} \bmod z = a$$

eftersom $ns \bmod \phi = 1$.

Säkerheten för RSA-systemet beror på att man inte känner till någon algoritm som kan faktorisera d-siffriga tal på polynom tid, $O\left(d^k\right), k \in Z^+$. 1977 utlyste Martin Gardner i Scientific American ett pris på \$100 till den som kunde knäcka en kod med ett 64-siffrigt och ett 65-siffrigt primtal och $n = 9007$. Detta lyckades några holländare med 1994. Arbetet koordinerades via Internet och 600 frivillga från 25 länder deltog. Sammanlagt 1600 datorer ingick i faktoriseringen.

Jag har avändt mig av Johnsonbaughs bok Discrete Mathematics (5:e upplagan). Beviset som utelämnats ovan hittar man i Introduction to Algorithms av T.H.Cormen m fl, MIT press 1990.