KRYPTOGRAFIAN ALKEET

3. RÄKNEÖVNINGEN

Några saker att lägga märke till:

- Det kommer en förfrågan av passliga tider för tenten på kurssidan.
- På föreläsningen sades det att om α är positivt, så är talen $a_0, a_1, \ldots$ positiva i kedjebråksrepresentationen. Naturligtvis kan a_0 även vara noll.
- Man får gärna delta i de svenskspråkiga räkneövningarna fastän man inte talar svenska som modersmål, så länge man anser sig kunna presentera sina lösningar på tavlan.
- Diffie-Hellmann flyttades till nästa vecka.

(1) Uttryck följande tal som kedjebråk:
   (a) $\frac{129}{47}$
   (b) $\frac{63}{8}$.

(2) Låt RSA:s offentliga nyckel vara $(n, e) = (8051, 5)$, där $8051 = 83 \cdot 97$. Bestäm d.

(3) Använd RSA-uppsättningen från föregående uppgift för att kryptera talet $w = 1023$.

(4) Vi använder igen RSA-uppsättningen från uppgift 2. Det mottagna meddelandet är 1000. Dekryptera meddelandet.

(5) Primtalsfaktorisera talet 159062543 (tips: talet är en produkt av två primtal, och metoden som bryter RSA då primtalsfaktorerna för talet n är för nära varandra kan mycket väl fungera även här).

(6) Använd Wieners attack för att bryta RSA, då $n = 43327327$ och $e = 38501369$.

(7) I Wieners attack antar vi att $p < q < 2p$. Hur förändras situationen, och speciellt vilken gräns skulle det räcka att sätta på talet d, ifall vi endast visste att $p < q < 8p$?