Ex. Min RSA nyckel.

Jag väljer $p = 31$ $\quad q = 43$

får $pq = 1333$

$(p-1)(q-1) = 30 \cdot 42 = 1260 = 2^2 \cdot 3^2 \cdot 5 \cdot 7.$

väljer $a = 143$ $\quad (= 11 \cdot 13$, relativt prim med $1260)$

publicera $pq = 1333$, $\quad a = 143$

förbereder mig för mottagande av meddelande:

vill hitta b : $143 \cdot b \equiv 1 \mod 1260$.

$= 4 \cdot 9 \cdot 5 \cdot 7$

Använ kinesiska restsatsen för att ~~hitta~~ pussla ihop det

$140 \equiv 0 \mod 4$

$144 = 12^2 = 2^2 \cdot 9^2$

$140 \equiv 0 \mod 5$

$140 \equiv 0 \mod 7$

$$\begin{cases} 143b \equiv 1 \mod 4 \rightsquigarrow 3b \equiv 1 \mod 4 \rightsquigarrow b \equiv -1 \mod 4 \\ 143b \equiv 1 \mod 9 \rightsquigarrow -b \equiv 1 \mod 9 \rightsquigarrow b \equiv -1 \mod 9 \\ 143b \equiv 1 \mod 5 \rightsquigarrow 3b \equiv 1 \mod 5 \rightsquigarrow b \equiv 2 \mod 5 \\ 143b \equiv 1 \mod 7 \rightsquigarrow 3b \equiv 1 \mod 7 \rightsquigarrow b \equiv 5 \mod 7. \end{cases}$$

$$\left.\begin{matrix} b \equiv -1 \mod 4 \\ b \equiv -1 \mod 9 \end{matrix}\right\} \rightsquigarrow b \equiv -1 \mod 36$$

$$\left.\begin{matrix} b \equiv 2 \mod 5 \\ b \equiv 5 \mod 7 \end{matrix}\right\}$$ lös med Kin. restsats : Bezout $3 \cdot 5 - 2 \cdot 7 = 1$

$\Rightarrow 5 \cdot 3 \cdot 5 - 4 \cdot 7 \equiv 2 \mod 5$

$\equiv 5 \mod 7.$

$= 75 - 28 = 47 \equiv 12 \mod 35$

så $\left.\begin{matrix} b \equiv -1 \mod 36 \\ b \equiv 12 \mod 35 \end{matrix}\right\}$ Bezout: $36 - 35 = 1$

så $b = 12 \cdot 36 - (-1) \cdot 35$

$= 360 + 72 + 35$

$= 467$

kolla att $467 \cdot 143 \equiv 1 \mod 1260$!