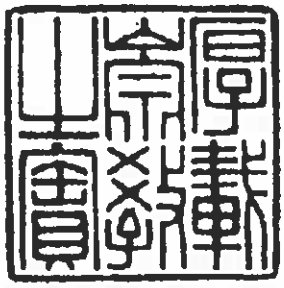

300+ AD

Sun Zi

孫子算經卷上

唐朝議大夫行太史令上輕車都尉臣李淳風等奉 勅注釋

度之所起起於忽欲知其忽蠛吐絲爲忽十忽爲一絲十絲爲一毫十毫爲一氂十氂爲一分十分爲一寸十寸爲一尺十尺爲一丈十丈爲一引五十尺爲一端四十尺爲一疋六尺爲一步二百四十步爲一畝三百步爲一里

稱之所起起於黍十黍爲一絫十絫爲一銖二十四銖爲一兩十六兩爲一斤三十斤爲一鈞

Exercise 5.13 (22)

$n = pq$, d – private key,

$decr(y) = y^d \bmod n$, $\quad n \approx 2^{2l}$, $\quad p, q \approx 2^l$

Algorithm 5.15: CRT-OPTIMIZED RSA DECRYPTION$(n, d_p, d_q, M_p, M_q, y)$

$x_p \leftarrow y^{d_p} \bmod p$
$x_q \leftarrow y^{d_q} \bmod q$
$x \leftarrow M_p q x_p + M_q p x_q \bmod n$
return (x)

$d_p = d \bmod (p-1)$
$d_q = d \bmod (q-1)$
$M_p = q^{-1} \bmod p$
$M_q = p^{-1} \bmod q$

exp. time cl^3

$c(2l)^3 \rightsquigarrow 2cl^3$

4 times faster

CRT: $(x_p, x_q) \longleftrightarrow (q^{-1} \bmod p)\, q\, x_p + (p^{-1} \bmod q)\, p\, x_q \bmod pq$