

MIDDLE - SQUARE METHOD

example: $5146 \xrightarrow{\text{square}} 26481396$ $100 = 10^2 = 10^{k/2}$

$k=4$

$4813 \xrightarrow{\text{square}} 23164969$

$1649 \xrightarrow{\text{sq.}} 02719201$

sequence: $5146, 4813, 1649, 7192, \dots$

$[5, 1, 4, 6, 4, 8, 1, 3, 1, 6, 4, 9, 7, 1, 9, 2, \dots]$

7192

LINEAR CONGRUENTIAL METHOD

- multiplier: α
- increment: β
- modulus: N
- seed: S_0

Repeat: $S_n = \alpha S_{n-1} + \beta \pmod{N}$

EXAMPLE: $\alpha = 37, \beta = 1, N = 100$

$S_0 = 17, S_1 = 37(17) + 1 = 630 \equiv 30 \pmod{100}$

$S_2 = 37(30) + 1 = 511 \equiv 11 \pmod{100}$

$S_3 = 37(11) + 1 = 408 \equiv 08 \pmod{100}$

sequence: $17, 30, 11, 8, \dots$

$[1, 7, 3, 0, 1, 1, 0, 8, \dots]$