Generatore BBS

Blum, Blum, Shub. Generatore di numeri binari pseudocasuali crittograficamente sicuro basato su una funzione one-way e predicato hard-core. Polinomiale ma lento, per generare molti numeri si utilizzano altri algoritmi (e.g. con cifrari simmetrici).

Input

- $n = pq$ con p, q primi grandi tali che:

$$p \equiv q \equiv 3 \mod 4$$

e

$$\left(2\left\lfloor\frac{p}{4}\right\rfloor + 1, 2\left\lfloor\frac{q}{4}\right\rfloor + 1\right) = 1;$$

- y coprimo con n.

Il seme è $x_0 = y^2 \mod n$ (le sequenze possibili sono n).

Generazione

Generiamo $m \leq n$ interi con:

$$x_i = x_{i-1}^2 \mod n$$

e usiamo come predicato la parità:

$$b_i = x_{m-i} \mod 2$$

dove con x_{m-i} invertiamo l'ordine di consumazione.

Esempio

$p = 11$, $q = 19$, $n = 209$, $y = 30$ $x_0 = 30^2 \mod 209 = 64$
Sequenza:

$$64 \quad 125 \quad 159 \quad 201$$

quindi l'output sarà 1, 1, 1, 0.