Generatori pseudocasuali basati su cifrari simmetrici

- C cifrario simmetrico (e.g. AES)
- r numero di bit delle parole prodotte da C (e.g. 128, 256)
- s seme casuale di r bit
- n numero di parole di r bit da generare
- k chiave segreta

GENERATORE(s, n)
1 $d =$ TIME() su r bit
2 $y = C(d, k)$
3 $z = s$
4 **for** $i = 1$ **to** n
5 $\quad x_i = C(y \oplus z, k)$
6 $\quad z = C(y \oplus x_i, k)$

Le proprietà del cifrario garantiscono che il generatore è crittograficamente sicuro. Più veloce di BBS.