

Entée: Coxemple 5mtP: comeco sempre com X, staonte jo sobre um prefixo, o que se fos: (G(K): pode prever o sasto Duestão: · G: K→ {0,1} por todo K: XOK (G(k))=1 Clericioner in 3° R: Mão, dodo N-1 bits i posicel person o iltimo let. E. siprostque me abrilitu con t PRO FRACO \* Gerador congruente linear: 3 parâmetres: 2 interios: A.B 4 + [0] = seed pr[i] = a.r[i-1]+b mod p Cily so stiel enuglo occ tuglies ++ i Pal Soul de prover. orbiblish ace regilitu somun \* Olila rondom (): r[i] + (r[i-3]+r[i-3]]% 232 Lec[i]>> 1

