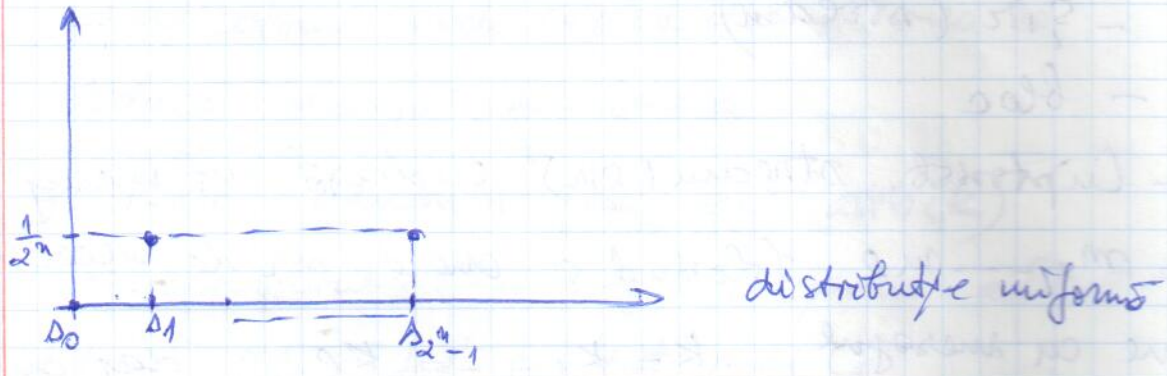
pseudoaleatoare: $\{0,1\}^n$, 2^n șiruri binare



$|k| = 128$ biți

→ vreau să generez chei de lungime n, $n \gg 128$

n e cu cât mai mare de 128 –

Dacă aleg de ~~lungime~~ lungime 1 au probab. cât mai mare decât distribuția uniformă

⇒ e un generator prost → dă indicii asupra cheii ⇒ distr. cheilor tb. să fie cât mai aproape de ~~uniformă~~ distribuția uniformă (caz pseudoaleatoare)

→ nimeni n-a demonstrat că i se generează bun pseudoaleatoare.

– RSA-gen și BBS gen sunt cele mai bune la ora actuală –

RSA$_{gen}$ → utilizează exponențiere modulară (e lentă)

$N = p_1 p_2$, e

$x_0 \in [1, N)$

$x_1 = x_0^e \bmod N$

$x_2 = x_1^e \bmod N$.

⋮

din fiecare x_i succesorul de la x_2 se alege