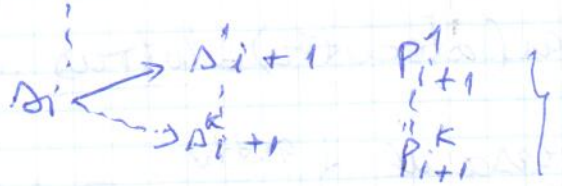
A_0.



$\mathcal{A}$ = algoritm.

$\mathcal{A}(x) = y$ dacă $\mathcal{A}$ este determinist și produce y, atunci odată ce x la intrare.

$y \leftarrow \mathcal{A}(x) \Leftrightarrow \mathcal{A}$ pe intrarea x produce y, cu $\mathcal{A}$ = probabilist.

Pe o intrare x, $\mathcal{A}$ poate produce mai multe ieșiri, fiecare cu o anumită probabilitate.

$x \xleftarrow{u} \mathcal{A} \Leftrightarrow x$ este selectat uniform random din mulțimea $\mathcal{A}$ (este ales echiprobabil)

$\mathcal{A}$ = finită: $\Rightarrow$ probabilitatea cu care este selectat x este $\frac{1}{|\mathcal{A}|}$

Comunicația între 2 entități = printr-un canal, care poate fi { sigur / nesigur.

Dacă toate canalele ar fi sigure $\Rightarrow$ n-am mai avea nevoie de criptografie; majoritatea canalelor = nesigure.

Canalele nesigure $\rightarrow$ sunt supuse la { atac pasiv / atac activ.

- atac pasiv: monitorizarea canalului, obț. inform. care circulă în canal

atac activ = monitorizare + alterarea informației (inclusiv injectarea de noi informații)