2) $\mathcal{E}$ = algoritm probabilist de criptare care primind de la o cheie k și un mesaj m generează criptotextul

$c \leftarrow \mathcal{E}(k, m)$ se mai notează $c \leftarrow \mathcal{E}_k(m)$

criptare probabilistă ($\Rightarrow$ mesajul m cu aceeași cheie k poate fi criptat diferit în fiecare dintre momentele în care este criptat.

3) $\mathcal{D}$ = algoritm determinist de decriptare, cu proprietatea $\forall k, \forall m, \forall c$, cu $c \leftarrow \mathcal{E}_k(m)$ are loc $\mathcal{D}(k, c) = m$ (se mai scrie $\mathcal{D}_k(c) = m$)

$$\mathcal{E}_k(m) \begin{cases} \xrightarrow{} c \\ \xrightarrow{} c' \\ \xrightarrow{} c'' \end{cases} \Rightarrow \mathcal{D}_k\begin{pmatrix} c \\ c' \\ c'' \end{pmatrix} = m.$$

În criptografie, principiul fundamental stabilit de către Kerckhoffs spune că:

- criptosistemul trebuie să fie public, și doar cheia de criptare să fie secretă. (Chiar dacă e public, nu asigură securitate)
- ex: criptosistemul A5/1 → fol. de GSM → a fost decriptat de atacatori – (e foarte slab).
  A5/2, A5/3 (mai bune).
- Păstrarea secretă → încurajează fraude.

Modele de securitate –

Când apreciem siguranța unui sistem de sec.

→ Modele pasive: