Introducere în criptografia simetrică

- Criptografia = instr. fundam. pt protejarea comunicației într-un sistem.

→ nu poate asigura securitate fără alte instrumente ajutătoare { controlul accesului / protocoale de securitate

- Criptografia. → 1) confidențialitate → canalul privat al inf între 2 sau > entități
2) integritate → integritatea informației (inf nu e alterată, modificată)
3) autentificare → stabilirea identit. entităților într. un sistem
4) nerepudiere – pt nerepudierea inf.

Criptografie { simetrică - (cu chei private)
- asimetrică (cu chei publice)

- Parametri de securitate

→ P. de sec. = lungimea unei chei de criptare sau: dimens minimă a unei informații pt a asigura securitate în modul general

→ În criptografie parcurs de sec se notează cu 1^n (unar = parm. de sec. n)
→ n biți de 1 pt a repet un nr natural n

- Algoritmi utilizați = probabiliști →
→ În anumite stări, algoritmul poate face o alegere cu o probabilitate - dar suma probabilităților în orice stare în fi dist. este 1.