CONTROLUL ACCESULUI - se referă la autorizarea de a folo și admite resurse și NU la autentificare (acces prin autentificare).
- Nu e suficient pt a proteja fluxul de inf între 2 entități.
- de criptată informația cu ajutorul primitivelor criptografice

Criptografia simetrică -
Nu poate asig. securitate fără alte instr. ajutătoare: controlul accesului ; protocoale de securitate

Securitate: 1) Confidențialitate → caracterul privat al inf
2) integritate = inf trebuie să fie nealterată, ne modif
3) autenticitate - stabilirea identității entităților
4) nerepudiere → (nu se poate nega paternitatea inf)

- Criptografia 1) simetrică - cu chei private
2) asimetrică - cu chei publice.

Parametri de securitate = lungimea unei chei de criptare - = dimens minimă a unei inf care să asigure securit la nivel.
- se notează cu 1^n
- Algoritmi utilizați = probabiliști - (suma tuturor prob. = 1)
- Canalele sigure (nu mai e nevoie de criptografie = ideal)
nesigure → atac pasiv → monitorizare canal, eavesdrop
activ → alterarea informației, injectare

Adversarul A = modelat de un algoritm probabilist cu complexitate timp polinomială
Oracol = entitate ce oferă informații algoritmului - cărui acesta i le cere.

Schemă de criptare simetrică: 3 uplu $\Pi(G, E, D)$
G = alg. probabilist de chei de criptare k, $k \leftarrow G(1^n)$ → generator de chei
E = alg probabilist de criptare $E(k, m)$
D = alg de decriptare
→ deci: 1 generator de chei, un alg de criptare, un alg de decriptare

M. de securitate Modele pasive
Criptosist să fie public, doar cheia de criptare să fie secretă
COA: ciphertext only attack: atacatorul vede criptotextele vrea să deducă mesajul sau cheia
KPA → known plaintext attack → atacatorul a învățat în timp că m_1 a fost criptat → c_1 (criptotext)
m_R - - - - - - - - c_e
și încearcă să găsească cheia știind și plaintextul inițial și ciphertextul rezultat.

Modele active:
CPA - chosen plaintext atack - adversarul poate obține criptotextul asociat unui plaintext ales de el
(Lunchtime attack).