Canalele nesigure: sunt supuse atacului realizat de un adversar (atacator) = intrus

în fct de atac, adversarul { activ / pasiv

- adversarul poate fi { intern / extern } sistemului

- În criptografie și SI - adversarul A este modelat printr-un algoritm probabilist de complexit. polinomială (Hmp) ⇒ PPT.

a poate avea acces la un oracol

oracol = un formalism general ce înzestrează un algoritm, furnizând informații. Algoritmul când acesta îi le are.

ex de întrebare: n este prim? (a consultat un oracol).

$\mathcal{O}$ = oracol; $A^{\mathcal{O}}$ = algoritmul A care are permisiunea de a consulta un oracol $\mathcal{O}$

Schemă de criptare simetrică

→ 3-uplu: $\Pi(\mathcal{G}, \mathcal{E}, \mathcal{D})$ unde

$\mathcal{G}$ = algoritm probabilist de chei de criptare k

$k \leftarrow \mathcal{G}(1^n)$

generatorul trb să fie f. important → trb să fie cât mai random.