3 CRIPTOLOGIA MODERNA

SISTEMES D'ENCRIPTAT SIMÈTRIC

La criptografia de clau simètrica, és un terme utilitzat pels algorismes criptogràfics que utilitzen la mateixa clau pel xifrat i desxifrat. La clau se sol dir "clau simètrica" o "clau secreta".

SISTEMES D'ENCRIPTAT ASIMÈTRIC

Els sistemes d'encriptació asimètrics, també coneguts com a xifratge de clau pública, són un tipus de sistema criptogràfic en què es fan servir dues claus diferents per xifrar i desxifrar informació. Cada usuari té un parell de claus: una clau privada i una clau pública.

La clau pública es pot compartir amb qualsevol persona, ja que només serveix per xifrar missatges. La clau privada, en canvi, només la coneix el propietari i s'utilitza per desxifrar missatges xifrats amb la clau pública.