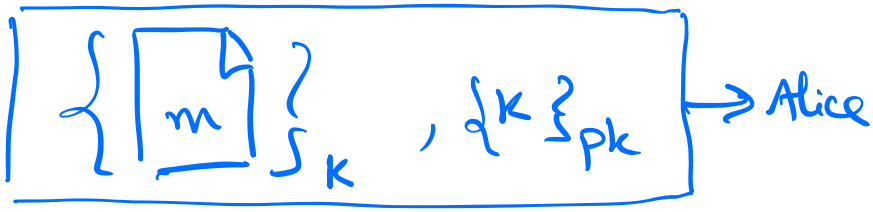
chiffrement hybride

combine clé secrète (rapide)
clé publique (chiffre la clé secrète)

$K \leftarrow$ genClé



transmettre K à Alice de clé publique pk privée sk
Alice reçoit le message : elle récupère K

$\{\{K\}_{pk}\}_{sk} = K$

elle peut déchiffrer $\{m\}_K$: $\{\{m\}_K\}_K = m$

clé publique pk → annuaire de clés PGP
certifié par un tiers (toile de confiance)

Quels chiffres ? - EC, RSA, ElG (DSA)
- IDEA

Open PGP

Ext. ce qui mon chiffr est sûr ?
mon protocole est sûr ?
mon implem. est sûre ?