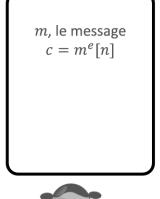
## RSA:



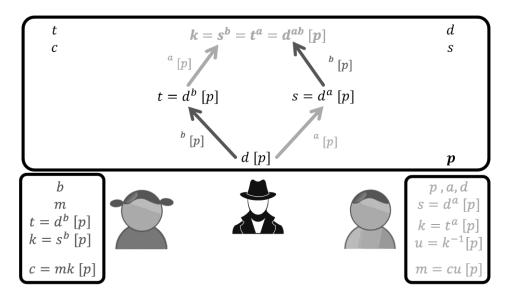
С

$$p,q$$
 premiers  $n=pq$   $\varphi(n)=(p-1)(q-1)$   $e$  tel que:  $-e<\varphi(n)$   $-pgcd(e,\varphi(n))=1$   $d=e^{-1}[\varphi(n)]$   $m=c^d[n]$ 





## **ElGamal:**



## **Elliptic Curves Cryptography:**

