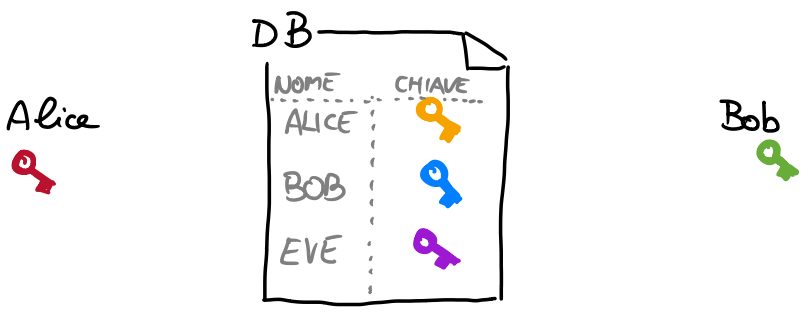
CIFRATURA CON CHIAVE PUBBLICA

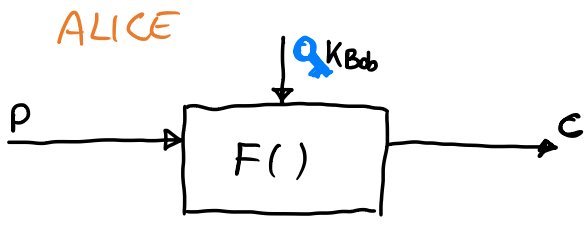
Alice e Bob si devono parlare in modo segreto ma sul canale ci sono intrusi.

Alice e Bob generano due chiavi e tasti:

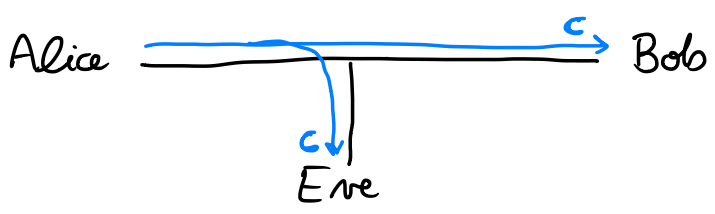
Ogni persona pubblica una delle due sue chiavi in un DB pubblico



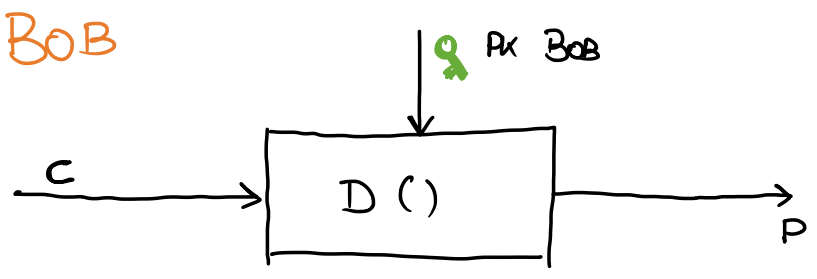
Se Alice vuole scrivere deve cifrare il messaggio con la chiave pubblica di Bob



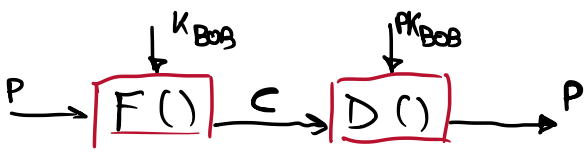
F(): funzione di cifratura
P: plaintext, messaggio in chiaro
KBob: Key Bob: chiave pubblica di Bob
C: cypher text: Testo cifrato non leggibile
Il testo C viene inviato sul canale.



Bob riceve C, chiama la funzione D() per decifrare il messaggio ricevuto.



1. Gli intrusi non riescono a decifrare il messaggio perché non hanno la chiave di Bob
2. Alice non è in grado di capire il messaggio di Bob se in qualche modo perde P.



Questo meccanismo è chiamato cifratura a chiave pubblica ed è stato pubblicato per la prima volta nel 1970 da tre ricercatori dell'MIT.
L'algoritmo pubblicato si chiama RSA ed è usato ancora oggi.

OSSERVAZIONE: PERCHÈ NON CIFRARE OGNI COSA CON QUESTO MECCANISMO?
La ragione principale è l'efficienza, si adottano quindi dei sistemi ibridi tra public-key encryption e Diffie-Hellman.

FIRMA

Alice manda un messaggio a Bob.
Come fa Bob ad essere sicuro che il messaggio arriva da Alice?

1. Alice cifra il messaggio con la sua chiave private.
2. Bob riceve il messaggio e usa la chiave pubblica di Alice per decifrare.
3. Se il messaggio viene decifrato Bob è matematicamente sicuro che il messaggio sia stato inviato da Alice.

L'algoritmo più utilizzato è il DSA.