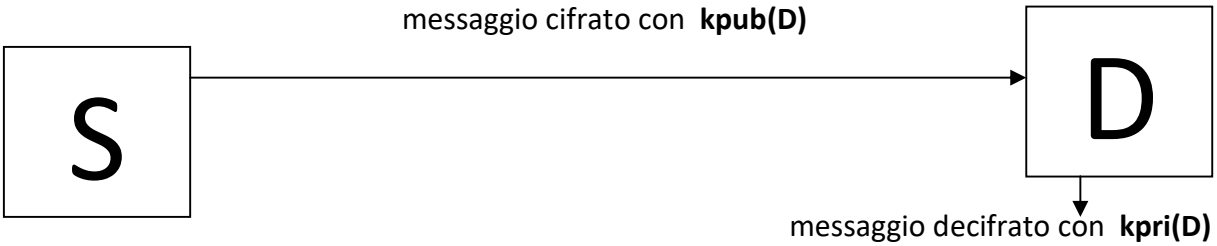
Crittografia asimmetrica

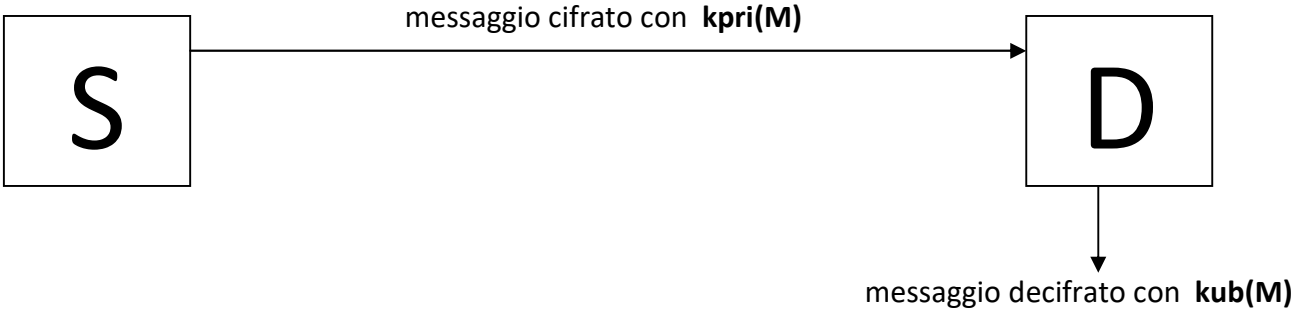
Nella crittografia asimmetrica, ogni utente ha due chiavi, entrambe possono essere usate sia per cifrare sia per decifrare il messaggio:

1) **Chiave pubblica(nelle figure seguenti sarà identificata da "kpub");**
2) **Chiave privata(nelle figure seguenti sarà identificata da "kpri").**
3) Se si utilizza kpub per cifrare si deve obbligatoriamente usare kpri per decifrare.

Invio di un messaggio cifrato avendo come obiettivo la segretezza e l'autenticazione del destinatario:
Il Mittente(**S**) per inviare un messaggio al Destinatario(**D**), preleva la chiave pubblica (**kpub**) del Destinatario che è conservata in un server accessibile a tutti, e, mediante la stessa chiave cripta il messaggio.
La segretezza è data dal fatto che solo D con la sua chiave privata può decifrare il messaggio; l'autenticazione del Destinatario è data dal fatto che solo D possiede la propria chiave privata.



Invio di un messaggio cifrato avendo come obiettivo l'autenticazione del Mittente tralasciando la segretezza(si suppone che il messaggio non sia riservato):
Il Mittente manda un messaggio cifrato con la propria chiave privata, così che il Destinatario, ma anche chiunque altro, possa decifrare il messaggio con la chiave pubblica del Mittente.
L'autenticazione del Mittente è data dal fatto che solo S possiede la propria chiave privata e quindi solo lui può aver cifrato il messaggio in questione.



Invio di un messaggio cifrato avendo come obiettivo l'autenticazione del Mittente, l'autenticazione del Destinatario e la segretezza del messaggio:

Il Mittente manda un messaggio (M) cifrato prima con la chiave pubblica di D (M1) , poi con la propria chiave privata (M2), così che il Destinatario, per decifrare il messaggio debba prima decifrare con la chiave pubblica di S (M1), e poi con la propria chiave privata (M) .