

CHIAVI

Il mittente che invia il messaggio cercherà su un elenco la chiave pubblica del destinatario e la utilizzerà per cifrarne il contenuto. Una volta che questo sarà cifrato, il mittente non avrà più modo di decifrarlo: solo il destinatario che fornisce la chiave pubblica, ma che soprattutto possiede la chiave privata, potrà decriptare il messaggio.

Schema delle Chiavi e della Comunicazione

Chiavi

- **Alice ha:**
 - **Chiave Privata di Alice (Kp_A):** segreta, usata per firmare i messaggi e per decifrarli.
 - **Chiave Pubblica di Alice (Kpub_A):** può essere condivisa con chiunque e per decifrarli.
 - **Chiave Pubblica di Bob (Kpub_B) che Alice possiede serve per decifrare il messaggio di Bob**
-
- **Bob ha:**
 - **Chiave Privata di Bob (Kp_B):** segreta, usata per firmare i messaggi.
 - **Chiave Pubblica di Bob (Kpub_B):** può essere condivisa con chiunque.
 - **Chiave Pubblica di Alice (Kpub_A) che Bob possiede serve per decifrare il messaggio di Bob**