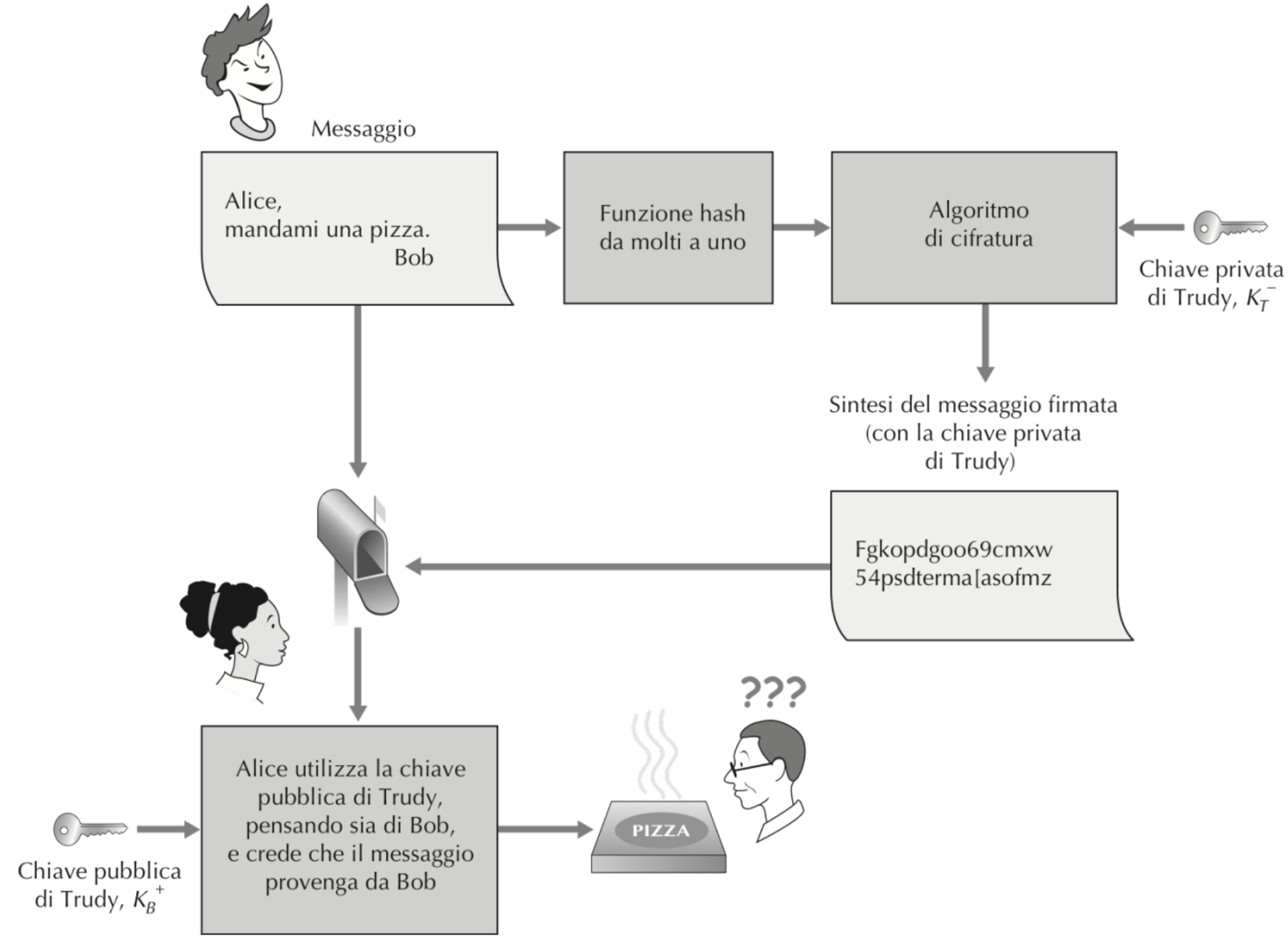
Messaggio
Alice,
mandami una pizza.
Bob
Funzione hash
da molti a uno
Algoritmo
di cifratura
Chiave privata
di Trudy, K_T^-
Sintesi del messaggio firmata
(con la chiave privata
di Trudy)
Fgkopdgoo69cmxw
54psdterma[asofmz
???
PIZZA
Alice utilizza la chiave
pubblica di Trudy,
pensando sia di Bob,
e crede che il messaggio
provenga da Bob
Chiave pubblica
di Trudy, K_B^+