



Messaggio
completo

Cara Alice,
questa è una lettera
MOLTO lunga ma
ci sono così tante cose
da dire.....
.....
.....

Bob

Funzione hash
da molti a uno

Hash
con lunghezza prefissata

Opgmdvboijrtnsd
gghPPdogm;lcvk

Pacchetto da inviare
ad Alice



Hash
firmata

Fgkopdgo069cmxw
54psdterma[asofmz

Algoritmo
di cifratura

Chiave privata
di Bob, K_B^-

Message Authentication
Code (MAC)