



Hash
firmata

Fgkopdgo069cmxw
54psdterma[asofmz

Algoritmo
di cifratura

Chiave pubblica
di Bob, K_B^+

Messaggio completo

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

Bob

Sintesi del messaggio
con lunghezza prefissata

Opgmdvboijrtnsd
gghPPdogm;lcvkb

Funzione hash
da molti a uno

Hash a lunghezza fissa

Opgmdvboijrtnsd
gghPPdogm;lcvkb

Confronto