Sender

Receiver

C

C

Attacker

C'

valid / invalid

C''

valid / invalid

...

m=dec(C)