

Schéma digitálního podpisu

příjemce

sk
pk
zveřejnil syž pk

msg

msg

hash
fun

pk \Rightarrow

dec
asym

hash
fun

sk

enc
asym

?

?

odesílatel

zde můžeme vložit
schéma utajení

