

Ensuring confidentiality with encryption









Er("request"debit=50")



Er("respose]950")

E, D, K

tkS3bffBpdJvr96+mpLlAp0=





tkS3b/LLuNVX1oLpw==

$$D_k('tks3bfffBp.\dots')$$



$D_k("tks3b"/IIu.u.u.")$

Ensuring confidentiality with encryption



$E_k("[request]debit=50")$

tkS3bffBpdJvr96+mpLIAp0=

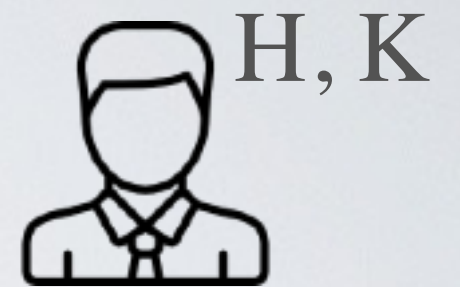
$D_k("tkS3bffBp...")$

$E_k("[response]950")$

tkS3b/LLuNVX1oLpww==

$D_k("tkS3b/LLu...")$

Ensuring integrity with an HMAC



$H_k(["request"]debit=50)$

