



Ensuring integrity with an HMAA









$H_k('request'_{debit=50}')$





H<sub>k</sub>("[response]950")

$H_k("responsee1950")$

H

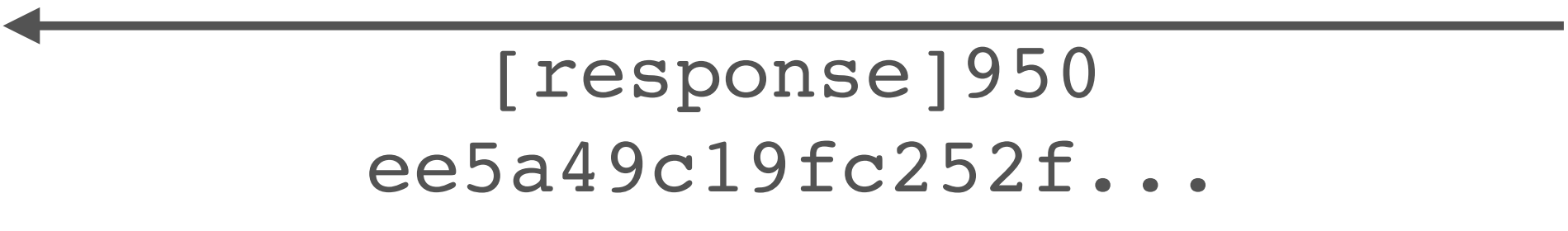
,

K

[request]debit=50

f89a73aa27f3ea6...





[response]950

ee5a49c19fc252f...

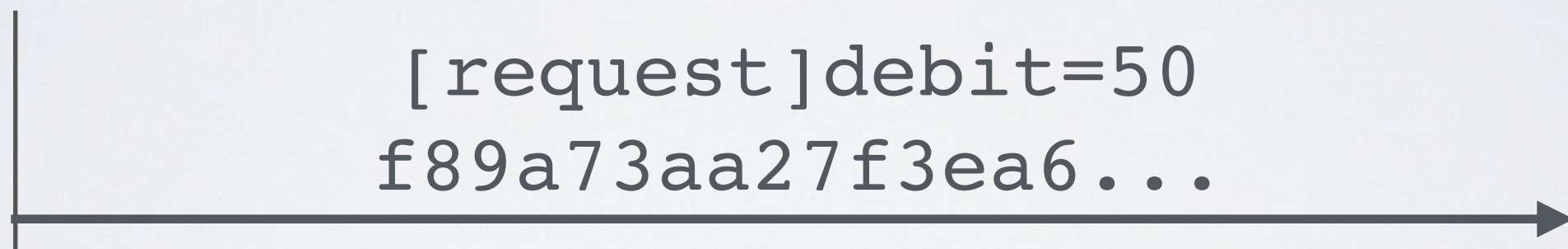
$H_k('request'_{deb}init=50')$



# Ensuring integrity with an HMAC



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



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




$H_k(["response"]950")$



$H_k(["response"]950")$



# Security mechanisms

	Encryption	MAC	Authenticated Encryption
Confidentiality			
Integrity	