

Ensuring confidentiality and integrity
with Authenticated Encryption







E, D, H, K

E, D, H, K





AEk("request"debit=50")

AE_k("[respose]950")

30354WxPYF...





15qcK3Xcdwd . . .

AD_k('30354WXPYF...')



AD_K("15qck3Xcdwd...")

Ensuring confidentiality and integrity with Authenticated Encryption



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

30354WxPYF...

$AD_k("30354WxPYF...")$

$AE_k(["response"]950)$

15qcK3Xcdwd ...

$AD_k("15qcK3Xcdwd...")$

Replay attacks