Ensuring confidentiality and integrity with Authenticated Encryption

E, D, H, K

E, D, H, K

$AE_k(\texttt{"[request]debit=50"})$

$$AE_k(\texttt{"[response]950"})$$

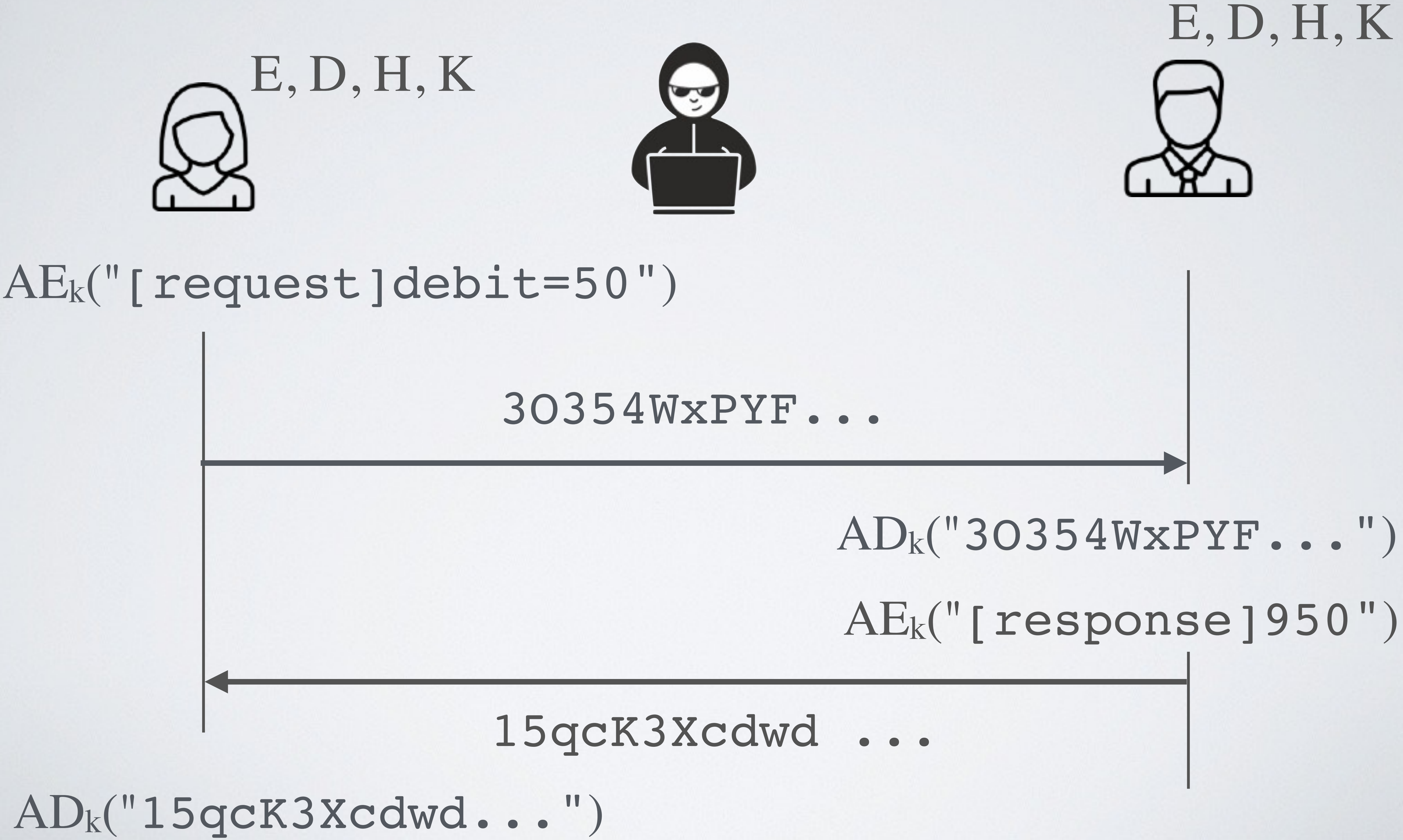
3O354WxPYF...

15qcK3Xcdwd ...

$$\mathrm{AD}_k(\texttt{"3O354WxPYF..."})$$

AD_{K}("15qcK3Xcdwd...")

Ensuring confidentiality and integrity with Authenticated Encryption



E, D, H, K

E, D, H, K

AE$_k$("[request]debit=50")

30354WxPYF...

AD$_k$("30354WxPYF...")

AE$_k$("[response]950")

15qcK3Xcdwd ...

AD$_k$("15qcK3Xcdwd...")

Replay attacks