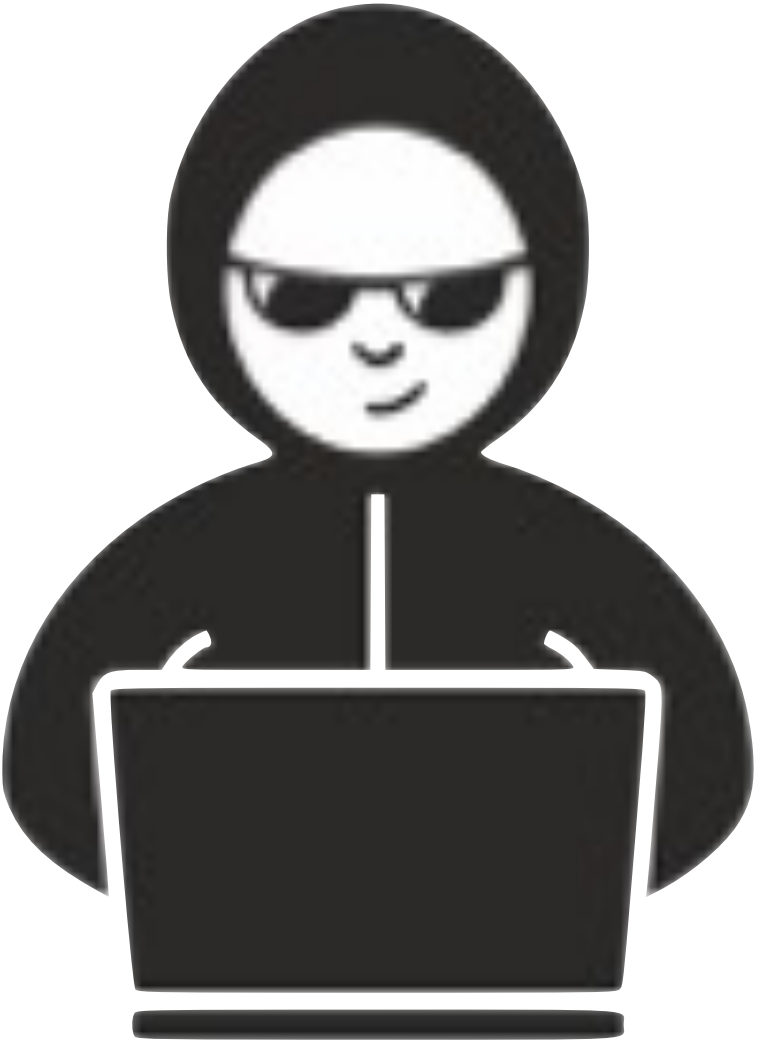
Ensuring confidentiality and integrity with Authenticated Encryption

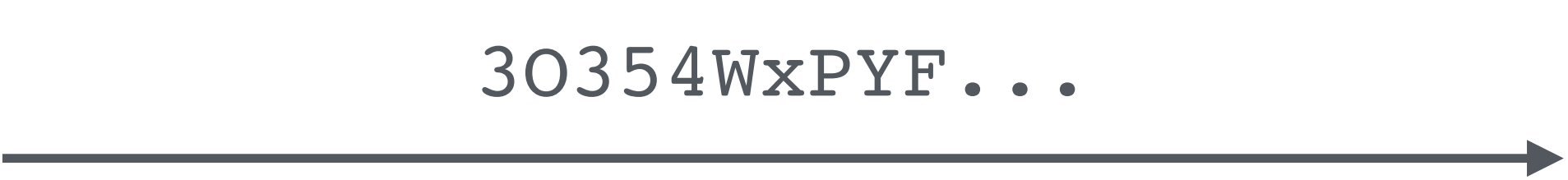


E, D, H, K


E, D, H, K

AE_k("[request]debit=50")

AE_k("[response]950")


3O354WxPYF...

15qcK3Xcdwd ...

AD_k("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...")

Overview

- Replay attacks in interactive protocols
- A symmetric protocol for key exchange (Needham–Schroeder Key Exchange Protocol)
- A symmetric protocol for key exchange (Diffie-Hellman-Merkle Protocol)
- The challenge of authentication (Needham–Schroeder Authentication Protocol)
- Putting it all together (TLS)
- Trust models (PKI)