Latest trends

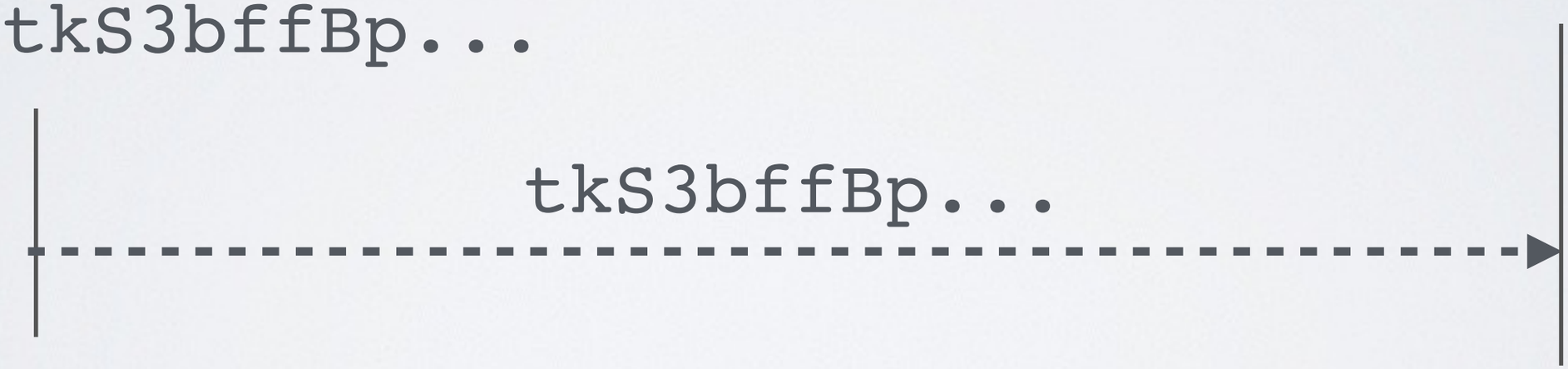
AES is now hardware accelerated (AES-NI native instruction)

➡ AES is fast enough (~1.3 cycles per byte)
to be used as the go-to cipher for any application

https://security.stackexchange.com/questions/22905/how-long-would-it-take-a-single-processor-with-the-aes-ni-instruction-set-to-bru

An issue ...

$E_k(m)$ = `tkS3bffBp...`



- How does Alice and Bob agree on a symmetric key?