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

Preventing Key Reused Attacks

At best, use a fresh symmetric key every time

- Key exchange problem

At least, change the seed to never it use it twice

✓ All modern stream cipher (Salsa/Chacha) and good encryption mode for block cipher (CBC, CTR) take a nonce

➡ Generate this nonce randomly and sent it in clear with cyphertext