CS 338

Fri. 22 Sep 2023

$p = 53$

$g = 3$

A & B want to share a secret

$X = 47$ A $\xrightarrow{g, p, g^X \bmod p}$ B $Y = 28$

$3, 53, 12$

B $\xrightarrow{\text{☺}, g^Y \bmod p}$ A

$a^Y \bmod p$

$b^X \bmod p$

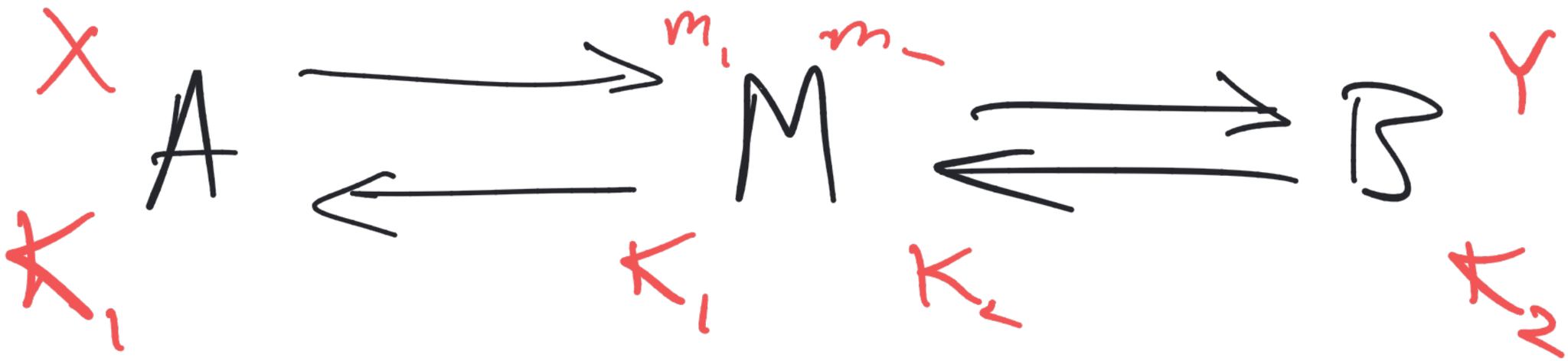
$= (g^Y \bmod p)^X \bmod p$

$= \ldots = g^{YX} \bmod p$ ✶

$= \ldots$

✶ $= g^{XY} \bmod p$

Adversary in the middle



How to stop this

CA = { certificate authority

- Let's Encrypt
- Verisign
- Google
- GoDaddy