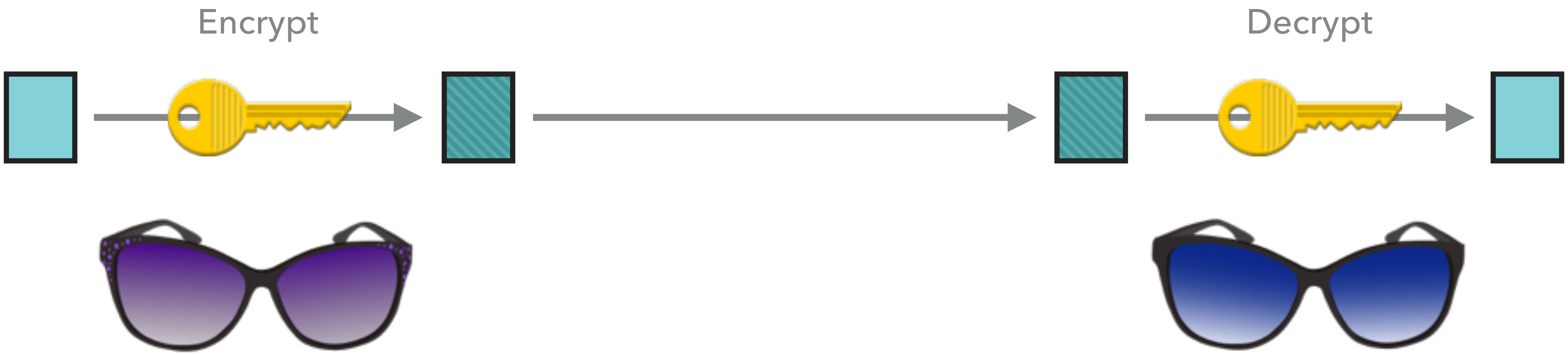
SERVLET AND JSP: A TUTORIAL 2ED

BY BUDI KURNIAWAN

SSL AND TLS

ORIGINALLY DEVELOPED BY NETSCAPE, THE SSL PROTOCOL (AND NOW TLS) ENABLES SECURE COMMUNICATIONS OVER THE INTERNET AND AT THE SAME TIME ENSURES CONFIDENTIALITY AND DATA INTEGRITY.

SYMMETRIC KEY CRYPTOGRAPHY

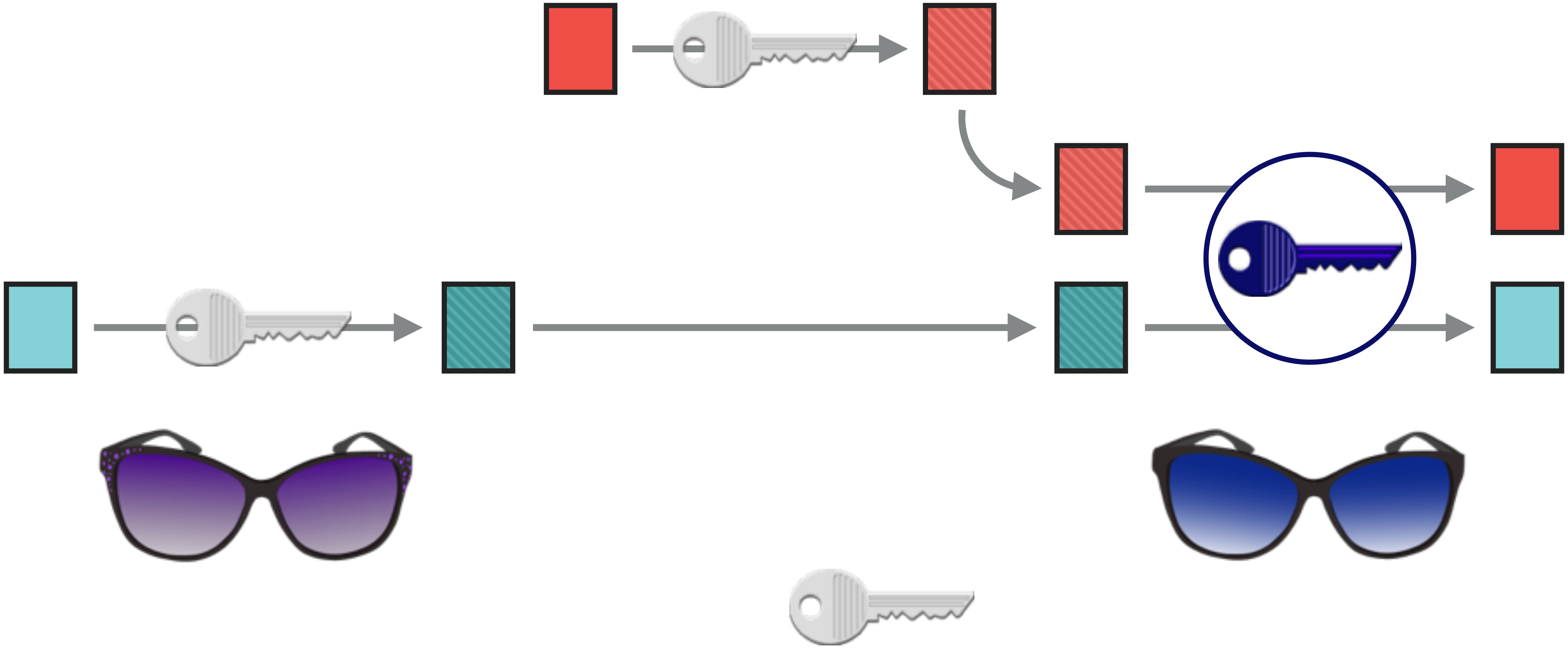


PROBLEMS WITH SECRET KEYS

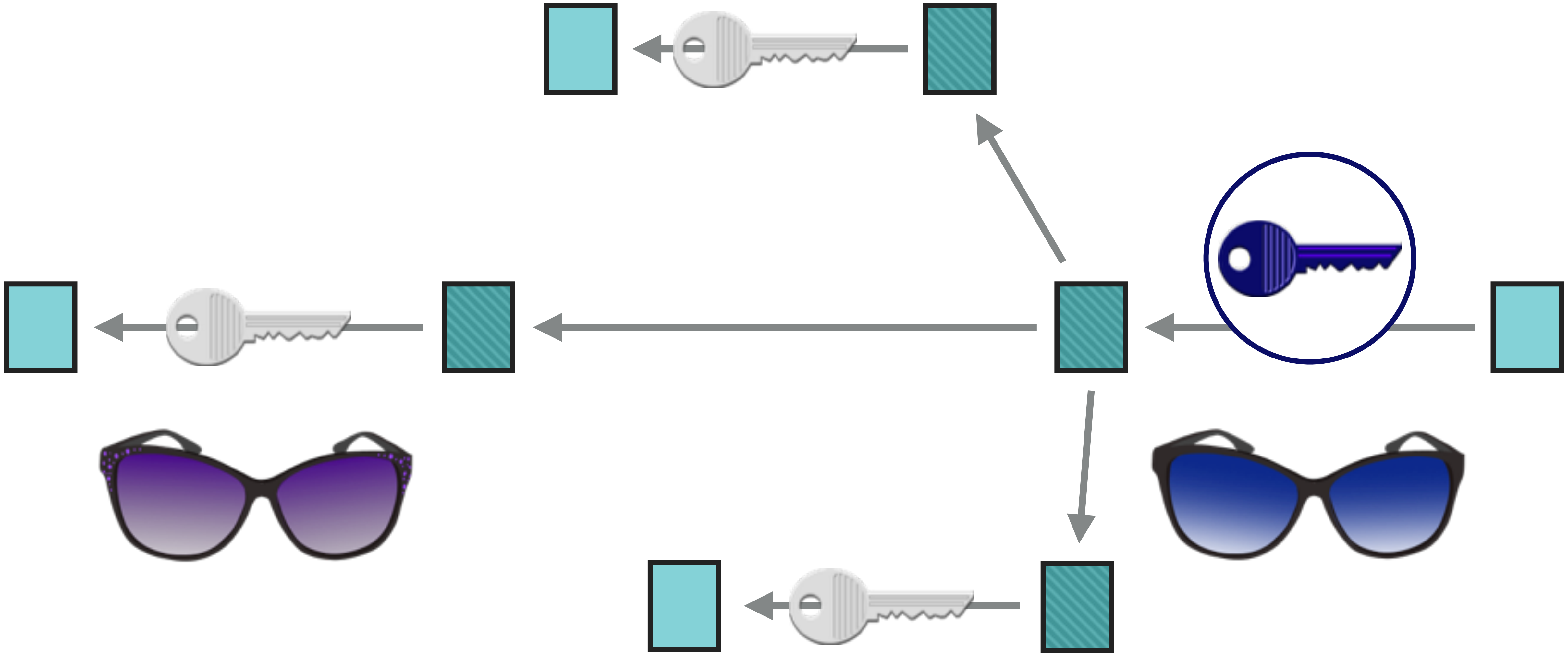
- The biggest problem with secret key cryptography for internet traffic is that both parties have to have the secret key **before** they can begin communicating
- Everyone want to be able to communicate with everyone else, so each pair would have to have their own unique key
- Since you do not know who you are going to communicate with, you must be sure that they are who they claim to be.

PUBLIC KEY CRYPTOGRAPHY

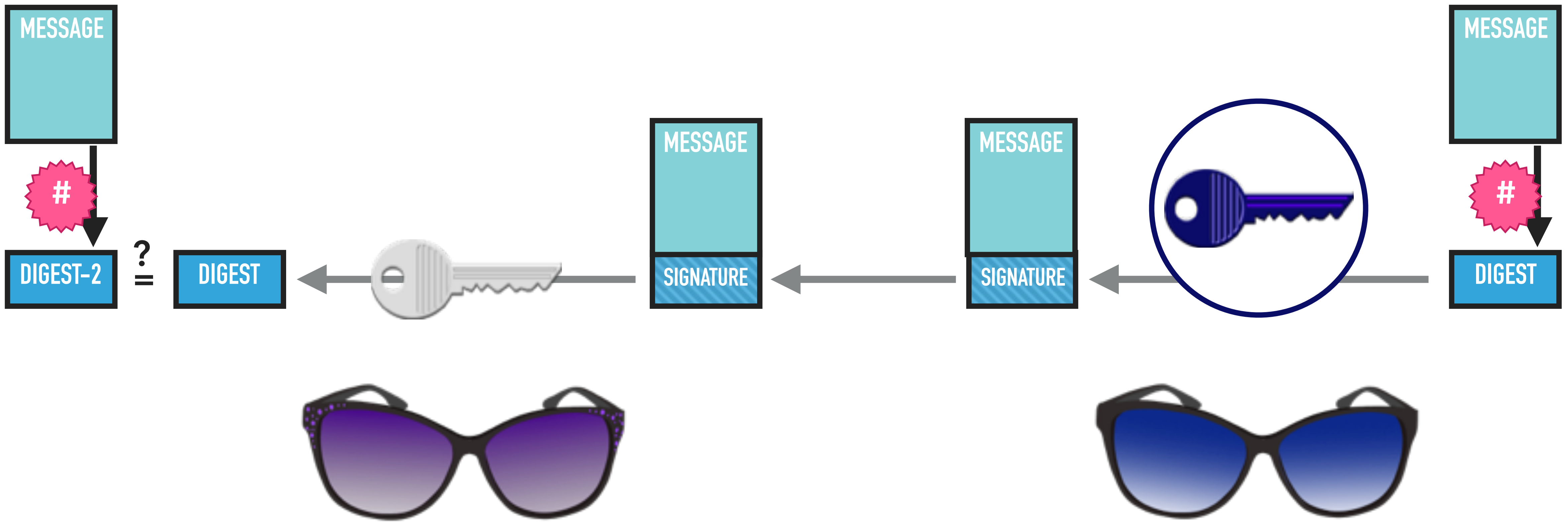
PUBLIC KEY CRYPTOGRAPHY



PUBLIC KEY CRYPTOGRAPHY

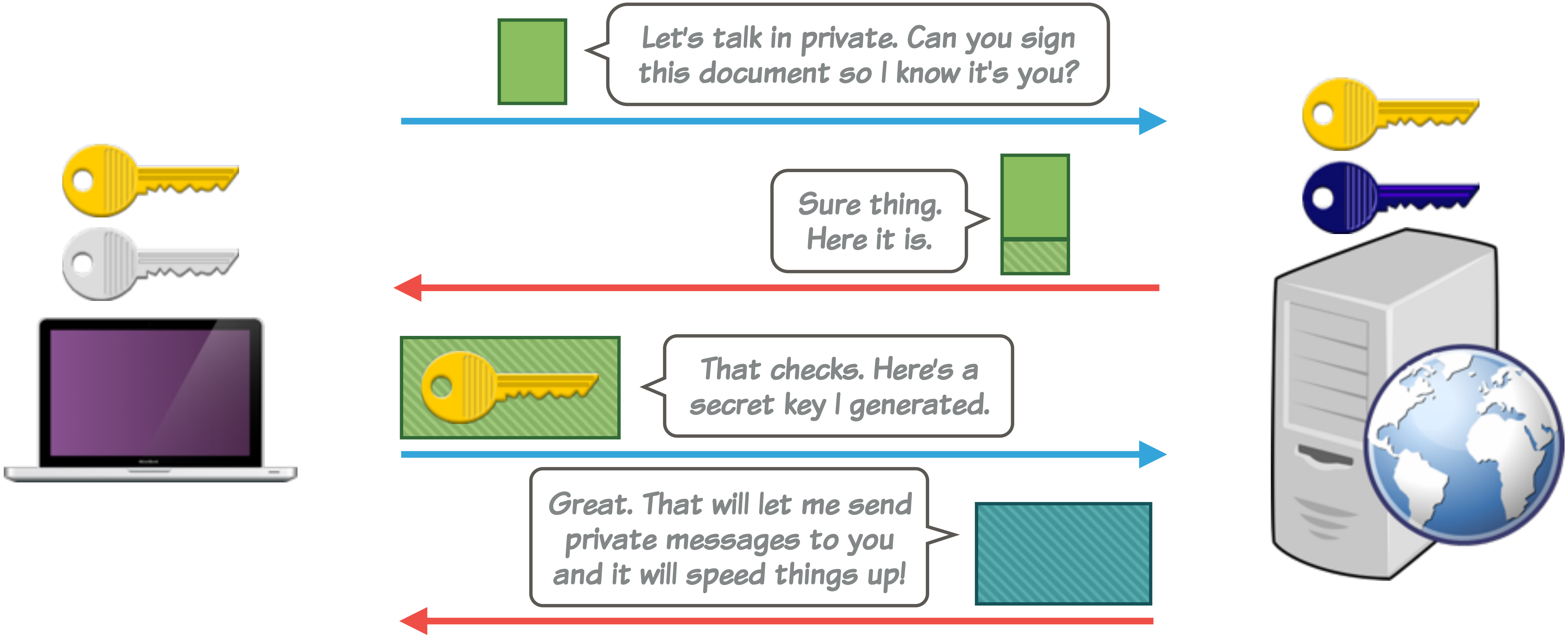


AUTHENTICATION OF DIGITAL SIGNATURES



SIMPLE PROTOCOL FOR PRIVATE CONVERSATION

NOTE: Assumes public key of server has been verified


Let's talk in private. Can you sign this document so I know it's you?
Sure thing. Here it is.
That checks. Here's a secret key I generated.
Great. That will let me send private messages to you and it will speed things up!

CERTIFICATES FOR AUTHENTICATION

- In TLS and SSL, authentication is addressed by using certificates, which contains the following
  - the subject’s **public key**
  - information about the subject (owner of the public key)
  - the certificate issuer’s name
  - a timestamp so the certificate will expire

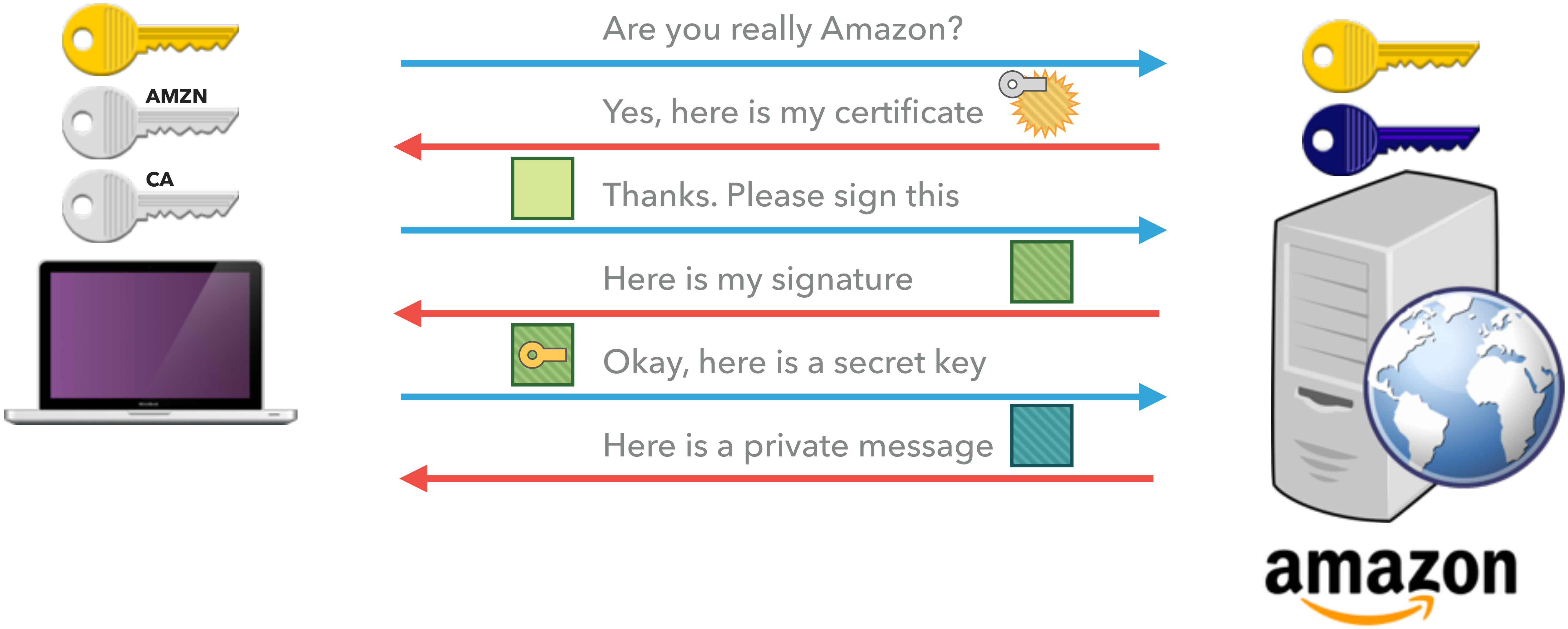
CERTIFICATES FOR AUTHENTICATION

- A certificate must be digitally signed by a trusted **certificate issuer**, like VeriSign or Thawte
- The public key of a certificate issuer is normally distributed widely. For example, Internet Explorer, Netscape, FireFox and other browsers by default include several certificate issuers’ public keys
- Because certificates can be digitally signed by a trusted certificate issuer, people make their certificates publicly available, instead of their public keys

DATA INTEGRITY

- Even if data is encrypted, a malicious entity could still intercept the data and modify it or deliver only a portion
- To make sure that the receiver knows when something is wrong, SSL uses **Message Authentication Codes** (MAC)
- A MAC can be a digest of the message encrypted by the (shared) secret key, similar to how digital signatures work
- Unlike digital sigs, MACs do not provide non-repudiation: The sender can always claim the receiver forged the message

HOW SSL AND TLS WORKS



AMZN
CA
Are you really Amazon?
Yes, here is my certificate
Thanks. Please sign this
Here is my signature
Okay, here is a secret key
Here is a private message
amazon