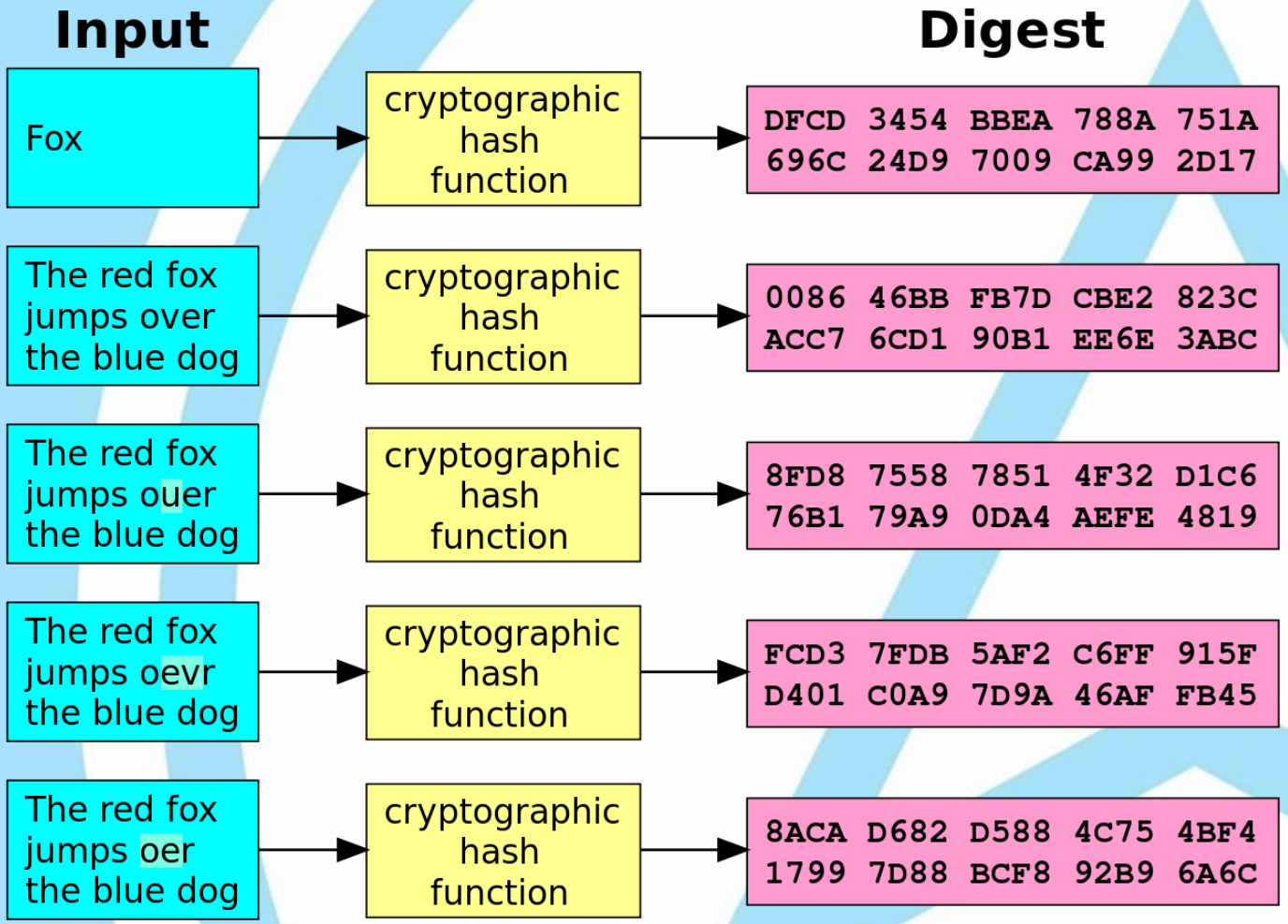
Module 2 Day 16

Encryption and Authentication

Hashing & Encryption

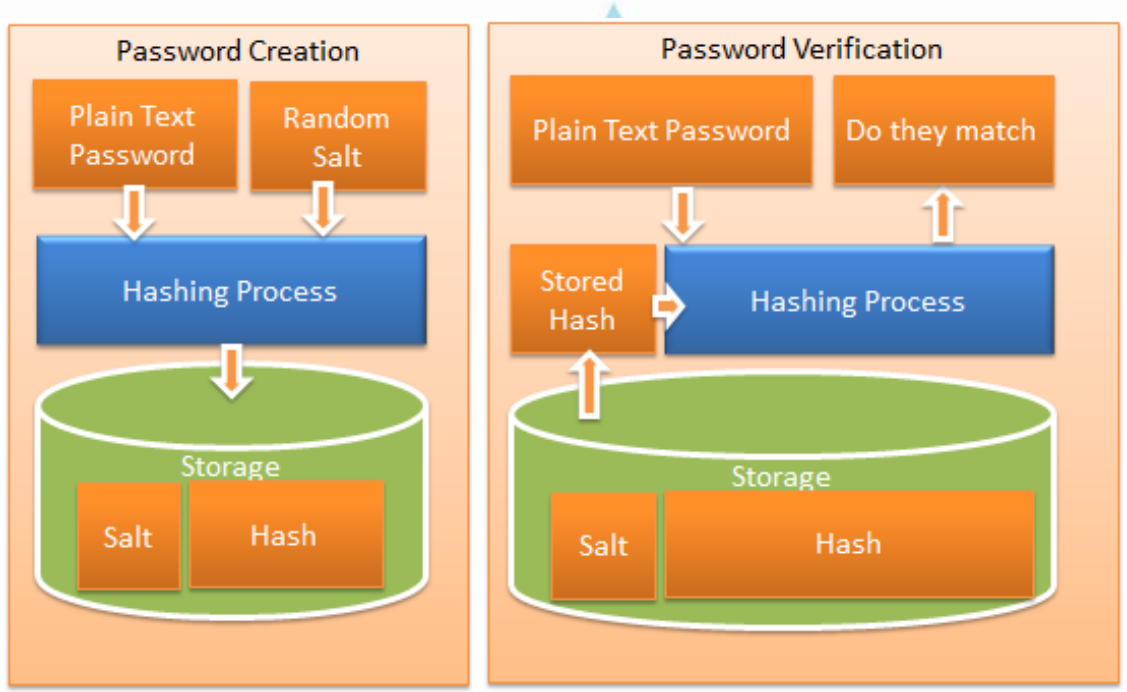
- Hashing
  - One-way, repeatable algorithm to change data into a “hash value”
    - One-way means there is no way to get to the original data, given only the hash
    - Repeatable means if I run the same original data through the algorithm again, I’ll get the same result
  - Used to verify data transmissions (aka, checksum)
  - Used for storing passwords securely
- Encryption
  - Two-way algorithm to render data unreadable for storage or transmission, and then converting back to readable using a "key"
  - Used for protecting data "at rest" or "in-transmission"

Hashing Data



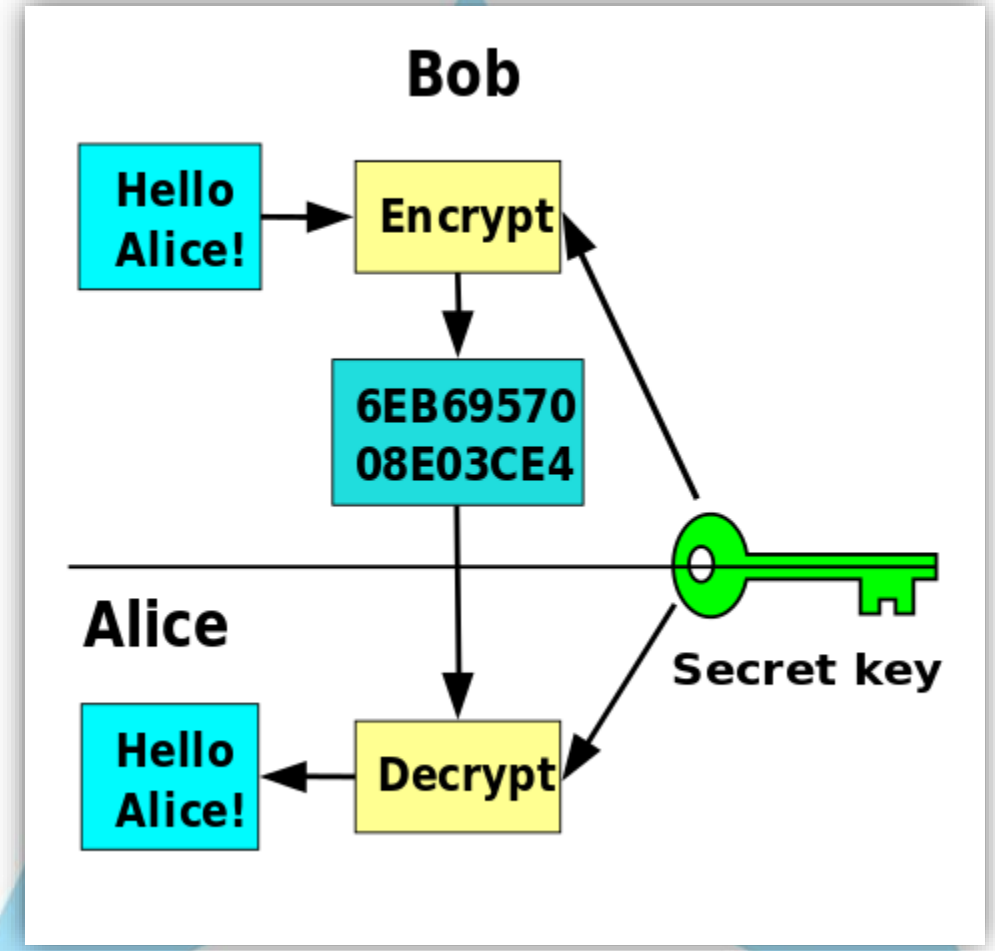
Hashing Passwords

- Password is hashed when created
  - Hash is stored in DB
- To login, password is hashed using the same algorithm
  - Hashes are compared.
- Adding a salt prevents dictionary attacks
  - Salt also stored in the DB
- Increasing work factor greatly increases security
  - Hash the hash



Encryption – Symmetric Key

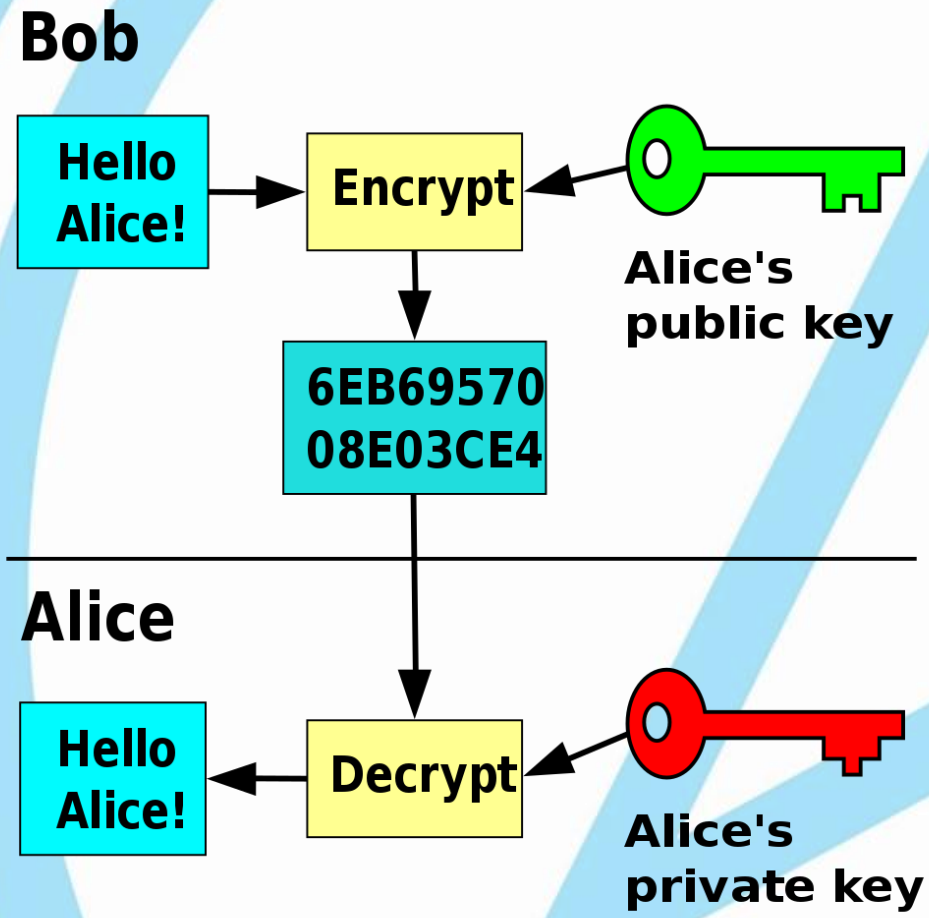
- Uses a single key to encrypt (lock) and decrypt (unlock) the data
- “Shared secret”
- Examples:
  - Password-protected files
  - Windows BitLocker
  - JWT, Single-server



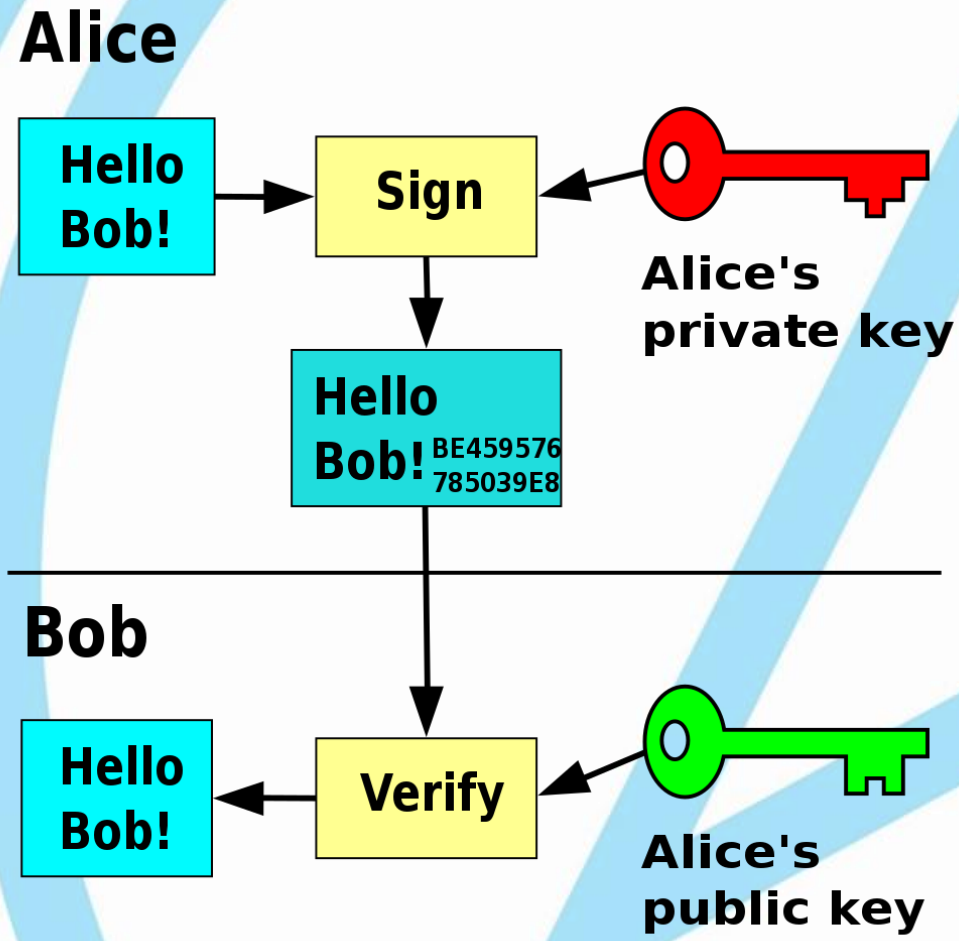
Encryption – Asymmetric Key

- Public key cryptography / Public Key Infrastructure (PKI)
- Two keys used: a “public” key and a “private” key
  - Messages encrypted using Public must be decrypted using Private
  - Message encrypted using Private must be decrypted using Public
- Can be used to
  - Securely send data to another user, or (encrypt public, decrypt private)
  - Guarantee the identity of the sender (encrypt private, decrypt public)
  - JWT, Third-party authentication server

Bob securely sends message to Alice



Alice proves this message is from her

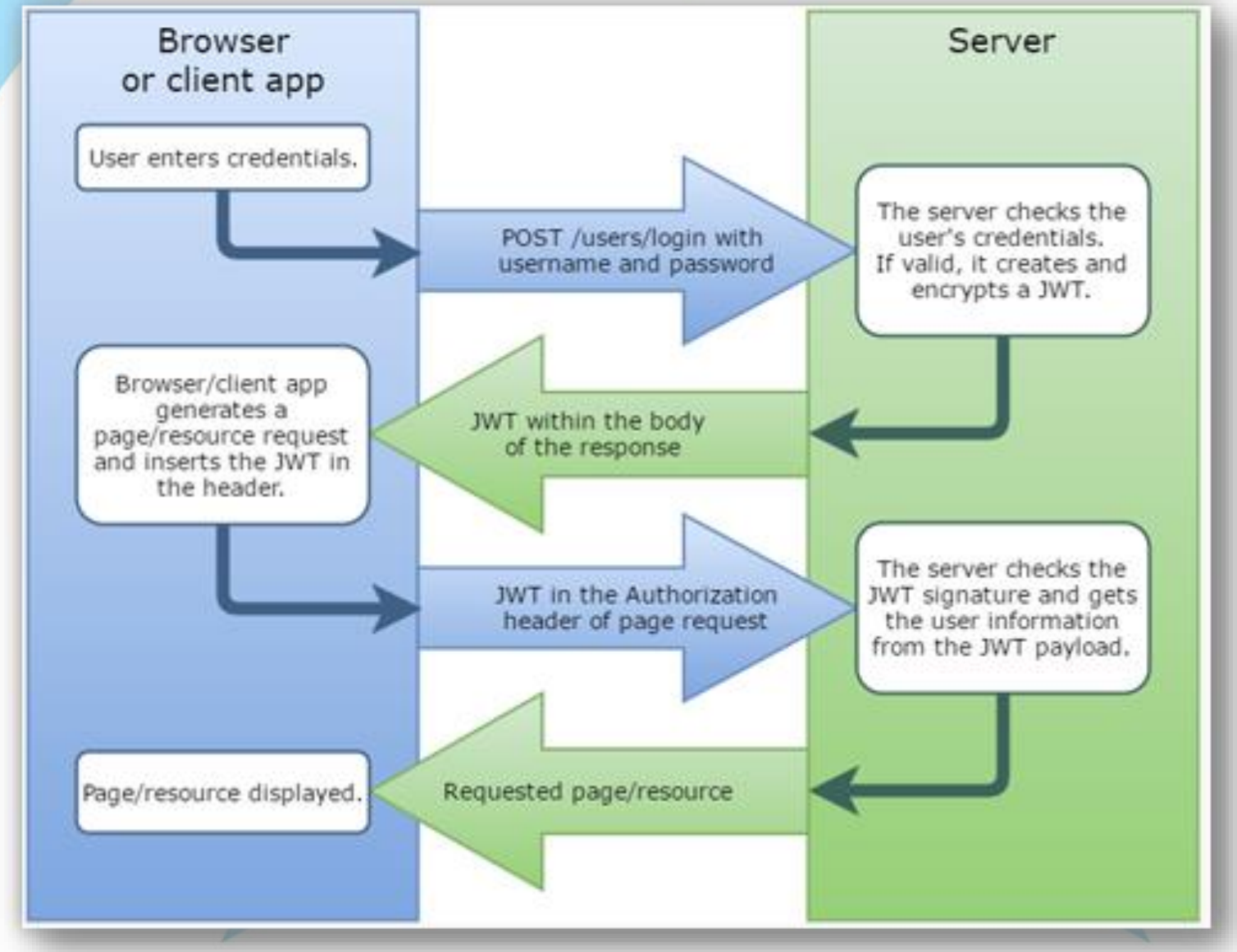


Authentication & Authorization

- Authentication
  - Who you are
  - Prove that you are who you claim to be
  - Often involves a password
  - “What you have, what you know and what you are” (MFA)
    - ATM card, cell phone, ID card
    - Password, PIN, Security Question
    - Biometric (fingerprint, retina, face)
  - My passport at airport security
- Authorization
  - What you can do
  - Can you view data, or edit it? Delete it? Add users? Etc.
  - Useless without Authentication
  - My visa at airport security

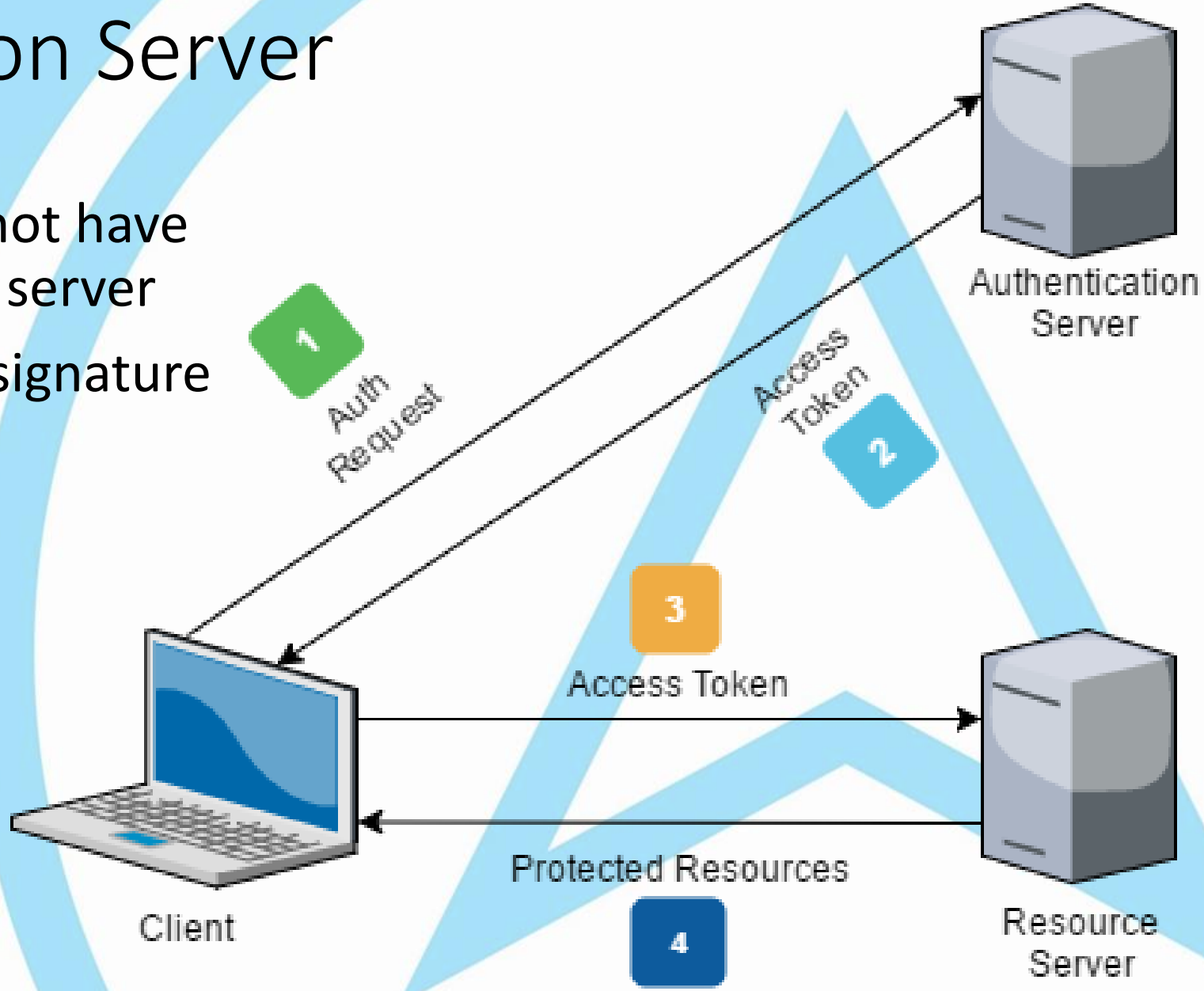
JWT Authentication

- HTTP is stateless
- User's credentials verified: JWT issued
- JWT "presented" with each subsequent Http Request
- JWT is verified on server
- Access is granted
- http://jwt.io



Authentication Server

- Auth server does not have to be same as app server
- PKI used to verify signature



Let's Code

Server Authorization in ASP.NET

- Parts of the app may be public, and parts may be protected to only authorized users
- Controllers or Actions can be protected with an [Authorize] attribute
- Some actions may require the user to be in a particular role
  - [Authorize(Roles="admin, superuser")]
- [Authorize] can be used to protect the entire controller
  - [AllowAnonymous] can override a specific method
- Some code required in Startup.cs (boilerplate)

Client Authentication in ASP.NET

- Client Logs In by POSTing to an endpoint on the server
- On successful login, client stashes JWT somewhere accessible
- For every request, client adds Authorization header ("bearer xxx")
- To "log out" client simply destroys the token