

AUTHENTICATION

- When exploring authentication with Alice and Bob, the question we want to ask is:
- if Bob wants to communicate with Alice, how can he be sure that he is communicating with Alice and not someone trying to impersonate her?

AUTHENTICATION

- Bob may be able to authenticate and verify Alice's identity based on **one or more of 3** types of methods:
 - **something** you know,
 - **something** you have, and
 - **something** you are.

Something You Know

Something You Know: Passwords

- The first general method Bob can use to authenticate Alice is to ask her for some **secret only she should know**, such as her secret password.
- If Alice produces the right password, then Bob can assume he is communicating with Alice.
- Passwords are so prevalently used that we will further study how to properly build a password management system.

Something You Know: Passwords

- There are advantages and disadvantages to using passwords.
- One advantage is that password schemes are simple to implement compared to other authentication mechanisms, such as **biometrics**, which we will discuss later.
- Another advantage of password security systems is that they are **simple for users** to understand.