Applications

This Video Covers:

- **Authentication**
- HTTPS and TLS/SSL
- Chip Technology Used in Credit Cards

Applications: ***Authentication***

- Typical way to conduct authentication is to use passwords

- **Disadvantage:**
  - A sends password to B:

    B could get hacked;

    A may use the same password for multiple accounts…
  - Cannot be used for many parties to authenticate a single party

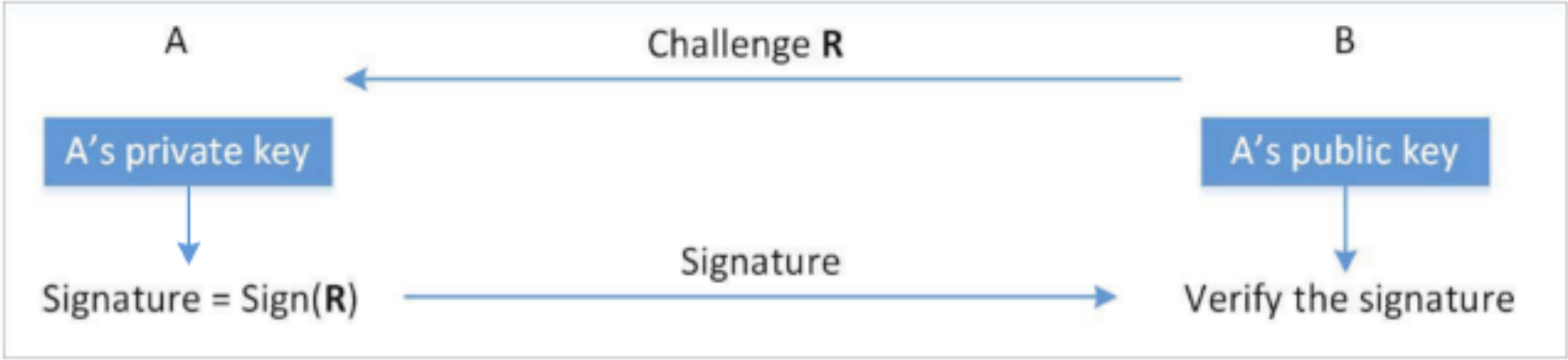
- **Fundamental problem:**

  password authentication depends on a shared secret

Applications: ***Authentication*** *(cont.)*

Solution:

- Make the encryption and decryption keys different
- Generate the authentication data using one key, and verify the data using a different key



Applications: ***Authentication*** *(cont.)*

SSH Case Study

- SSH uses public-key based authentication to authenticate users
- Generate a pair of public and private keys: `ssh-keygen -t rsa`
  - private key: `/home/seed/.ssh/id_rsa`
  - public key: `/home/seed/.ssh/id_rsa.pub`
- **Server:**
  - public key file is sent to the remote server using a secure channel
  - add public key to the authorization file `~/.ssh/authorized_keys`
  - Server can use key to authenticate clients