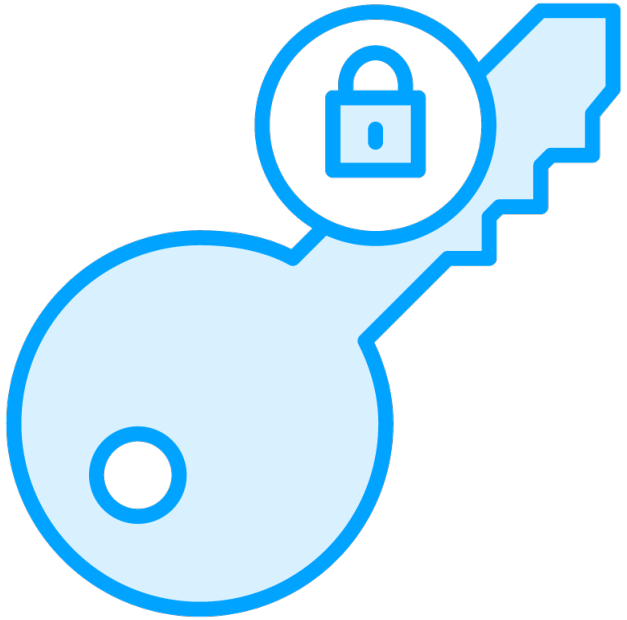
Identify Common Use Cases for Encryption



Phil Chapman
Senior Instructor and Subject Matter Expert

www.cyberphil.co.uk

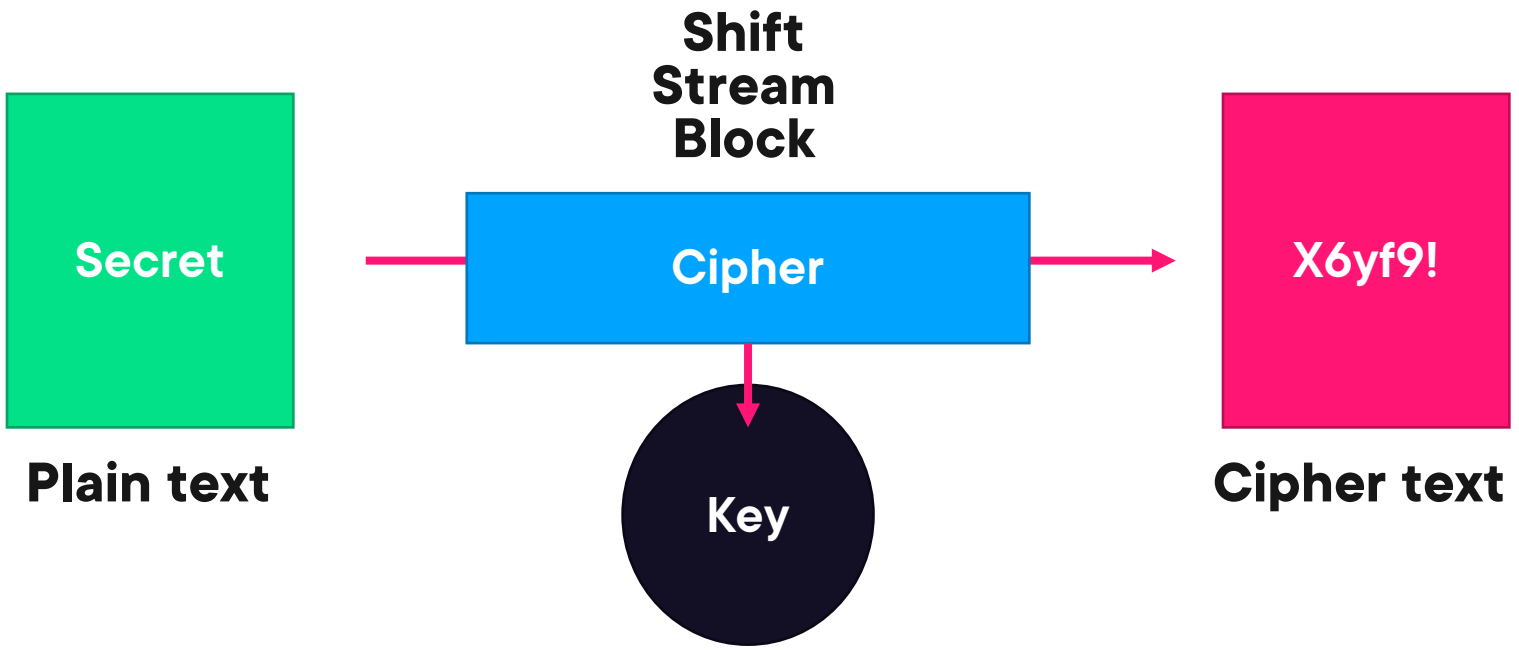
Understanding Fundamental Encryption Concepts



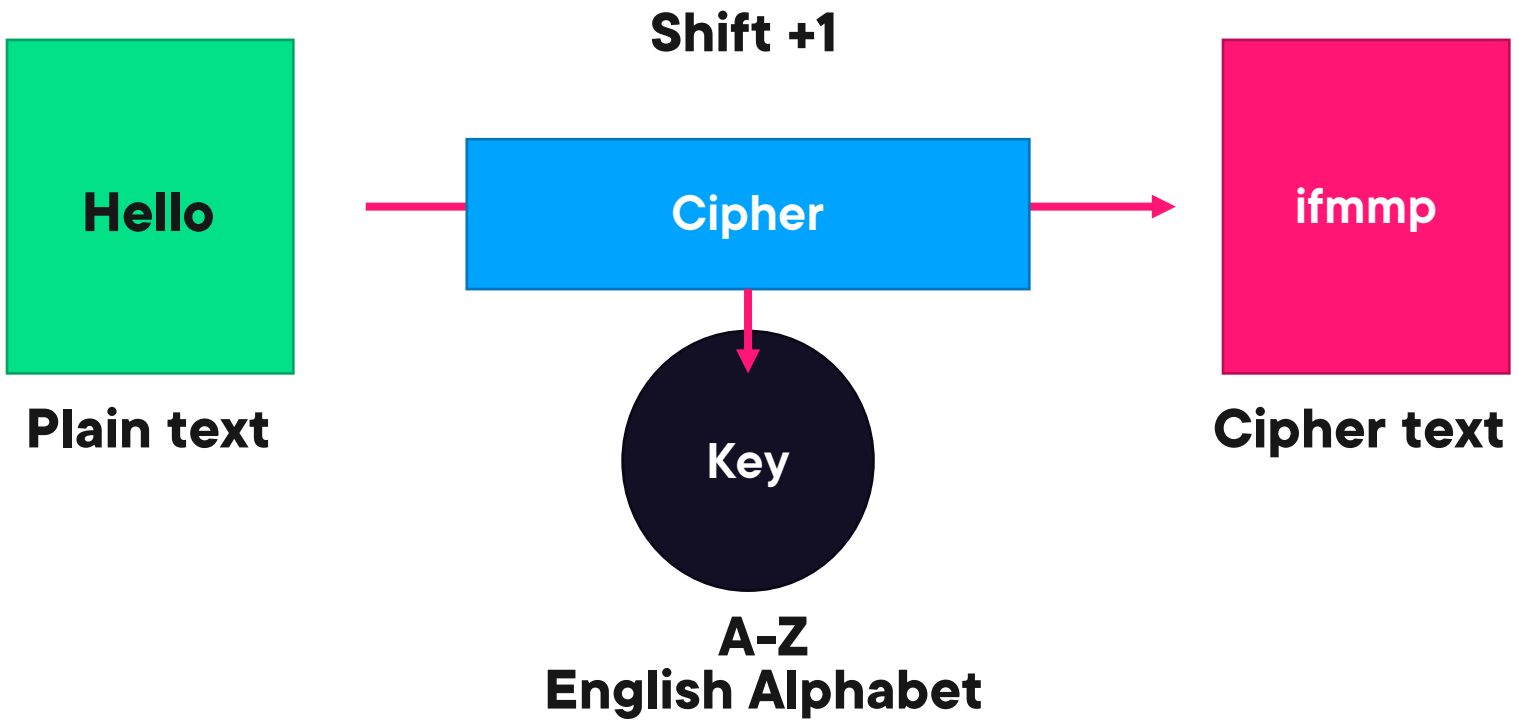
What is encryption?

- The process of protecting data by making it human unreadable
- Only the person with the key may decrypt the data
- Provides digital confidentiality

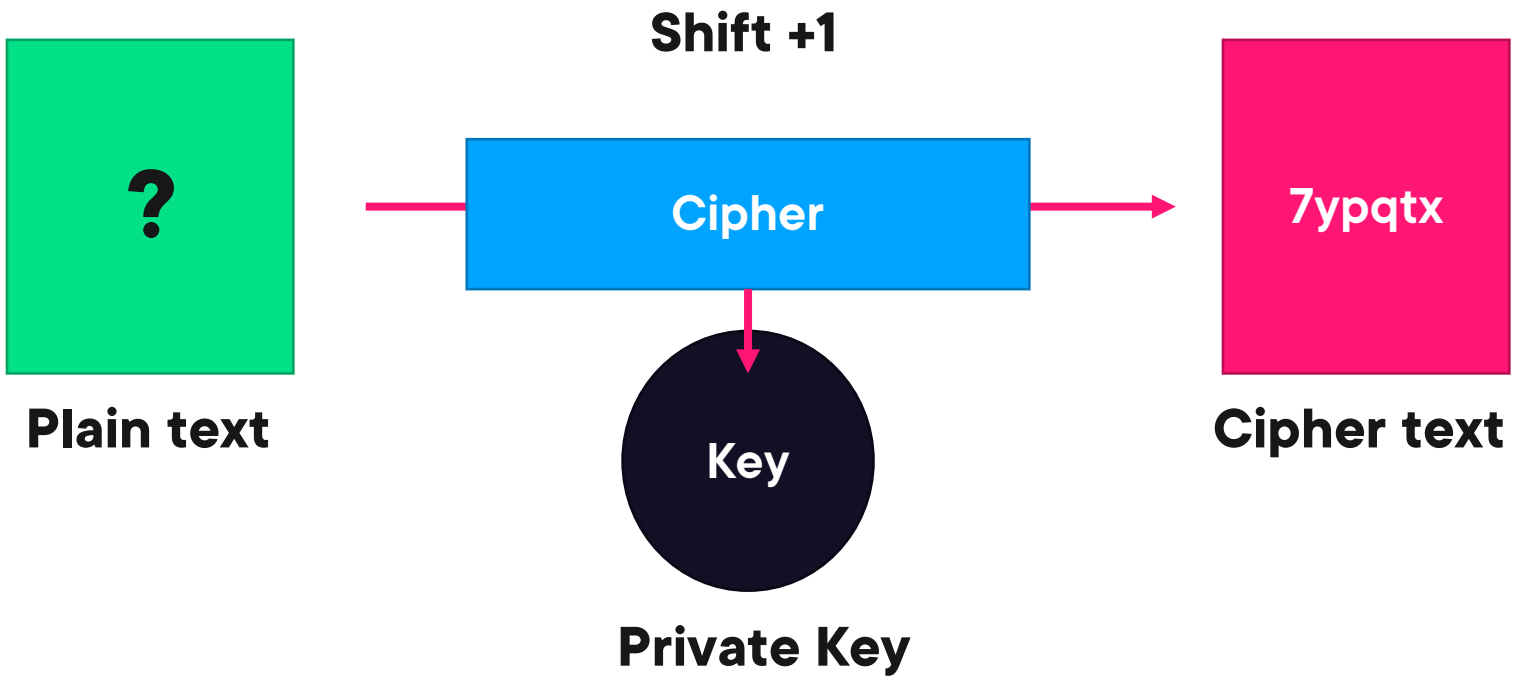
How Does Encryption Work?

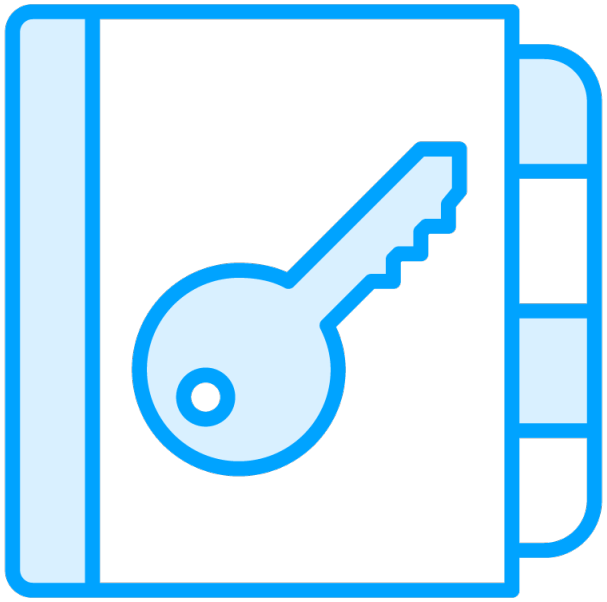


How Does Encryption Work?



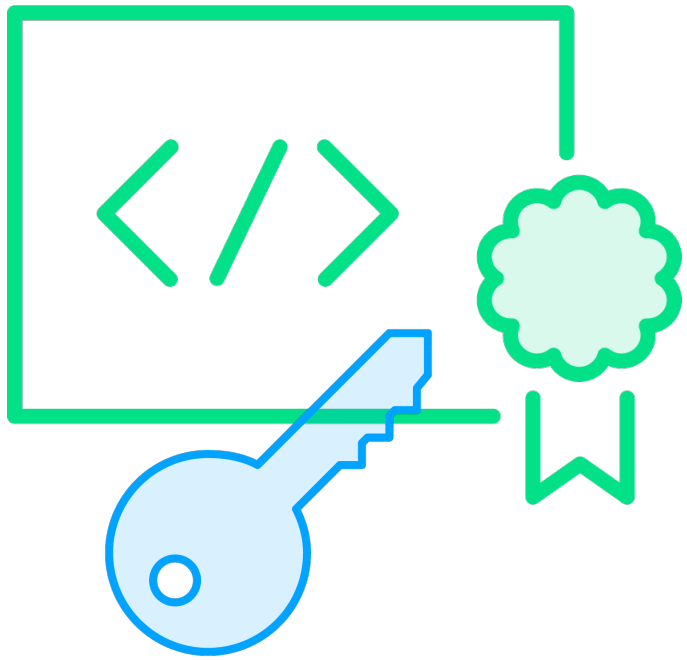
How Does Encryption Work?





Key exchange

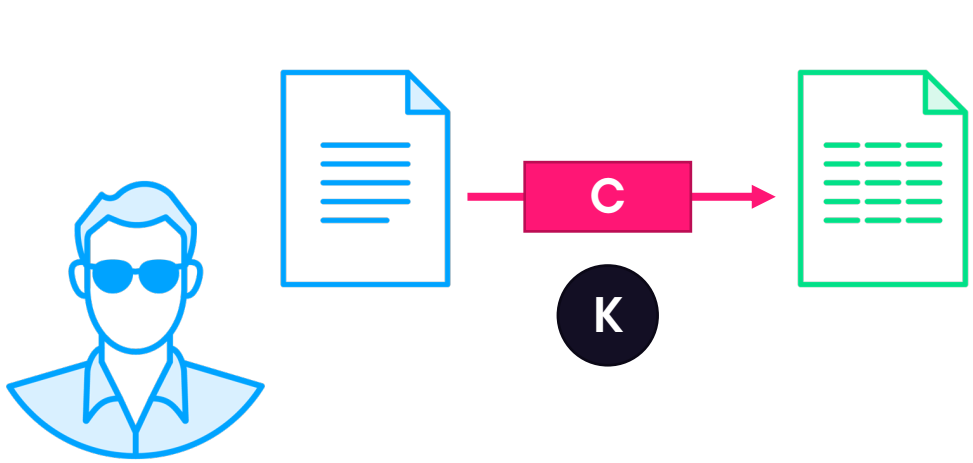
- The cipher will be known
- Keeping a private key secret is essential
- Private key exchange is a problem
  - In band
  - Out of band
- Vulnerable to interception
- Known as a symmetric cryptography

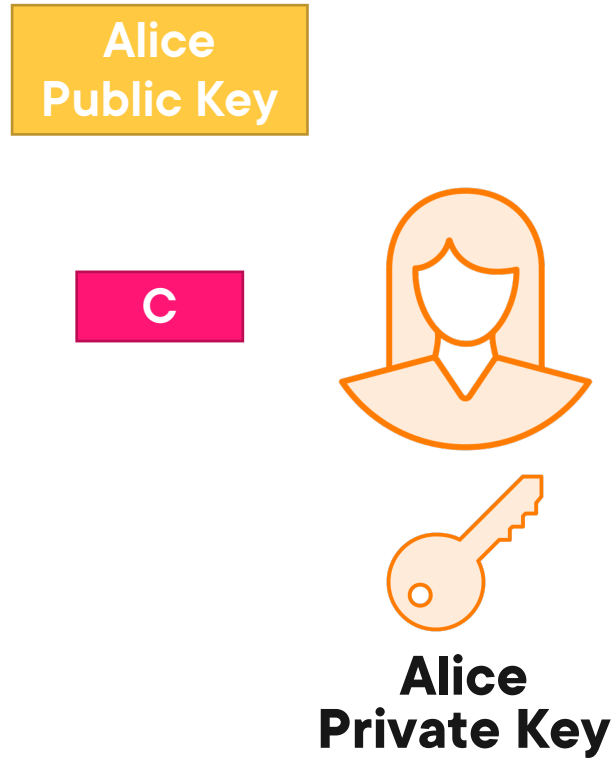


Asymmetric cryptography

- Uses 2 keys in the exchange process
  - Public key
  - Private key
- Public key infrastructure (PKI)
  - Digital certificates
- Used for confidentiality and integrity

Asymmetric Cryptography for Encryption

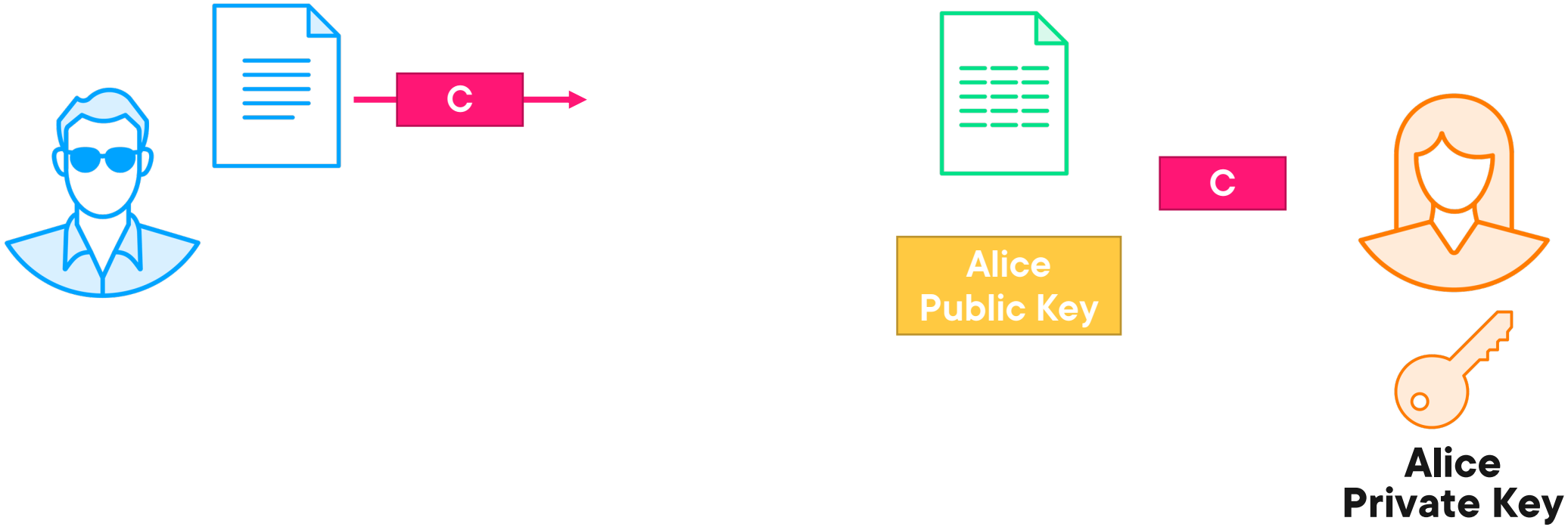




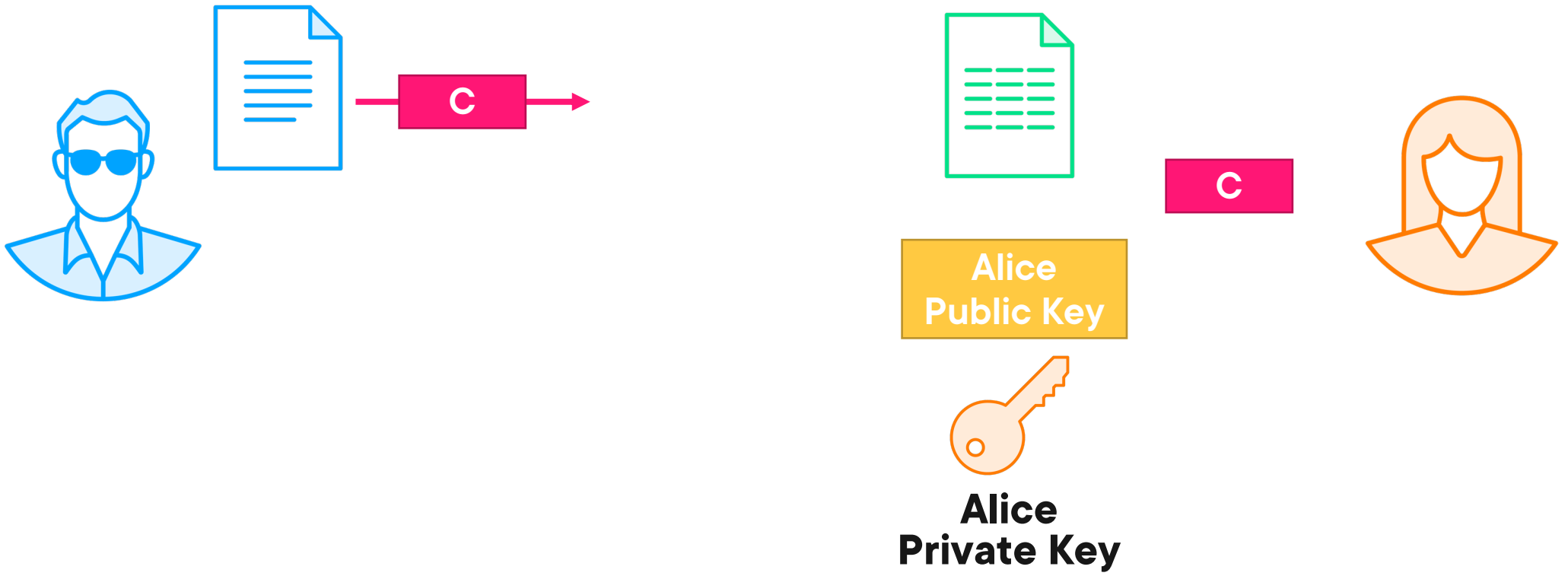
Asymmetric Cryptography for Encryption



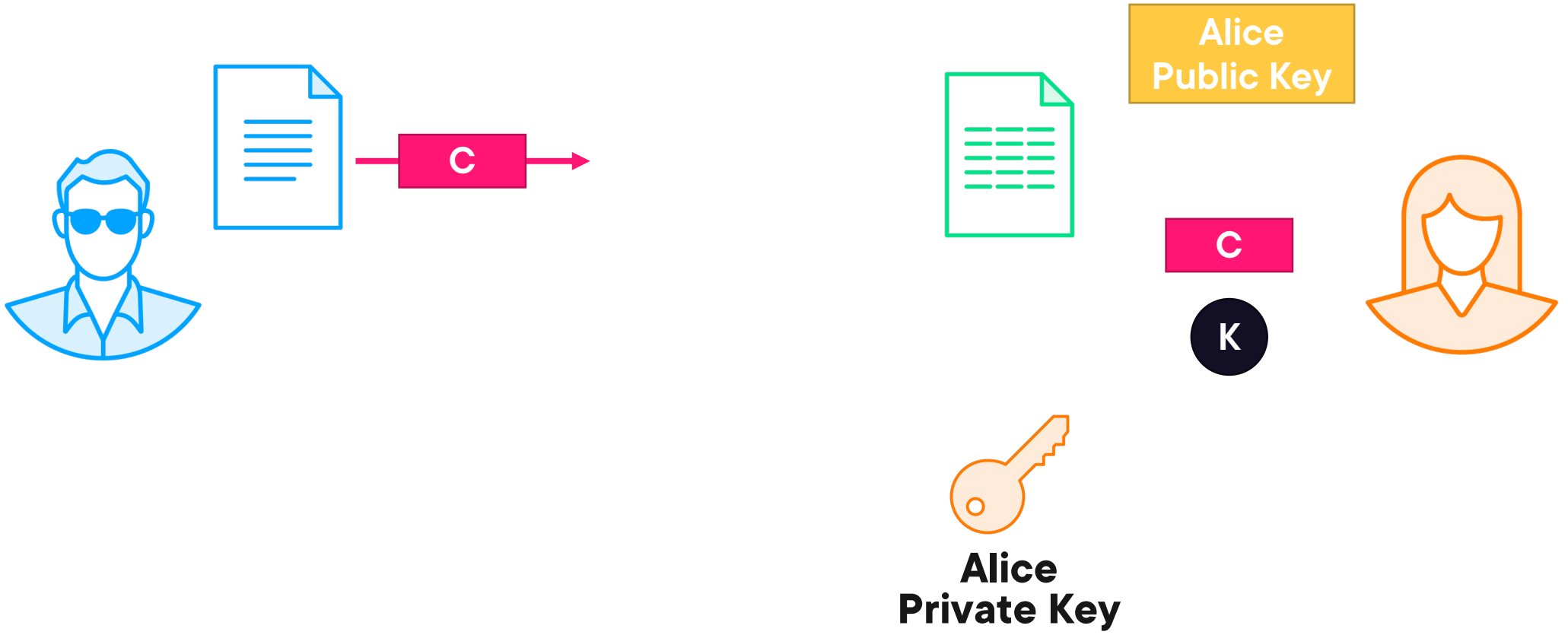
Asymmetric Cryptography for Encryption



Asymmetric Cryptography for Encryption



Asymmetric Cryptography for Encryption



Asymmetric Cryptography for Encryption





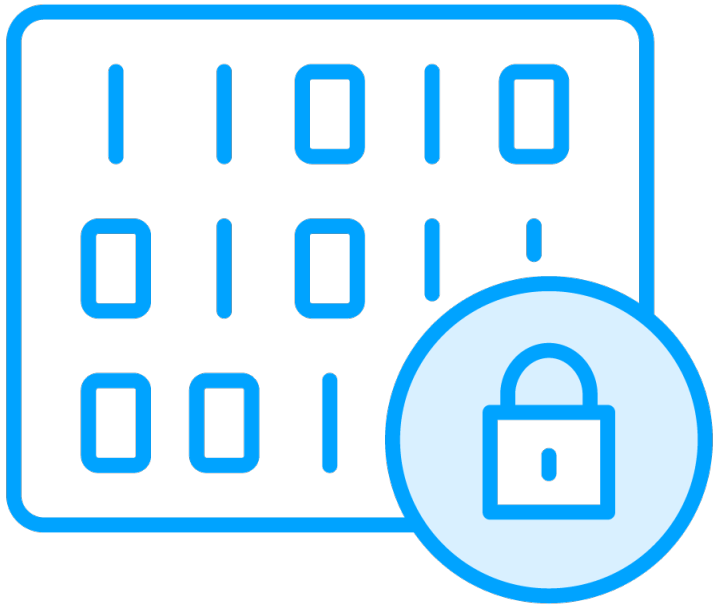
Public key cryptography is widely used to support

- Encryption (confidentiality)
- Digital signatures (integrity)
- Authentication
- Non-repudiation

Up Next:

Understanding Data States

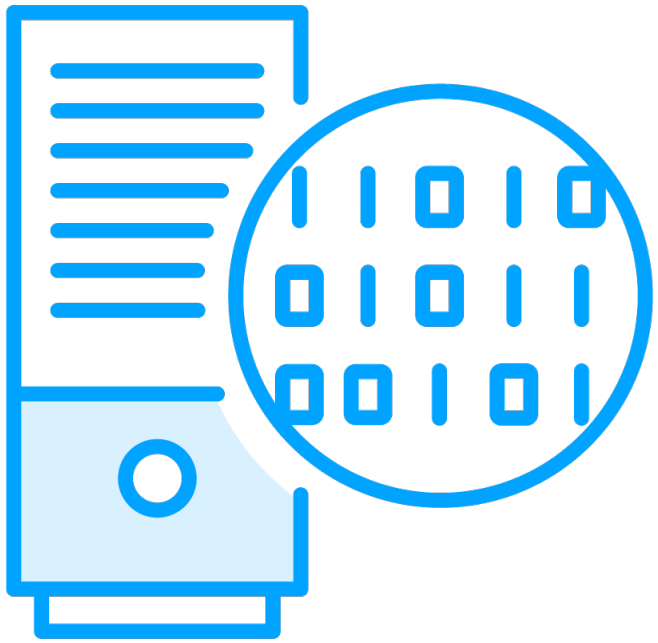
Understanding Data States



Data may be in one of three ‘states’

- Data at rest
- Data in transit
- Data in use

CIA applies to data in all states



Data at rest

- Stored on a hard drive and encrypted
  - File-level encryption
  - Disk-level encryption
  - Full-drive encryption (FDE)
    - Mobile devices



Data in transit

When data is sent or received across a network or replicated between data stores

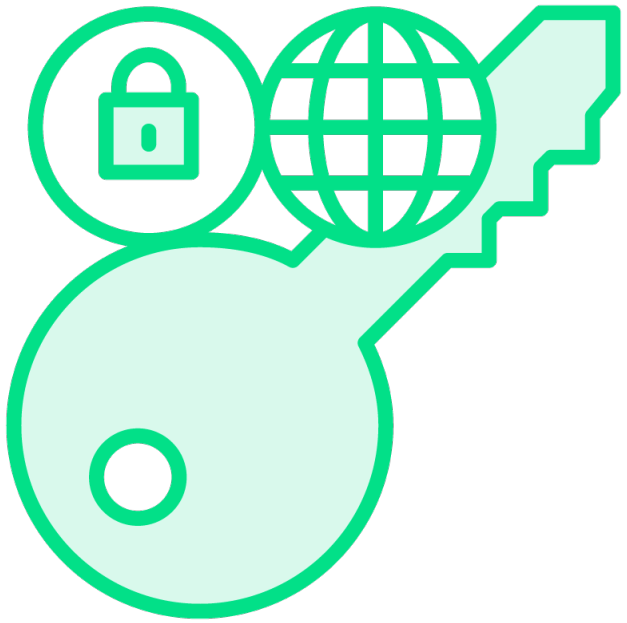
- Email systems
- Web servers (HTTPS)
- Virtual private network (VPN)
- Mobile communications
- Remote access connections



Data in use

When a user or system is physically using data within an application on a device

- Documents
- Spreadsheets
- Web browsers
- Email clients
- Graphic editing tools



Encryption provides us with the following:

- Confidentiality and integrity of data at rest and in transit
- We need to take care when accessing confidential data in public places or across public networks (in use)

Up Next:

Configuring Security Settings for a Small Wireless Network