IV1013 Introduction to Computer Security

Introduction

Peter Sjödin, psj@kth.se

Defining Security

- The security of a system, application, or protocol is always relative to
  - A set of desired properties
  - An adversary* with specific capabilities
- For example, standard file access permissions in Linux and Windows are not effective against an adversary who can boot from a CD

*Adversary is security jargon for ”bad guy”

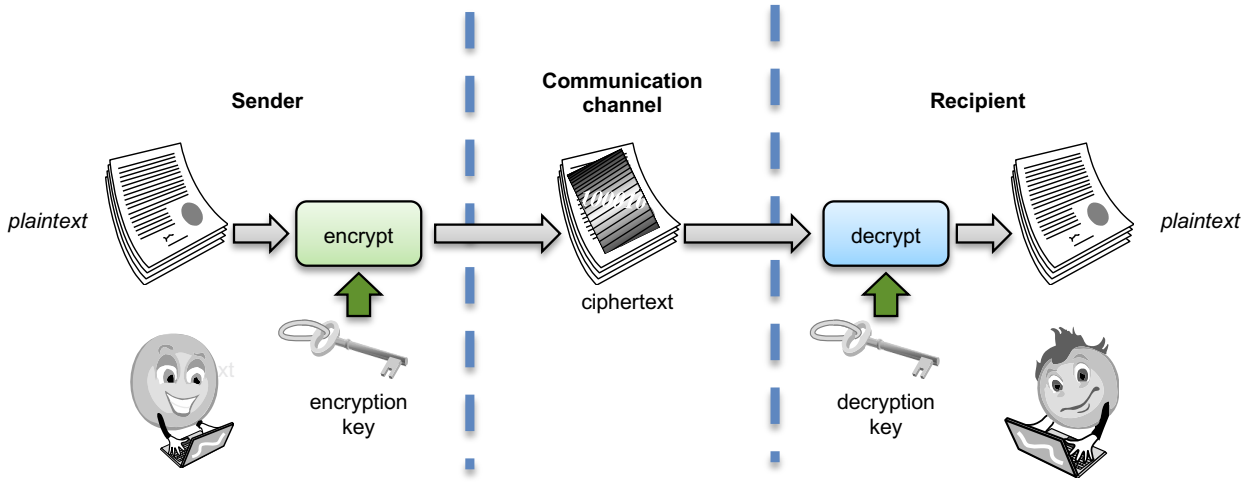
Security Goals – The C.I.A. Triad

Confidentiality

- **Confidentiality** or privacy is about not revealing information.
  - Protection of data.
  - Providing access for those who are allowed to see it, while disallowing others.

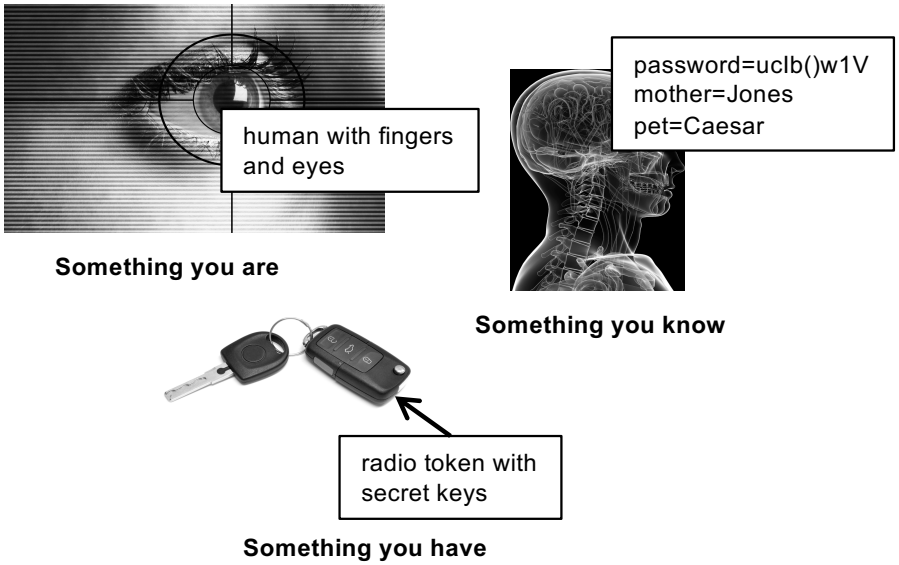
Tools for Confidentiality

- **Cryptography:** encoding of information so that only authorized persons can read it
- **Access control:** limit access to information
- **Authentication:** establish the identity of a person or system
- **Authorization:** establish whether a person or system is allowed access
- **Physical security:** limiting access through physical barriers



Authentication

- **Authentication:** the determination of the identity or role that someone has. It is usually based on a combination of:
  - **something the person has** (like a smart card or a radio key fob storing secret keys),
  - **something the person knows** (like a password),
  - **something the person is** (like a human with a fingerprint).



Integrity

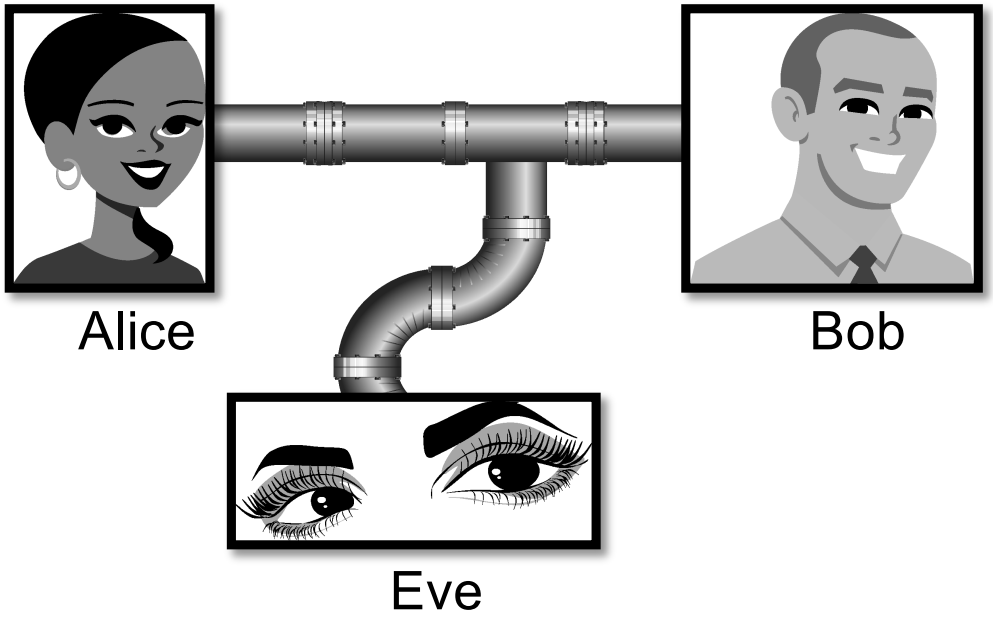
- **Integrity:** information has not been altered.
- **Tools:**
  - Backups
  - Cryptographic checksums
  - Data correcting codes

Availability

- **Availability:** the property that information is accessible and modifiable in a timely fashion by those authorized to do so.
- **Tools:**
  - Physical protection
  - Computational redundancies

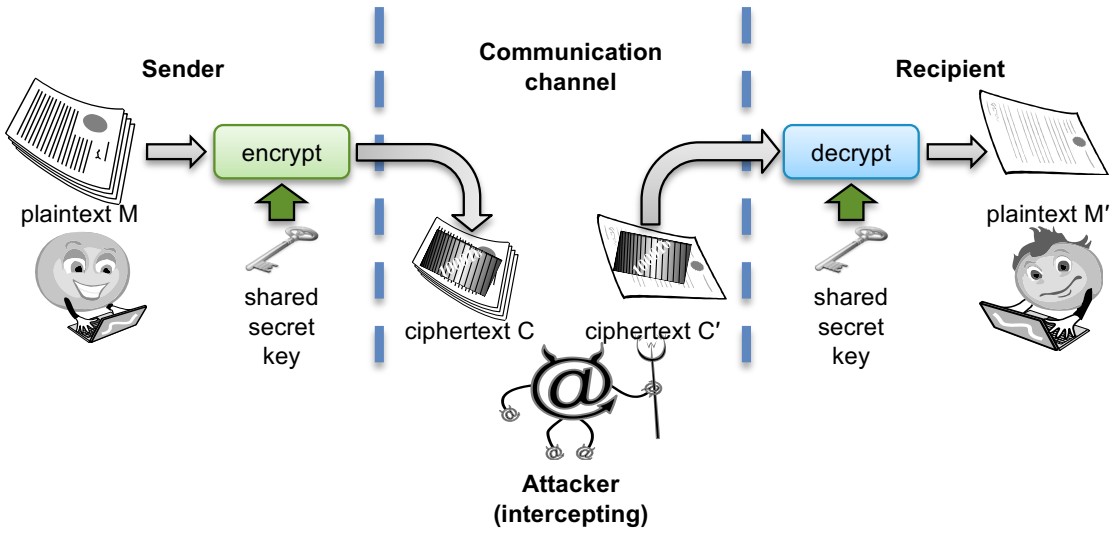
Threats and Attacks

- **Eavesdropping:** interception of information.



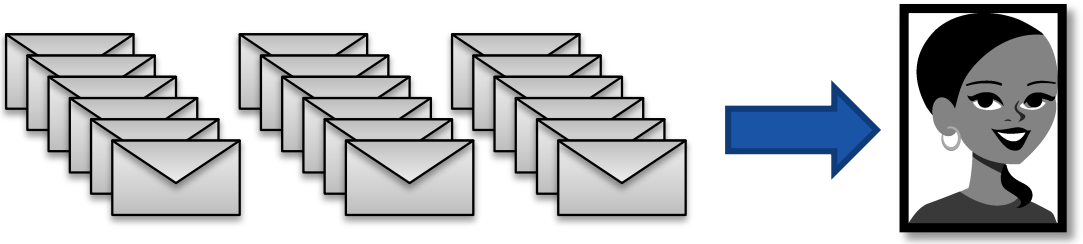
Threats and Attacks

- **Alteration:** unauthorized modification of information.
  - **Example:** the **man-in-the-middle attack,** where a network stream is intercepted, modified, and retransmitted.



Threats and Attacks

- **Denial-of-service:** the interruption or degradation of a data service or information access.
  - **Example:** email **spam,** to the degree that it is meant to simply fill up a mail queue and slow down an email server.

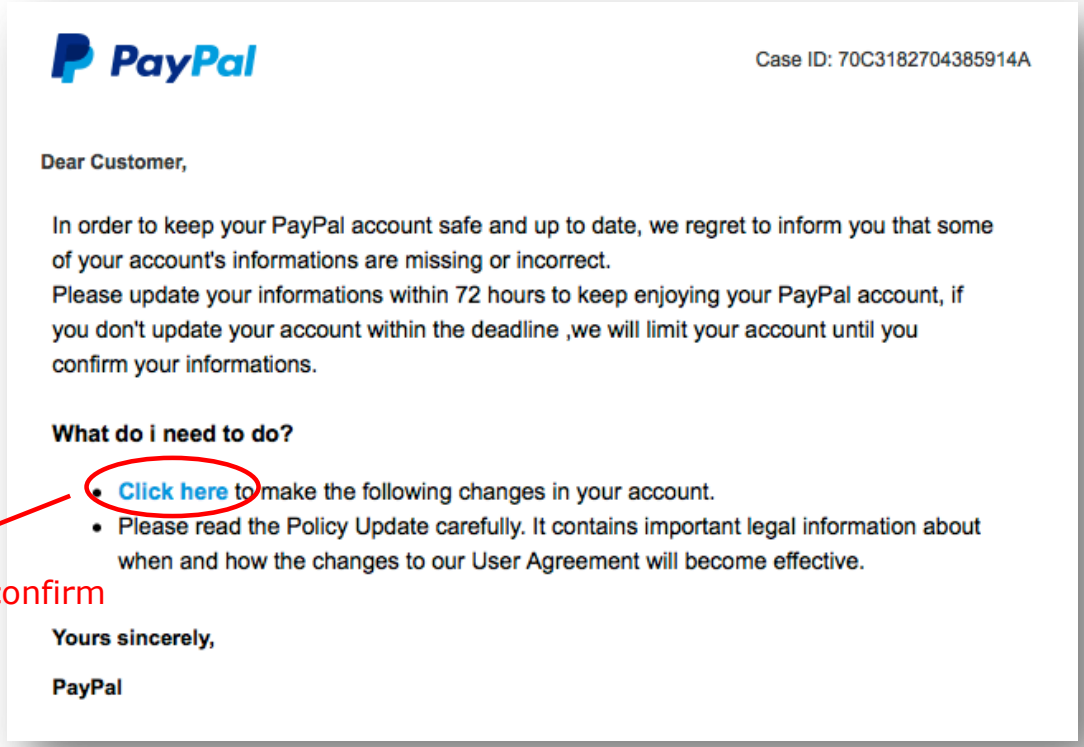


Distributed Denial-of-Service Attack

- Use many computers to send traffic to site under attack
- Attack against anti-spam organization Spamhaus. “Rekordstor nätattack drabbar många” – Nyheter (Ekot) *March 27, 2013*
- Online attack hits Swedish media sites – Radio Sweden. *March 20, 2016*

Threats and Attacks

- **Masquerading:** information is purported to be from someone who is not actually the author.



PayPal

Case ID: 70C3182704385914A

Dear Customer,

In order to keep your PayPal account safe and up to date, we regret to inform you that some of your account's informations are missing or incorrect.
Please update your informations within 72 hours to keep enjoying your PayPal account, if you don't update your account within the deadline ,we will limit your account until you confirm your informations.

What do i need to do?

- Click here to make the following changes in your account.
- Please read the Policy Update carefully. It contains important legal information about when and how the changes to our User Agreement will become effective.

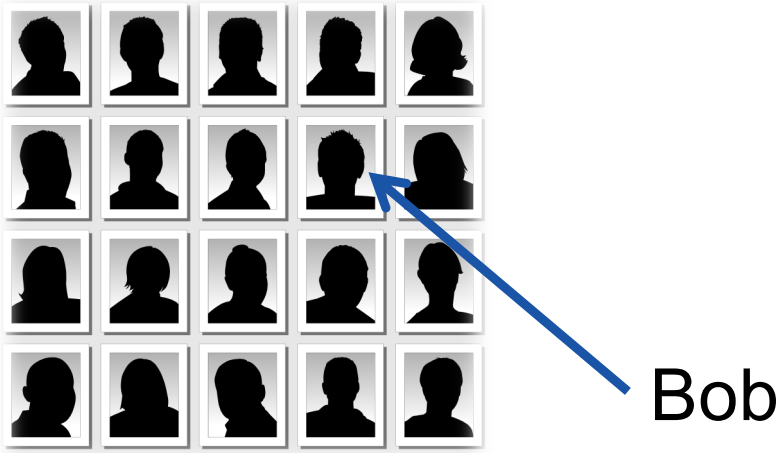
Yours sincerely,

PayPal

http://paypgl.com/confirm

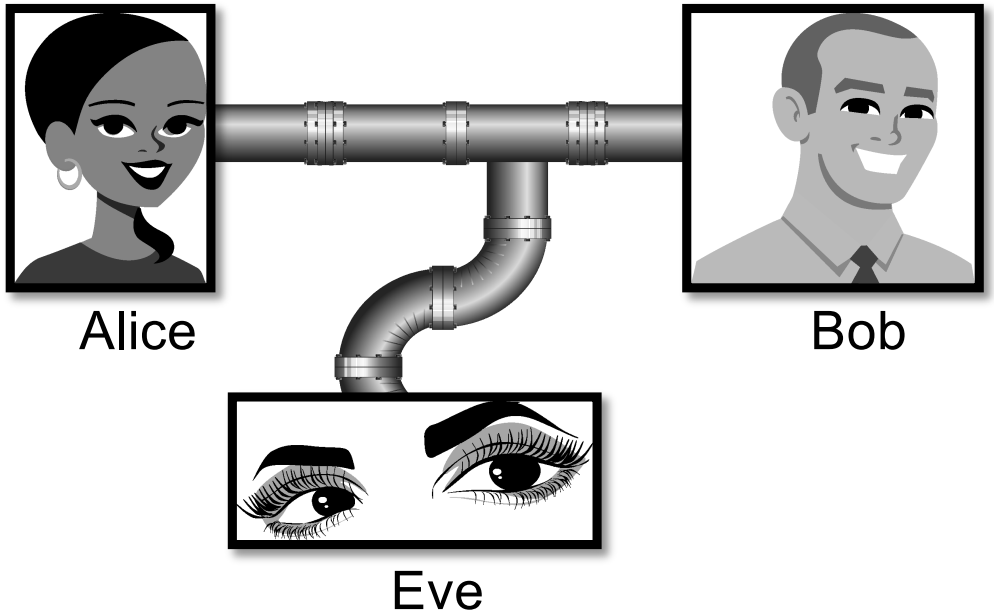
Threats and Attacks

- **Correlation** and **traceback:** the integration of multiple data sources and information flows to determine the source of a particular data stream or piece of information.



Cryptographic Concepts

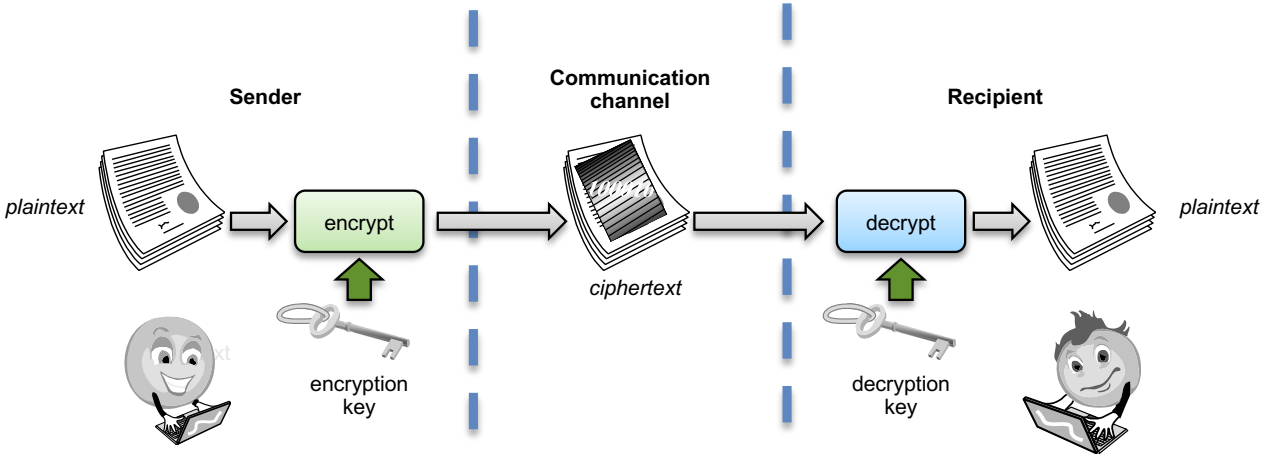
- **Encryption**: a means to allow two parties, customarily called Alice and Bob, to establish confidential communication over an insecure channel that is subject to eavesdropping.



Encryption and Decryption

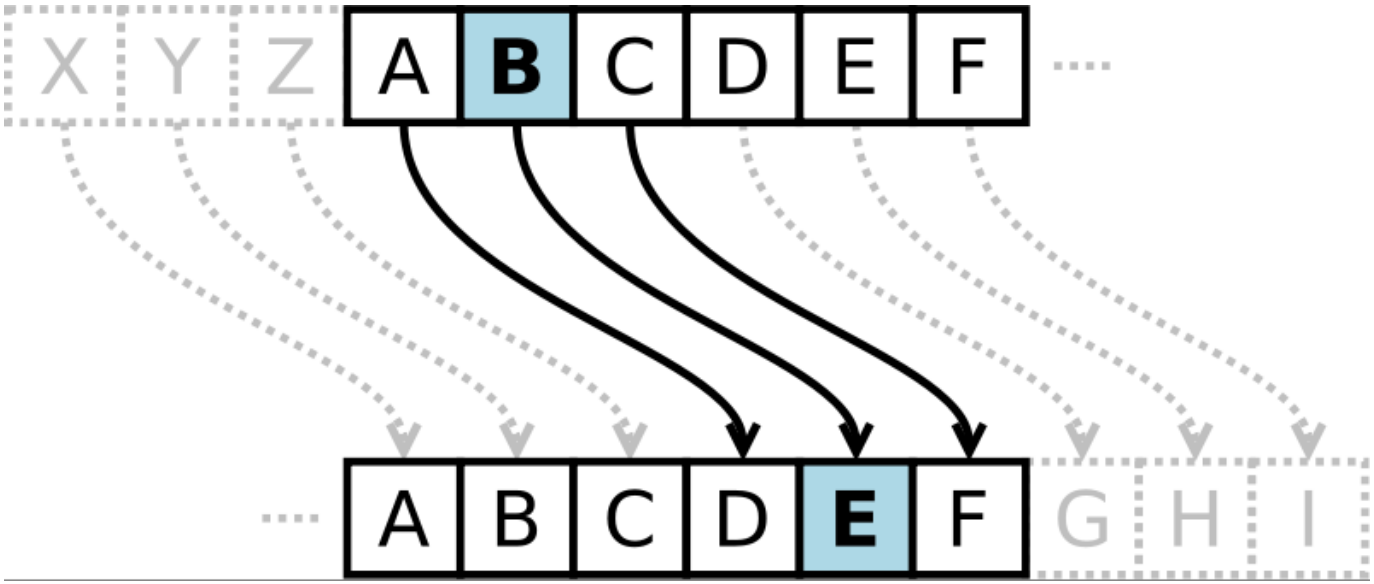
- The message M is called **plaintext.**
- Sender uses encryption algorithm E to convert plaintext M to **ciphertext** C = E(M)
- The intended receiver (and no one else) can get M from C by using decryption algorithm D: M = D(C)

$$M = D(C) = D(E(M))$$



Example: Caesar Cipher

- Replace each letter with the one “three over” in the alphabet.

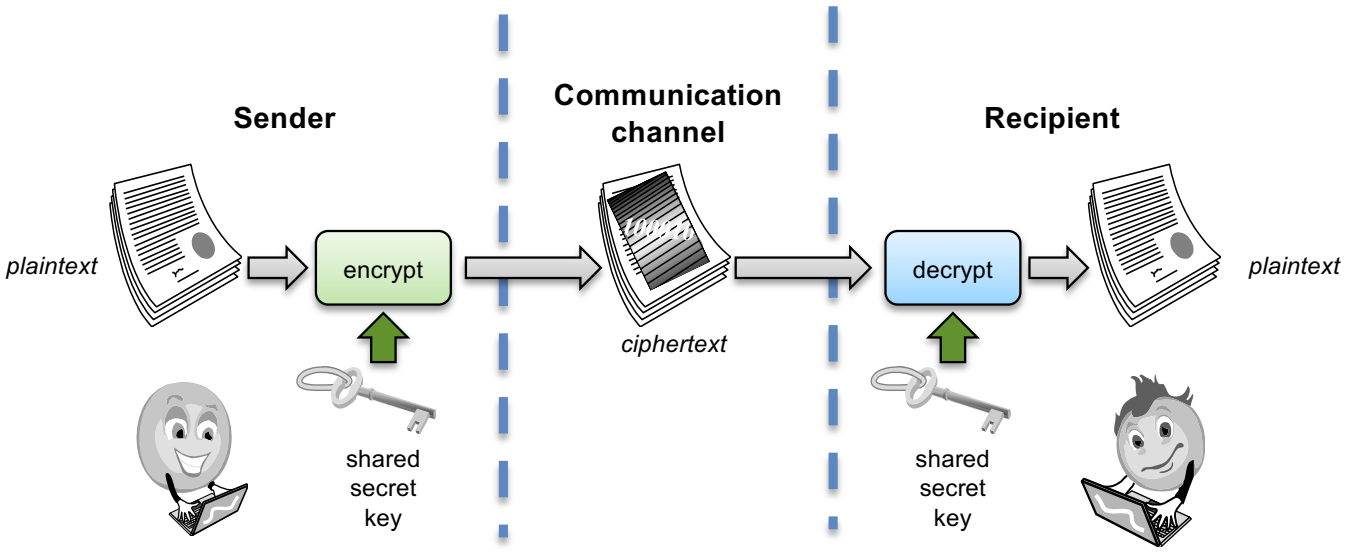


Public domain image from http://commons.wikimedia.org/wiki/File:Caesar3.svg

Symmetric Cryptosystems

- Alice and Bob share a secret key S, which is used for both encryption and decryption.

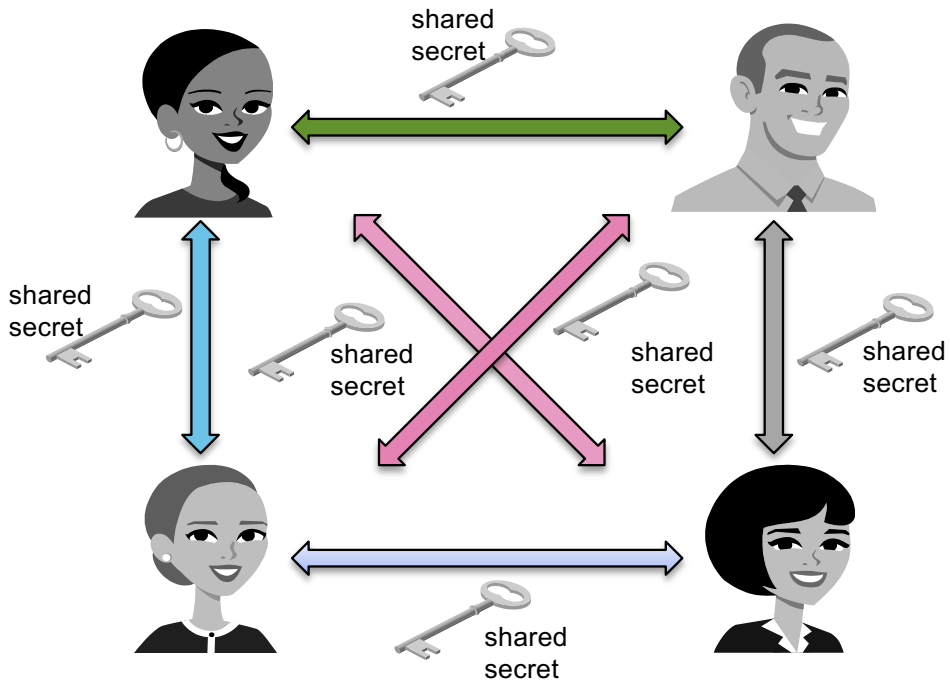
$$M = D_S(E_S(M))$$



Symmetric Key Distribution

- Requires each pair of communicating parties to share a (separate) secret key.

Key distribution problem: How to get the key?



n (n–1)/2 keys

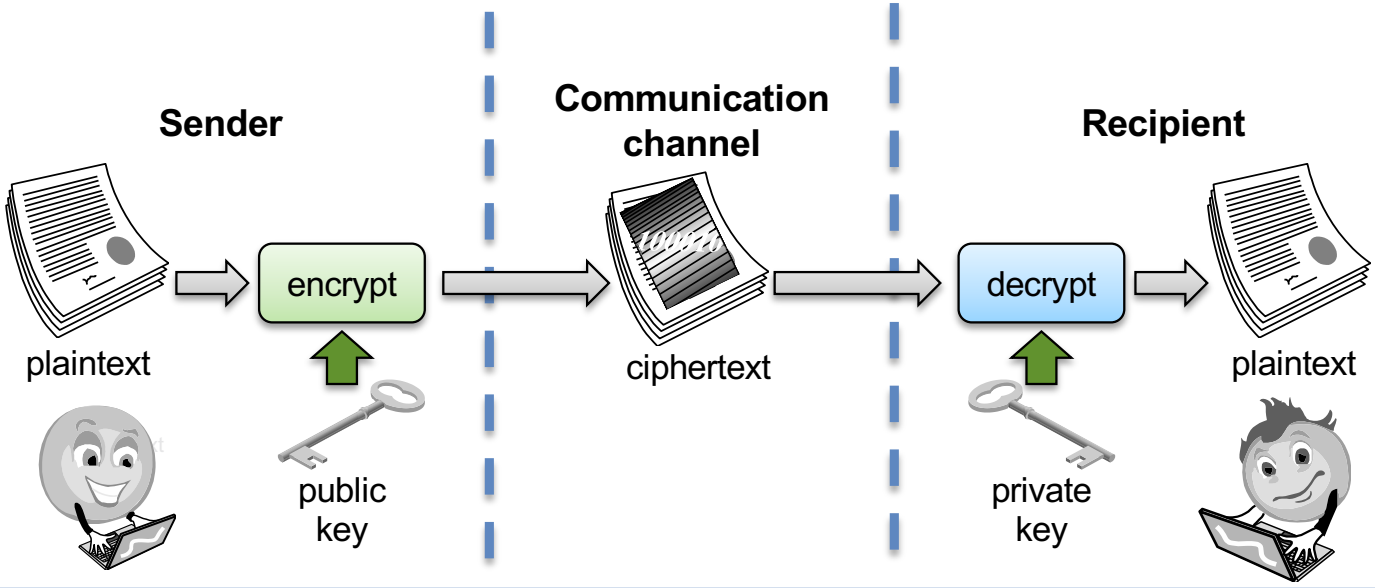
Public-Key Cryptography

- Bob has two keys: a **private key,** SB, which Bob keeps secret, and a **public key,** PB, which Bob broadcasts widely.
  - In order for Alice to send an encrypted message to Bob, she need only obtain his public key, PB, use that to encrypt her message, M, and send the result, $C = E_{PB}(M)$, to Bob.
  - Bob then uses his secret key to decrypt the message as $M = D_{SB}(C)$.

Public-Key Cryptography

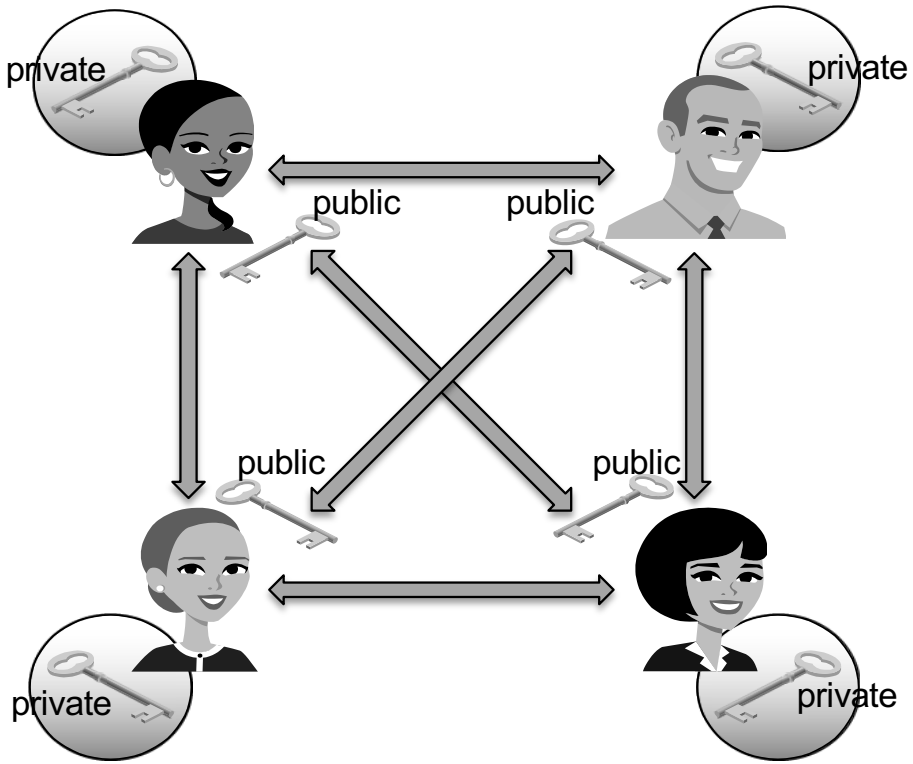
- Separate keys for encryption and decryption.

$$D_{SB}(E_{PB}(M)) = M$$



Public Key Distribution

- Only one key is needed for each recipient



n key pairs

Important Property of Public-Key Encryption

- Alice generates two keys: private key, SA, and public key, PA.
- A plaintext encrypted with one of the keys can be decrypted with the other.

$$D_{PA}(E_{SA}(M)) = D_{SA}(E_{PA}(M)) = M$$

Digital Signatures

- Public-key encryption provides a method for doing digital signatures
- To sign a message, M, Alice just encrypts it with her private key, SA, creating $C = E_{SA}(M)$.
- Anyone can decrypt this message using Alice's public key, as $M' = D_{PA}(C)$, and compare that to the message M.
  - If M' = M, the signature has been verified:
    - *Alice signed the message (and no one else)*
    - *Alice signed M (and no other message)*

Summary

- CIA Triad
  - Confidentiality
    - *Encryption and control of who can access data*
  - Integrity
    - *Checksums, backups*
  - Availability
    - *Physical protection, redundancy*
- Threats
  - Man-in-the-middle – interception, modification, replay
  - Denial-of-service
  - Masquerading
- Encryption
  - Symmetric-key and public-key encryption
  - Cryptographic hash and digital signatures