Introduction to Computer Networks

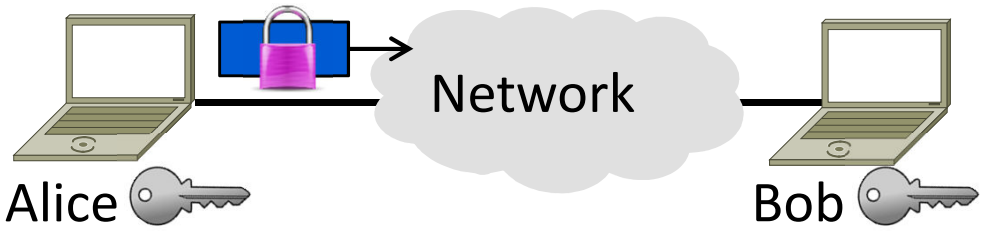
Message Confidentiality

(§8.1.1, §8.2-8.3)

David Wetherall (djw@uw.edu)
Professor of Computer Science & Engineering
UNIVERSITY of WASHINGTON

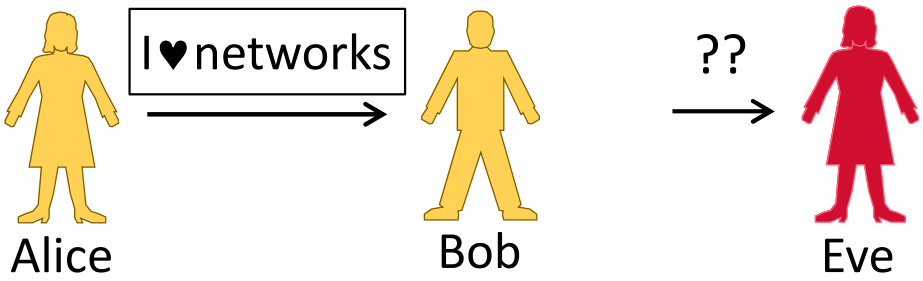
Topic

- Encrypting information to provide confidentiality
  - Symmetric and public key encryption
  - Treat crypto functions as black boxes



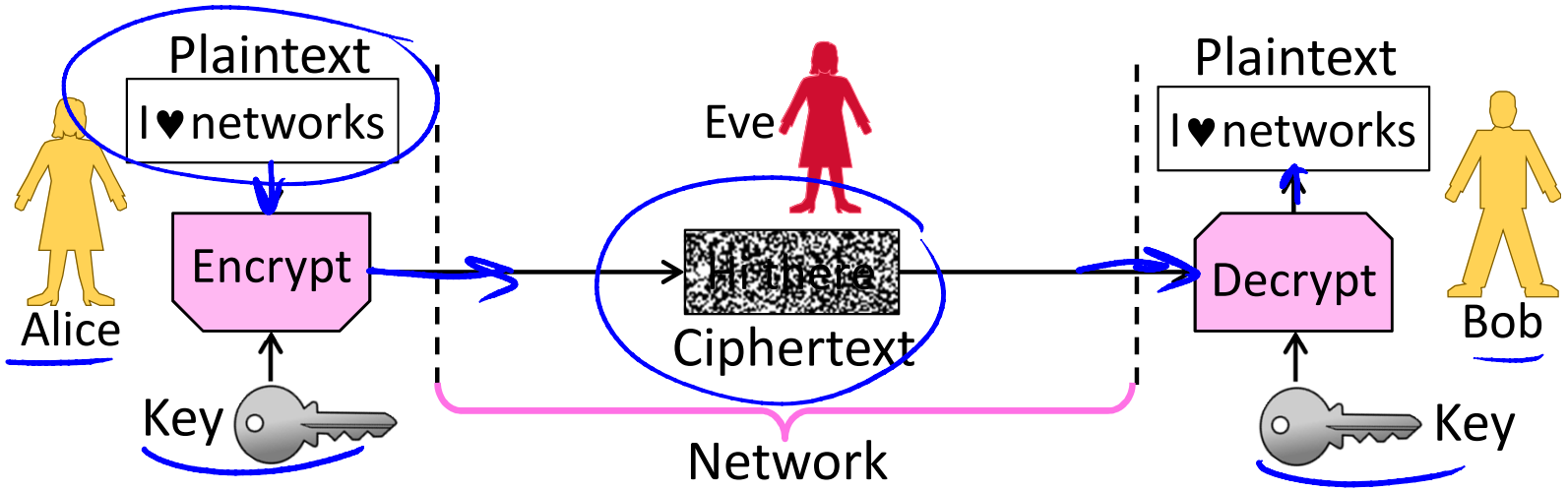
Goal and Threat Model

- Goal is to send a private message from Alice to Bob
  - This is called confidentiality
- Threat is Eve will read the message
  - Eve is a passive adversary (observes)



Encryption/Decryption Model

- Alice encrypts private message (plaintext) using key
- Eve sees ciphertext but can't relate it to private message
- Bob decrypts using key to obtain the private message



Encryption/Decryption (2)

- Encryption is a reversible mapping
  - Ciphertext is confused plaintext
- Assume attacker knows algorithm
  - Security does not rely on its secrecy
- Algorithm is parameterized by keys
  - Security does rely on key secrecy
  - Must be distributed (Achilles' heel)

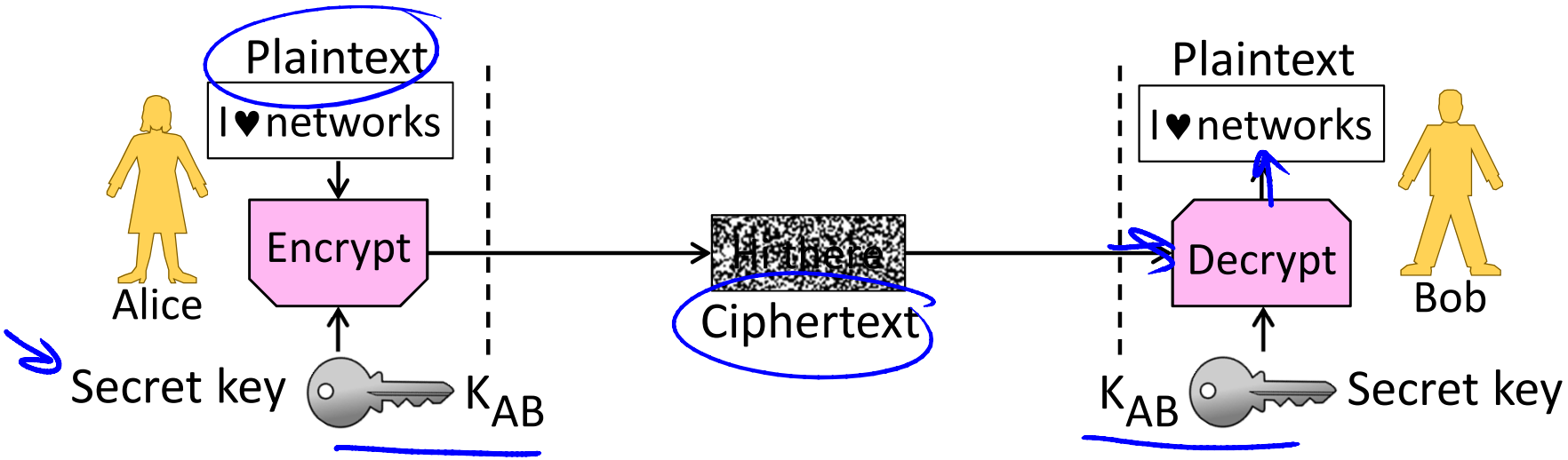
Encryption/Decryption (3)

Two main kinds of encryption:

1. Symmetric key encryption », e.g., AES
   - Alice and Bob share secret key
   - Encryption is a bit mangling box
2. Public key encryption », e.g., RSA
   - Alice and Bob each have a key in two parts: a public part (widely known), and a private part (only owner knows)
   - Encryption is based on mathematics (e.g., RSA is based on difficulty of factoring)

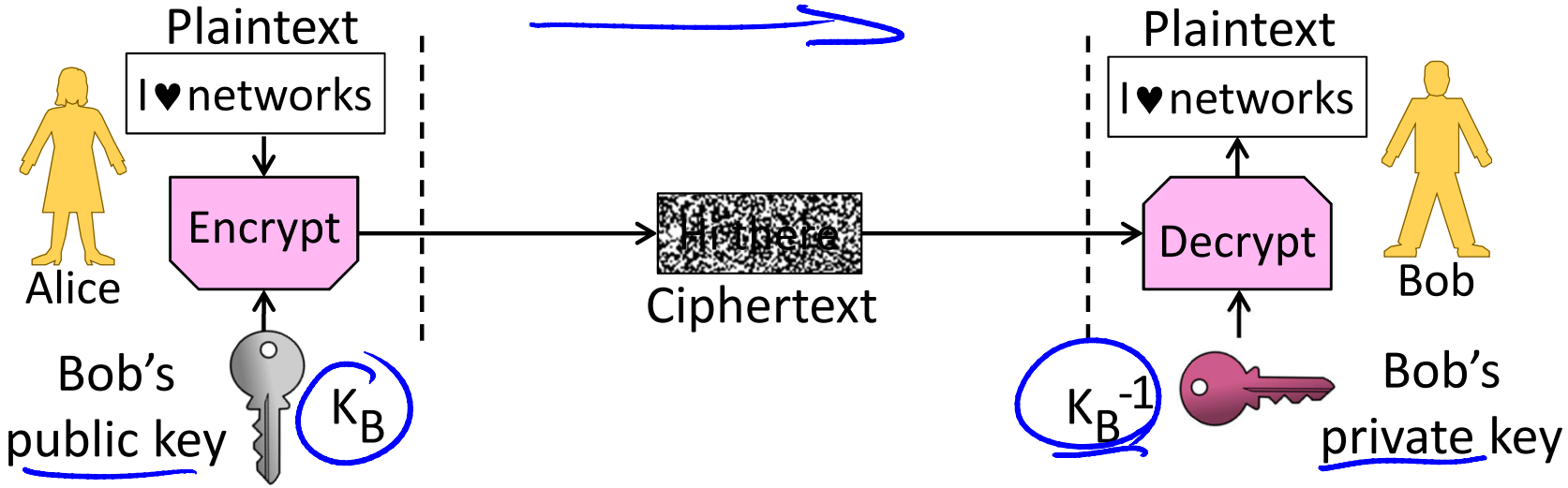
Symmetric (Secret Key) Encryption

- Alice and Bob have the same secret key, K_{AB}
  - Anyone with the secret key can encrypt/decrypt



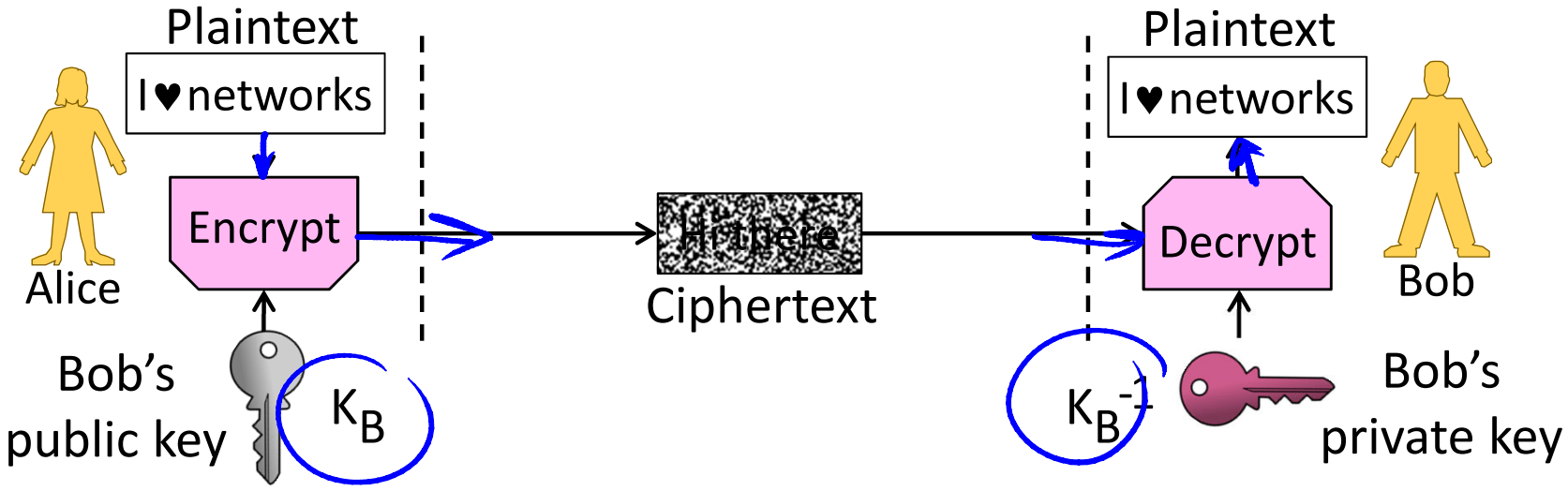
Public Key (Asymmetric) Encryption

- Alice and Bob each have public/private key pair (K_B / K_B^{-1})
  - Public keys are well-known, private keys are secret to owner

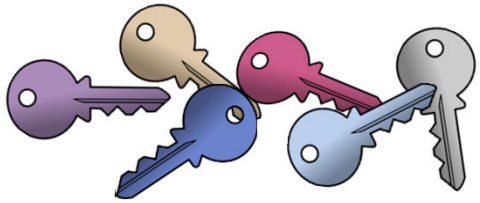


Public Key Encryption (2)

- Alice encrypts with Bob's public key K_B; anyone can send
- Bob decrypts with his private key K_B^{-1}; only he can do so



Key Distribution



- This is a big problem on a network!
  - Often want to talk to new parties
- Symmetric encryption problematic
  - Have to first set up shared secret
- Public key idea has own difficulties
  - Need trusted directory service
  - We'll look at certificates later

Symmetric vs. Public Key

- Have complementary properties
  - Want the best of both!

Property	Symmetric	Public Key
Key Distribution	Hard – share secret per pair of users	Easier – publish public key per user
Runtime Performance	Fast – good for high data rate	Slow – few, small, messages

Winning Combination

- Alice uses public key encryption to send Bob a small private message
  - It's a key! (Say 256 bits.)
- Alice and Bob send large messages with symmetric encryption
  - Using the key they now share
- The key is called a session key
  - Generated for short-term use

END