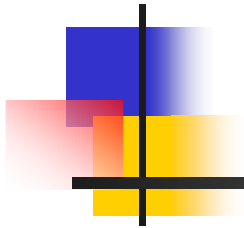


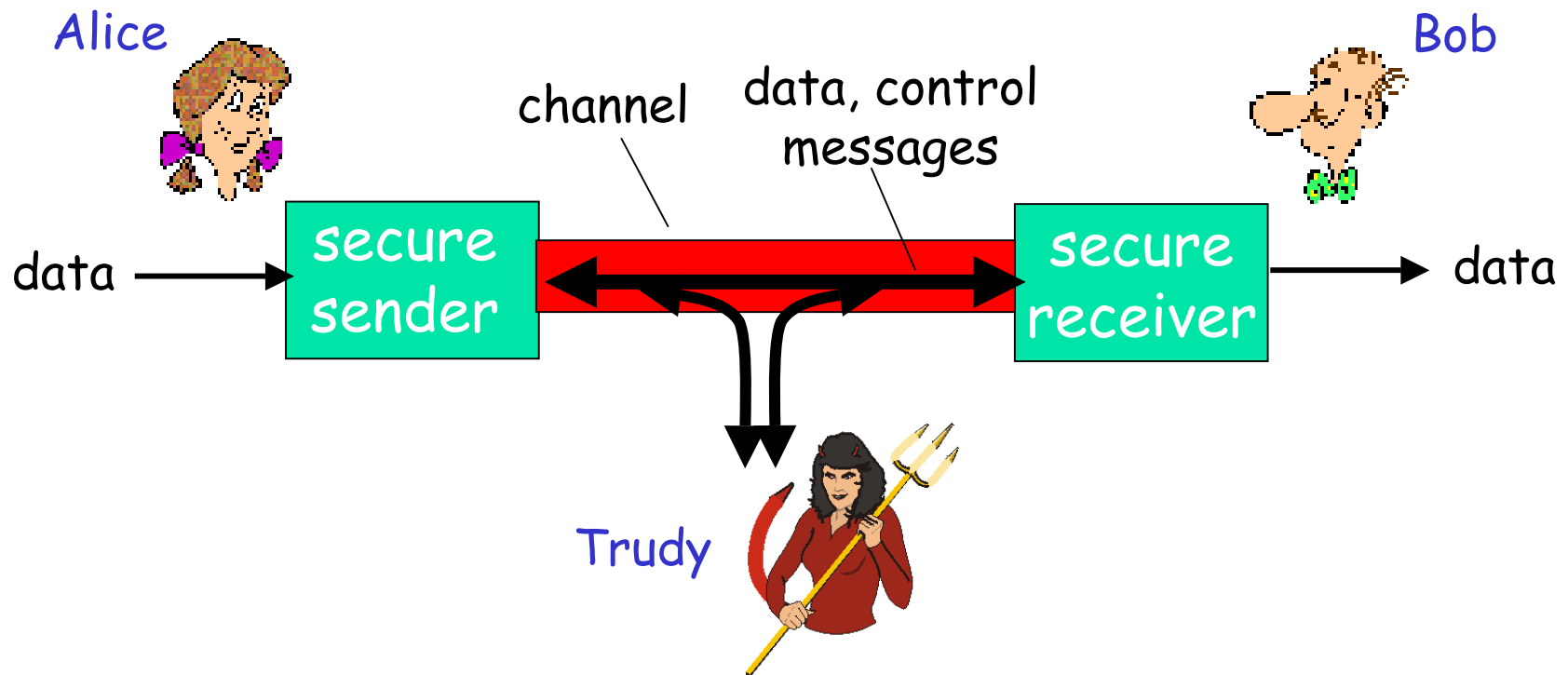
Principles of Network Security



Dept. of Computer Science, University of Rochester

The Network Security Model

- Bob and Alice want to communicate "securely".
- Trudy (the adversary) has access to the channel.





Who might Bob and Alice be?

- Web browser/server for electronic transactions (e.g., on-line purchases/banking)
- DNS servers
- routers exchanging routing table updates
- ... well, *real-life* Bobs and Alices!



What can an adversary do?

- **eavesdrop**: understand the content of messages
- actively **changing** messages
- **impersonation**: can fake (spoof) source address in packet (or any field in packet)
- **denial of service**: prevent service from being used by others (e.g., by overloading resources)



What is Network Security?

Confidentiality: only sender, intended receiver should “understand” message contents

Authentication: sender, receiver want to confirm identity of each other

Message Integrity: sender, receiver want to ensure message not altered (in transit, or afterwards)

Access and Availability: services must be accessible and available to (and only to) legitimate users.

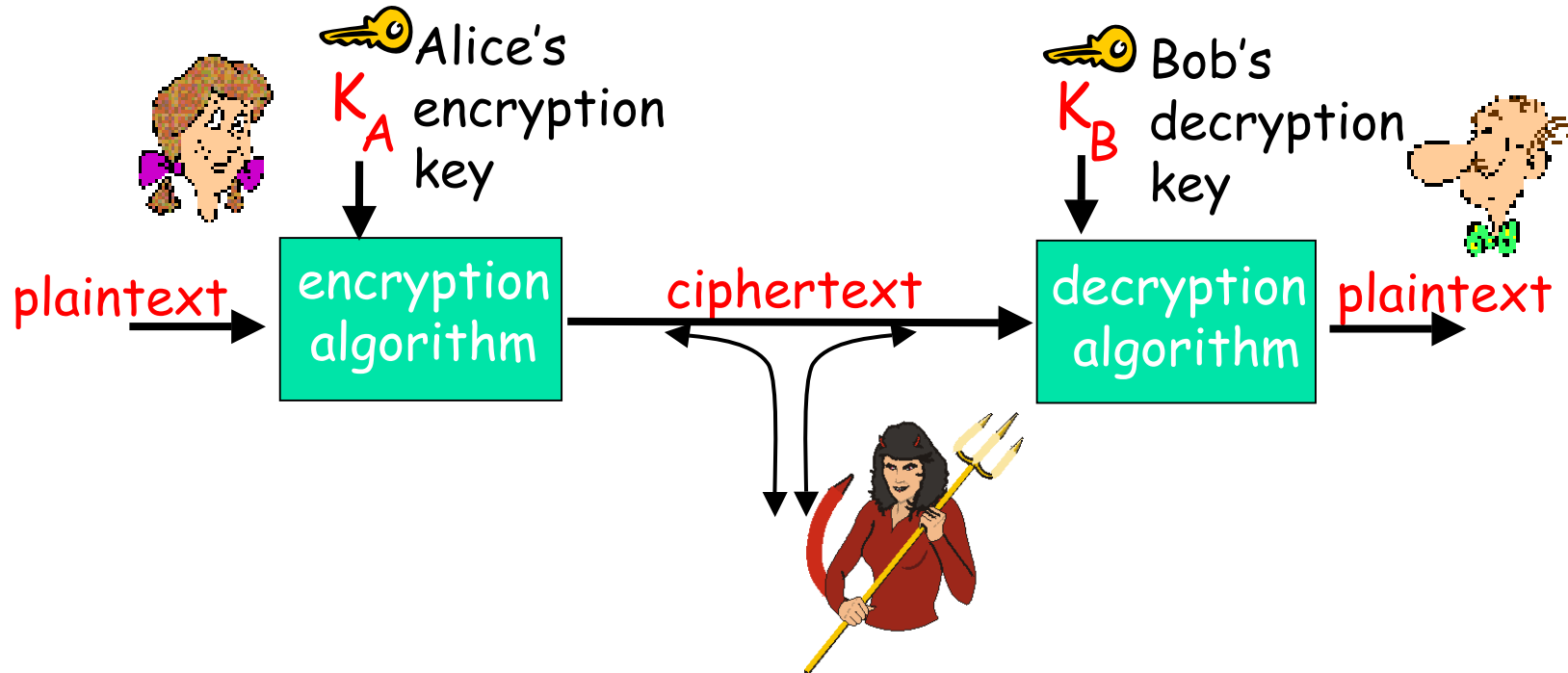


Outline

- What is network security?
- Confidentiality: cryptography
- Authentication
- Integrity

The Language of Cryptography

First goal of cryptography: **confidentiality**.

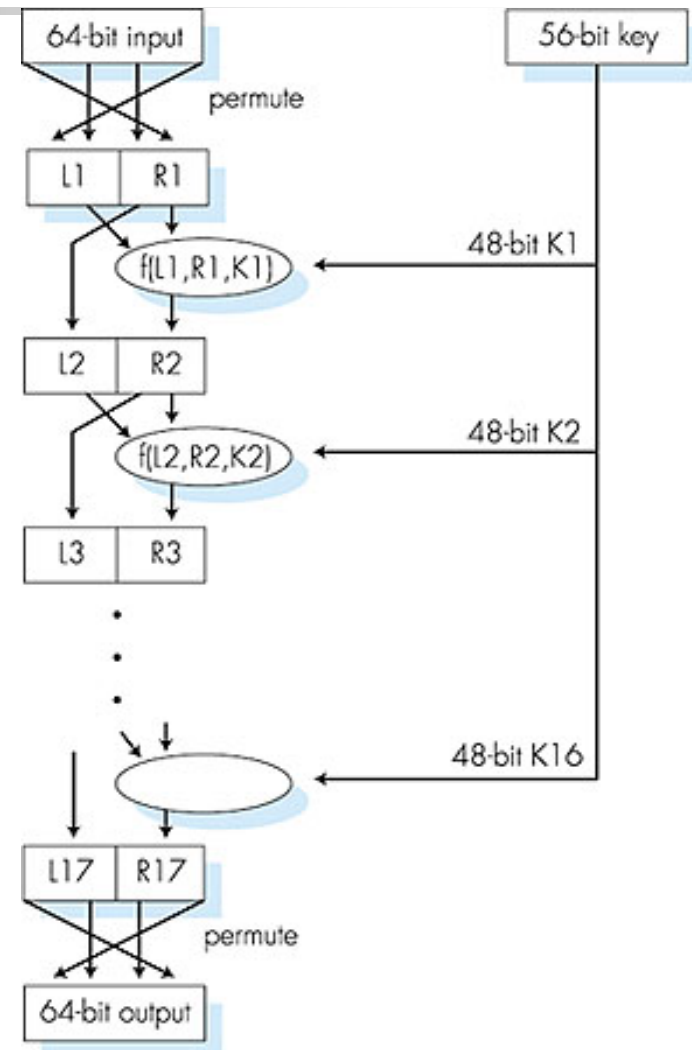


- **symmetric key** crypto: encryption and decryption keys are identical. (both are **secret**)
- **public key** crypto: encryption key is **public**, decryption key is **secret**.

Symmetric Key Cryptography: DES

■ DES: Data Encryption Standard

- US encryption standard [NIST 1993]
 - 56-bit symmetric key, 64-bit plaintext input
 - **encryption**: initial permutation \Rightarrow 16 "rounds", each using different 48 bits of key \Rightarrow final permutation
 - **decryption**: reverse operation using the same key
- ## ■ How secure is DES?
- DES Challenge (1999): 56-bit-key-encrypted phrase decrypted (brute force) in 22 hours 15 minutes
- ## ■ Making DES more secure:
- use three keys sequentially (3-DES)
 - use more bits



AES: Advanced Encryption Standard



- new (Nov. 2001) symmetric-key NIST standard, replacing DES
- processes data in 128 bit blocks
- 128, 192, or 256 bit keys
- brute force decryption (try each key) taking 1 sec on DES, takes 149 trillion years for 128-bit AES



Public Key Cryptography

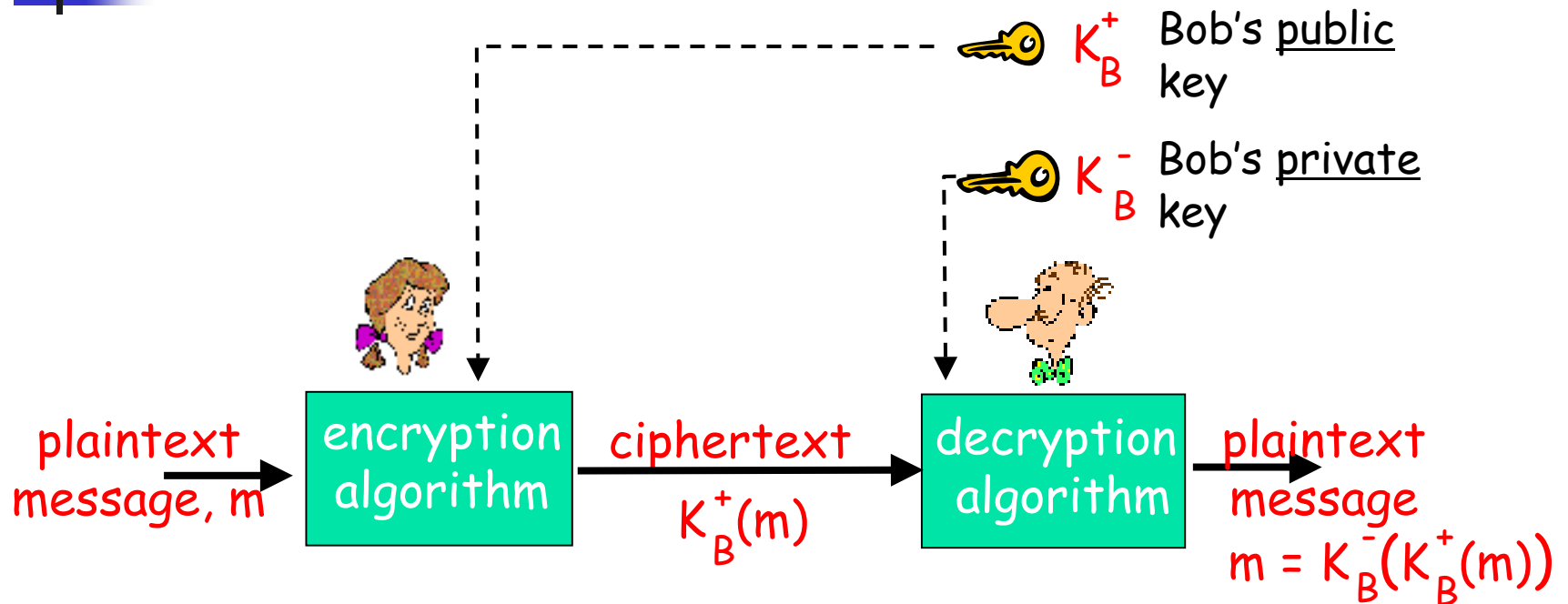
symmetric key cryptography

- requires sender, receiver know shared secret key
- Q: how to agree on key in first place? (particularly difficult if Trudy is eavesdropping on all communication)

public key cryptography

- encryption key is different from decryption key
- encryption key is **public**, known to **everyone**, also called **public key**
- decryption key is **secret**, known only to **receiver**, also called **private key**

Public Key Cryptography



Principle for choosing the public/private key pair:
One should not be able to derive the private key from the public key.

Public Key Cryptography: RSA

(Ron Rivest, Adi Shamir and Len Adleman)

- Choosing keys:
 - Choose two large prime numbers p, q . (e.g., 1024 bits each)
 - Compute $n = pq$, $z = (p-1)(q-1)$
 - Choose e (with $e < n$) that has no common factors with z .
 - Choose d such that $ed-1$ is exactly divisible by z .
 - Public key is (n,e) . Private key is (n,d) .
- To encrypt a message, m ($< n$): do $c = m^e \bmod n$
- To decrypt a received ciphertext, c : do $m = c^d \bmod n$
- RSA is much slower than the symmetric key cryptos.

RSA Example 1

- Choosing keys:
 - Choose two prime numbers $p = 5, q = 7$.
 - Compute $n = pq = 35, z = (p-1)(q-1) = 24$ (factors: 2,2,2,3)
 - Choose $e=5$ (with $e < n$) that has no common factors with $z=24$.
 - Choose $d=29$ such that $ed-1=144$ is exactly divisible by $z=24$. It is!
 - Public key is (n,e) . Private key is (n,d) .
- To encrypt a message, m ($< n$): do $c = m^e \bmod n$
 - $m = 12 \Rightarrow c = 12^5 \bmod 35 = 248832 \bmod 35 = 17$
- To decrypt a received ciphertext, c : do $m = c^d \bmod n$
 - $c = 17 \Rightarrow m = 17^{29} \bmod 35 = 481968572106750915091411825223071697 \bmod 35 = 12$

RSA Example 2

■ Choosing keys:

- Choose two prime numbers $p = 19, q = 23$.
- Compute $n = pq = 437, z = (p-1)(q-1) = 396$ (factors: 2,2,3,3,11)
- Choose $e=13$ that has no common factors with $z=396$.
- Choose $d=61$ such that $ed-1=792$ is exactly divisible by $z=396$. It is!
- Public key is (n,e) . Private key is (n,d) .

■ To encrypt a message, $m (<n)$: do $c = m^e \bmod n$

- $m = 12 \Rightarrow c = 12^{13} \bmod 437 = 106993205379072 \bmod 437 = 259$

■ To decrypt a received ciphertext, c : do $m = c^d \bmod n$

- $c = 259 \Rightarrow m = 259^{61} \bmod 437 =$
16266181314803209896440891867103597432080542047515074104
3425752186988745216832900688919130573319060853500553266
3824241192471465591947264079086947859 $\bmod 437 = 12$



Disclaimer

- Parts of the lecture slides contain original work of James Kurose, Larry Peterson, and Keith Ross. The slides are intended for the sole purpose of instruction of computer networks at the University of Rochester. All copyrighted materials belong to their original owner(s).