UNIVERSITY OF BIRMINGHAM

Introduction to Computer Science
Week 10 – Network Security

Based on material and slides from
Computer Networking: A Top Down Approach, 7th Edition – Chapter 8
Jim Kurose, Keith Ross
Pearson/Addison Wesley

Lecture Objective

The objective of this lecture is to understand the conceptual aspects of network security with emphasis on cryptography.

Lecture Outline

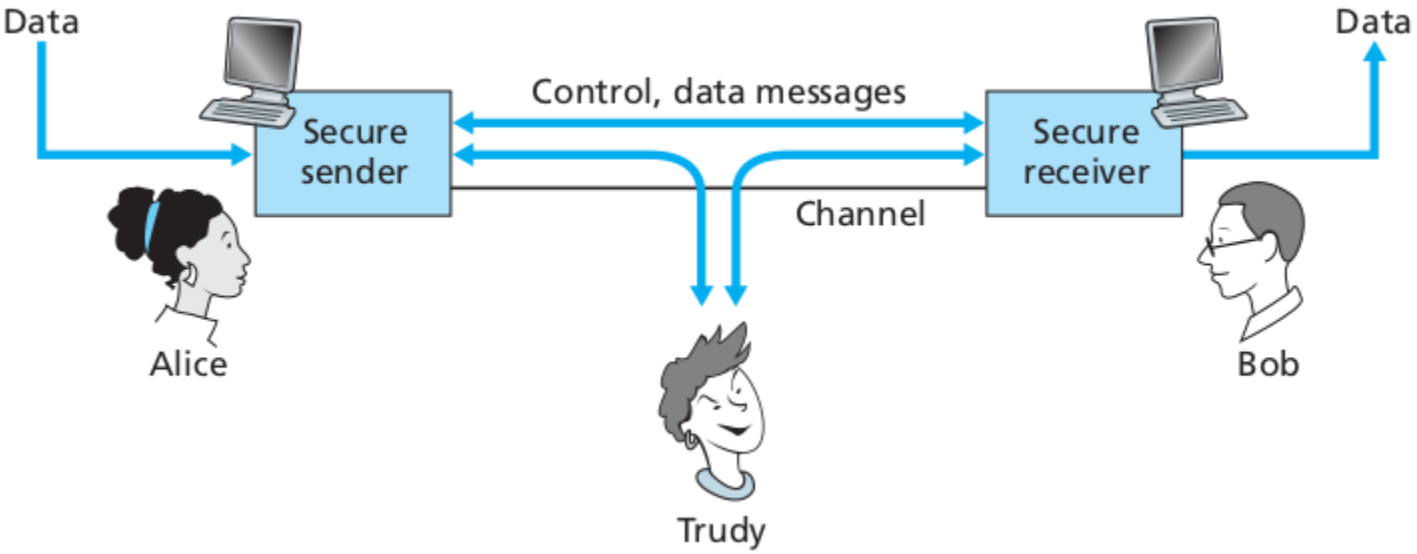
- Introduction to Network Security
- Principles of Cryptography
- Symmetric Key Cryptography
- Public Key Cryptography
- Summary

What is Network Security?

- *Confidentiality*: only sender, intended receiver should "understand" message contents
  - sender encrypts message
  - receiver decrypts message
- *End-point Authentication:* sender, receiver want to confirm identity of each other
- *Message Integrity:* sender, receiver want to ensure message not altered (in transit, or afterwards) without detection
- *Access and Availability:* services must be accessible and available to users

Friends and Enemies: Alice, Bob & Trudy

- Well-known in network security world
- Bob, Alice want to communicate “securely”
- Trudy (intruder) may intercept, delete, add messages



Who might Bob, Alice be?

- … well, real-life Bobs and Alices!
- Web browser/server for electronic transactions (e.g., on-line purchases)
- On-line banking client/server
- DNS servers
- Routers exchanging routing table updates
- other examples?

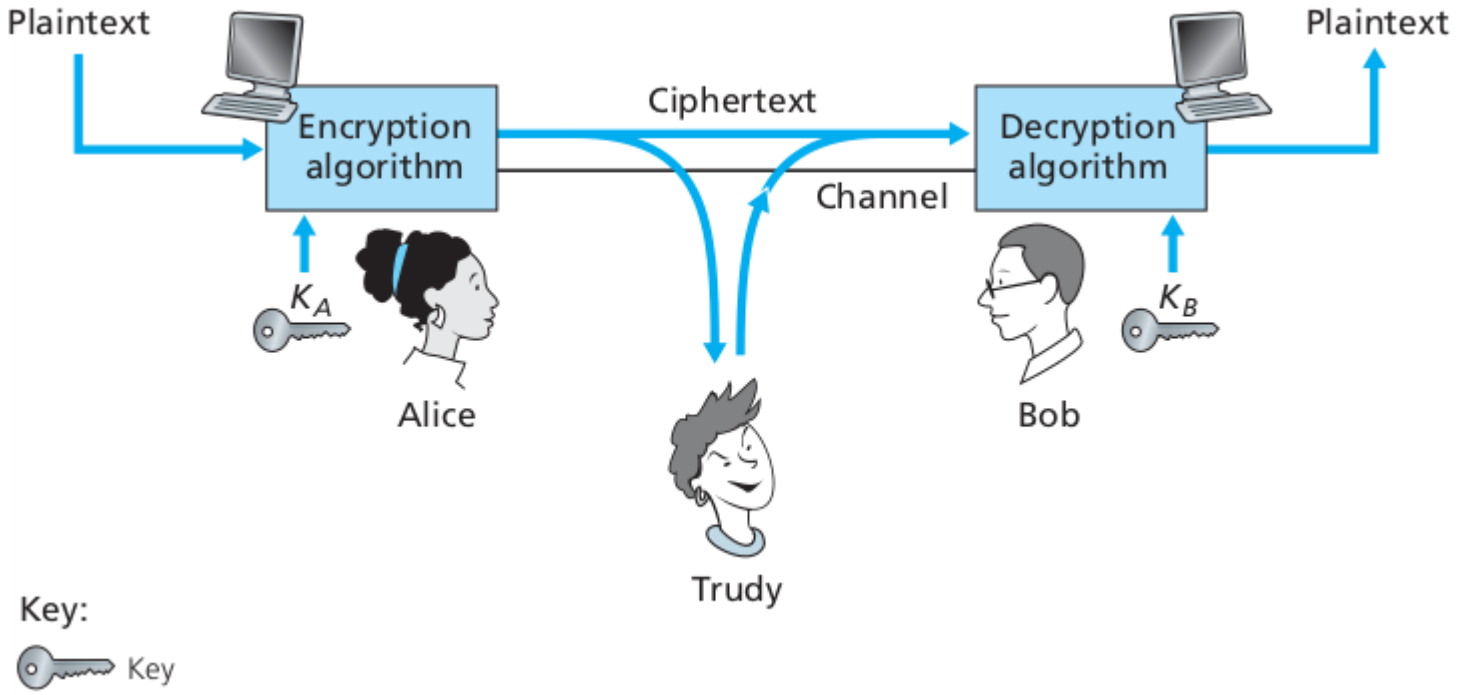
There are Bad Guys (and Girls) Out There!

Q: What can a "bad guy" do?

A: A lot!

- *Eavesdrop:* intercept messages
- Actively *insert* messages into connection (e.g. man in the middle attack)
- *Impersonation:* can fake (spoof) source address in packet (or any field in packet)
- *Hijacking:* "take over" ongoing connection by removing sender or receiver, inserting himself in place
- *Denial of Service*: prevent service from being used by others (e.g., by overloading resources)

Principles of Cryptography



m plaintext message

$K_A(m)$ ciphertext, encrypted with key K_A

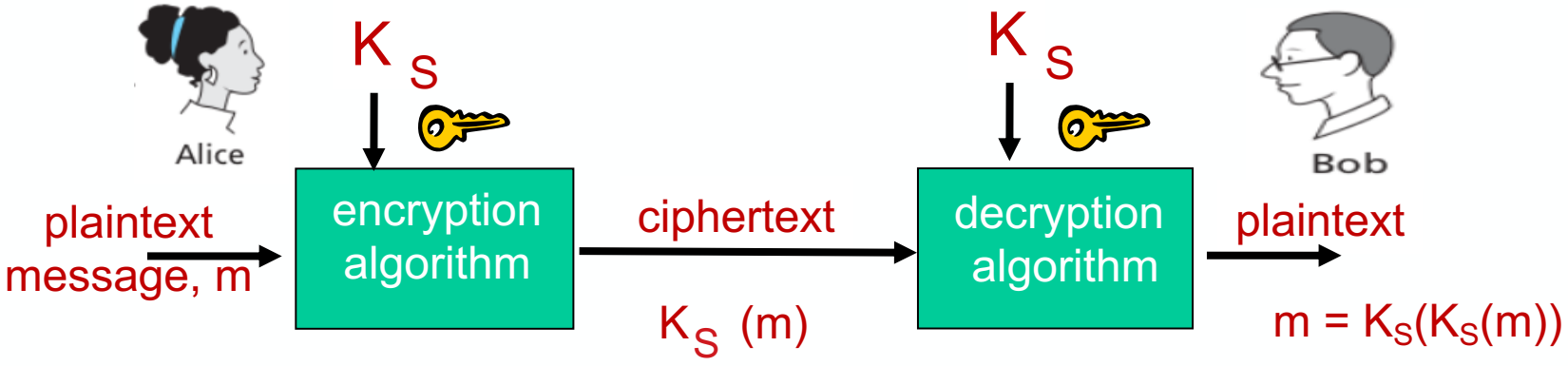
$m = K_B(K_A(m))$

Encryption Schemes

There are two main types of encryption schemes:

- Symmetric Key Systems: Alice's and Bob's keys are identical and are secret.
- Public Key Systems, a pair of keys is used. One of the keys is known to both Bob and Alice (known to the whole world). The other key is known only by either Bob or Alice (but not both).

Symmetric Key Cryptography



Symmetric Key cryptography: Bob and Alice share same (symmetric) key: K_s

- e.g., key is knowing substitution pattern in mono alphabetic substitution cipher

单字母

Q: How do Bob and Alice agree on key value?

Simple Encryption Scheme

Substitution Cipher*:* substituting one thing for another

- monoalphabetic cipher: substitute one letter for another

```
plaintext:   abcdefghijklmnopqrstuvwxyz
                ↓                     ↓
ciphertext:  mnbvcxzasdfghjklpoiuytrewq
```

e.g.:

```
Plaintext: bob. i love you. alice
ciphertext: nkn. s gktc wky. mgsbc
```

Encryption key: mapping from set of 26 letters to set of 26 letters

Symmetric Key Crypto: DES

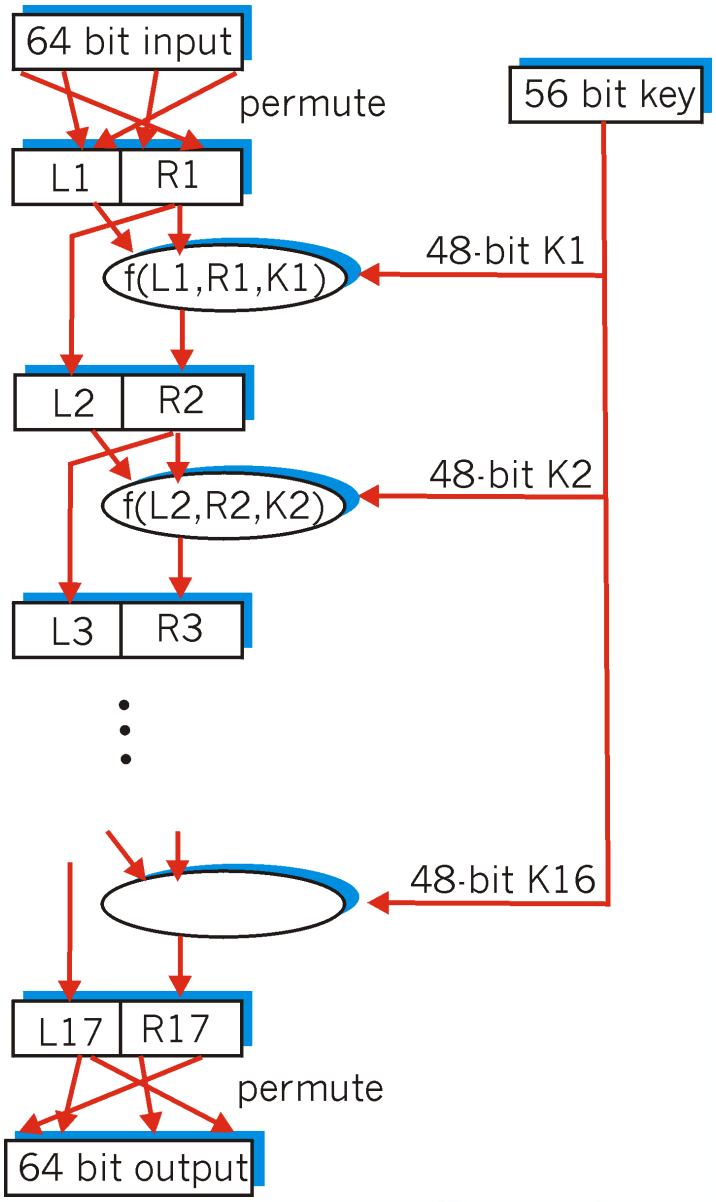
DES: Data Encryption Standard

- US encryption standard [NIST 1993]
- 56-bit symmetric key, 64-bit plaintext input
- Block cipher with cipher block chaining
- How secure is DES?
  - DES Challenge: 56-bit-key-encrypted phrase decrypted (brute force) in less than a day!
  - No known good analytic attack
- Making DES more secure:
  - 3DES: encrypt 3 times with 3 different keys

Symmetric Key Crypto: DES

DES Operation

- Initial permutation
- 16 identical “rounds” of function application, each using different 48 bits of key
- Final permutation



AES: Advanced Encryption Standard

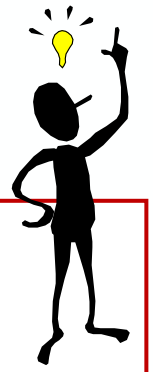
- Symmetric-key NIST standard, replaced DES (Nov 2001)
- Processes data in 128 bit blocks
- 128, 192, or 256 bit keys
- Brute force decryption (try each key) taking 1 second on DES, takes 149 trillion years for AES

Public Key Cryptography

Symmetric Key Crypto

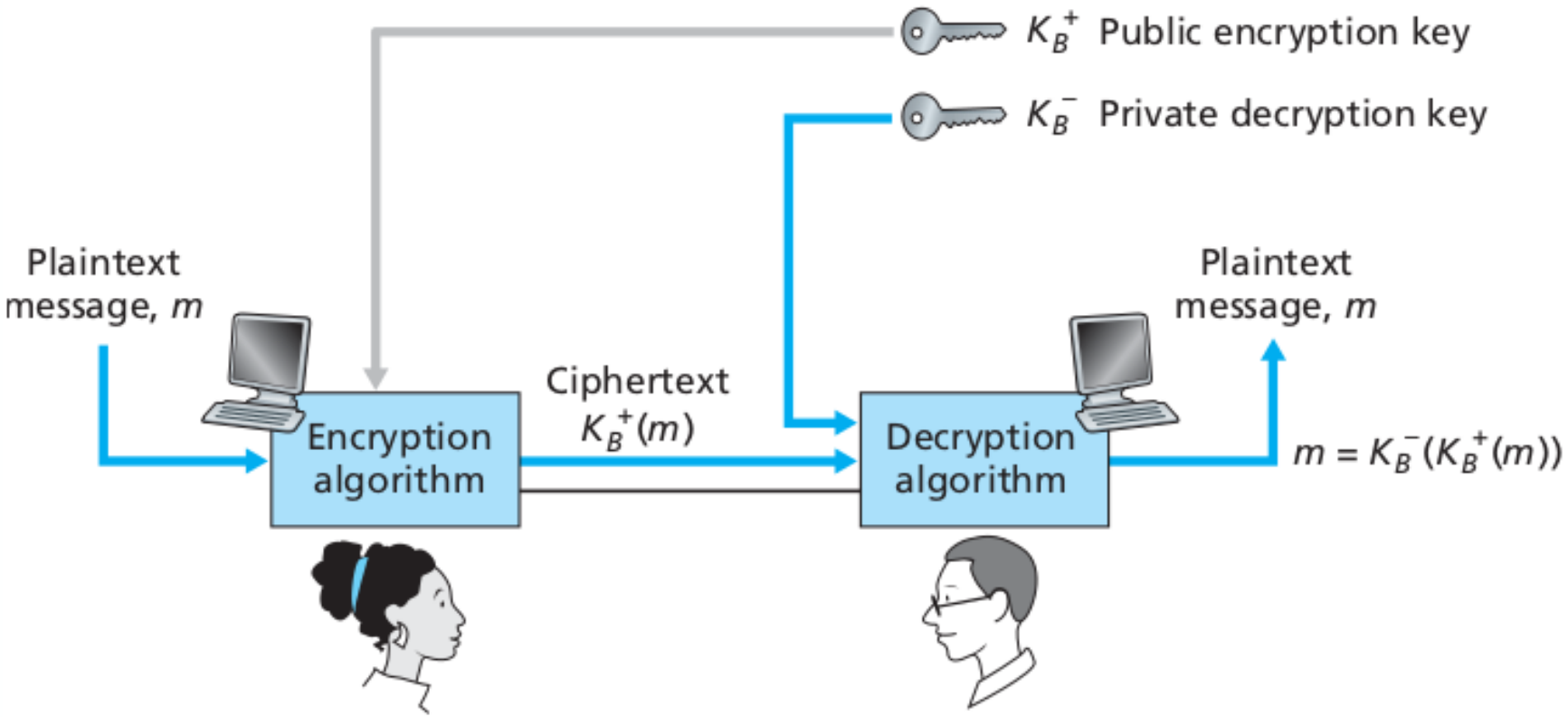
- Requires sender, receiver know shared secret key
- Q: How to agree on key in first place (particularly if never "met")?

~~Public Key Crypto~~



- Radically different approach [Diffie-Hellman76, RSA78]
- Sender, receiver do not share secret key
- Public encryption key known to All
- Private decryption key known only to receiver

Public Key Cryptography



Public Key Encryption Algorithms

Requirements:

1. Need $K_B^+(\cdot)$ and $K_B^-(\cdot)$ such that

$$K_B^-(K_B^+(m)) = m$$

2. Given public key K_B^+, it should be impossible to compute private key K_B^-

RSA: Rivest, Shamir, Adelson algorithm

Pre-Requisite: Modular Arithmetic

- x mod n = remainder of x when divided by n
- Facts:

  $[(a \bmod n) + (b \bmod n)] \bmod n = (a+b) \bmod n$
  $[(a \bmod n) - (b \bmod n)] \bmod n = (a-b) \bmod n$
  $[(a \bmod n) * (b \bmod n)] \bmod n = (a*b) \bmod n$
- Thus (from the last fact)

  $$(a \bmod n)^d \bmod n = a^d \bmod n$$

  Example: a=14, n=10, d=2:
  $(a \bmod n)^d \bmod n = a^d \bmod n$
  $\Rightarrow (14 \bmod 10)^2 \bmod 10 = 14^2 \bmod 10$
  $\Rightarrow 16 \bmod 10 = 196 \bmod 10 = 6$

RSA: Getting Ready!

- Message: just a bit pattern
- Bit pattern can be uniquely represented by an integer number
- Thus, encrypting a message is equivalent to encrypting a number.

Example:

- m = 10010001 . This message is uniquely represented by the decimal number 145.
- To encrypt m, we encrypt the corresponding number, which gives a new number (the ciphertext).

RSA: Creating Public/Private Key Pair

1. choose two large prime numbers *p*, *q*. (e.g., 1024 bits each)

2. compute $n = pq$, $z = (p-1)(q-1)$

3. choose e (with e<*n*) that has no common factors with z (e, z are "relatively prime").

4. choose *d* such that $ed - 1$ is exactly divisible by z. (in other words: $ed \bmod z = 1$).

5. *public* key is (*n*,e). *private* key is (*n*,*d*).

K_B^+ K_B^-

RSA: Encryption/Decryption

0. Given (*n*,*e*) and (*n*,*d*) as computed above

1. To encrypt message *m* (*<n*), compute

$$c = m^e \bmod n$$

2. To decrypt received bit pattern, *c*, compute

$$m = c^d \bmod n$$

Magic Happens!

$$m = \underbrace{(m^e \bmod n)}_{c}{}^d \bmod n$$

RSA: Encryption/Decryption – Example

Bob chooses *p=5, q=7*. Then *n=35, z=24*.
e=5 (so *e*, *z* relatively prime).
d=29 (so *ed-1* exactly divisible by z).

Plaintext Letter	*m*: numeric representation	m^e	Ciphertext $c = m^e \bmod n$
l	12	248832	17
o	15	759375	15
v	22	5153632	22
e	5	3125	10

Table 8.2 ♦ Alice's RSA encryption, $e = 5$, $n = 35$

Ciphertext *c*	c^d	$m = c^d \bmod n$	Plaintext Letter
17	481968572106750915091509141182522307169 7	12	l
15	127834039403948858939111232757568359375	15	o
22	851643319086537701956194499721106030592	22	v
10	10000000000000000000000000000000	5	e

Table 8.3 ♦ Bob's RSA decryption, $d = 29$, $n = 35$

Why does RSA Work?

- Must show that $\mathbf{c^d \bmod n = m}$ where $c = m^e \bmod n$
- Fact: for any x and y: $x^y \bmod n = x^{(y \bmod z)} \bmod n$
  - where n= pq and z = (p-1)(q-1)
- Thus,

$$c^d \bmod n = (m^e \bmod n)^d \bmod n$$
$$= m^{ed} \bmod n$$
$$= m^{(ed \bmod z)} \bmod n$$
$$= m^1 \bmod n$$
$$= m$$

RSA: Another Important Property

The following property is *very* useful:

$$\underbrace{K_B^-(K_B^+(m))}_{\text{use public key first, followed by private key}} = m = \underbrace{K_B^+(K_B^-(m))}_{\text{use private key first, followed by public key}}$$

Result is the Same!

Why $K_B^-(K_B^+(m)) = m = K_B^+(K_B^-(m))$?

Follows directly from modular arithmetic:

$$(m^e \bmod n)^d \bmod n = m^{ed} \bmod n$$
$$= m^{de} \bmod n$$
$$= (m^d \bmod n)^e \bmod n$$

Why RSA is Secure?

- Suppose you know Bob's public key (n,e). How hard is it to determine d?
- Essentially need to find factors of n without knowing the two factors p and q
  - Fact: factoring a big number is hard!

RSA in Practice: Session Keys

- Exponentiation in RSA is computationally intensive
- DES is at least 100 times faster than RSA
- Use public key cryptography to establish secure connection, then establish second key – symmetric session key – for encrypting data.

Session Key, K_S

- Bob and Alice use RSA to exchange a symmetric key K_S
- Once both have K_S, they use symmetric key cryptography

Summary

In this lecture, we have been introduced to

- The basic principles of Network Security
- The principles of Cryptography
- Symmetric and Asymmetric Cryptography including DES, AES and RSA schemes.

References / Links

- Chapter #8: **Security in Computer Networks,** th Computer Networking: A Top-Down Approach (7 edition) by Kurose & Ross