CS 330: Network Applications & Protocols

Network Security

Galin Zhelezov
Department of Physical Sciences
York College of Pennsylvania

Overview of Network Security

- **What is Network Security?**
- **Principles of Cryptography**
- **Message Integrity, Authentication**
- **Operational Security: Firewalls and IDS**

Overview of Network Security

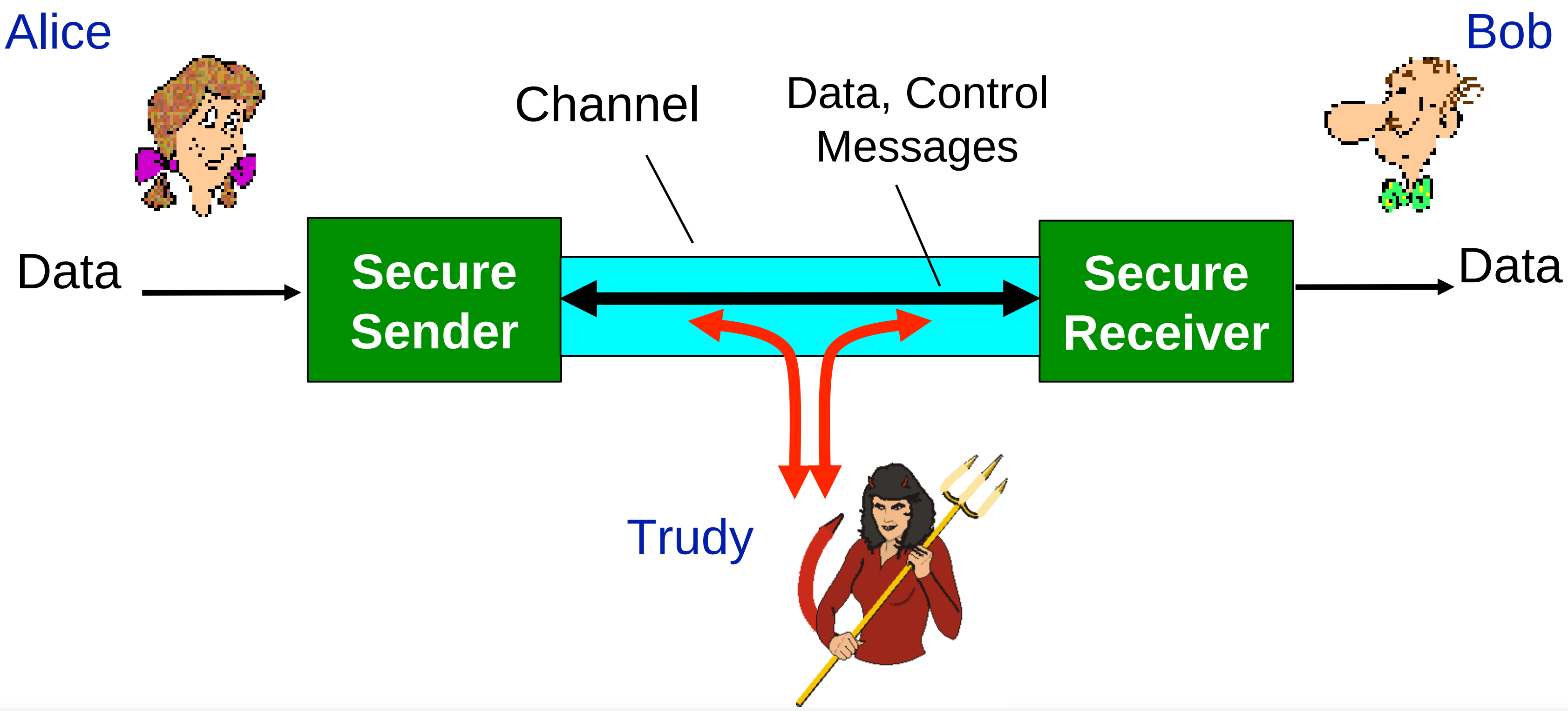
- **What is Network Security?**
- **Principles of Cryptography**
- **Message Integrity, Authentication**
- **Operational Security: Firewalls and IDS**

What is Network Security?

- **The following four items are desirable properties of secure communication:**
  - Confidentiality - only sender and intended receiver should “understand” message contents
    - Sender encrypts message
    - Receiver decrypts message
    - Eavesdropper should not be able to understand message
  - End-point Authentication - sender and receiver want to confirm identity of each other
    - Am I really talking to who I think I’m talking to?
  - Message Integrity - sender and receiver want to ensure message is not altered (in transit, or afterwards) without detection
  - Operational Security - services must be accessible and available to users
    - Protect network from downtime through redundancy
    - Protect network from attacks with firewalls, intrusion detection systems, etc.

Network Security

- **Bob and Alice want to communicate "securely" to prevent others from understanding their communication**
- **Trudy, the intruder, may intercept, delete, add messages**
  - Bob and Alice want to be able to detect changes made by an intruder
  - Bob and Alice don't want the intruder to be able to understand their messages



Network Security

- **In previous example:**
  - Bob and Alice don’t necessarily have to represent ‘users’
  - Can represent any number of machines that need to communicate with each other
- **Other examples of machines that may want secure communication**
  - Web browser/server for electronic transactions (e.g., on-line purchases)
  - On-line banking client/server
  - DNS servers
  - Routers exchanging routing table updates

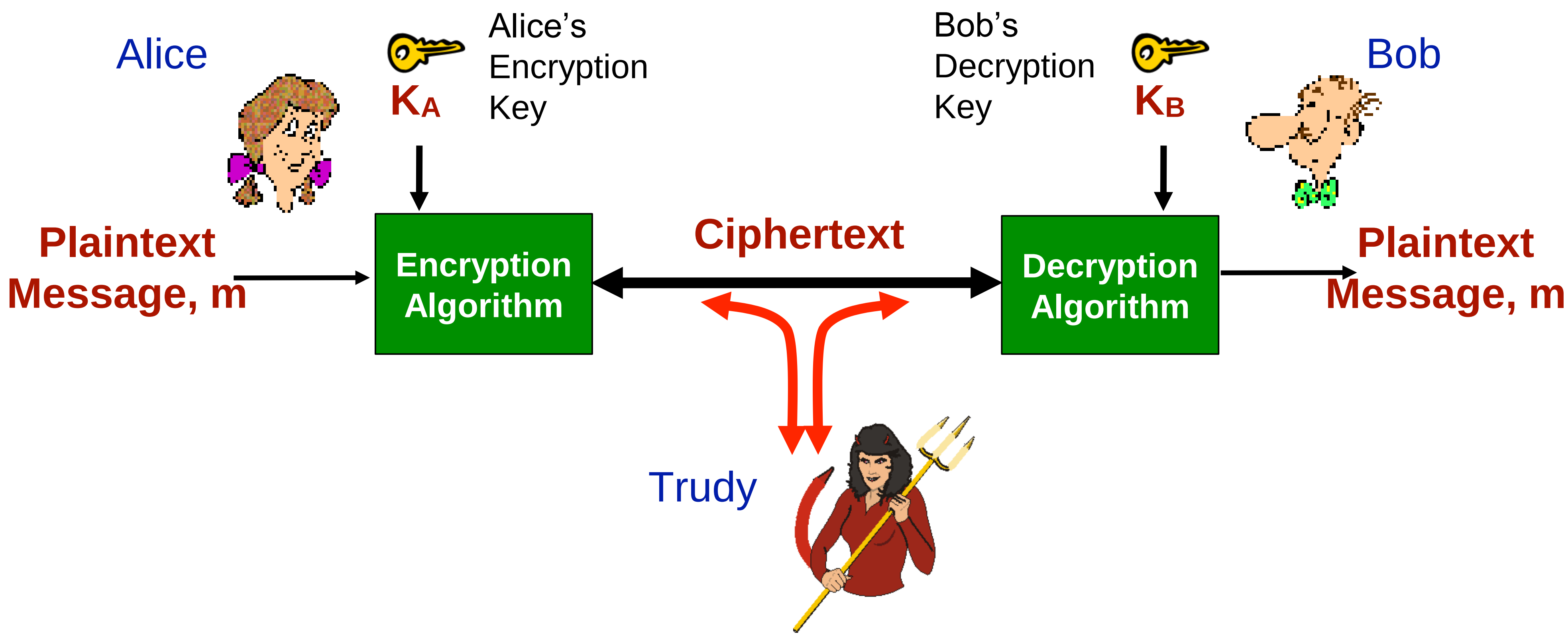
What Can an Intruder Do?

- **Eavesdrop - intercept or listen to messages**
- **Modification, Insertion, or Deletion of messages or message content**
- **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)**

Overview of Network Security

- **What is Network Security?**
- **Principles of Cryptography**
- **Message Integrity, Authentication**
- **Operational Security: Firewalls and IDS**

The Language of Cryptography



m - plaintext message

K_A(m) - ciphertext, encrypted with key **K_A**

m = K_B(K_A(m)) - original plaintext message can be recovered with **K_B**

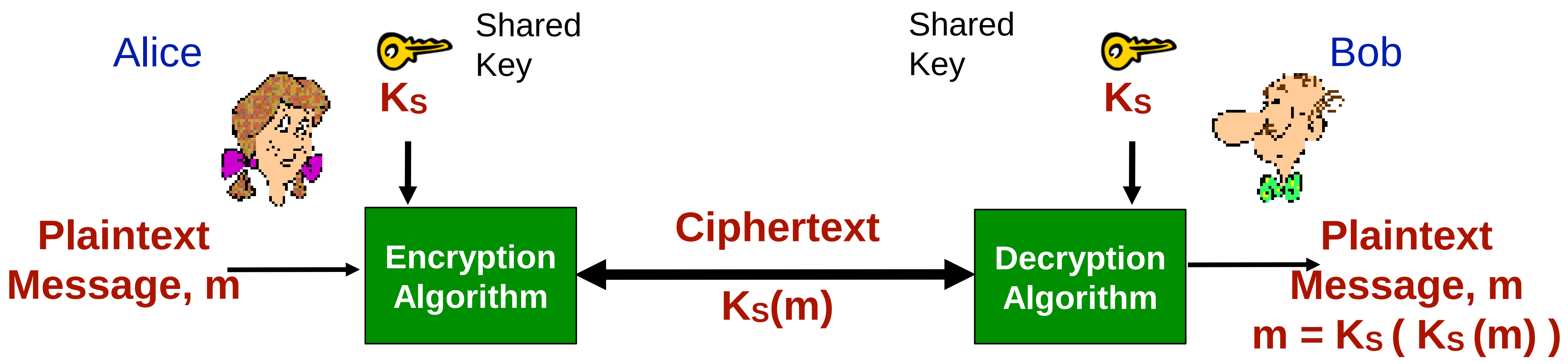
In **symmetric key systems**, both keys are the same

In **public key systems**, multiple keys are used:
- a shared public key, and
- a private key for each user

Breaking an encryption scheme

- **cipher-text only attack:** **Trudy has ciphertext she can analyze**
- **two approaches:**
  - brute force: search through all keys
  - statistical analysis
- **known-plaintext attack:** **Trudy has plaintext corresponding to ciphertext**
  - e.g., in monoalphabetic cipher, Trudy determines pairings for a,l,i,c,e,b,o,
- **chosen-plaintext attack:** **Trudy can get ciphertext for chosen plaintext**

Symmetric Key Cryptography



- **Symmetric Key Cryptograph - Bob and Alice share the same (symmetric) key K_S**
  - Key may be a simple substitution pattern in monoalphabetic substitution cipher
- **How should Bob and Alice agree on a key?**
- **How should Bob and Alice exchange the shared key?**

Simple Encryption Scheme

- **Substitution cipher - substituting one thing for another**
  - Monoalphabetic cipher substitutes one letter for another
- **Encryption key is the mapping from set of 26 letters to set of 26 letters**

```
plaintext:   abcdefghijklmnopqrstuvwxyz

ciphertext:  mnbvcxzasdfghjklpoiuytrewq
```

- **Example:**

```
hello world

acggk rkogv
```

Pretty easy to break this type of cipher; same as crypto puzzles in weekly newspapers

A More Sophisticated Encryption Approach

- **Polyalphabetic encryption uses *n* monoalphabetic substitution ciphers**
  - Cycles through monoalphabetic ciphers in some pattern
    - For example, if *n*=4: M_1,M_3,M_4,M_3,M_2; M_1,M_3,M_4,M_3,M_2; ...
  - For each new plaintext symbol, use subsequent substitution pattern in cyclic pattern
    - For example, dog: d from M_1, o from M_3, g from M_4
    - Symbols may be substituted by ciphers throughout message
      - Much more difficult to break using crypto puzzle approach
- **Encryption key includes the *n* monoalphabetic substitution ciphers <u>and</u> the cyclic pattern in which they are applied**

Block Ciphers

- **Modern ciphers divide messages into k bit blocks and encrypt each of those block independently**
  - For small values of k, a simple lookup table is suitable

input	output	input	output
000	110	100	011
001	111	101	010
010	101	110	000
011	100	111	001

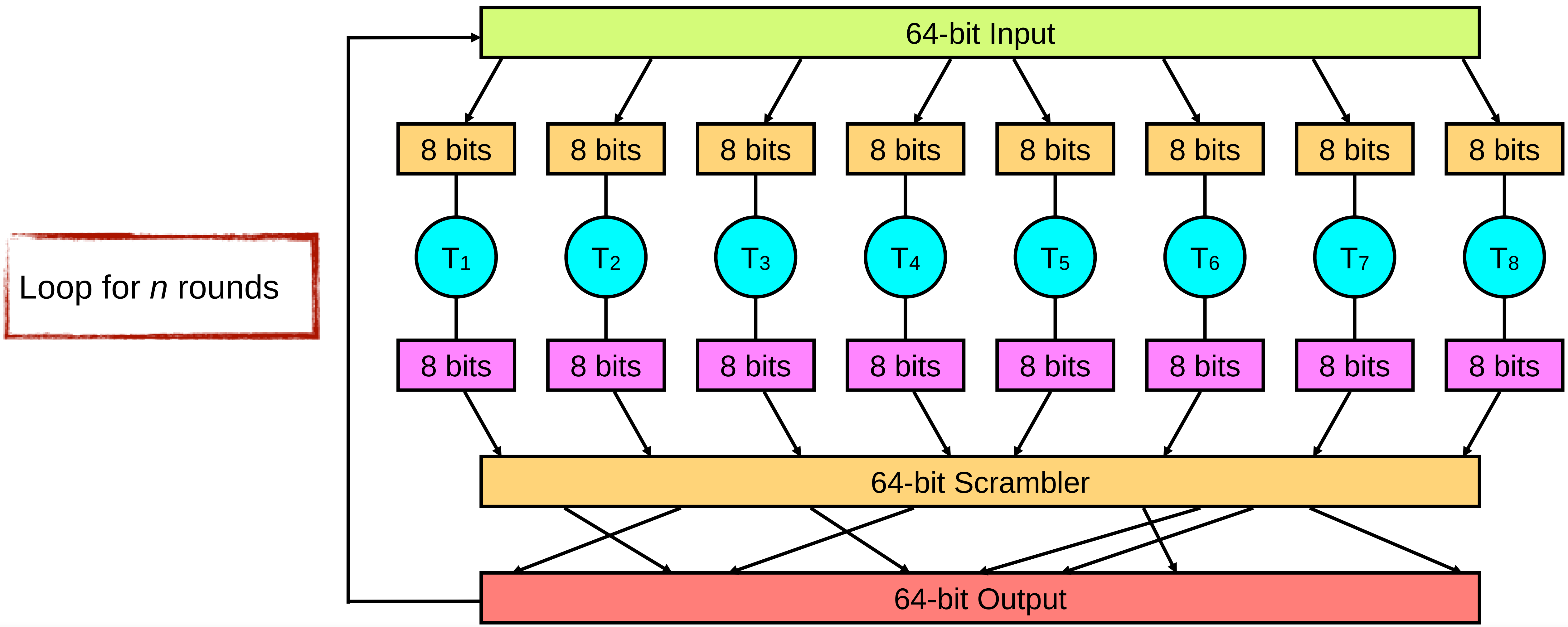
Simple 3-bit block cipher

  - For large values of k (i.e. k=64, k=128, etc.), a lookup table would be too large
    - Instead, modern ciphers use mathematical functions to simulate these tables

Block Ciphers (Cont.)

- **Example of a block cipher function**
  - Divide input blocks into smaller 8-bit chunks
  - Use smaller, more manageable 8-bit lookup tables
  - Scramble the bits and feed them back around to the input
  - Loop this *n* times such that each input bit can affect the output bits

This is similar to the approach used by DES and AES



Cipher Block Chaining

- **Since block cipher is a mathematical function, the same input will always produce the same output**
  - This is bad and provides an attack vector for an adversary
- **Cipher block chaining introduces randomness into the encrypted message using a randomly generated Initialization Vector (IV)**
  - IV is the same size as a block in the block cipher
  - The first block to be encrypted is XORed with the IV *before* being encrypted with the block cipher
    - The encrypted first block is XORed with second block to propagate randomness (output of second block is XORed with third, etc.)
  - IV is typically prepended as plaintext to encrypted message and sent along with message
    - Introduces a small overhead for sending encrypted messages
    - Receiver cannot decrypt the message without the IV

Common Block Cipher Algorithms

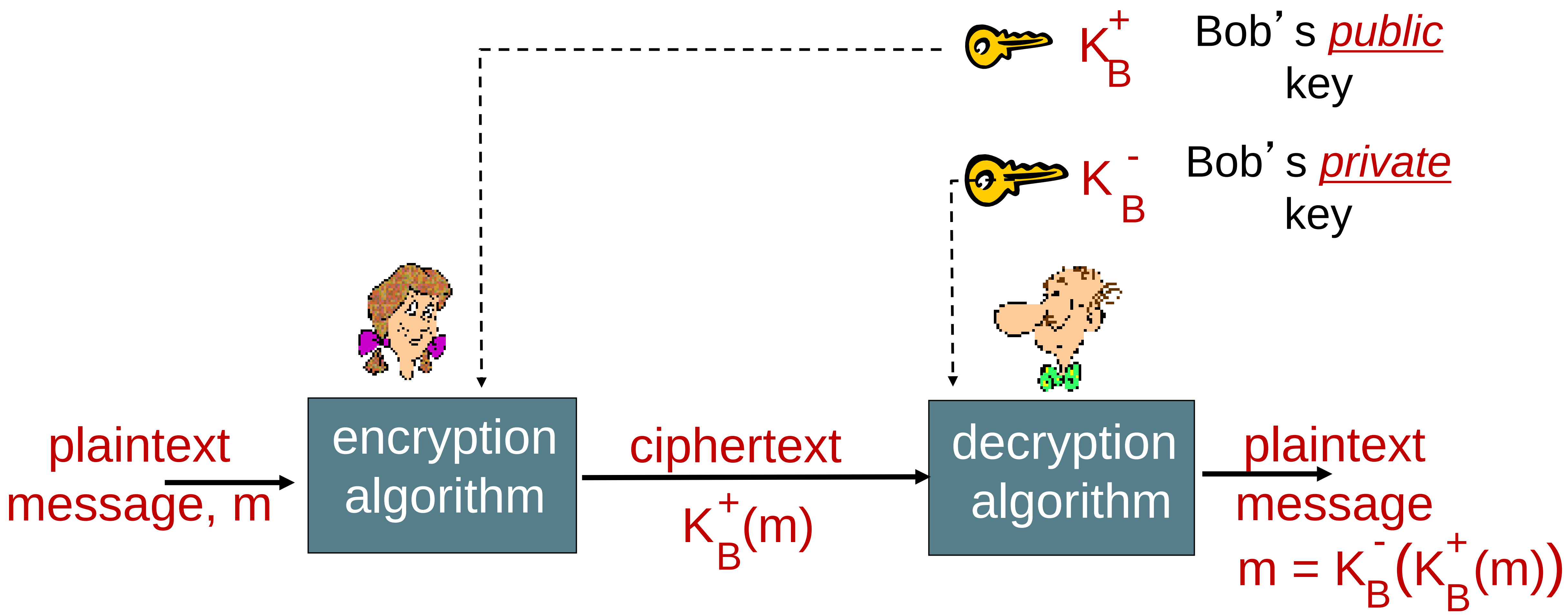
- **DES: Data Encryption Standard**
  - 56-bit symmetric key, 64-bit plaintext input
  - Block cipher with cipher block chaining
- **3DES: Triple Data Encryption Standard**
  - Same as DES, but encrypt message 3 times with 3 different keys
- **AES: Advanced Encryption Standard**
  - Replaced DES in most applications
  - Processes data in 128 bit blocks
  - 128, 192, or 256 bit keys

Nation Institute of Standards and Technology estimates that if theoretically had a machine that could crack DES in 1 second, it would take that same machine 149 trillion years to crack AES.

Public Key Cryptography

- **Symmetric Key Cryptography**
  - Requires sender and receiver to know a shared secret key
  - How should they agree on key in first place (particularly if never “met”)?
  - How should they share the key?
- **Public Key Cryptography**
  - Radically different approach
  - Sender and receiver do not share a secret key
  - Sender and receiver each have two keys: a shared public key and a private key
  - Public encryption key is known to all (even intruders)
  - Private decryption key known only to receiver

Public key cryptography



Public Key Cryptography (Cont.)

- **Sender determines a private key to use**
  - DOES NOT provide that private key to ANYONE
- **Receiver determines a private key to use**
  - DOES NOT provide that private key to ANYONE
- **Sender and receiver agree on a shared public key**
  - Does not matter if an intruder sees the shared public key
  - Public key can be exchanged over an unsecured channel
  - Great video provides general idea of how this works (Diffie Hellman key exchange)
    - http://www.youtube.com/watch?v=YEBfamv-_do

VIDEO:

http://www.youtube.com/watch?v=YEBfamv-_do

Diffie-Hellman Vulnerabilities

- **Does NOT provide authentication**
- **Vulnerable to man-in-the-middle attacks**
  - Intruder can establish one connection to Bob and another to Alice, intercept messages, re-encrypt and send
- **Another public key cryptography technique that avoids this problem is RSA**
  - Great video provides general idea of how RSA works
    - http://www.youtube.com/watch?v=wXB-V_Keiu8

Prerequisite: modular arithmetic

- **x mod n = remainder of x when divide by n**
- **facts:**

  [(a mod n) + (b mod n)] mod n = (a+b) mod n

  [(a mod n) - (b mod n)] mod n = (a-b) mod n

  [(a mod n) * (b mod n)] mod n = (a*b) mod n

- **thus**

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

- **example: x=14, n=10, d=2:**
  $(x \bmod n)^d \bmod n = 4^2 \bmod 10 = 6$
  $x^d = 14^2 = 196$ $x^d \bmod 10 = 6$

VIDEO:

http://www.youtube.com/watch?v=wXB-V_Keiu8

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 is RSA 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

Session Keys

- **Exponentiation required by RSA is time-consuming process**
- **DES and AES can encrypt messages much faster than RSA**
- **So ... don't use RSA to encrypt *entire* communication between sender and receiver**
  - Use RSA to establish a secure connection between sender/receiver
    - The only data exchanged using RSA is a session key
    - The session key is used as the encryption key for one of the faster symmetric key cryptography methods such as DES or AES
  - Remainder of communication between sender and receiver is encrypted using the faster symmetric key cryptography
- **Example:**
  - Bob and Alice use RSA to exchange a symmetric key K_S
  - Once both have K_S, they use symmetric key cryptography