COMP 3331/9331: Computer Networks and Applications

Week 9

Network Security

Reading Guide: Chapter 8: 8.1 – 8.2

Network Security: Overview

Our goals:

- understand principles of network security:
  - cryptography and its *many* uses beyond "confidentiality"
  - authentication
  - message integrity

Network Security: roadmap

8.1 What is network security?

8.2 Principles of cryptography

8.3 Message integrity

8.4 Authentication

8.5 Securing email

8.6 - 8.9 SSL, IPSec, Firewall/IDS not covered.

There are several security electives offered

What is network security?

confidentiality: only sender, intended receiver should "understand" message contents

- sender encrypts message
- receiver decrypts message

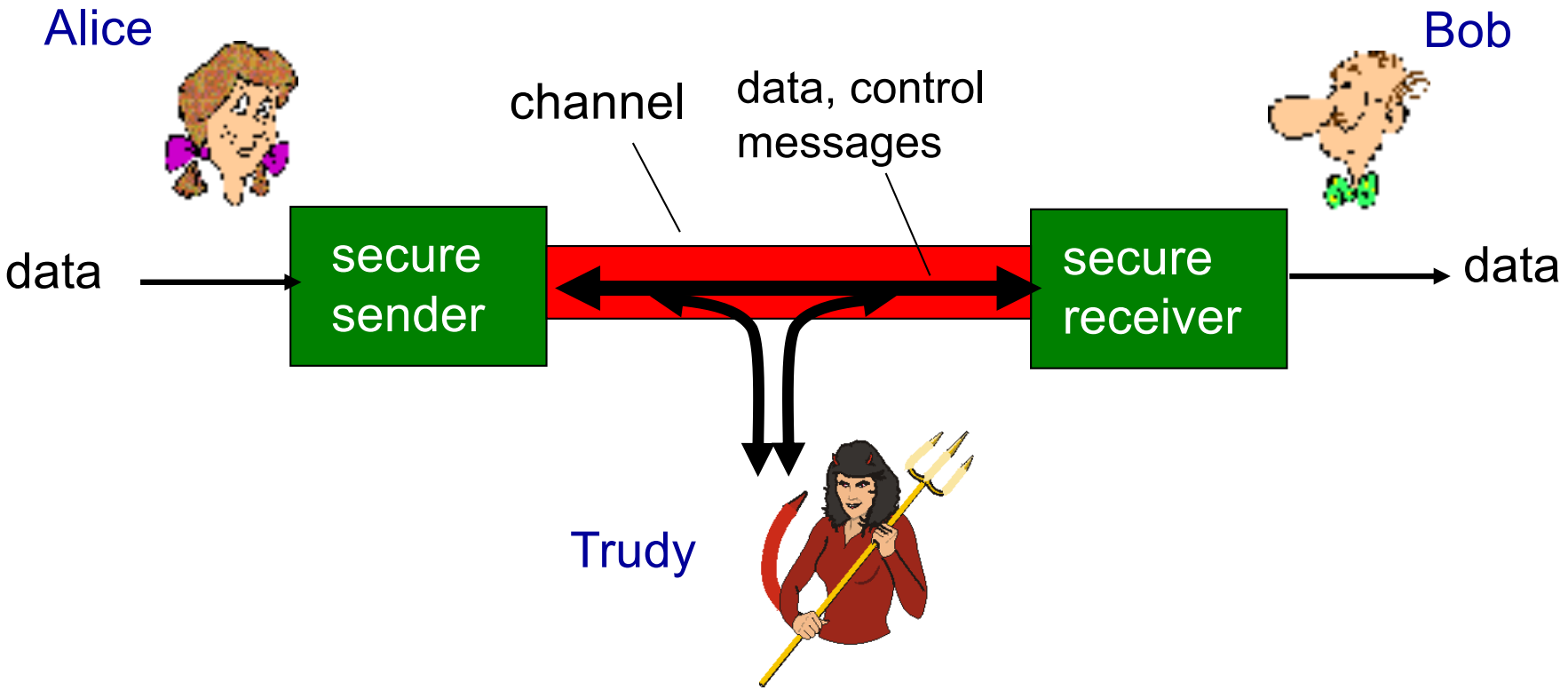
authentication: sender, receiver want to confirm identity of each other

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 (lovers!) 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
- etc.

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
- *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)

Network Security: roadmap

8.1 What is network security?

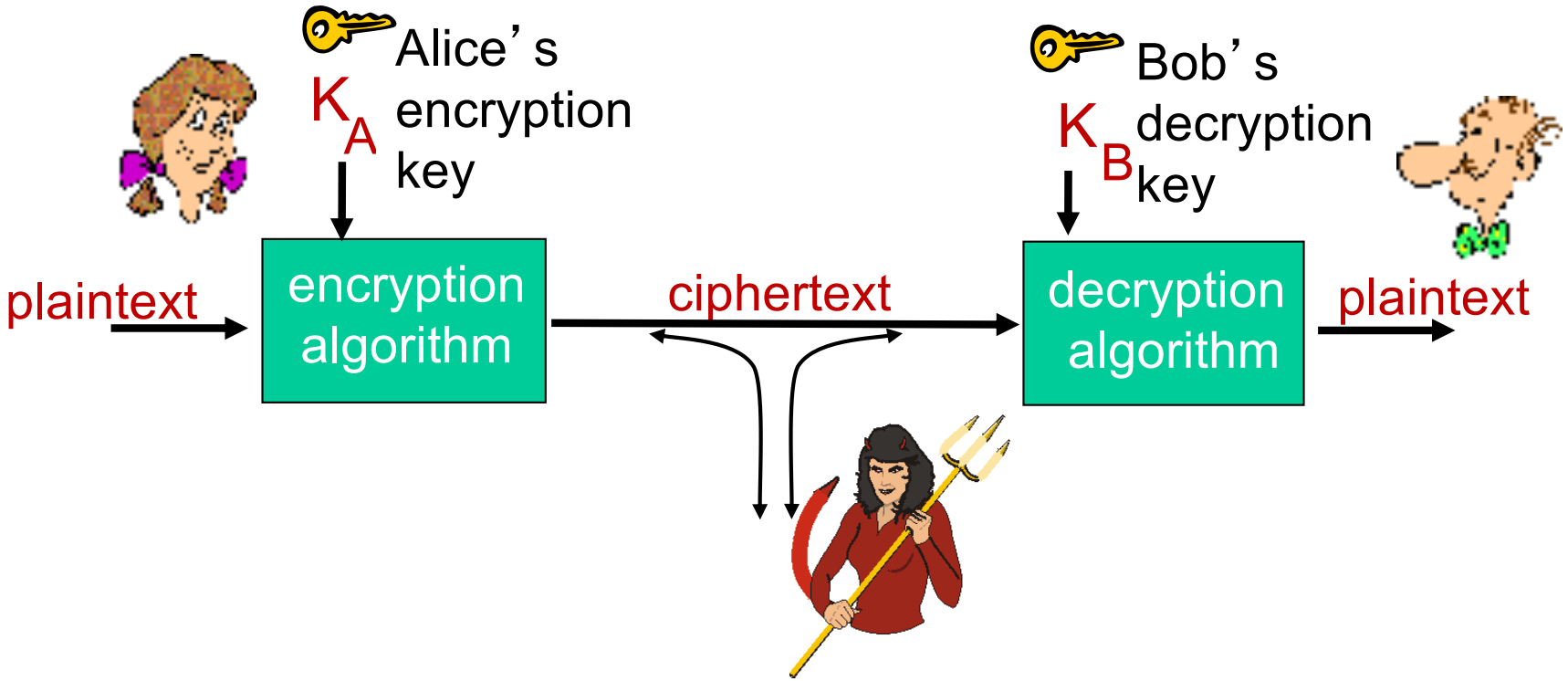
8.2 Principles of cryptography

8.3 Message integrity

8.4 Authentication

8.5 Securing email

The language of cryptography

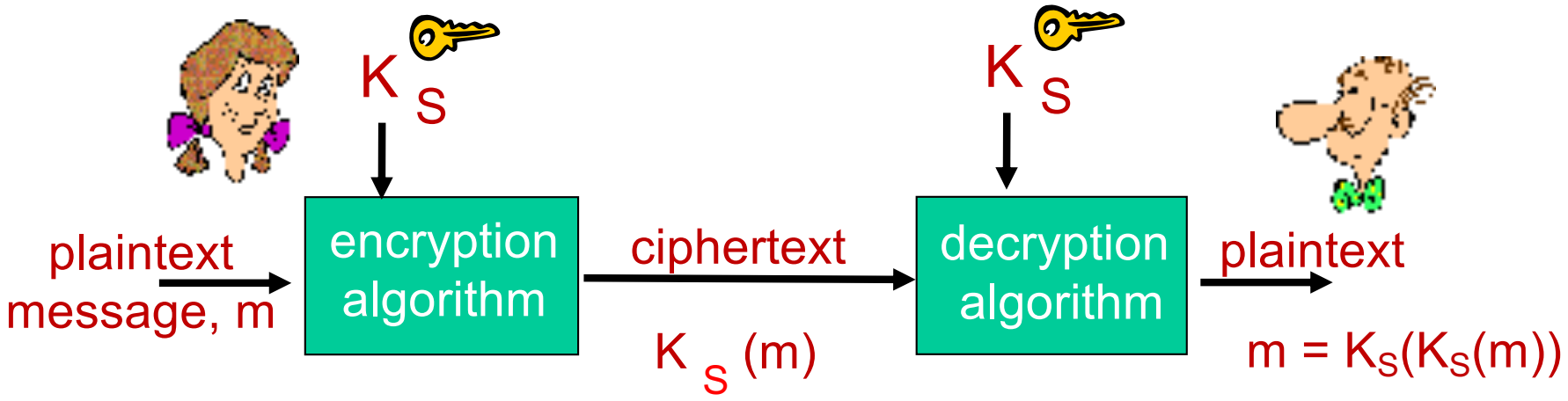


m plaintext message

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

$m = K_B(K_A(m))$

Symmetric key cryptography



symmetric key crypto: Bob and Alice share same (symmetric) key: K_S

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
- Ceaser Cipher: replace each letter of the alphabet with the letter standing three places further down the alphabet.

Plain : a b c d e f g h i j k l m n o p q r s t u v w x y z
cipher: d e f g h i j k l m n o p q r s t u v w x y z a b c

e.g.: **Plaintext: meet me after the party**

ciphertext: phhw ph diwhu wkh sduwb

Encryption key: c = (p+3) mod 26

Each plaintext letter p substituted by the ciphertext letter c
In general, we have c = (p+k) mode 26
where k is in range 1 to 25

Simple encryption scheme

- With only 25 possible keys, the Caeser cipher is vulnerable to brute force cryptanalysis
- Cipher can be any permutation of the 26 alphabet characters

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

e.g.:

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

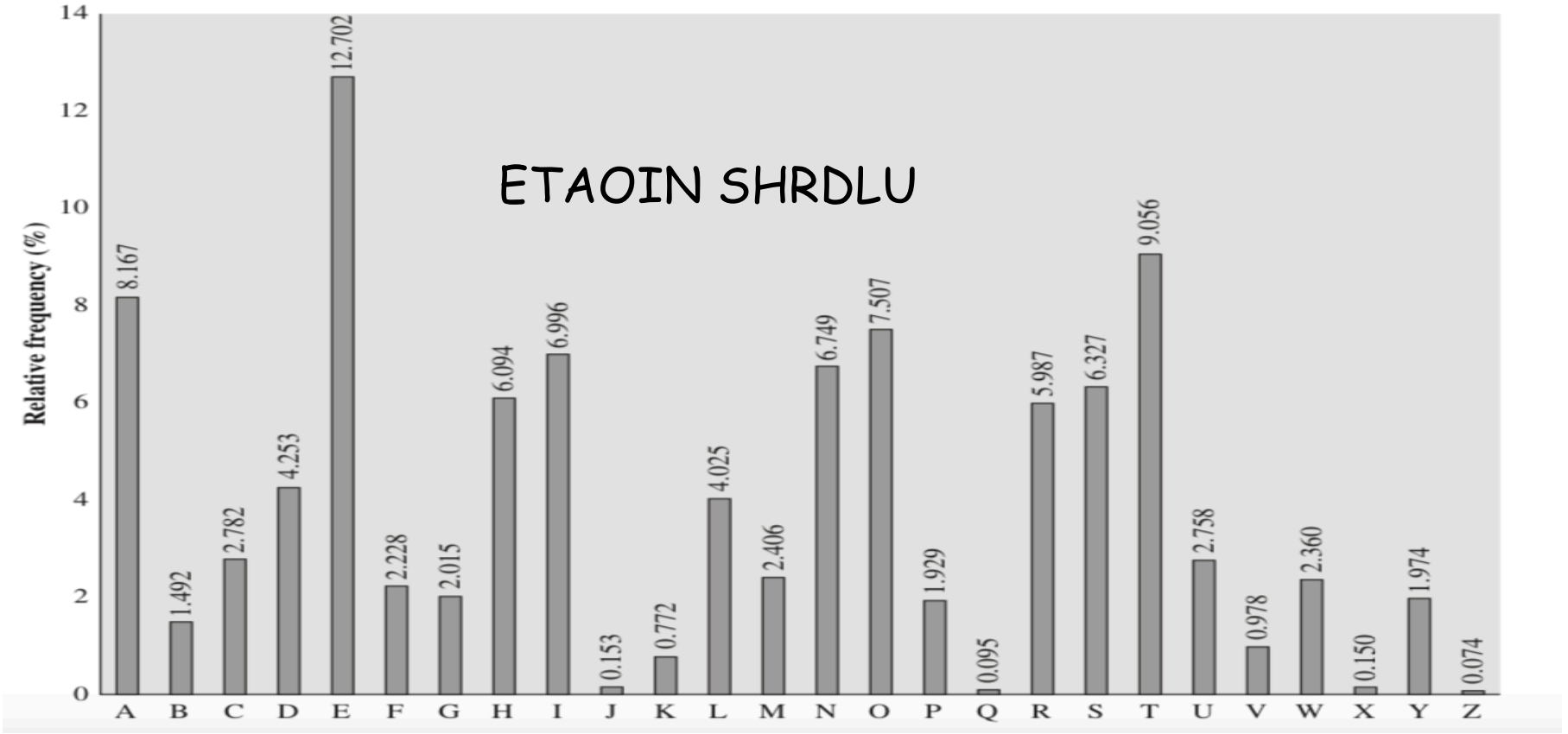
Encryption key: mapping from set of 26 letters to set of 26 letters

We have 26! (> 4 x10^{26}) possible keys

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 (part of) plaintext corresponding to ciphertext
  - e.g., in monoalphabetic cipher, Trudy determines pairings for a,l,i,c,e,b,o,b
- chosen-plaintext attack:
  Trudy can get ciphertext for chosen plaintext

Breaking an encryption scheme



Frequency Histogram Analysis for letters in English language

Monoalphabetic ciphers are easy to break because they reflect the frequency data of the original alphabet

A more sophisticated encryption approach

- Polyalphabet ciphers
- n substitution ciphers, $M_1,M_2,\ldots,M_n$
- cycling pattern:
  - e.g., n=4: and key is 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 subsitution pattern in cyclic pattern
  - dog: d from M_1, o from M_3, g from M_4

Encryption key: n substitution ciphers, and cyclic pattern

A more sophisticated encryption approach

- Vigen`ere Cipher
- 26 substitution ciphers with shifts of 0 through 25
- cycling pattern:
  - Assume Key consist of m sequence of letters
  - $(p_0 + k_0)$ mode 26, $(p_1 + k_1)$mode 26, …, $(p_{m-1} + k_{m-1})$ mode 26, $(p_m + k_0)$mode 26, $(p_{m+1} + k_1)$mode 26, …, $(p_{2m-1} + k_{m-1})$ mode 26, …
  - $(p_i + k_{i \bmod m})$ mod 26
- There are multiple ciphertext letters for each plaintext letter, one for each unique letter of the keyword