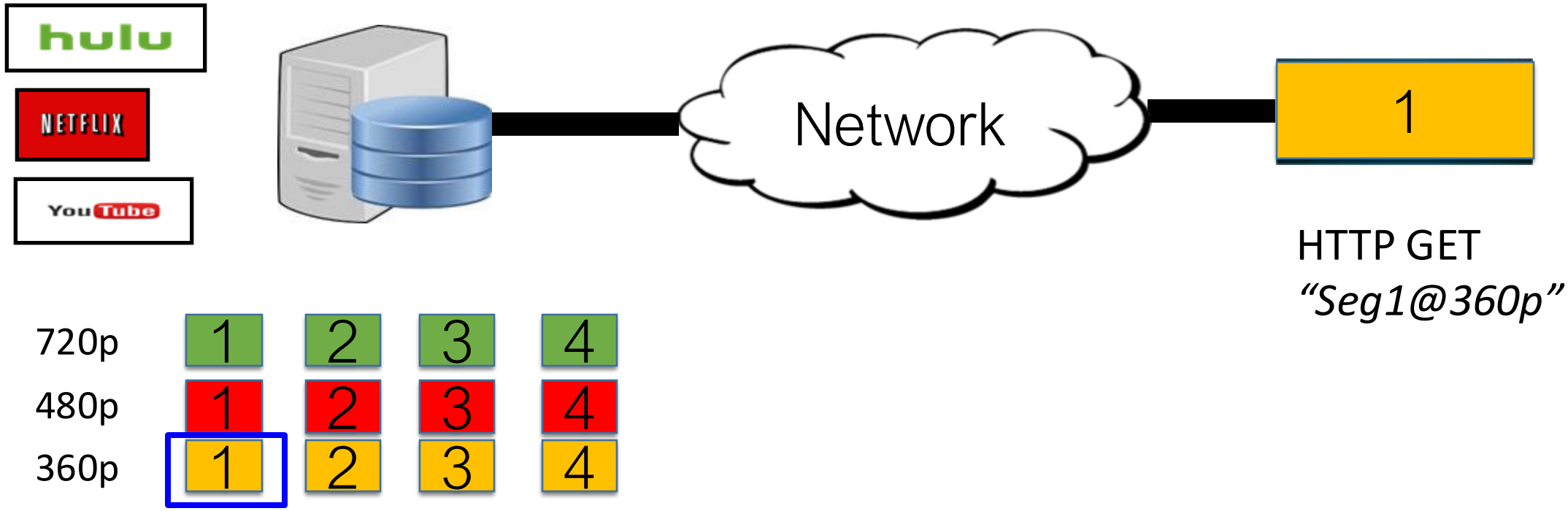
Computer Networks
COL 334/672

Video Streaming, Network Security

Slides adapted from KR

Sem 1, 2025-26

HTTP Adaptive Streaming (HAS): Recap



- *"intelligence"* at client: client determines
  - *when* to request chunk (so that buffer starvation, or overflow does not occur)
  - *what encoding rate* to request (higher quality when more bandwidth available) → Bitrate Adaptation

Rate-based Bitrate Adaptation Algorithm: Recap

Idea:

- Estimate network bandwidth based on the past download rate.
- Download chunk at a bitrate just less than the estimated network bandwidth

Algorithm

- **Estimation**: Take into account historical values, not just the last chunk throughput
- **Smoothing**: Apply a smoothing filter such as average, harmonic mean or EWMA
- **Quantization**: Select bitrate from the discrete set of bitrates based on estimated throughput

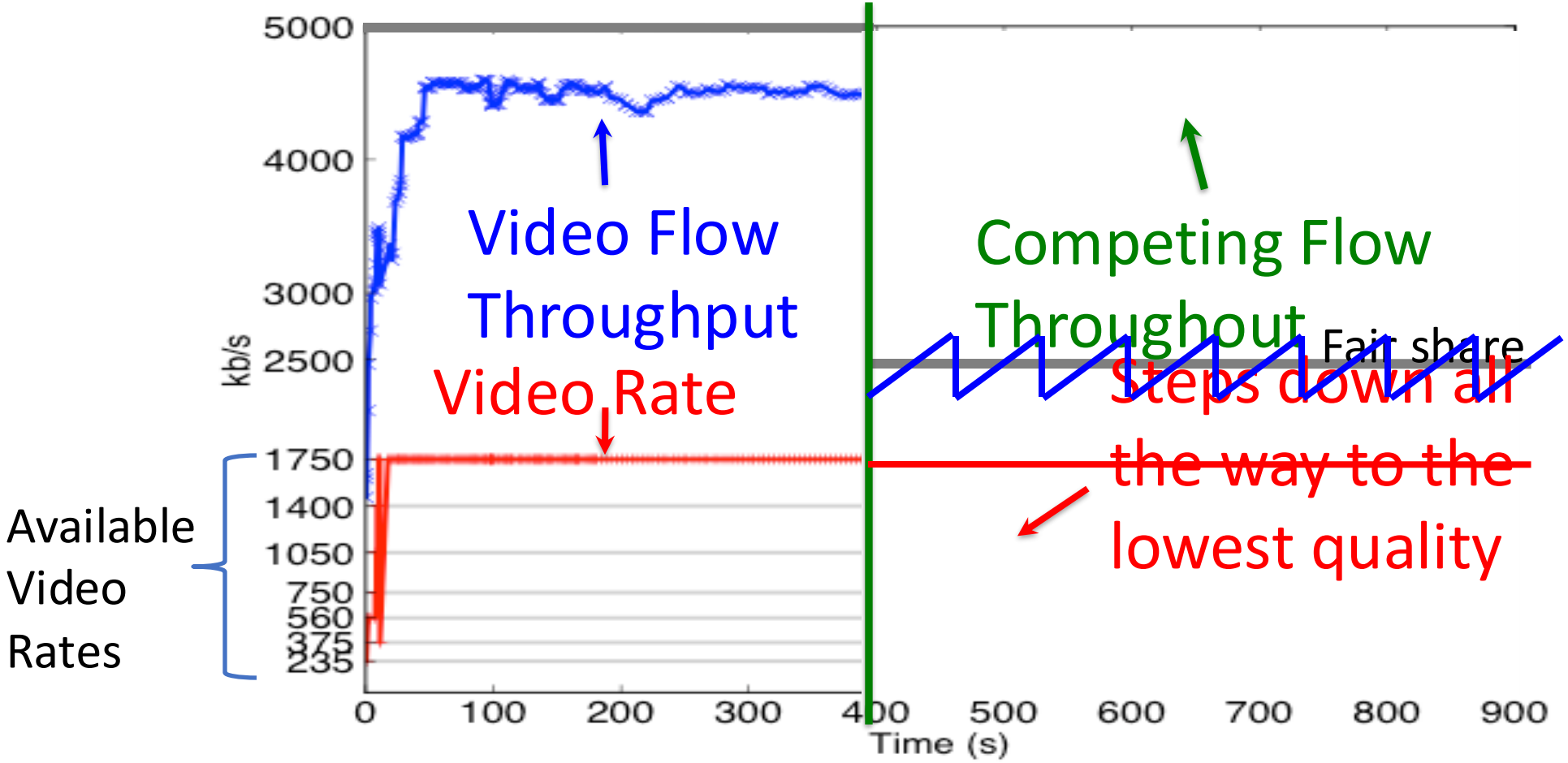
$$Est = \left(\frac{T_{past}}{1+\alpha} \right)$$

Pick highest bitrate $R \leq Est$

$$T_{past} = \frac{\text{Size of last chunk}}{\text{Time taken to download chunk}}$$

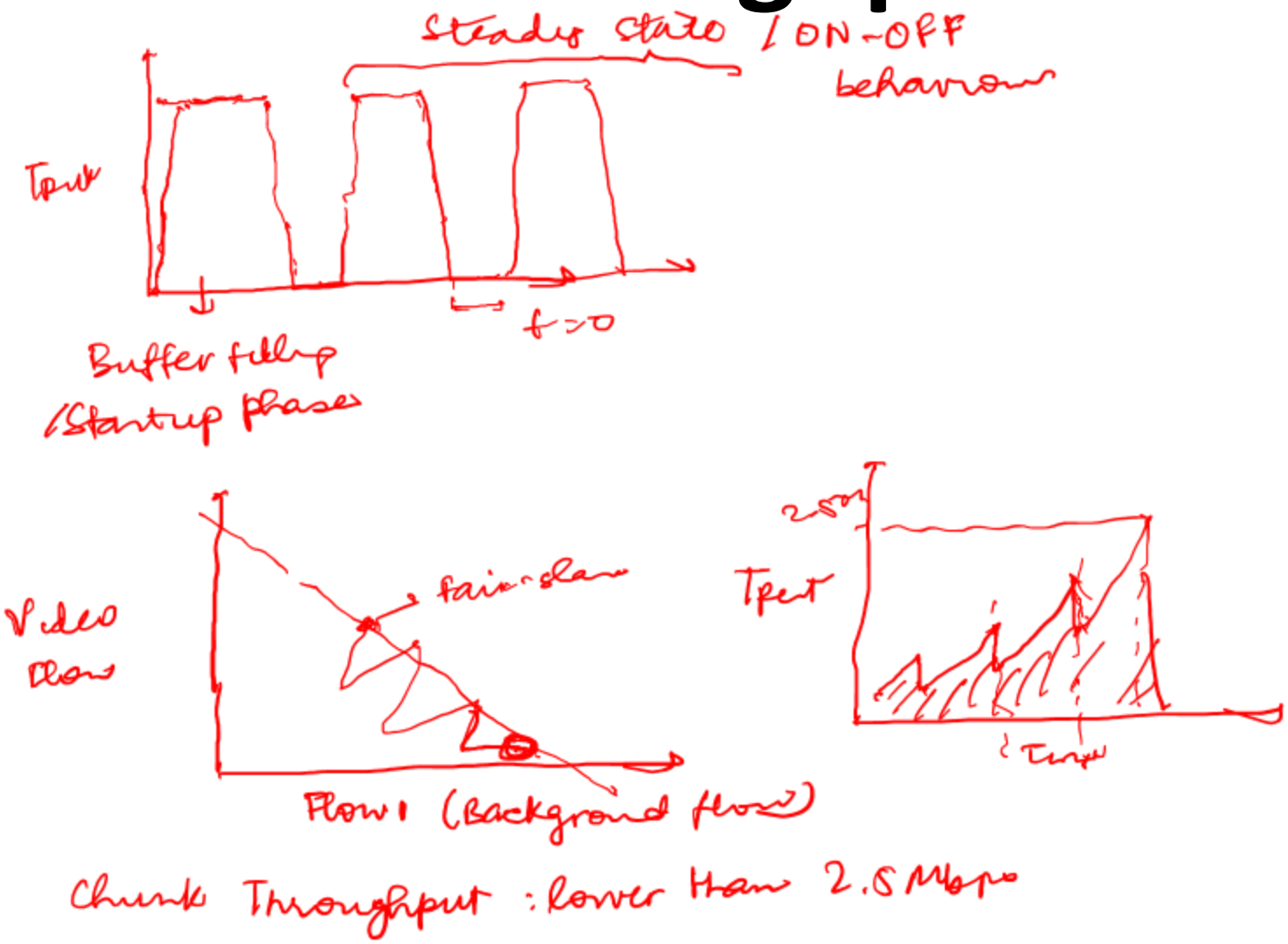
Issue with Rate-based Adaptation

- Poor interaction with the underlying TCP congestion control



Source: Confused, Timid and Unstable: Picking a Video Rate is Hard

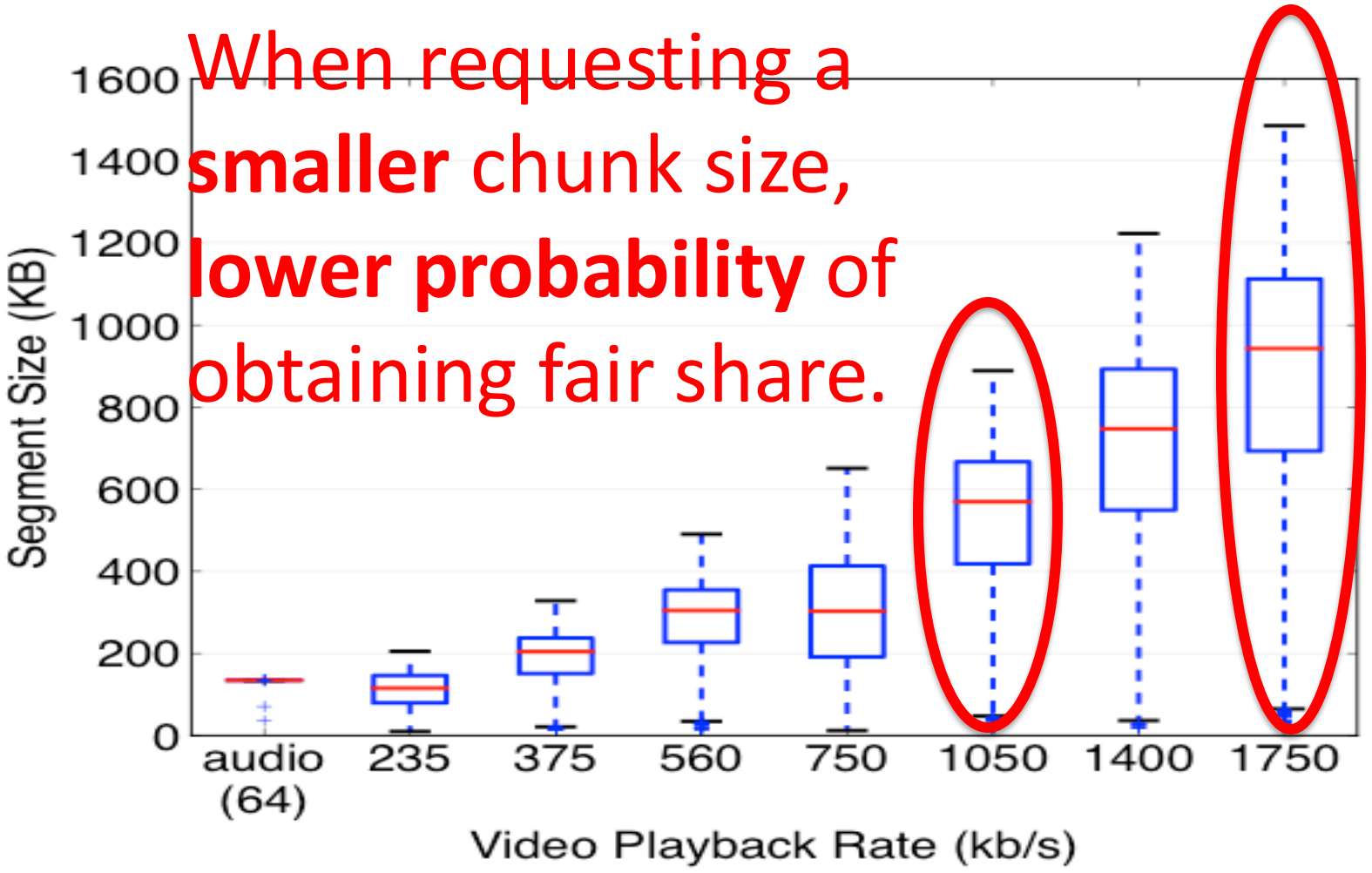
TCP Throughput of the Video Flow



- TCP sender resets its congestion window during OFF period
- Throughput will be affected especially with a competing flow
- Experience packet loss during slow start
- 50% of the segments get < 1.8Mb/s

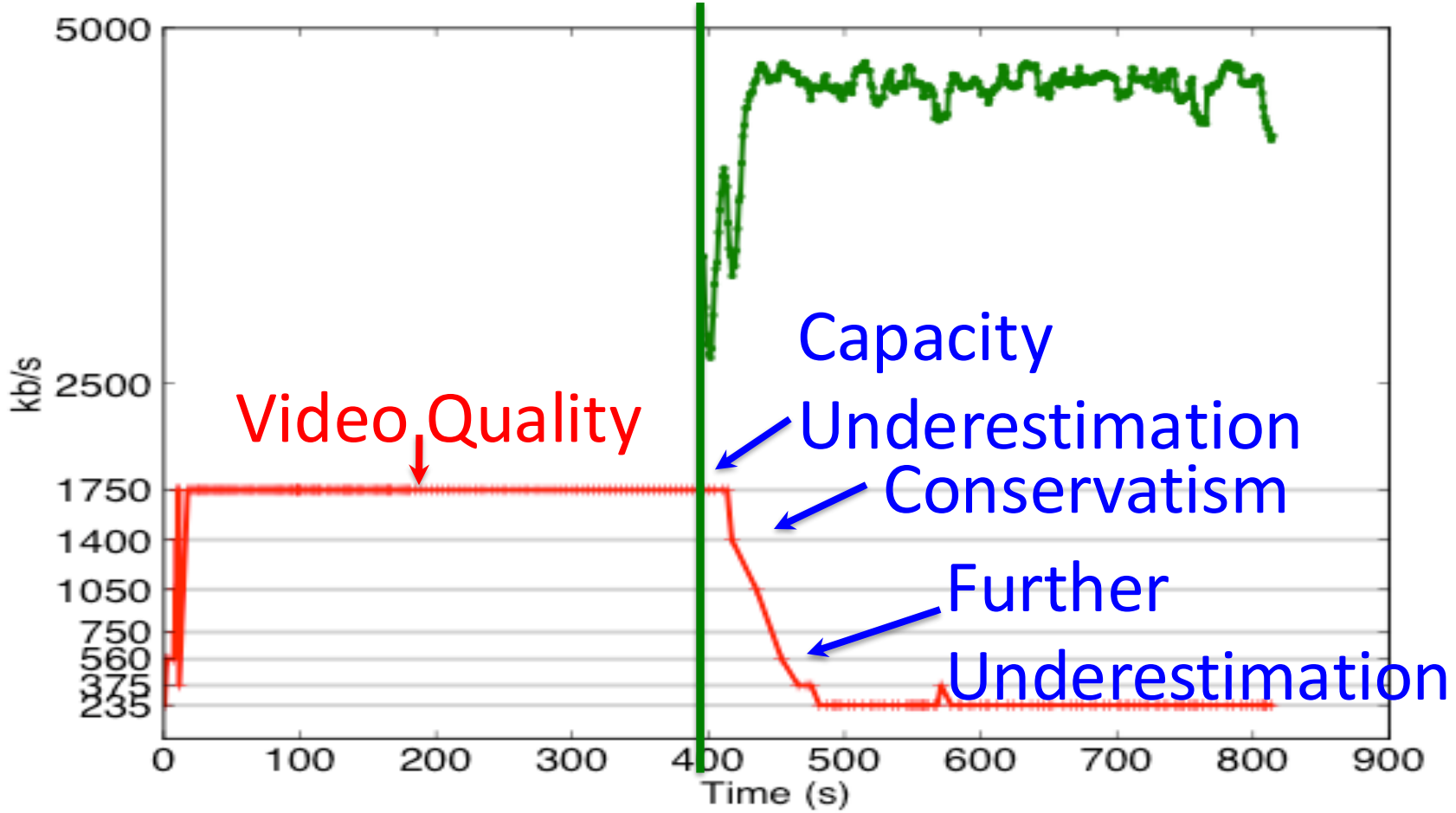
Source: Confused, Timid and Unstable: Picking a Video Rate is Hard

Smaller Chunk Size for Lower Video Rate



Source: Confused, Timid and Unstable: Picking a Video Rate is Hard

The Complete Story



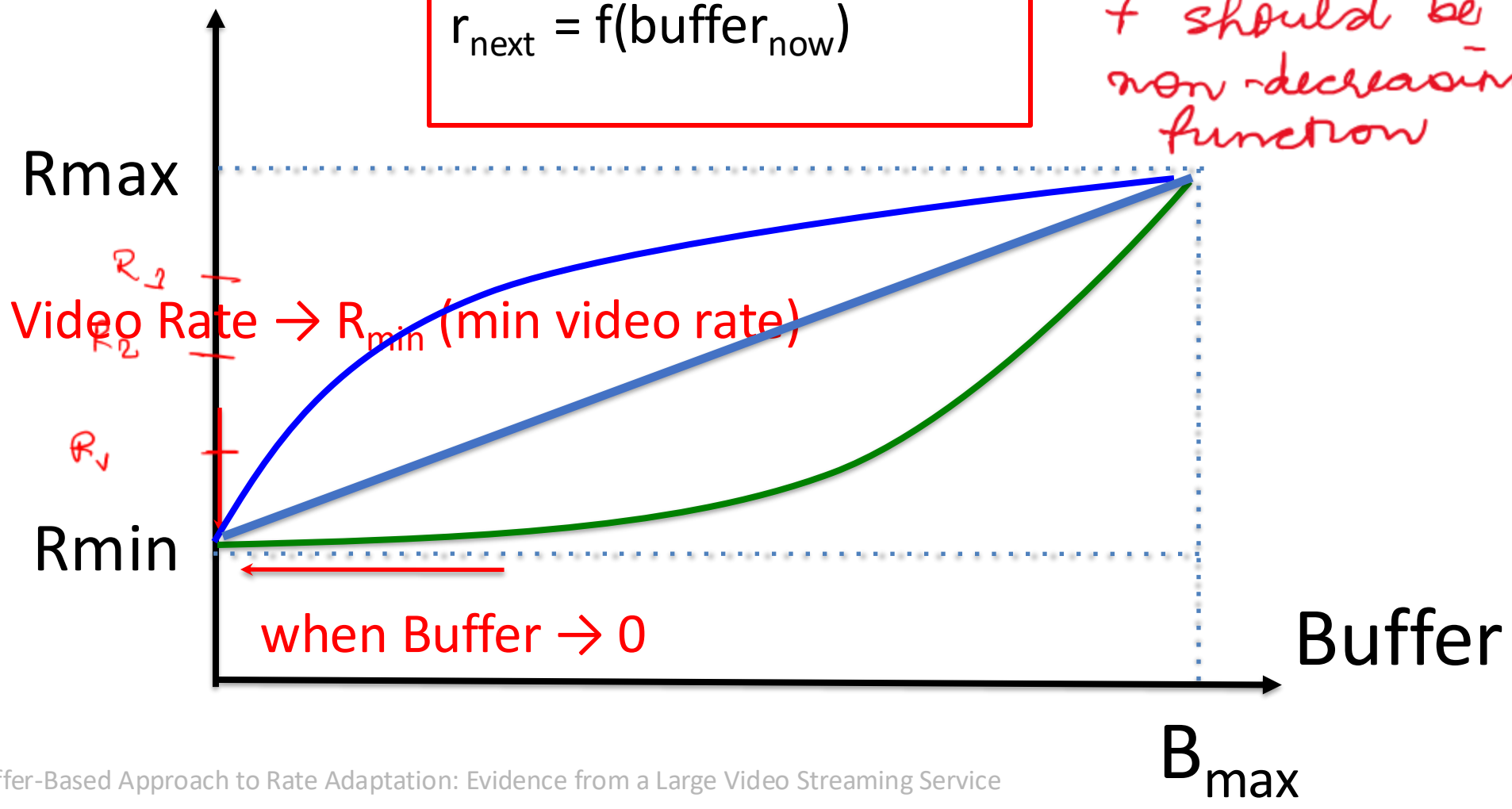
Being conservative can trigger a vicious cycle!

Source: Confused, Timid and Unstable: Picking a Video Rate is Hard

Buffer-based adaptation: Algorithm Sketch

$r_{next} = f(buffer_{now})$

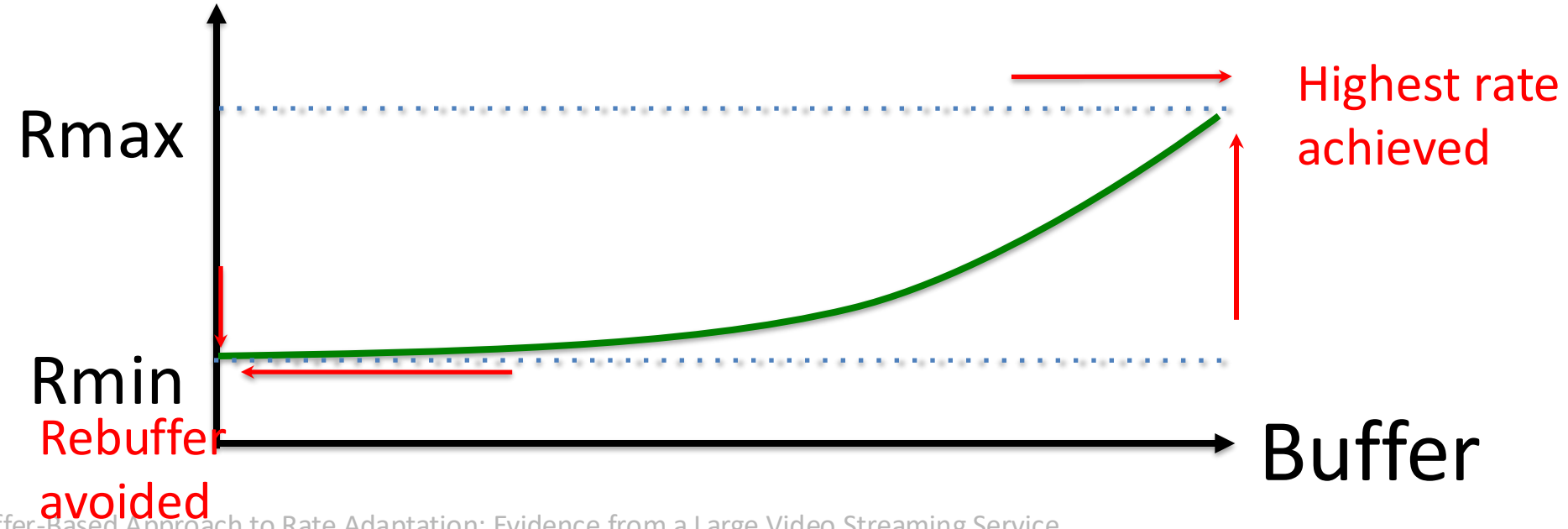
f should be a non-decreasing function



Source: A Buffer-Based Approach to Rate Adaptation: Evidence from a Large Video Streaming Service

Advantages of buffer-based adaptation

- Avoid “unnecessary” re-buffering
  - Reduce the bitrate as the buffer occupancy decreases
- Utilize the full capacity of the link
  - Avoid on-off behavior as long as the video quality is less than maximum
  - Request the highest video rate before the buffer is full



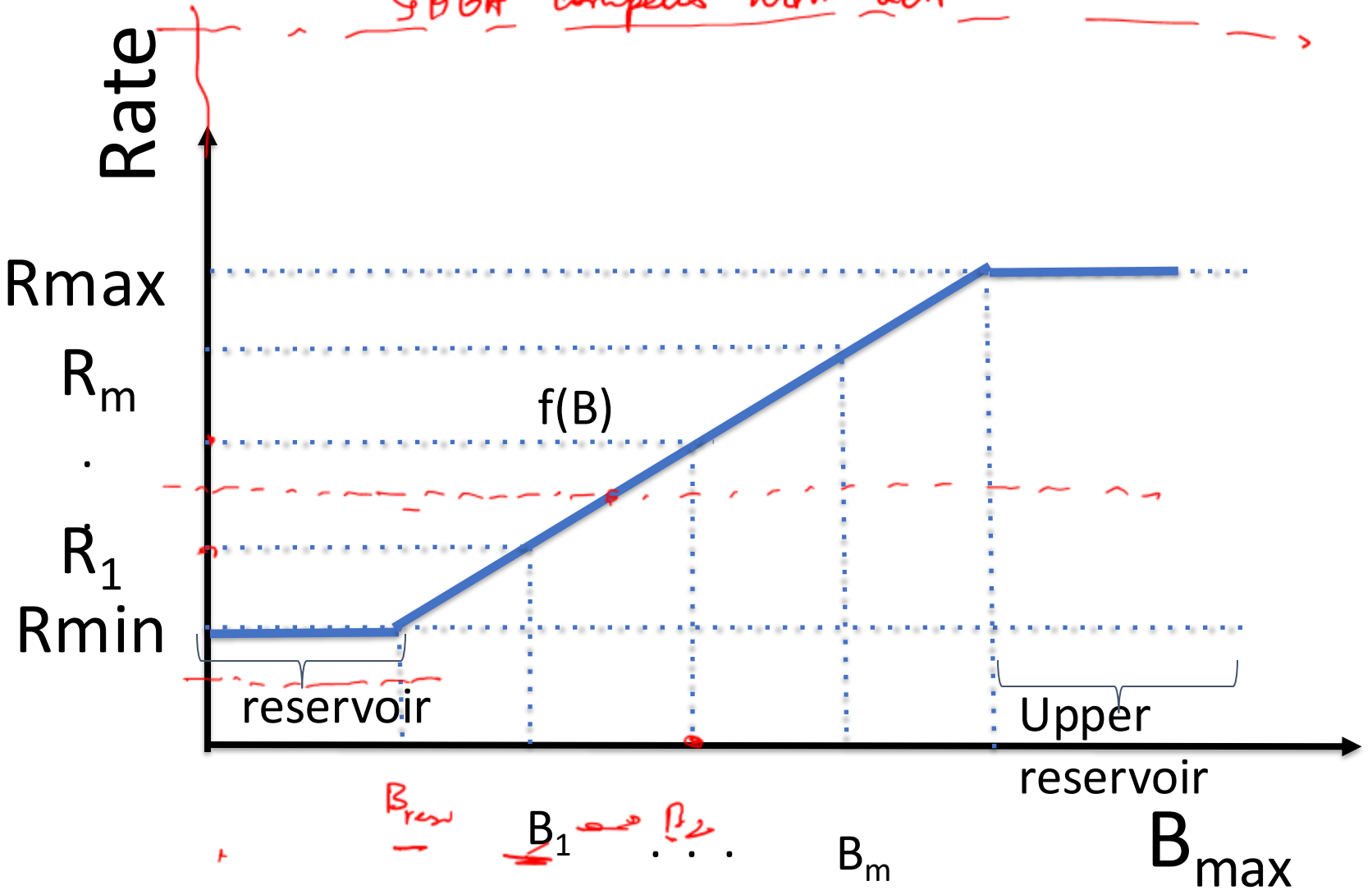
Source: A Buffer-Based Approach to Rate Adaptation: Evidence from a Large Video Streaming Service

BOLA : Handles small buffer sizes

Netflix

Buffer-based adaptation: Algorithm

↳ BBA competes with RBA



① Unnecessary bitrate oscillations

②. Bmax needs to be large enough (otherwise, unnecessary oscillations)

[Live streaming]

Bitrate Adaptation Algorithm and Congestion Control

- Fundamentally similar problems, rate control
- Differences:
  - Kind of signals that are available
  - Decision time scale
  - Optimization variable
- Like TCP congestion control, bitrate adaptation is also an active area of research

Network Security

- What: protecting network from an attack

Ransomware hits Telangana and Andhra Pradesh power department websites

Mahesh Buddi / TNN / Updated: May

The computer systems of Telangar
Ransomware attacked the systems
Officials in the Telangana power de

1.3 TB data encrypted and five servers affected in AIIMS ransomware attack: Centre

CERT-In and other stakeholder entities have advised necessary remedial measures, Minister tells Rajya Sabha

India Recorded 79 Million Cyber Attacks In 2023, Ranks 3rd Globally: Report

- Historical perspective: Internet was not designed with in mind (?)
  - Patches added to provide cybersecurity

What are the aspects of secure communication over the Internet?

User

User

Router 1

Public

Internet

Web server / DNS server

Manager / Parents /

Router 2

1. No data fudging (Message integrity)
   tampering
2. Confidentiality
3. End-points should be available (Denial-of-service)
4. Authentication

Anonymous communication

(ToR)

Covert communication

Aspects of network security

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

- sender encrypts message
- receiver decrypts message

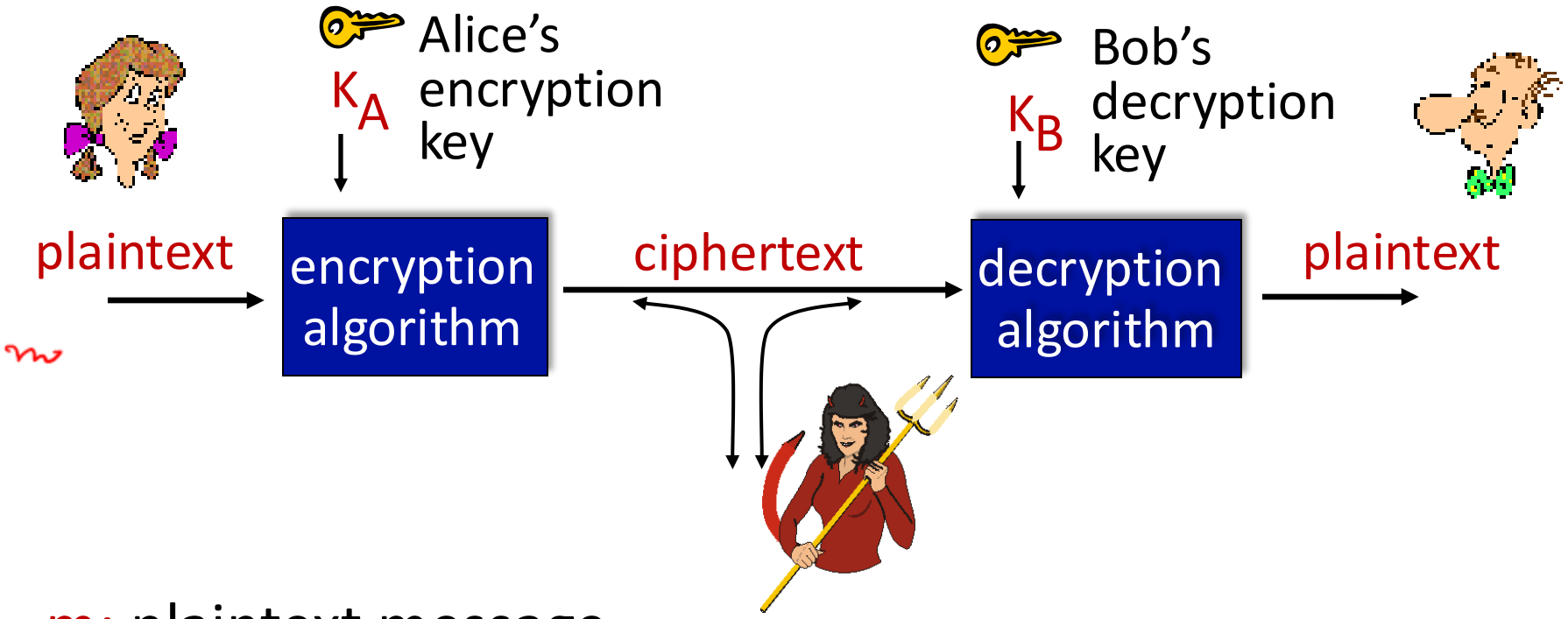
authentication: sender, receiver want to confirm identity of each other

message integrity: sender, receiver want to ensure message not altered (in transit, or afterwards) without detection

Cryptography

access and availability: services must be accessible and available to users

Principles of Cryptography



m: plaintext message

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

$m = K_B(K_A(m))$

$K_A \neq K_B$

$K_A = K_B$ [Symmetric key cryptography]

Asymmetric / Public key cryptography

Symmetric key cryptography (example)

Asymmetric + RSA

substitution cipher: substituting one thing for another

- monoalphabetic cipher: substitute one letter for another

Shared secret key

```
plaintext:   abcdefghijklmnopqrstuvwxyz
             |                       |
             v                       v
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

How will you break such encryption?

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