Lecture 13: Security

CS/ECE 438: Communication Networks

Prof. Matthew Caesar

April 23, 2010

Roadmap

- Requirements (Goals)
- Attacks
  - Denial of Service
  - Man-in-the-middle
  - Spam
  - Forged identity
- Countermeasures
  - Encryption
  - Filtering/CAPTCHAs

Security Requirements

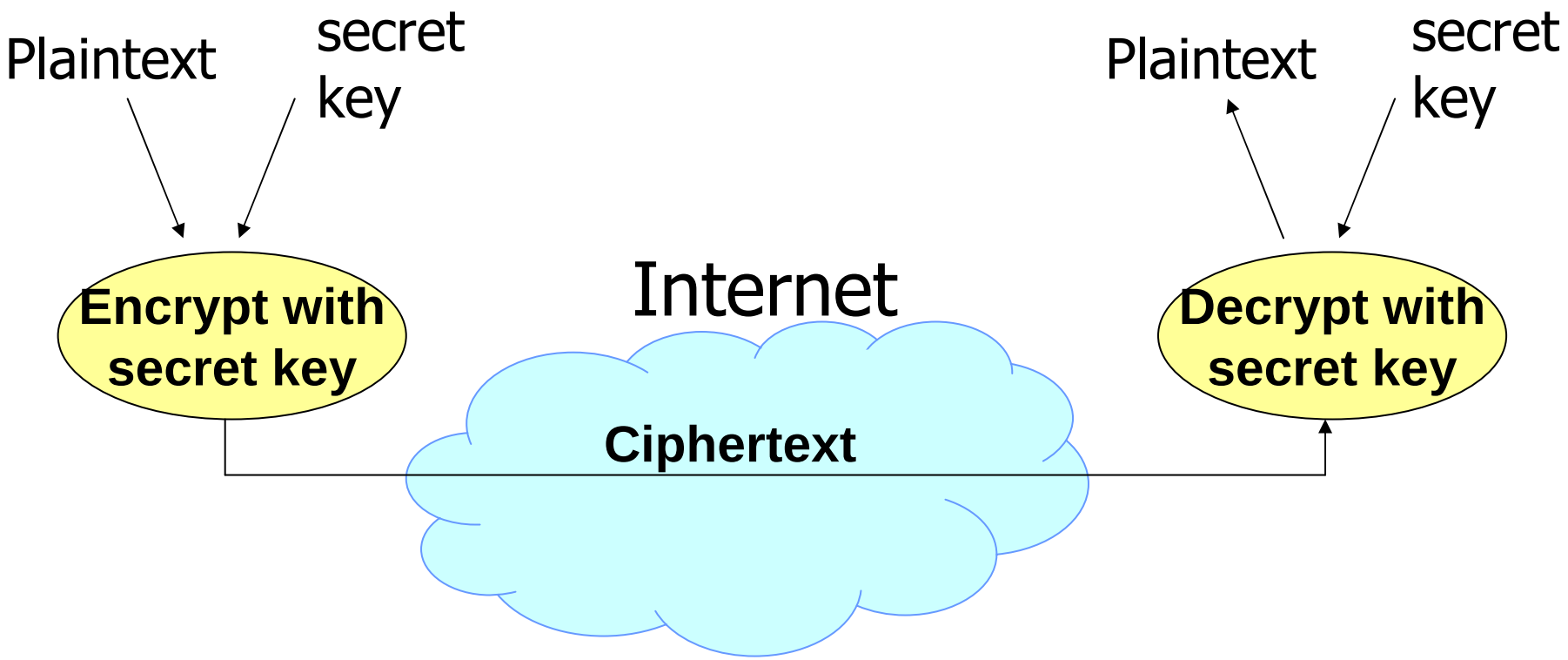
- Authentication
  - Ensures that the sender and the receiver are who they are claiming to be
- Data integrity
  - Ensure that data is not changed from source to destination
- Confidentiality
  - Ensures that data is read only by authorized users
- Non-repudiation
  - Ensures that the sender has strong evidence that the receiver has received the message, and the receiver has strong evidence of the sender identity, strong enough such that the sender cannot deny that it has sent the message, and the receiver cannot deny that it has received the message

Cryptographic Algorithms

- Security foundation: cryptographic algorithms
  - Secret key cryptography: Data Encryption Standard (DES)
  - Public key cryptography: RSA algorithm
  - Message digest: MD5 algorithm

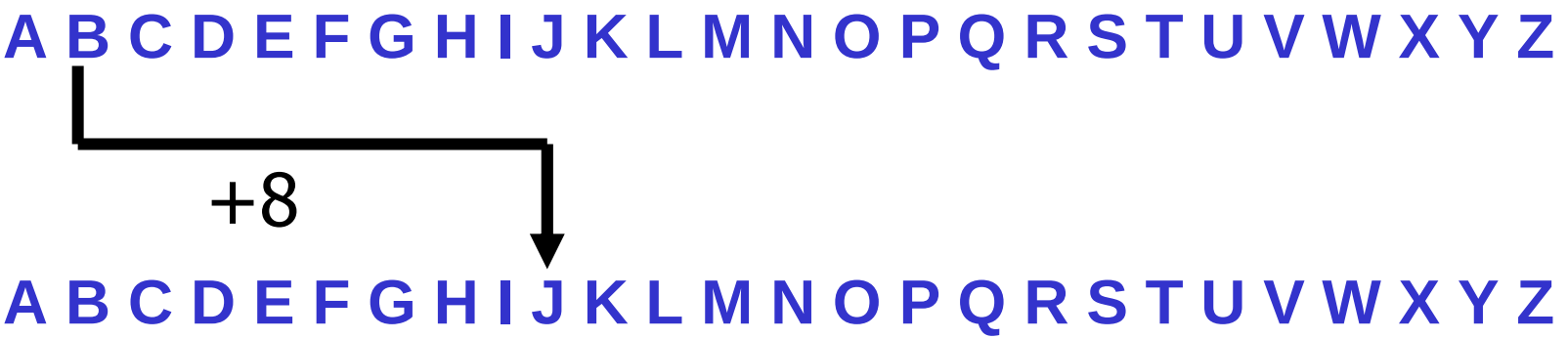
Symmetric Key Cryptography

- Both the sender and receiver use the same secret keys



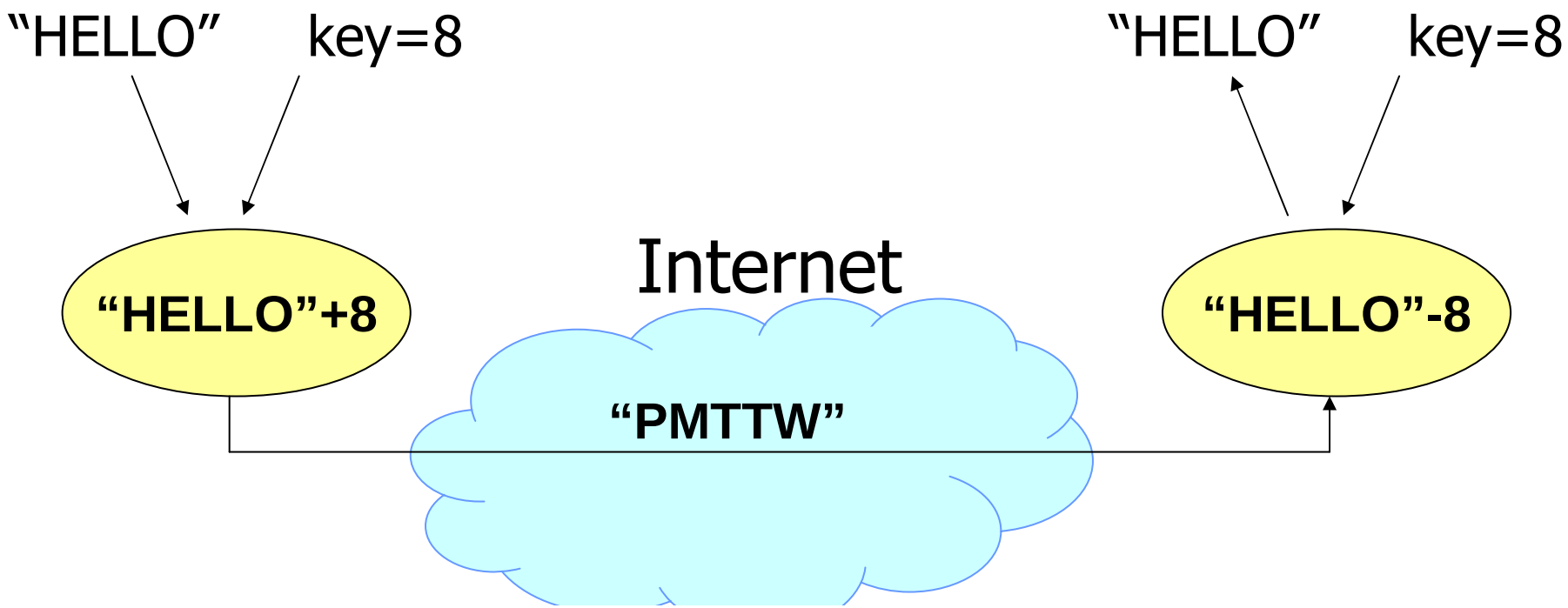
Symmetric Key Example: Rot-X

- Rotate ASCII text by X letters
  - E.g., X=8 translates "B" into "J", "HELLO" into "PMTTW"



Symmetric Key Example: Rot-X

- Rotate ASCII text by X letters
  - E.g., X=8 translates "B" into "J", "HELLO" into "PMTTW"

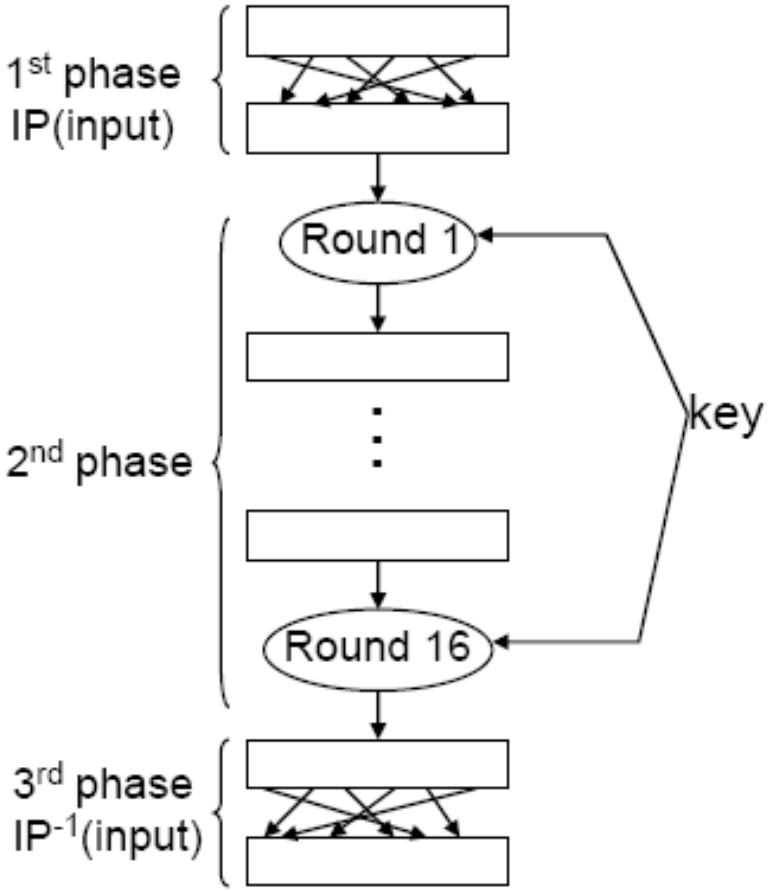


Data Encryption Standard

- Shortcoming of Rot-X: easy to break
  - e.g., analyze frequency of character occurrences
- More secure alternative: the Data Encryption Standard
  - block cipher (operating on fixed-length groups of bits)
  - later superseded by Advanced Encryption Standard (AES)
- DES encrypts a 64-bit block of plain text using a 64-bit key

Data Encryption Standard

- Three phases
  - Permute the 64 bits in the block
  - Apply a given operation 16 times on the 64 bits
  - Permute the 64 bits using the inverse of the original permutation

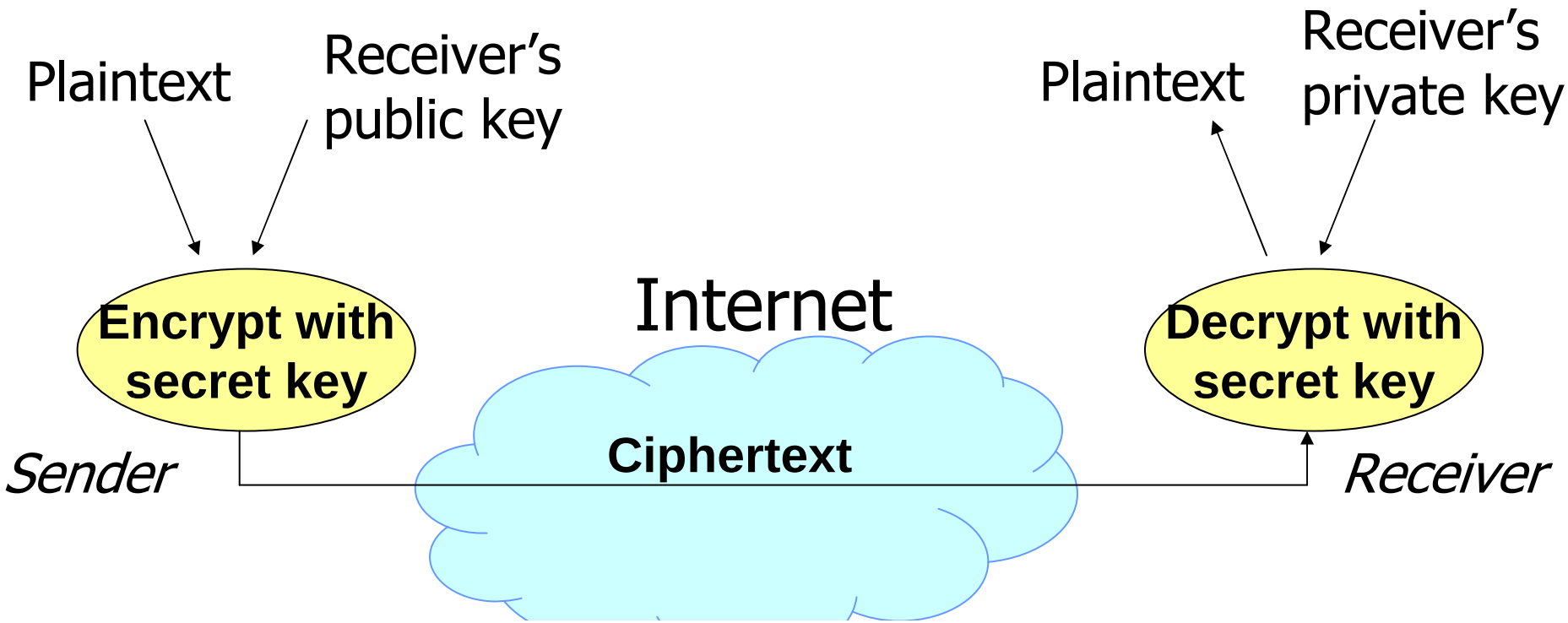


Data Encryption Standard

- No mathematical proof, but practical evidence suggests decrypting message without knowing the key requires exhaustive search
  - However, DES no longer considered secure due to short key length
  - 2006: Custom hardware costing $10k breaks DES in 9 days
- To increase security, use triple-DES, i.e., encrypt the message three times

Public Key Cryptography

- Sender uses a public key
  - Advertised to everyone
- Receiver uses a private key



Public Key Cryptography with RSA (Rivest, Shamir, and Adleman)

- Choose two large prime numbers p and q (~256 bits long) and multiply them: $n=p*q$
- Choose encryption key e such that e and $(p-1)*(q-1)$ are relatively prime
- Compute decryption key d as $d=e^{-1} \bmod ((p-1)*(q-1))$
- Public key consists of pair (n,e)
- Private key consists of pair (d,e)

RSA encryption and decryption

- Encryption of message block m:
  - $c=m^e \bmod n$

- Decryption of ciphertext c:
  - $m = c^d \bmod n$

Denial of Service (DoS)

- Problem:
  - You want to access a web page on a server
  - A 10,000 node botnet repeatedly sends high rates of requests to that server
  - Your request can't be serviced

May 1, 2006 12:03 PM PDT

'Second Life' fending off denial-of-service attacks

4 comments

...as shut down twice over the ...ded off denial-of-service attacks.

...ting self-replicating objects in the ...d San Francisco-based Linden ...e down the entire "Second Life" grid.

...e "Second Life" has been hit by denial-of-service ...s hit with similar assaults. Shortly thereafter Philip

DoS Attack Cripples Internet Root Servers

The denial-of-service attack hit Tuesday and nearly took down three of the 13 root servers that help manage worldwide Internet traffic.

By Sharon Gaudin
InformationWeek
February 6, 2007 07:50 PM

The 13 servers that help manage worldwide Internet traffic were hit Tuesday by a denial-of-servi... that nearly took down three of them.

It was the fiercest attack on the 13 root servers since an October 2002 assault that took down m... roots that help manage worldwide Internet traffic, according to Ben Petro, a senior VP of NeuSta... provides clearinghouse services to the communications and Internet industry. Three of the serv... nearly overloaded by the attack, but they didn't go down, says Petro, who adds that they were in a... slowed-down brownout stage.

More Internet Insights

Tuesday's attack nearly matched the 2002 attack in terms ... but surpassed the old attack in sophistication, Petro says.

DoS Attacks Cripple Yahoo, CNN, Amazon and Buy.com

0730 Hrs 09 February 2000

A series of Denial of Service (DoS) attacks that commenced on Monday with the crippling of portal site www.yahoo.com has extended to www.amazon.com , www.cnn.com and www.buy.com - these sites were performing poorly with the amazon.com site completely timing out at various stages through the night.

Monday's attack on Yahoo led to traffic levels of 1GB a second through the routers serving the portal site. The attack on Yahoo is believed to have been a distributed one involving a number of compromised computers.

Dealing with DoS

- Traceback
  - Tag packets with information about where they originated, trace back to source
- Speak-up
  - If well-behaved hosts can’t get through, they should communicate more aggressively

Man-in-the-middle (MITM)

- Attacker places itself in middle of session
  - Attacker may eavesdrop on communications, drop messages, or fabricate new messages

Dealing with MITM

- Encryption
  - Sender and receiver can share a "secret key"
  - Encryption/decryption functions take key as input to produce encrypted value
  - Public/private-key encryption simplifies key distribution by having different keys for encryption and decryption

Spam

- Unsolicited/unwanted messages
- 95% of email sent in 2007 was spam, growing
- Instant messaging, blogs, newsgroups, search engines, mobile phones, Internet forums, fax transmissions, wikis, online classifieds…
- Top ten countries sourcing spam:
  - 1. USA: 28.4%;
  - 2. South Korea: 5.2%;
  - 3. China (including Hong Kong): 4.9%;
  - 4. Russia: 4.4%;
  - 5. Brazil: 3.7%;
  - 6. France: 3.6%;
  - 7. Germany: 3.4%;
  - 8. Turkey: 3.%;
  - 9. Poland: 2.7%;
  - 10. United Kingdom (specifically Great Britain): 2.4%;

Dealing with Spam

- CAPTCHAs
  - Force human sender to answer a challenge computers can't solve
- Hashcash
  - Force computer to perform intensive computation
- Filtering
  - Tools like SpamAssassin separate spam from non-spam (ham)
  - Leverage Bayesian filtering, regular expression matching against dictionaries

Forged identity

- Sybil attacks
  - One host pretends to be many hosts
    - Bad if resources are allocated per-host
- Hijacks
  - One host pretends to be another host, intercepts traffic for that host
  - One host intercepts ongoing connection to a different host
  - An ISP advertises a prefix owned by another ISP

Dealing with forged identity

- Public key infrastructure
  - Procedures and infrastructure to allocate and revoke digital certificates
- Digital signature
  - A signs content with private key, B confirms A's signature with A's public key

In the News

- Denial of service attacks cripple e-commerce and various major Internet-based companies
  - What is denial of service?
  - How does it traditionally work?
    - IP spoofing example
    - key elements
  - What's new about the recent attacks?
  - What has changed to make the new attacks possible?

What Is Denial of Service?

- Denial of service is
  - A malicious attack
  - Based on the concept of overloading components along the route to a server or the server itself
- Increased workload
  - The overloaded component responds slowly or not at all to legitimate requests.

Example: Misbehaving TCP receiver

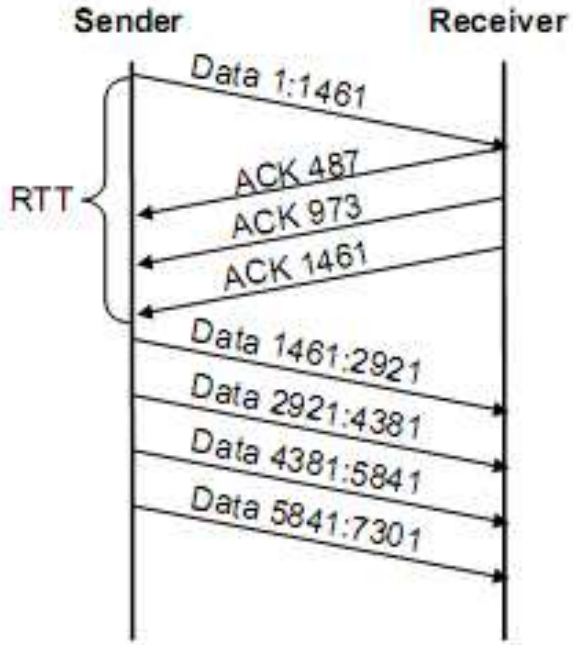


Figure 1: Sample time line for a ACK division attack. The sender begins with *cwnd*=1, which is incremented for each of the three valid ACKs received. After one round-trip time, *cwnd*=4, instead of the expected value of *cwnd*=2.

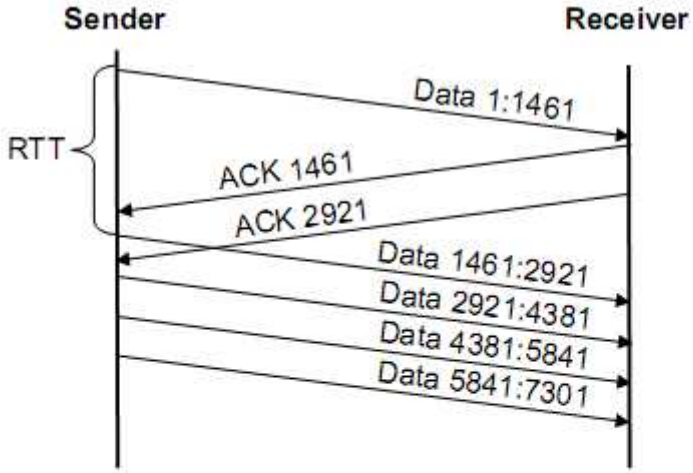


Figure 3: Sample time line for optimistic ACKing attack. The ACK for the second segment is sent before the segment itself is received, leading the receiver to grow *cwnd* more quickly than otherwise. At the end of this example, *cwnd*=3, rather than the expected value of *cwnd*=2.

- ACK Division

Optimistic ACKing

Conclusions: Attacks and countermeasures

- Denial of Service
  - Host overutilizes network for sole purpose of denying resources to other hosts
- Man-in-the-middle
  - Host hijacks/intercepts connection intended for a different host
- Spam
  - Host sends unwanted traffic
- Forged identity
  - Host pretends to be someone else, or pretends to be a large number of hosts