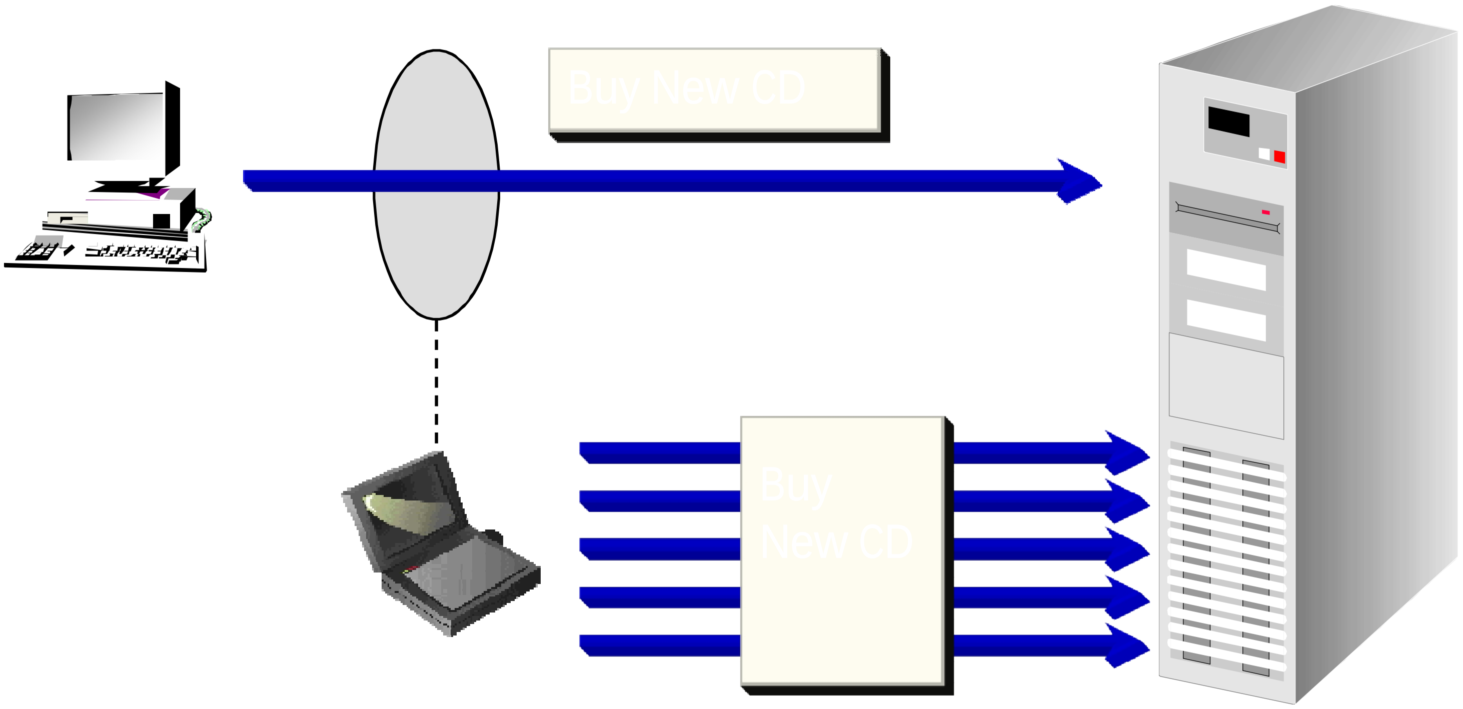
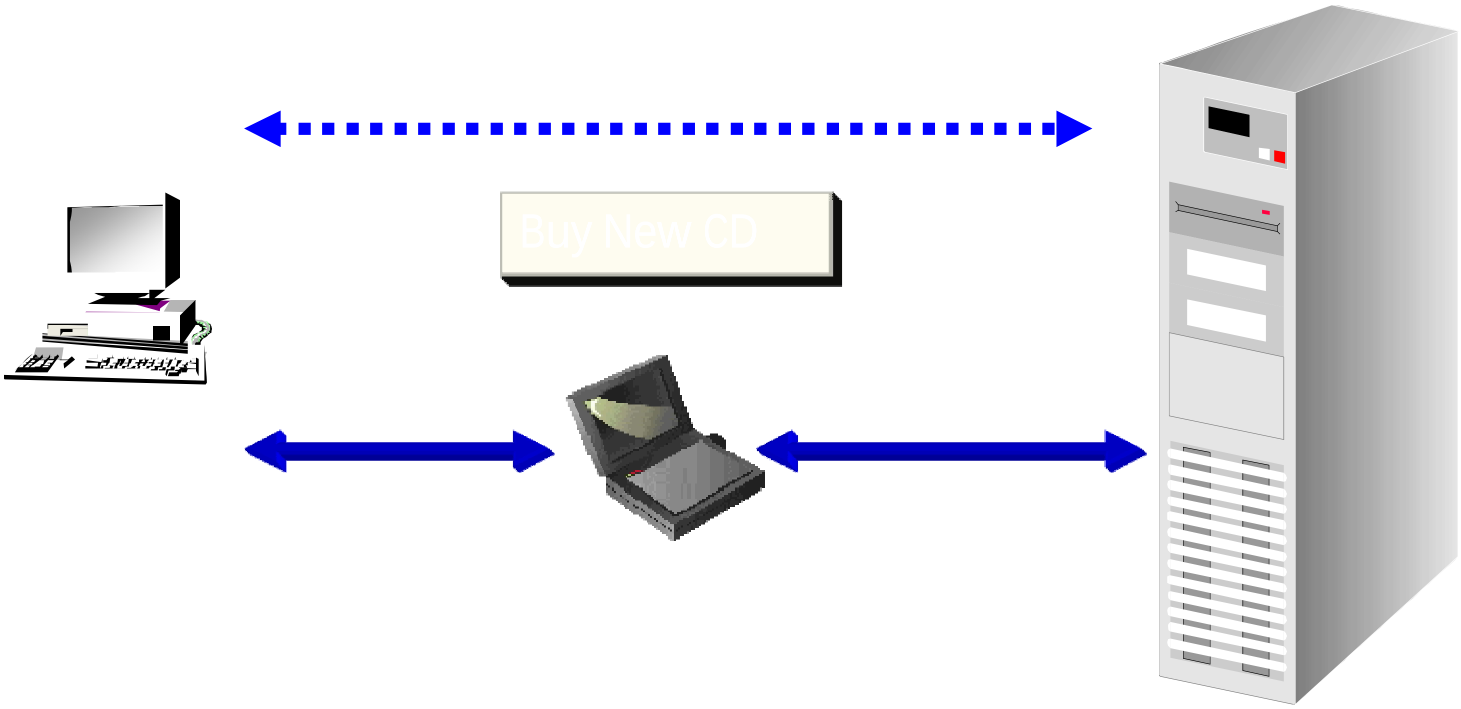
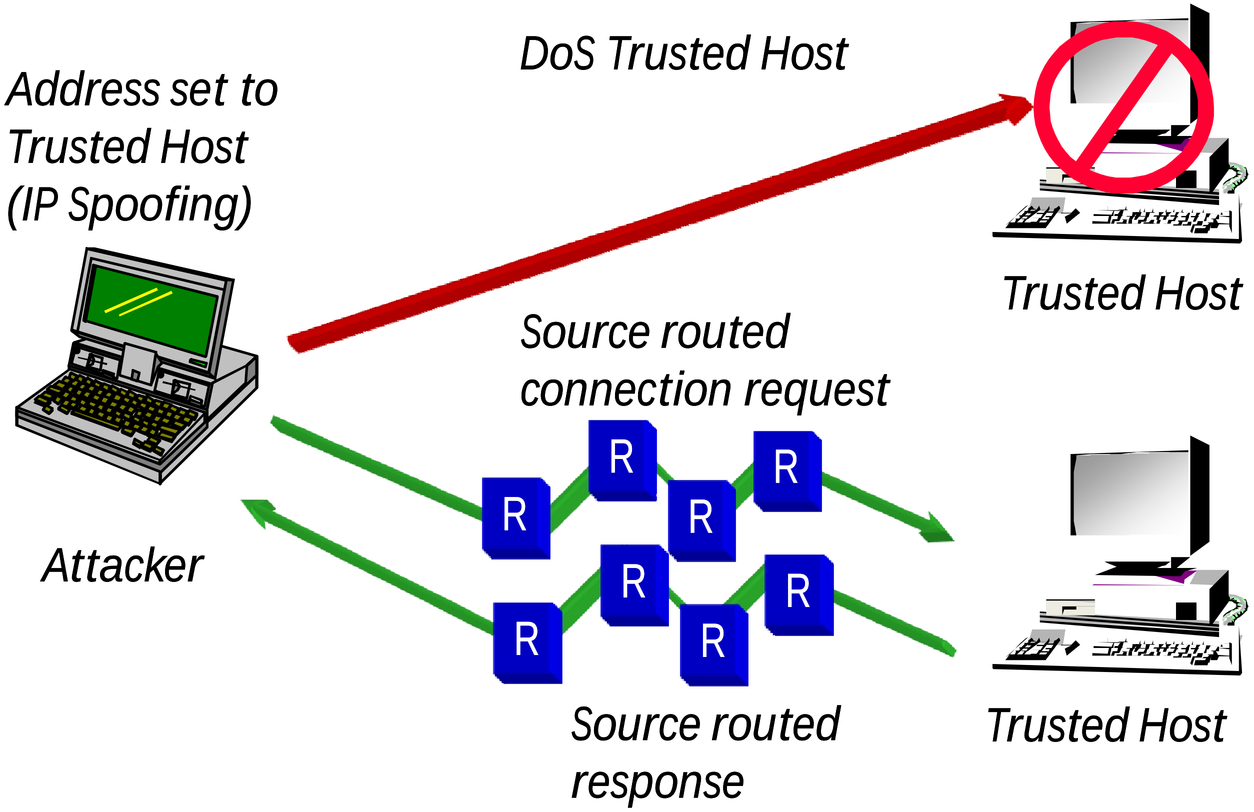
Replay Attacks



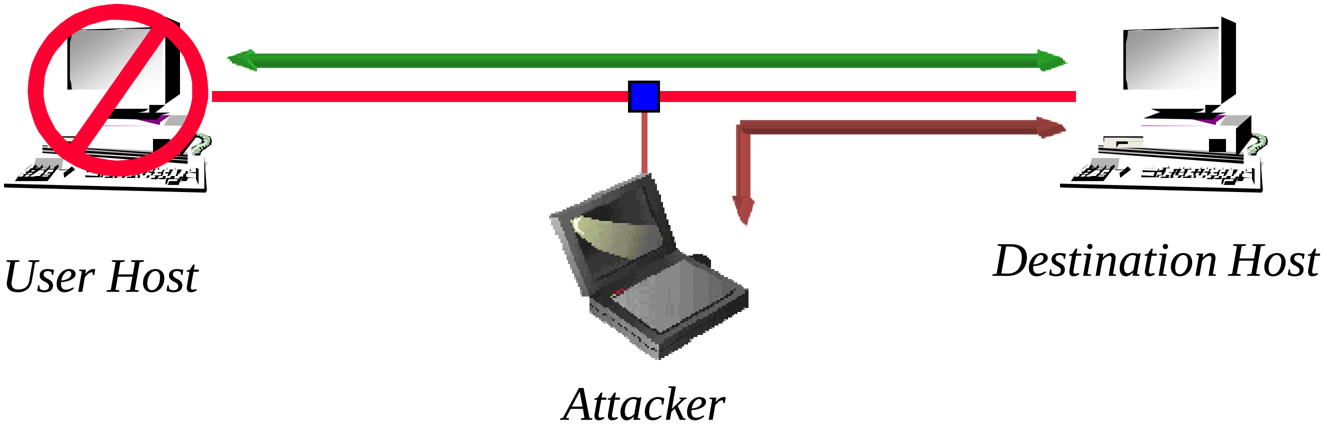
Man in the Middle Attack



Source Routing Attacks



Session Hijacking

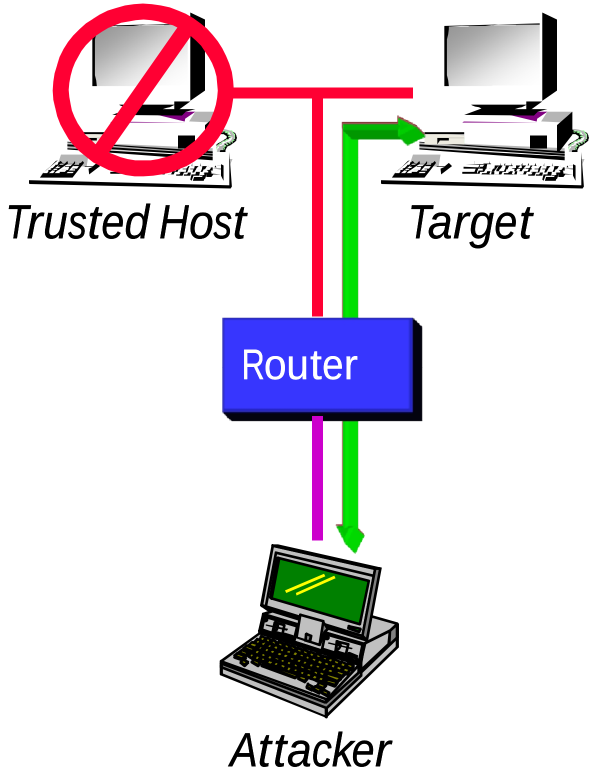


- Attacker watches live sessions to record sequence numbers
- Attacker DoS’s User Host and IP spoofs packets to Destination using User Host’s sequence numbers
- Destination continues session as if nothing happened

TCP Sequence Guessing

- Attacker DoS’s Trusted Host

- Attacker attempts to connect to target many times and records sequence numbers
- Attacker *calculates* sequence numbers which will be assigned for next connection.
- Attacker *spoofs* address of trusted host and uses calculated sequence numbers (router passes trusted *internal address*
- Target runs command from *spoofed* trusted host



Port Scanning

- Checking of all ports on a target
- Banner Grabbing
- Can looks for known service bugs/exploits
- Can leave a big footprint
- Common Scanners
  - Satan/Saint/Sara
  - Nmap
  - Nessus

Service Exploits

- Banner Grabbing/Vulnerability Scanners
- Stack/Buffer Overflow
- Backdoors
- File Transfer Programs
  - Anonymous FTP
  - TFTP
- FTP Bounces

OS Fingerprinting

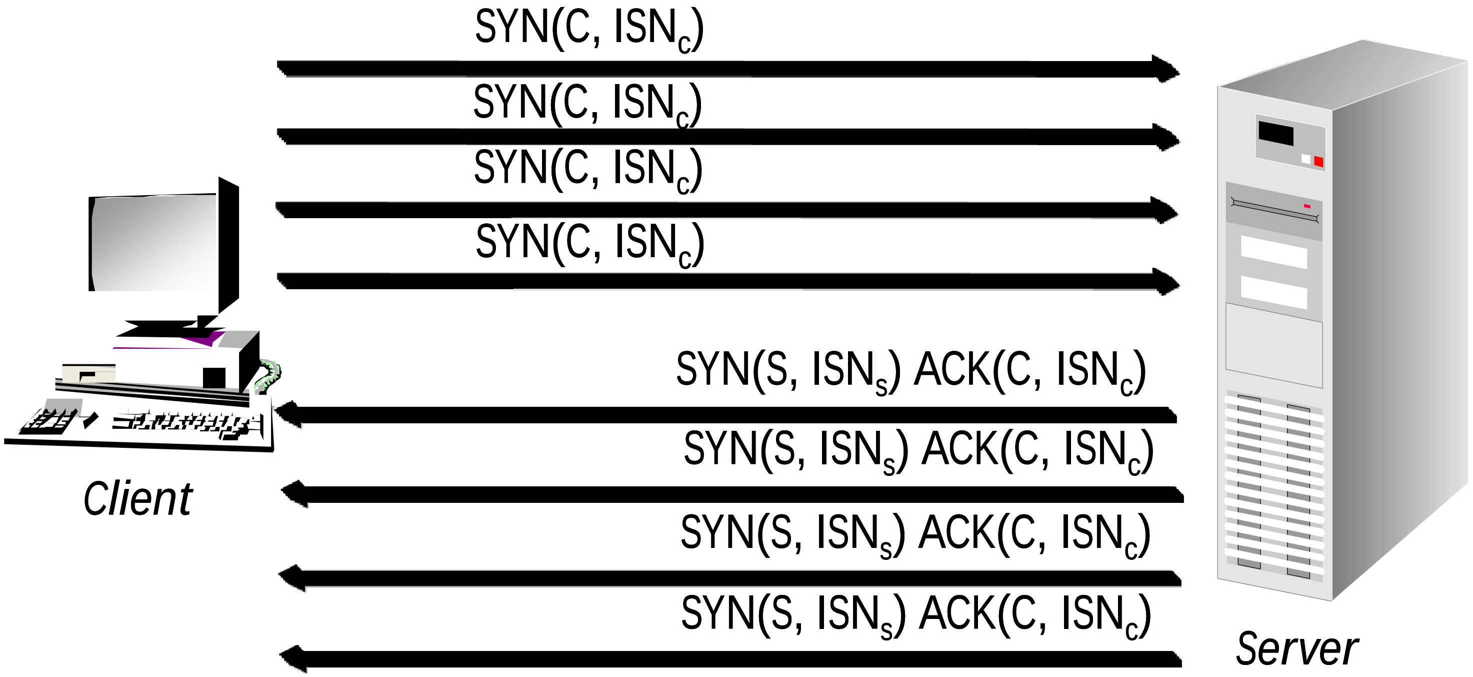
- FIN Probing
- TCP ISN Sampling
- IPID Sampling
- TCP Timestamp
- TCP Options
- Fragmentation Handling
- TCP Retransmission Timeouts
- TCP Initial Window
- ACK Values
- ICMP Error Quoting
- ICMP Error Message Echo Integrity
- ICMP Error Message Type of Service (TOS)
- ICMP Error Message Limiting

Denial of Service Attacks

- ICMP Redirects
- SYN Flooding
- Smurf Attacks
- Service Bombing
  - FTP
  - Finger
- Mail Bombing
- Service Bugs
  - Ping o’ Death
  - WinNuke
- Teardrop
- Distributed DoS

Targets may be Upstream

SYN Flood Attack



SYN(C, ISN_c)

SYN(C, ISN_c)

SYN(C, ISN_c)

SYN(C, ISN_c)

SYN(S, ISN_s) ACK(C, ISN_c)

SYN(S, ISN_s) ACK(C, ISN_c)

SYN(S, ISN_s) ACK(C, ISN_c)

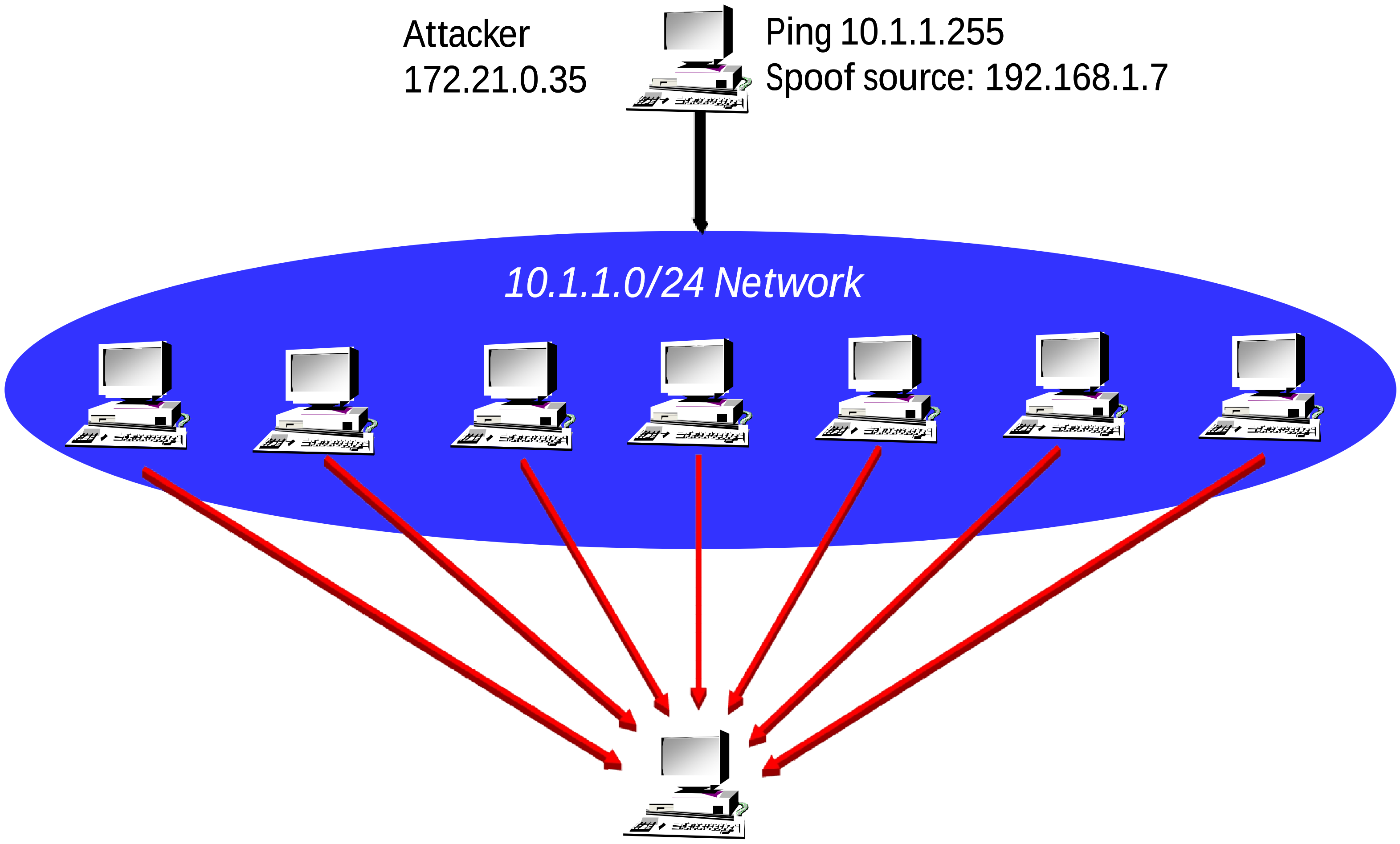
SYN(S, ISN_s) ACK(C, ISN_c)

Client

Server

Server never gets ACKs to its SYN
Half Open Connections

Smurf Attacks



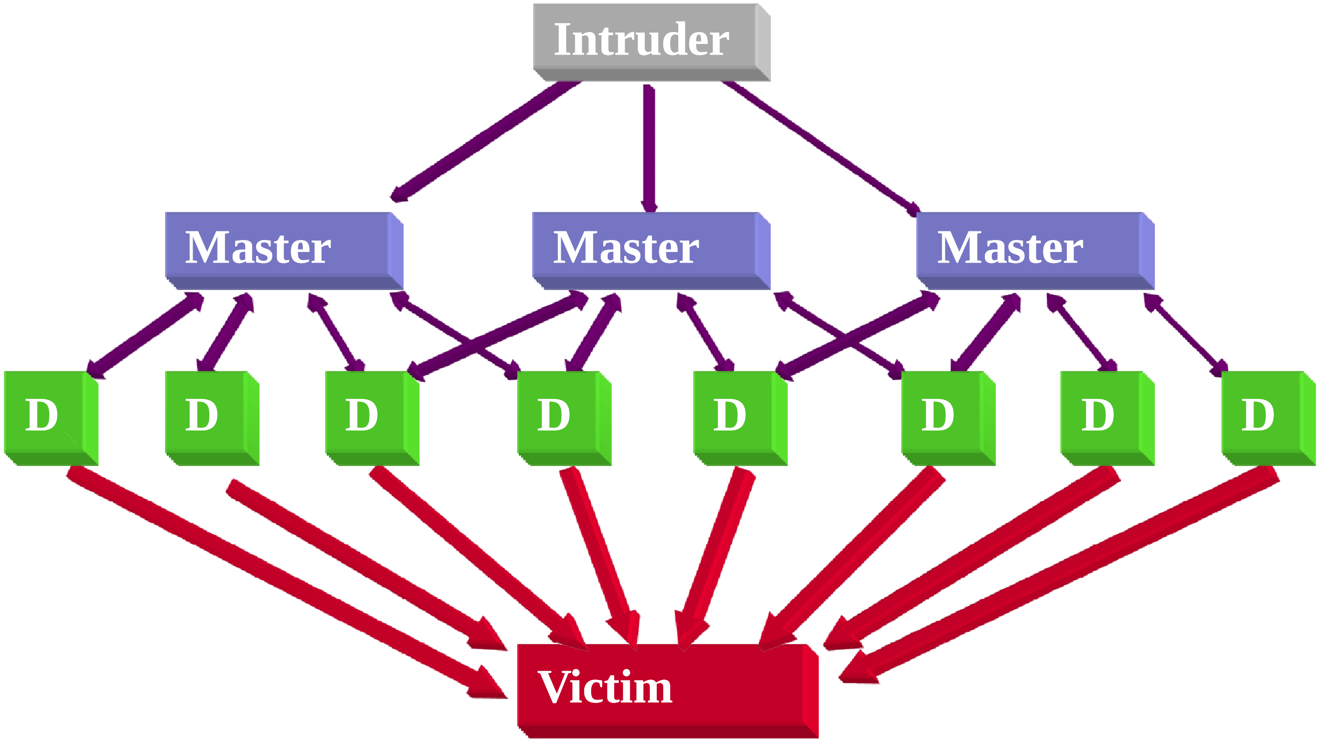
Attacker
172.21.0.35

Ping 10.1.1.255
Spoof source: 192.168.1.7

10.1.1.0/24 Network

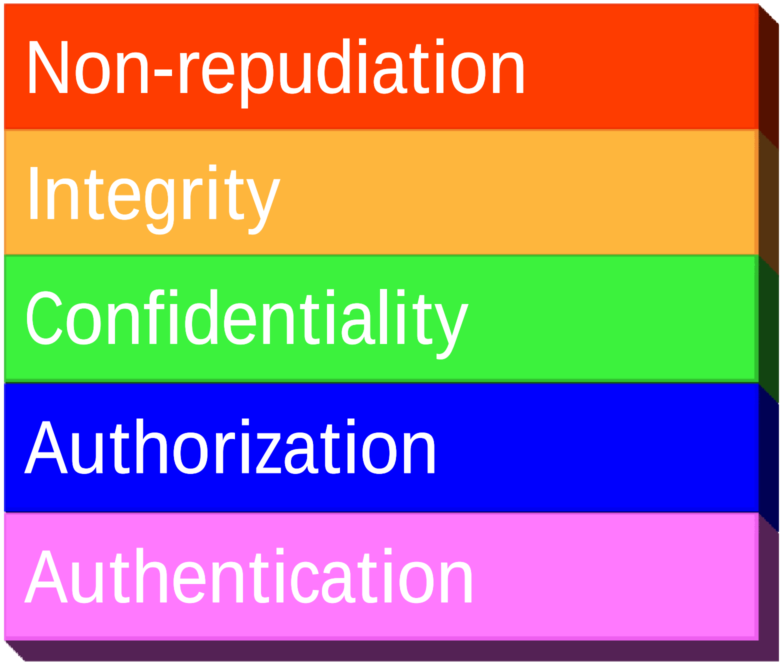
192.168.1.7

Distributed DoS Attacks



Source: *Results of the Distributed Intruder Tools Workshop*

Cryptography can help!



Non-repudiation

Integrity

Confidentiality

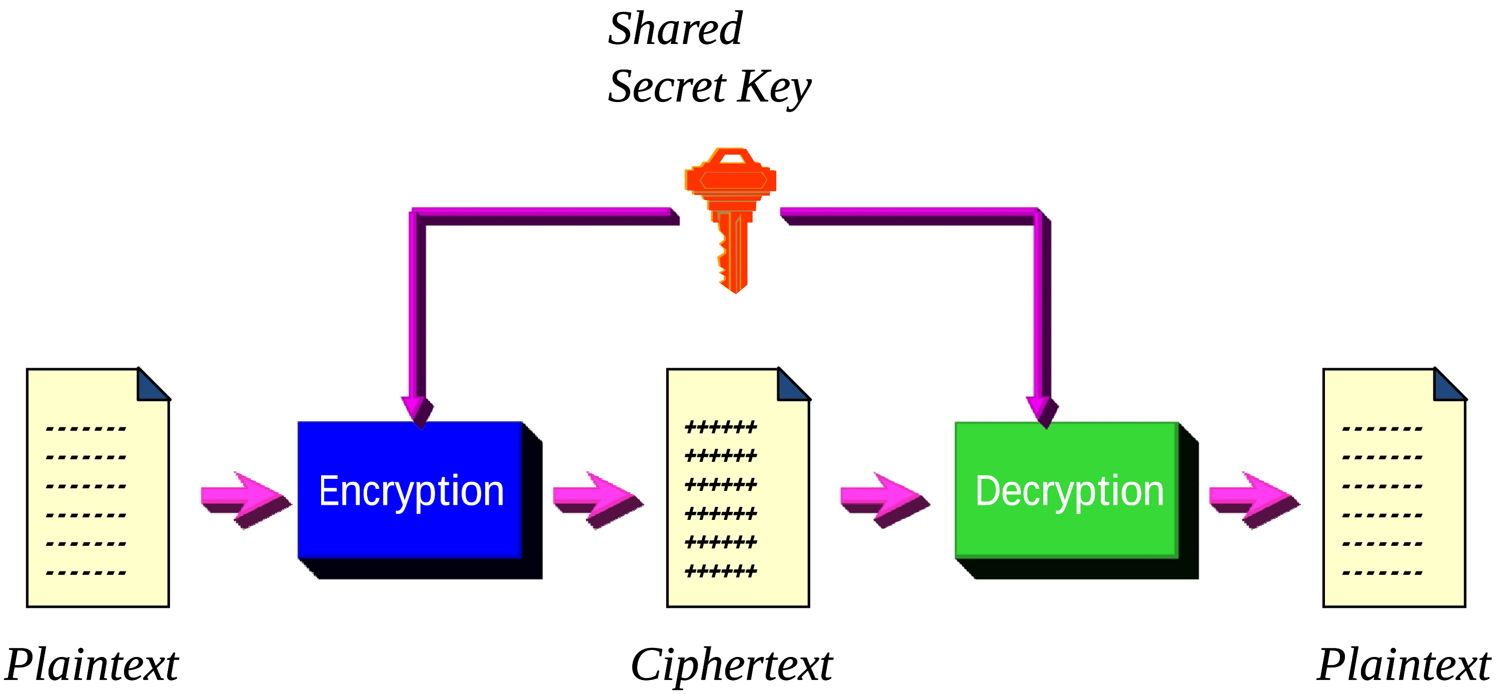
Authorization

Authentication

Classical Cryptography

- Alphabetic Substitutions
  - Shifts
  - Mono-Alphabetic Replacements
  - Poly-Alphabetic Replacements
  - One-Time Pads
- Transpositions/Permutations
- Most were stream ciphers

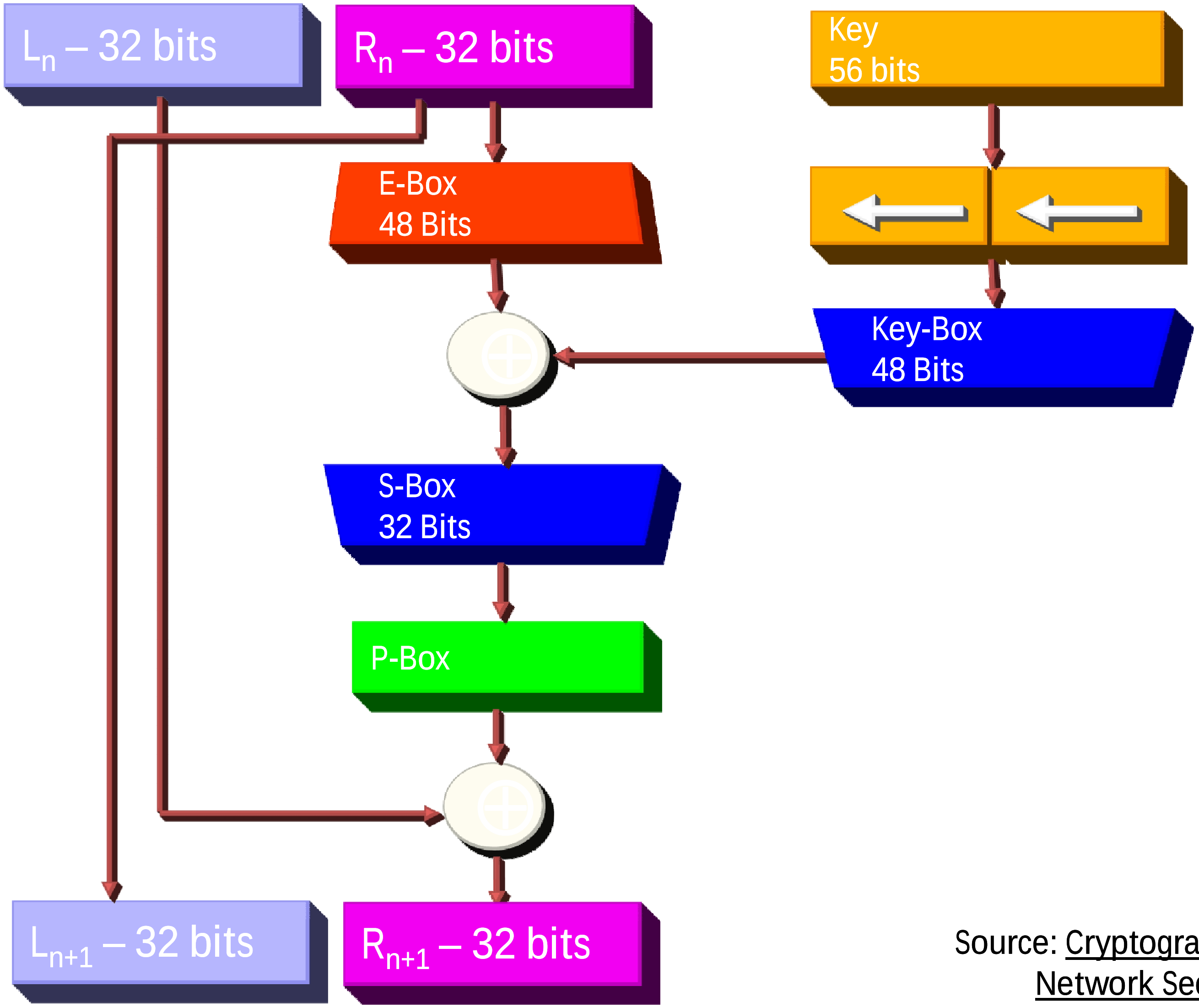
Symmetric Key Encryption



Data Encryption Standard

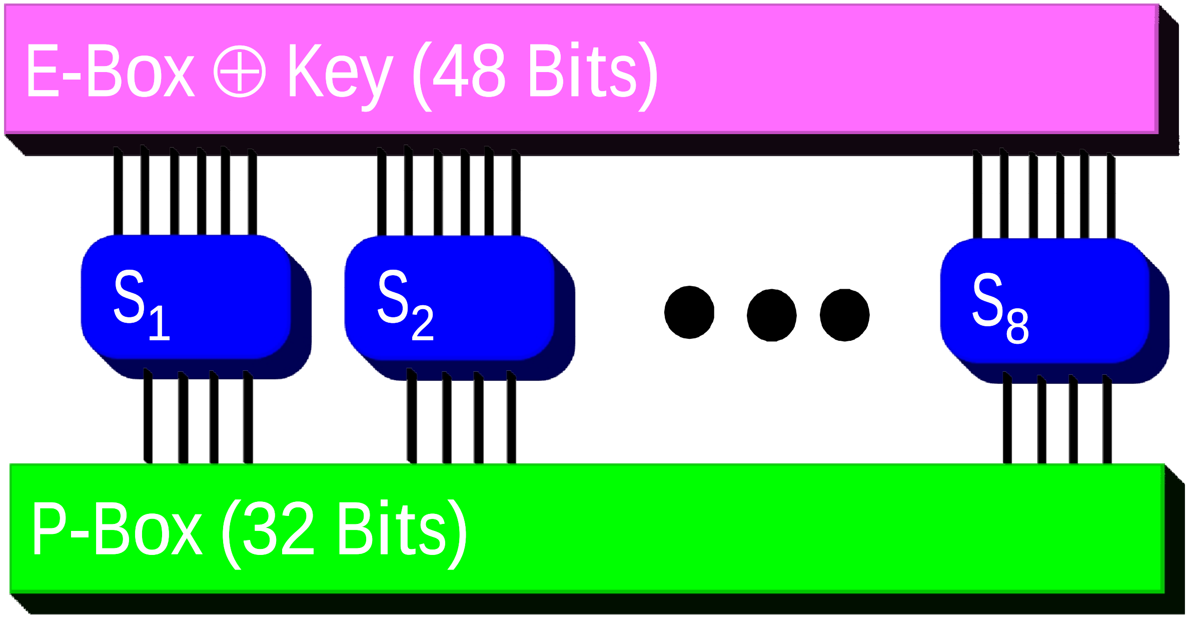
- Created by IBM called LUCIFER
- Adopted in 1977 by National Bureau of Standards (now NIST)
- 56 bit key to encrypt 64 bit blocks
- Consists of 16 stages plus initial/final permutations
- Advanced Encryption Standard (AES)

DES – One Round



Source: Cryptography and Network Security, 2E
by William Stallings

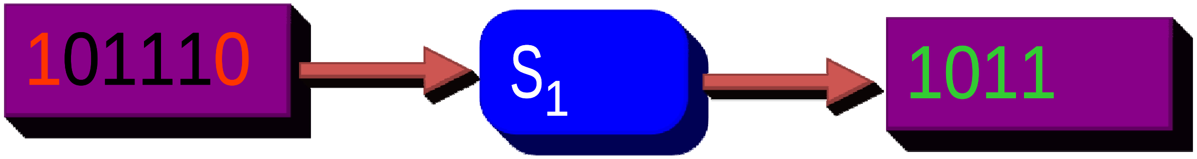
DES Substitution Boxes



Source: Cryptography and Network Security, 2E
by William Stallings

S-Box Lookups

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	▨	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

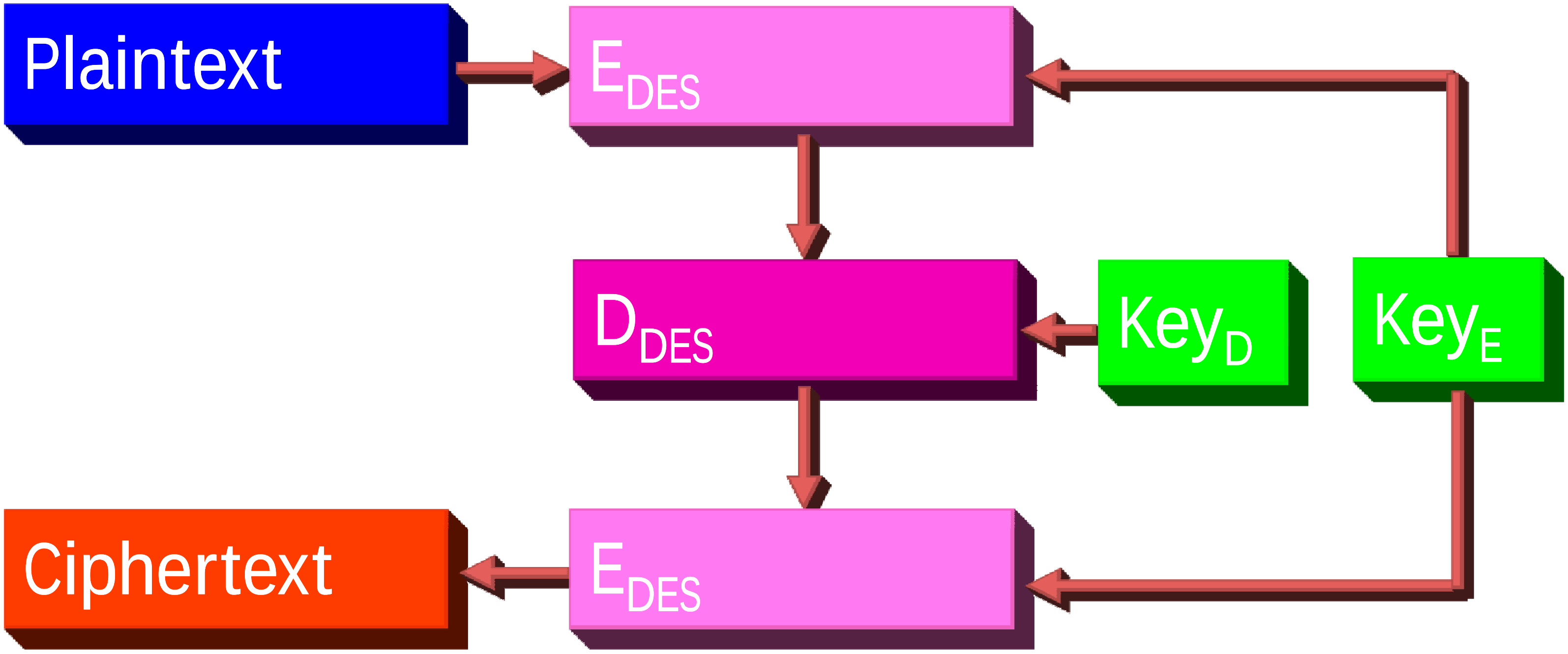


Source: Cryptography and Network Security, 2E
by William Stallings

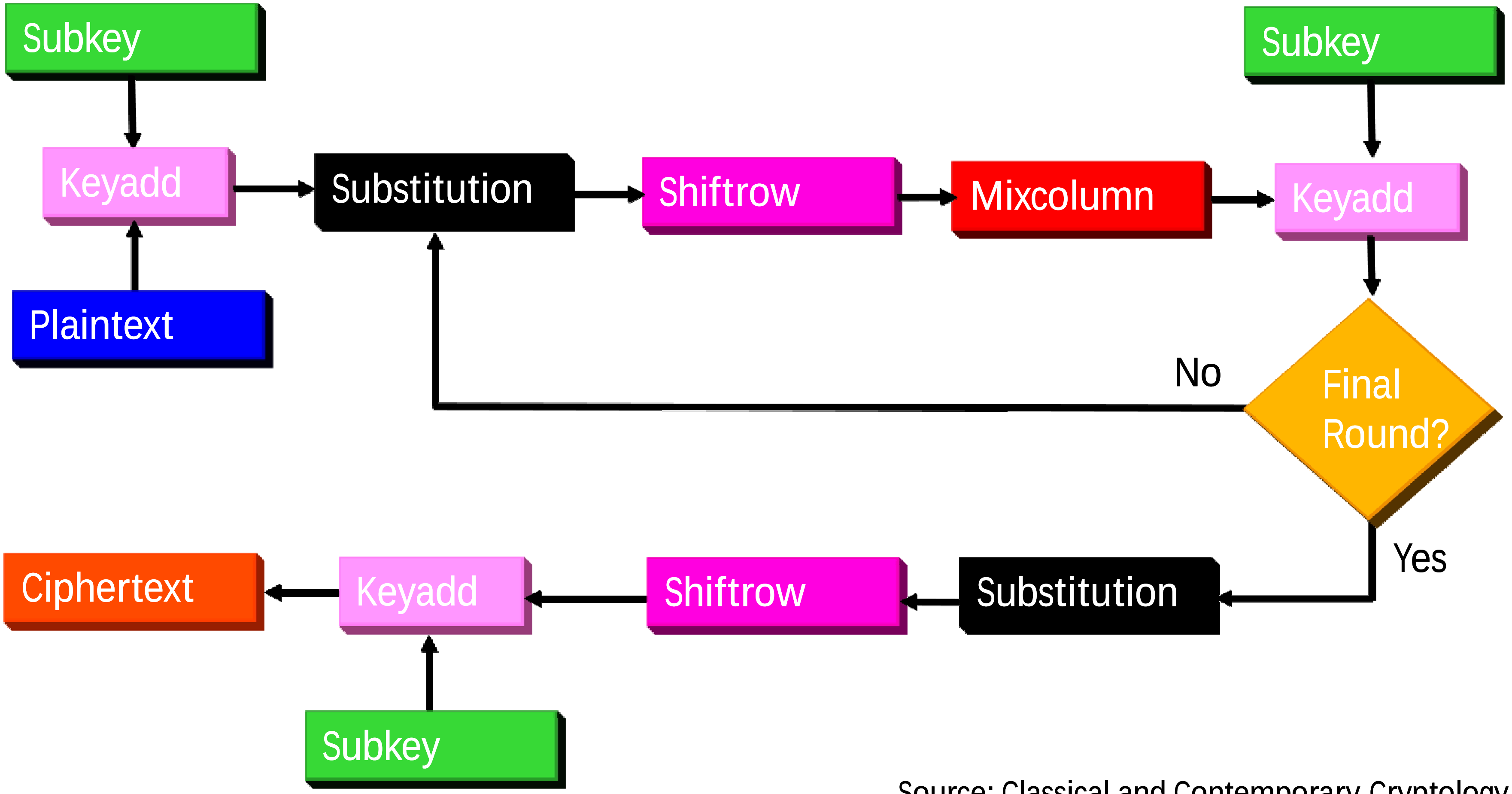
Attacks on DES

- Weak key size
  - Originally used a 128 bit key
  - Shortened to 56 bits to fit on 1 chip
- Brute force attacks
  - RSA Challenges
  - Deep Crack – EFF built $210K system
  - Distributed.Net – 1000s of Internet connected systems working together

Triple DES (3DES)

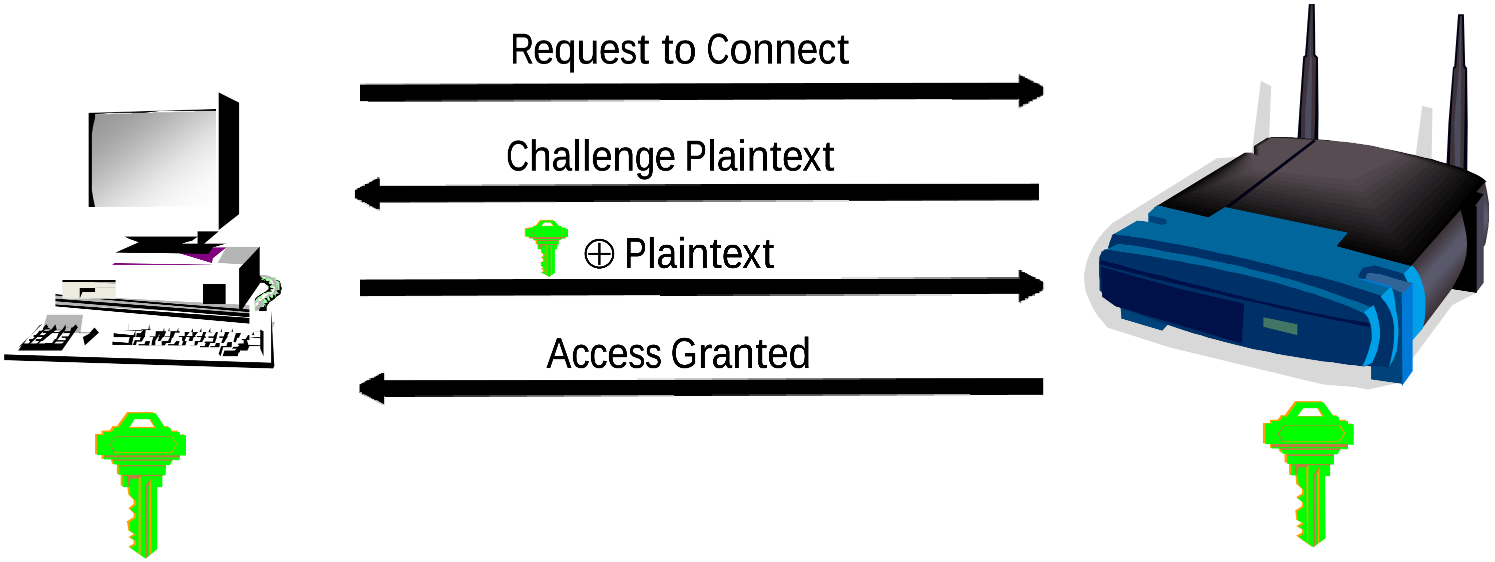


Rijndael (AES) Structure



Source: Classical and Contemporary Cryptology
by Richard J. Spillman

WEP Authentication



Request to Connect

Challenge Plaintext

🔑 ⊕ Plaintext

Access Granted

WEP
Key

WEP
Key