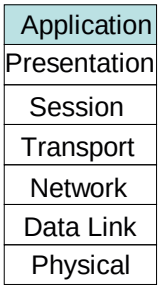
CSE/EE 461
Network Security
Part 1

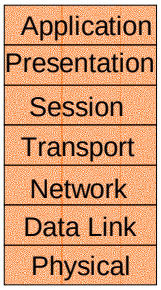
Last Time

- Tunnelling, Translating and Booting
- More generally, throughout this quarter, we've focussed on how to use networks to get something good to happen.
- And now for something completely different…



This Time

- How to keep something bad from happening.
  - Network security
    - How do we secure distributed systems?
- Topics
  - Privacy, integrity, authenticity
  - Cryptography



What do we mean by "Security"?

- Networks are fundamentally shared
  - Sharing a resource is "safe" if everybody behaves well.
  - It becomes unsafe if people badly
- Three ways to behave badly
  - Eavesdrop
  - Forge
  - Transform
- Leads to three desirable security properties
  - Privacy: messages can't be eavesdropped
  - Authenticity: messages were sent by the right party
  - Integrity: messages can't be tampered with

Examples of Not P, A or I

- SPAM
- Vote tampering
- Identify theft/credit card theft
- DOS/DDOS
- Phishing

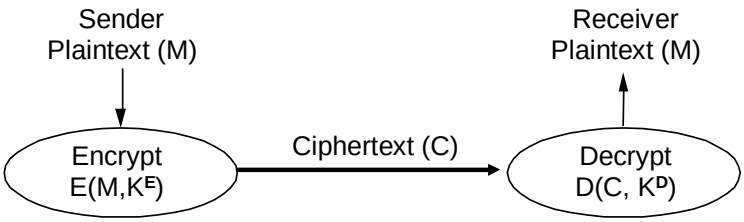
Why is security hard to achieve?

- It is an ill-defined goal
- It is hard to express goal
  - you can do X, but you can't do Y
  - What are X and Y?
- It's a negative goal
  - requires that you know there are no vulnerabilities
  - like proving there are no bugs
- It's a valuable goal to subvert

Approaches at 10,000 ft

- **Locks**
  - Physical security
    - Tackle the problem of sharing directly
  - "Security through obscurity"
    - Hope no-one will find out what you're doing!
  - Throw math at the problem
    - Cryptography
- **Alarms**
  - Watch for the bad guys
    - Beware the false positives/negatives
- **Fingerprints**
  - Audit trails
    - Tracebacks
  - Hard not to get lost in a sea of data

Use Encryption for Privacy

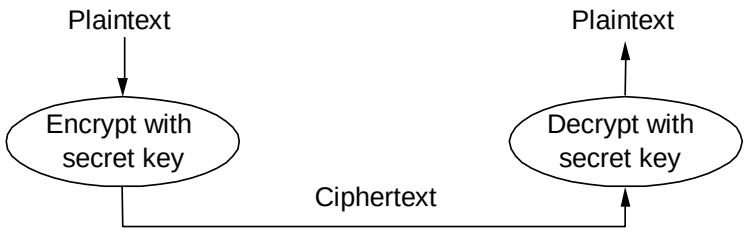


- *Cryptographer* chooses functions E, D and keys K^E, K^D
- *Cryptanalyst* tries to "break" the system
  - Depends on what is known: E and D, M and C?

Two Basic Encryption Strategies

- Secret Key
  - Bob and Alice each share a secret (K)
  - The secret is used to encrypt communication between Bob and Alice.
    - D(E(M,K),K) = M
  - DES
- Public Key (RSA)
  - Bob has a secret key (K) and a matching public key (K')
    - D(E(M, K'), K) = M
    - D(E(M, K), K') = M

Secret Key Functions (DES)



- Single key (symmetric) is shared between parties
  - Often chosen randomly, but must be communicated
  - Turns out to be a hard problem (key distribution)

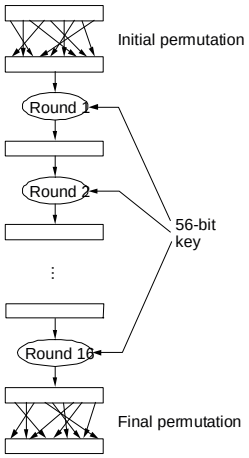
DES Is a Bit Scrambler

- The bits go in one way and come out another according to some scrambling rules
- Unscrambling runs it backwards
  - Not unlike the WW2

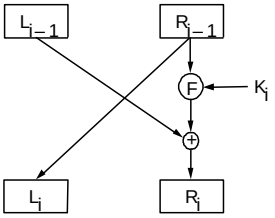
QuickTime™ and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

QuickTime™ and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

DES as a Digital Scrambling

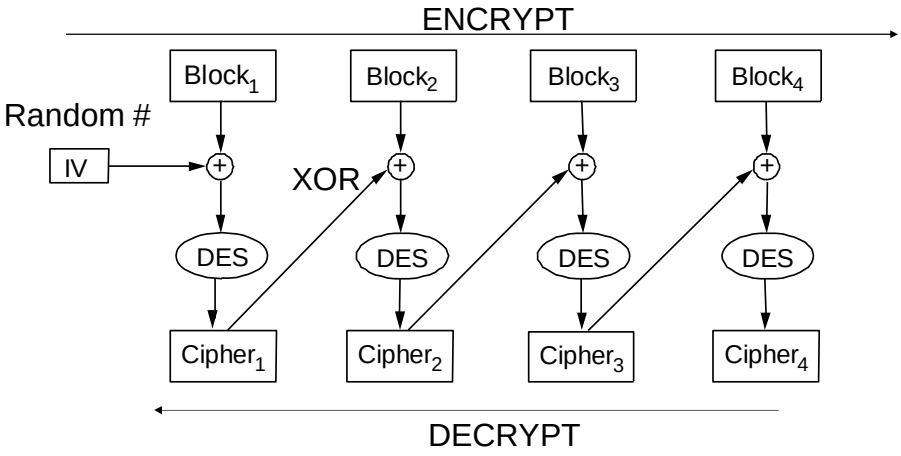


Each Round:



DES uses a 64 bit key (56 + 8)
Message encrypted 64 bits at a time
16 rounds in the encryption
Each round scrambles 64 bits

Larger messages with "chaining"



On the Security of DES

- Exhaustive search is the only known attack
  - Not much is known about the unknown attacks
- Size of key space determines cost of attack
  - Key space needs to track Moore's law just to stay even (future proof keys)
    - a key that's just barely long enough today won't be long enough in a few years
      - today's 52 bit DES key is "equivalent" to a 40 bit key from 20 years ago
  - Easy to parallelize

Exhaustive key searches:

Key Size (bits)	Number of Alternative Keys	Time Required at 1 Decryption / μs	Time Required at 10^9 Decryptions / μs
32	$2^{32} = 4.3 \times 10^9$	2^{31} μs = 35.8 minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	2^{55} μs = 1142 years	10 hours
128	$2^{128} = 3.4 \times 10^{38}$	2^{127} μs = 5.4×10^{24} years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	2^{167} μs = 5.9×10^{36} years	5.9×10^{30} years

But more fundamentally

- Secret key systems are vulnerable because it's hard to keep a secret.
  - **you've got to tell somebody your secret to use it.**
    - **There's no protection from blabbermouths.**
  - Also, key needs to be kept somewhere in order to use it.
    - user can type it in
      - but the keys won't be very long
    - keep it in a file?
      - that won't work unless the file is encrypted
    - keep it on a removable device
      - smartcard, PCMCIA
- Needed is a strategy that doesn't require me to tell you my secret.