Announcements

- Project #4 Due this week
- Midterm #2 is Tuesday
- No Office hours next week
- Reading: Chapter 7 (7.1)

Computer And Network Security

Issues

- secrecy: can someone read a message
- authentication: determine who you are communicating with
 - this can be one way or two way
- nonrepudiation: verify that something send can't be recanted
- integrity: a third party can't change a message in flight
- denial of service: make the system unavailable to others

• Threat Model

- must consider acceptable risks
 - value of item to be protected
 - \$2,000 of computer time to steal 50 cents of data
 - this is a sufficient deter someone
 - but computers keep getting faster
- who do you trust?
 - employees
 - vendor of security software
 - network provider

Where to Provide Security?

- Short Answers: at all levels
- physical:
 - wrap gas or tripwires around cable
- link:
 - encryption protects the wire but not the router
- network:
 - firewalls filter packets
 - end-to-end encryption
- session/presentation:
 - "secure" socket layer
- application:
 - PGP signed messages
 - application specific authentication

Other Attacks

• Random Messages

- Will a random message likely be a valid message
- Need to have redundancy in the message
- tension more redundancy ease cryptoanalysis

• Replay Attacks

- can the same message be sent twice?
 - transfer \$10,000 from Smith to Jones
 - make an exact copy of a metro fare card
- need to ensure messages apply exactly once
 - use a timestamped lifetime
 - sequence numbers

Digital Water Marks

- Issue: If I have a copy of a digital object, I can make many
 - if you pay per-copy for the object, how to you prevent copies?
- Goal: Track where an object came from
 - make every object unique
 - the objects should not appear different

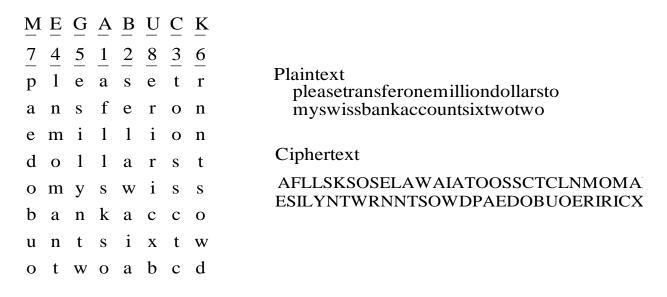
Cryptography

• Terms

- plaintext (P): the raw message to be sent
- key (K): data used to protect one or more messages
- ciphertext (C): output of applying key to plaintext
- encrypt (E): a function to combine the key and plaintext
- decrypt (D): a function to combine ciphertext and key
 - may be the same as E
- $C = E_k(P)$ and $D_k(E_k(P)) = P$
- Substitution Cipher
 - Ceaser Cipher
 - shift letters by a constant amount
 - key is how many letters to shift
 - Monoalphabetic substitution
 - for each letter pick some a different letter to use
 - key is 26 characters representing substitution
 - can use properties of language to break it

Transposition Cipher

- Block of text is used to break up digrams
- To Break:
 - each letter is itself, so normal distribution of letters is seen
 - guess number of columns (verify with known plaintext)
 - order columns using trigram frequency



From: *Computer Networks*, 3rd Ed. by Andrew S. Tanenbaum, (c)1996 Prentice Hall.

One Time Pad

- Key Idea: randomness in key
- Create a random string as long as the message
 - each party has the pad
 - xor each bit of the message with the a bit of the key
- Almost impossible to break
- Some practical problems
 - need to ensure key is not captured
 - a one bit drop will corrupt the rest of the message
- Pseudo-random is not good enough
 - Japanese JN-25 during WWII was pseudo random onetime pad