Announcements

- Project #6 is on the web
- Deadline for MT#2 re-grade requests is today

Monitoring

- Record (log) significant events
  - attempts to login to the system
  - changes to selected files or directories
- Possible to compromise the log
  - the user or software breaking in could delete all or part of the logs
  - could record logs to non-erasable storage
    - have a line printer attached to the machine
    - use WORM drives
  - send data to a secure remote host

Tripwire

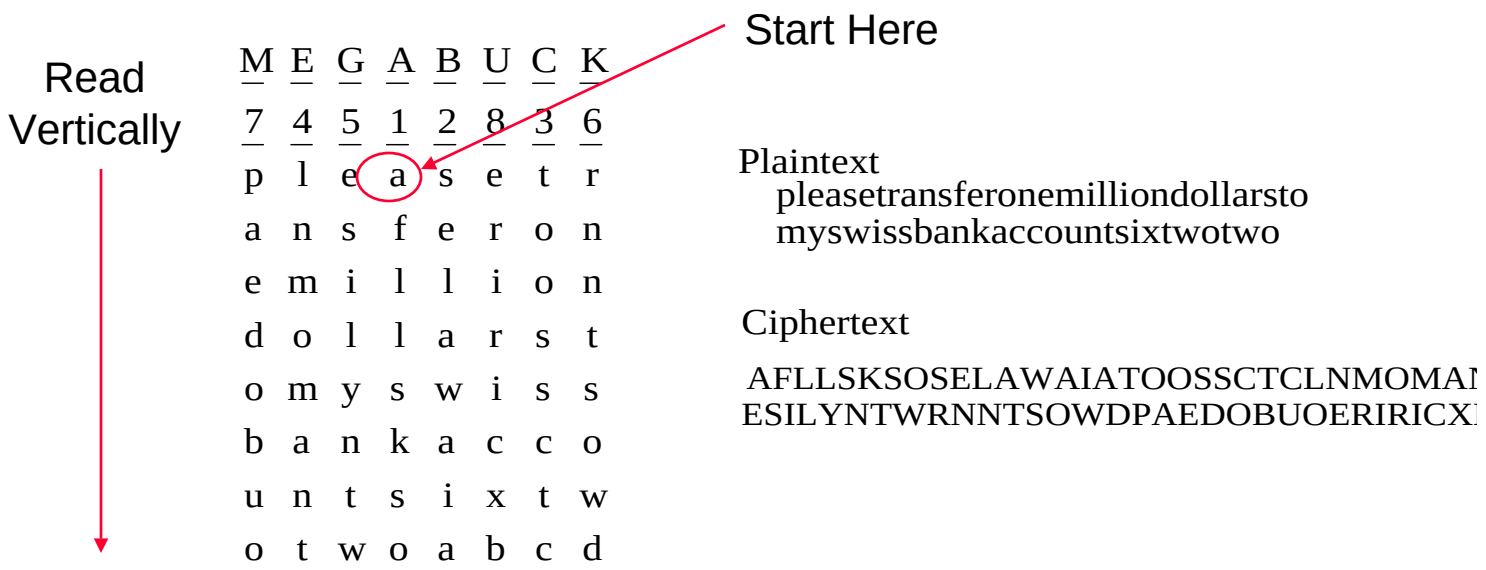
- Compute a set of expectorations about system
  - Hash of file contents
  - Dates on files
- Store database of values
  - On read-only media
  - Offline
- Periodically
  - Compare database to current system
  - Report any differences

Encryption: protecting info from being read

- Given a message m
  - use a key k, and function E_k to compute $E_k(m)$
  - store or send only $E_k(m)$
  - use a second second key k and function $D_{k'}$ such that
    - $D_{k'}(E_k(m)) = m$
  - E_k and $D_{k'}$ need not be kept a secrete
- If k=k' it's called private key encryption
  - need to keep k secret
  - example DES
- if k != k', it's called public key encryption
  - need only keep one of them secret
  - if k' is secret, anyone can send a private message
  - if k is secret, it is possible to "sign" a message
  - still need a way to authenticate k or k' for a user
  - example RSA

Transposition Cipher

- 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
- Block of text is used to break up digrams



Plaintext

pleasetransferonemilliondollarsto
myswissbankaccountsixtwotwo

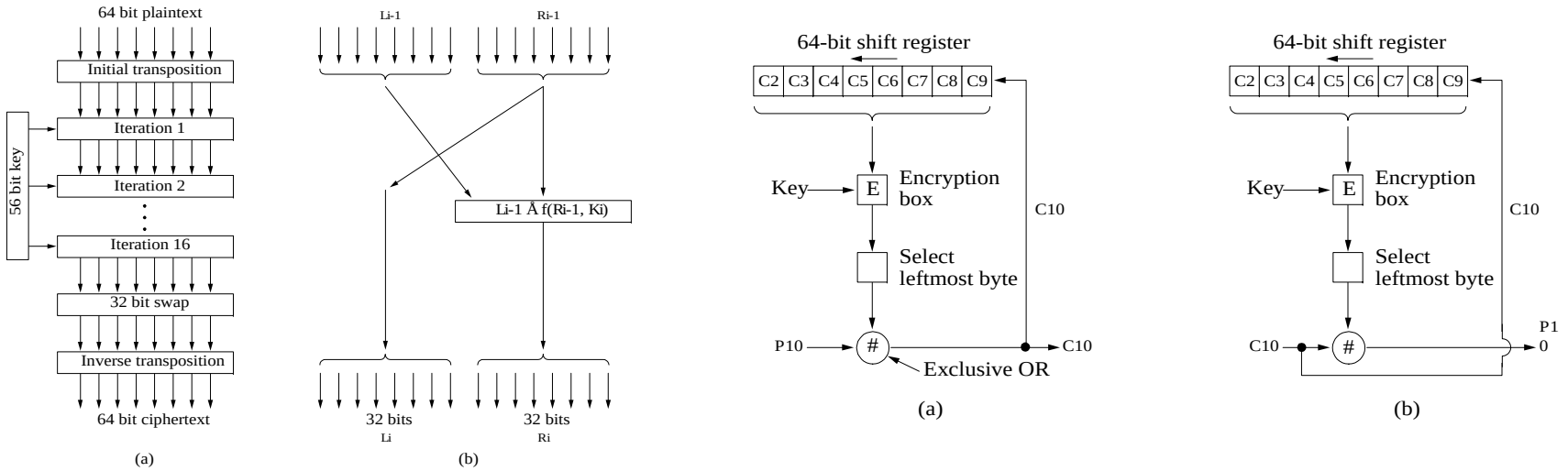
Ciphertext

AFLLSKSOSELAWAIATOOSSCTCLNMOMAI
ESILYNTWRNNTSOWDPAEDOBUOERIRICXI

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

DES

- Block cipher: uses 56 bit keys, 64 bits of data
- Uses 16 stages of substitution
- Variations
  - cipher block chaining: xor output of block n with into block n+1
  - cipher feedback mode: use 64bit shift register
    - can produce one byte at a time



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

Secure Socket Layer

- Goal:
  - Provide secure access to remote services
  - Authenticate remote servers to local users
  - Allow remote systems to authenticate users
  - Permit encrypted communication
- Approach
  - Public Key Cryptography
    - Certificates (signed by certificate authorities)
  - Sever sends:
    - Certificate (signed use CA's private key)
    - Certificate contains server's public key
    - Client responds by encrypting reply using servers pub key
    - Server checks response with private key

Sending Data

- Data is split into *packets*
  - limited size units of sending information
  - can be
    - fixed sized (ATM)
    - variable size (Ethernet)
- Need to provide a destination for the packet
  - need to identify two levels of information
    - machine to send data to
    - comm abstraction (e.g. process) to get data
  - address may be:
    - a globally unique destination
      - for example every host has a unique id
    - may unique between hops
      - unique id between two switches