I. Announcements

II. Next topic – encryption
   a. A simple statement of the problem
      i. Alice wants to send a message to Bob
         1. But Eve might be listening on the line
      ii. Alice and Bob may know one another and so could have set a protocol
         iii. Or they might not know one another
   b. A few pieces of the puzzle
      i. Sending a message to someone you know via Caesar cipher
         1. Fubswrjudskb Ghfubswhg
      ii. Could also do keyed cipher
         1. Final is next month
         2. EDLPH DS LCXT KMLTB
         3. ABCDEFGHIJKLMNOPQRSTUVWXYZ <-> princeABDFGHJKLMNOPQRSTUVWXYZ
      iii. Or cipher that changes as you encode message
         1. Final is next month
         2. Start from +2 and go up 1 for each word
            a. Hkpcn lv ribx rtsym
         3. Have a key (by the word) key is 5862
            a. Knsfq qa tkdž oqpvj
      iv. Setting up a channel for secure communications
         1. Exchange key to keyed Caesar cipher
         2. Navajo talkers during WW2
         3. One time pad
      v. Intercepting a message (substitution cipher) and cracking it
         1. a po ifydwafm tkacafm qdgi af ypsprqkaxc. ow qdgi fisik epr pfw hvmr
      vi. Making it more complicated
         1. Have a key that is used to compute a new key
         2. Have a secondary key that computes with the new key to compute a third key
         3. ....
   c. Basic idea – there is a key (or two)
      i. A key encodes the message
      ii. A key decodes the encrypted message
   d. First challenge
      i. Key distribution
         1. Key cannot be too complicated
         2. What if we’ve never met, how do we exchange keys?
            a. E.g. want to share credit card with amazon securely
      e. Has to be possible to publish the algorithm used so that it all depends on the key

III. Early standard – DES 64 bit key (1976)
    a. F(eistel) block
       i. Work on 32 bit input (half of block)
ii. Expand to 48 bits by choosing boundary bits
iii. Derive 16 48 bit keys from the original key
iv. XOR key to input (48 bits each)
v. Divide into 8 bit blocks
vi. Run each of these blocks through an S block which chooses 4 of the 6 bits (according to a schedule)
vii. Take the 32 bits and permute their order

b. Do this 16 times
c. Same key is used to decrypt
d. Brute force breaking it requires $2^{56}$ steps
   i. With parallel machines done in 22 hours (1999)
e. Can improve with triple DES (3 keys used) which (to date) is secure.
f. But, we need something better – led to AES (2001)
   i. 128, 192, 256 bit lengths with 128 bit keys;
   ii. Does a combination of substitution and permutation

IV. Creepy or not creepy
   a. An artificial intelligence algorithm developed by Stanford researchers can determine a neighborhood’s political leanings by its cars
   b. Train your algorithm to recognize all cars and thus determine demographics of neighborhood (from Google StreetView data)
      i. For instance, if the number of sedans in a neighborhood is greater than the number of pickups, there is an 88 percent chance that the precinct with vote Democratic.

V. But, how do you share your credit card with Amazon?
   a. Find a “one way hard problem”
      i. Problem which is hard to solve but if a solution is given, it is easy to verify
      ii. E.g. knapsack problem
         1. Here are a set of weights and a capacity, does any subset exactly pack the knapsack?
         2. To find a solution, might have to try all possibilities
         3. Given a solution, easy to verify it is right.
   b. Magically divide the problem in half creating 2 keys
      i. Public key that anyone can know (equivalent to checking a solution)
      ii. Private key that only you know (equivalent to solving the problem)
   c. Publish your public key
      i. So, anyone can use it to send a message to you
   d. Keep you private key private
      i. So, only you can decode the message once received
   e. For example, you want to send your credit card to Amazon
      i. Get Amazon’s private key from a registry
      ii. Encode your credit card number using their public key
      iii. Send the result to Amazon
iv. If someone listens to the conversation, they cannot decode; only Amazon can do so
v. Information exchange is secure
f. We're not there yet...
i. How does Amazon know that it was you who sent the message?
ii. Properties we'd like
   1. can only be done by the right person: can't be forged
   2. can't re-use a signature to sign something else
   3. signature attached to a document: signs specific contents
   4. signature can't be repudiated
g. Signing messages
   i. Alice encodes her message with her private key and then with Bob's public key
   ii. Bob can then decode with his private key and then with Alice's public key
   iii. No one else can do the first round of decoding because they don't know Bob's private key;
   iv. No one else could have signed the message because they don't know Alice's private key