Notes for October 26, 2000

1. Greetings and Felicitations!
   a. Homework #2 now available on the web page
2. Puzzle of the day
3. Long key generation
   a. Running-key cipher: M=THETREASUREISBURIED; K=THESECONDCIPHERISAN; C=MOIL-VGOFXTMXZFLZAEQ; wedge is that (plaintext,key) letter pairs are not random (T/T, H/H, E/E, T/S, R/E, A/O, S/N, etc.)
   b. Enigma/rotor systems; wheels, 3 rotors and a reflecting one. Go through it; UNIX uses this for *crypt*(1) command.
   c. Perfect secrecy: when the probability of computing the plaintext message is the same whether or not you have the ciphertext
   d. Only cipher with perfect secrecy: one-time pads; C=AZPR; is that DOIT or DONT?
4. DES
   a. Go through the algorithm
5. Public-Key Cryptography
   a. Basic idea: 2 keys, one private, one public
   b. Cryptosystem must satisfy:
      i. given public key, CI to get private key;
      ii. cipher withstands chosen plaintext attack;
      iii. encryption, decryption computationally feasible [note: commutativity ***not*** required]
   c. Benefits: can give confidentiality or authentiction or both
6. Use of PKC
   a. Normally used as key interchange system to exchange secret keys (cheap)
   b. Then use secret key system (too expensive to use PKC for this)
7. Diffie-Hellman
   a. Provides authenticity; used to compute shared keys for messages
   b. Go through algorithm:

      Idea: choose a; given g, p, compute $n = g^a \bmod p$; strength is inability to find a given other 3 parameters. Public key is n; g, p are shared; private key is a.
   c. Example: $p = 53$, $g = 17$. Alice's private key is 5 and Bob's is 7. Alice's public key is $17^5 \bmod 53 = 40$, Bob's is $17^7 \bmod 53 = 6$.

      To generate a shared key, Alice raises Bob's public key to her private key: $6^5 \bmod 53 = 38$. Bob raises Alice's public key to his private key: $40^7 \bmod 53 = 38$
8. RSA
   a. Provides both authenticity and confidentiality
   b. Go through algorithm:

      Idea: $C = M^e \bmod n$, $M = C^d \bmod n$, with $ed \bmod \phi(n) = 1$.

      Proof: $M^{\phi(n)} \bmod n = 1$ [by Fermat's theorem as generalized by Euler]; follows immediately from $ed \bmod \phi(n) = 1$.

      Public key is (e, n); private key is d. Choose $n = pq$; then $\phi(n) = (p–1)(q–1)$.
   c. Example:

      $p = 5$, $q = 7$; $n = 35$, $f(n) = (5–1)(7–1) = 24$. Pick $d = 11$. Then $de \bmod \phi(n) = 1$, so choose $e = 11$. To encipher

2, $C = M^e \bmod n = 2^{11} \bmod 35 = 2048 \bmod 35 = 18$, and $M = C^d \bmod n = 1811 \bmod 35 = 2$.

d. Example: $p = 53$, $q = 61$, $n = 3233$, $f(n) = (53–1)(61–1) = 3120$. Take $d = 791$; then $e = 71$. Encipher M = RENAISSANCE: A = 00, B = 01, …, Z = 25, blank = 26. Then:
M = RE NA IS SA NC Eblank = 1704 1300 0818 1800 1302 0426
$C = (1704)^{71} \bmod 3233 = 3106$; *etc.* = 3106 0100 0931 2691 1984 2927

Puzzle of the Day

These reflections of impossible prognostications were compiled by Pat Strickland of PG&E.

Computers in the future may weigh no more than 1.5 tons.

— Popular Mechanics, forecasting the relentless march of science, 1949.

I think there is a world market for maybe five computers.

— Thomas Watson, chairman of IBM, 1943.

I have traveled the length and breadth of this country and talked with the best people, and I can assure you that data processing is a fad that won't last out the year.

— The editor in charge of business books for Prentice Hall, 1957.

But what ... is it good for?

— Engineer at the Advanced Computing Systems Division of IBM, 1968, commenting on the microchip.

There is no reason anyone would want a computer in their home.

— Ken Olson, president, chairman and founder of Digital Equipment Corp., 1977.

This "telephone" has too many shortcomings to be seriously considered as a means of communication. The device is inherently of no value to us.

— Western Union internal memo, 1876.

The wireless music box has no imaginable commercial value. Who would pay for a message sent to nobody in particular?

— David Sarnoff's associates in response to his urgings for investment in the radio in the 1920s.

The concept is interesting and well-formed, but in order to earn better than a "C," the idea must be feasible.

— A Yale University management professor in response to Fred Smith's paper proposing reliable overnight delivery service. (Smith went on to found the Federal Express Corp.)

I'm just glad it'll be Clark Gable who's falling on his face and not Gary Cooper.

— Gary Cooper on his decision not to take the leading role in "Gone With The Wind."

A cookie store is a bad idea. Besides, the market research reports say America likes crispy cookies, not soft and chewy cookies like you make.

— Response to Debbi Fields' idea of starting Mrs. Fields' Cookies.

We don't like their sound, and guitar music is on the way out.

— Decca Recording Co. rejecting the Beatles, 1962.

Heavier-than-air flying machines are impossible.

— Lord Kelvin, president, Royal Society, 1895.

If I had thought about it, I wouldn't have done the experiment. The literature was full of examples that said you can't do this.

— Spencer Silver on the work that led to the unique adhesives for 3-M "Post-It" Notepads.

So we went to Atari and said, "Hey, we've got this amazing thing, even built with some of your parts, and what do you think about funding us? Or we'll give it to you. We just want to do it. Pay our salary, we'll come work for you." And they said, "No." So then we went to Hewlett-Packard, and they said, "Hey, we don't need you. You haven't got through college yet."

— Apple Computer Inc. founder Steve Jobs on attempts to get Atari and HP interested in his and Steve Wozniak's personal computer.

Professor Goddard does not know the relation between action and reaction and the need to have something better than a vacuum against which to react. He seems to lack the basic knowledge ladled out daily in high schools.

— 1921 New York Times editorial about Robert Goddard's revolutionary rocket work.

You want to have consistent and uniform muscle development across all of your muscles? It can't be done. It's just a fact of life. You just have to accept inconsistent muscle development as an unalterable condition of weight training.

— Response to Arthur Jones, who solved the "unsolvable" problem by inventing Nautilus.

Drill for oil? You mean drill into the ground to try and find oil? You're crazy.

— Drillers who Edwin L. Drake tried to enlist to his project to drill for oil in 1859.

Stocks have reached what looks like a permanently high plateau.

— Irving Fisher, Professor of Economics, Yale University, 1929.

Airplanes are interesting toys but of no military value.

— Marechal Ferdinand Foch, Professor of Strategy, Écßœole Superieure de Guerre.

Everything that can be invented has been invented.

— Charles H. Duell, Commissioner, U.S. Patent Office, 1899.

Louis Pasteur's theory of germs is ridiculous fiction.

— Pierre Pachet, Professor of Physiology at Toulouse, 1872.

The abdomen, the chest, and the brain will forever be shut from the intrusion of the wise and humane surgeon.

— Sir John Eric Ericksen, British surgeon, appointed Surgeon-Extraordinary to Queen Victoria, 1873.

640K ought to be enough for anybody.

— Bill Gates, 1981.