Notes for November 16, 2000

1. Greetings and Felicitations!
2. Puzzle of the day
3. Snake Oil Cryptography: Warning signs
    a. Pseudo-mathematical gobbledygook
    b. New mathematics
    c. Proprietary cryptography
    d. Extreme cluelessness
    e. Ridiculous key lengths
    f. One-time pads
    g. Unsubstantiated claims
    h. Security proofs
    i. Cracking contests
4. Ultimate in aging: One-Time Pads
    a. Password is valid for only one use
    b. May work from list, or new password may be generated from old by a function
    c. Example: S/Key™
5. Challenge-response systems
    a. Computer issues challenge, user presents response to verify secret information known/item possessed
    b. Example operations: $f(x) = x+1$, random, string (for users without computers), time of day, computer sends $E(x)$, you answer $E(D(E(x))+1)$
    c. Note: password never sent on wire or network
    d. Attack: monkey-in-the-middle
    e. Defense: mutual authentication
6. Biometrics
    a. Depend on physical characteristics
    b. Examples: pattern of typing (remarkably effective), retinal scans, *etc*.
7. Location
    a. Bind user to some location detection device (human, GPS)
    b. Authenticate by location of the device
8. Identity
    a. Principal and identity
    b. Users, groups, roles
    c. Identity on the web
    d. Host identity: static and dynamic identifiers
    e. State and cookies
    f. Anonymous remailers

Puzzle of the Day

"Our ancestors, and those who were considered to be wise, were accustomed to say that it was necessary to control Pistoia by means of factions and Pisa by means of fortresses; so they fostered strife in various of their subject towns, so as to control them more easily. In those days, when there was stability of a sort in Italy, this was doubtless sensible; but I do not think it makes a good rule today. I do not believe any good at all ever comes from dissension. On the contrary, on the approach of the enemy, cities which are so divided inevitably succumb at once; the weaker faction will always go over to the invader, and the other will not be able to hold out."[1]

What does this paragraph say to a system administrator or security officer seeking insight to defend her systems?

[1] Niccolò Machiavelli, *The Prince*, George Bull *trans*., Penguin Books, New York, NY ©1995, p. 67